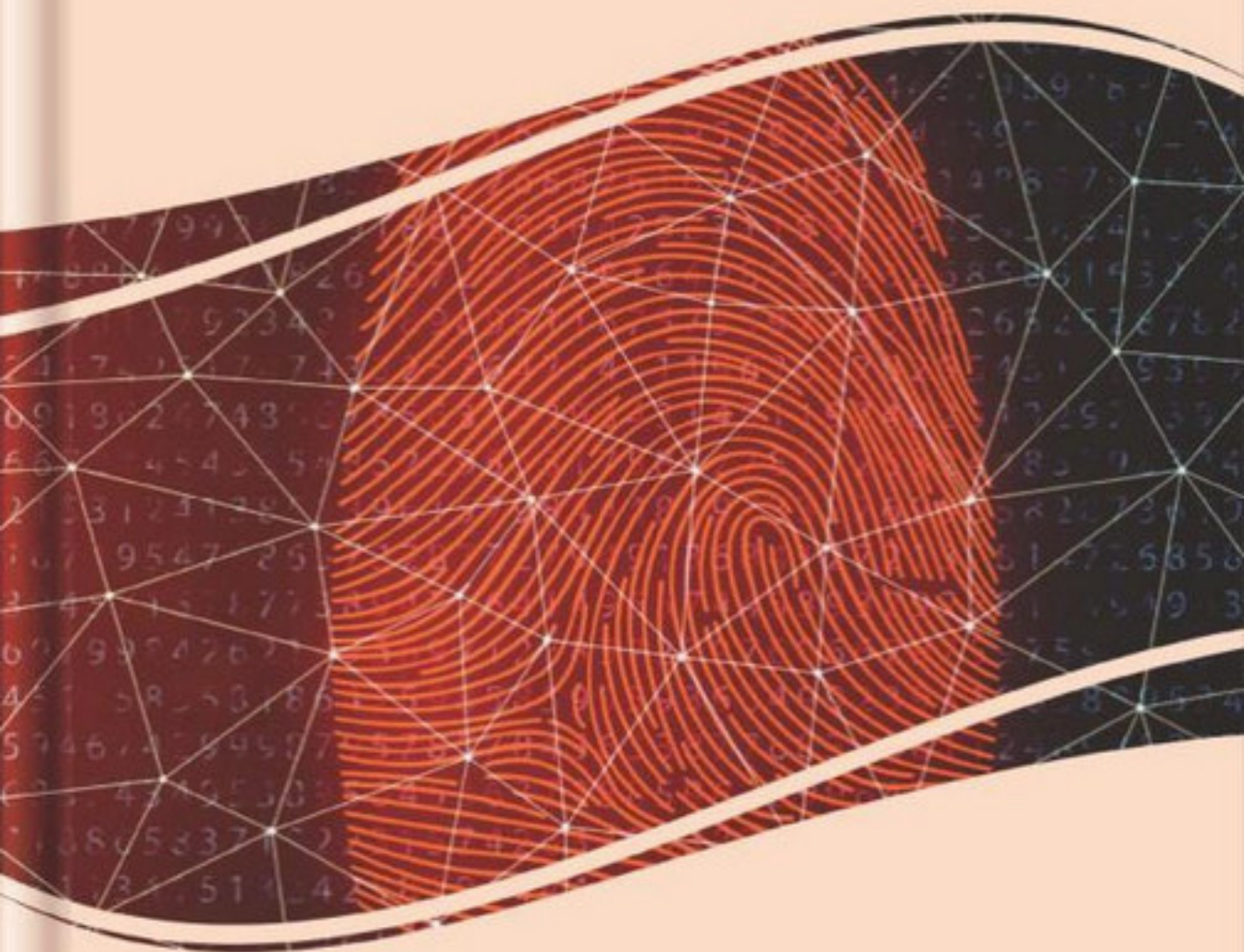


Premier Reference Source

Confluence of AI, Machine, and Deep Learning in Cyber Forensics



**Sanjay Misra, Chamundeswari Arumugam, Suresh Jaganathan,
and Saraswathi Shunmuganathan**

IGI Global
PUBLISHER OF TIMELY KNOWLEDGE

Confluence of AI, Machine, and Deep Learning in Cyber Forensics

Sanjay Misra
Covenant University, Nigeria

Chamundeswari Arumugam
SSN College of Engineering, India

Suresh Jaganathan
SSN College of Engineering, India

Saraswathi S.
SSN College of Engineering, India

A volume in the Advances in
Digital Crime, Forensics, and Cyber
Terrorism (ADCFT) Book Series



Published in the United States of America by

IGI Global
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: <http://www.igi-global.com>

Copyright © 2021 by IGI Global. All rights reserved. No part of this publication may be reproduced, stored or distributed in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher. Product or company names used in this set are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.

Library of Congress Cataloging-in-Publication Data

Names: Misra, Sanjay, editor. | Arumugam, Chamundeswari, 1971- editor. | Jaganathan, Suresh, 1972- editor. | Saraswathi, Shunmuganathan, 1977- editor.

Title: Confluence of AI, machine, and deep learning in cyber forensics / Sanjay Misra, Chamundeswari Arumugam, Suresh Jaganathan, and Shunmuganathan Saraswathi.

Description: Hershey, PA: Information Science Reference, [2021] | Includes bibliographical references and index. | Summary: "The book provides original research about cyber forensics and its relationship to Artificial Intelligence (AI) and presents the results of research and case studies that advance the practice and understanding of cyber forensics methods and techniques to support efficient and effective investigations. It covers a variety of topics, including forensic analysis, cloud forensics, forensics storage, mobile device forensics, forensic reporting, forensics tools, and more"-- Provided by publisher.

Identifiers: LCCN 2020018677 (print) | LCCN 2020018678 (ebook) | ISBN 9781799849001 (hardcover) | ISBN 9781799858386 (paperback) | ISBN 9781799849018 (ebook)

Subjects: LCSH: Computer crimes--Investigation. | Artificial intelligence.

Classification: LCC HV8079.C65 C6648 2021 (print) | LCC HV8079.C65 (ebook) | DDC 363.250285/63--dc23

LC record available at <https://lcn.loc.gov/2020018677>

LC ebook record available at <https://lcn.loc.gov/2020018678>

This book is published in the IGI Global book series Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) (ISSN: 2327-0381; eISSN: 2327-0373)

British Cataloguing in Publication Data

A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material.

The views expressed in this book are those of the authors, but not necessarily of the publisher.

For electronic access to this publication, please contact: eresources@igi-global.com.



Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series

ISSN:2327-0381
EISSN:2327-0373

Editor-in-Chief: Bryan Christiansen Global Research Society, LLC, USA Agnieszka Piekarcz Independent Researcher, Poland

MISSION

The digital revolution has allowed for greater global connectivity and has improved the way we share and present information. With this new ease of communication and access also come many new challenges and threats as cyber crime and digital perpetrators are constantly developing new ways to attack systems and gain access to private information.

The **Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series** seeks to publish the latest research in diverse fields pertaining to crime, warfare, terrorism and forensics in the digital sphere. By advancing research available in these fields, the **ADCFCT** aims to present researchers, academicians, and students with the most current available knowledge and assist security and law enforcement professionals with a better understanding of the current tools, applications, and methodologies being implemented and discussed in the field.

COVERAGE

- Encryption
- Data Protection
- Cyber Warfare
- Cryptography
- Identity Theft
- Database Forensics
- Telecommunications Fraud
- Computer Virology
- Digital surveillance
- Hacking

IGI Global is currently accepting manuscripts for publication within this series. To submit a proposal for a volume in this series, please contact our Acquisition Editors at Acquisitions@igi-global.com or visit: <http://www.igi-global.com/publish/>.

The Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series (ISSN 2327-0381) is published by IGI Global, 701 E. Chocolate Avenue, Hershey, PA 17033-1240, USA, www.igi-global.com. This series is composed of titles available for purchase individually; each title is edited to be contextually exclusive from any other title within the series. For pricing and ordering information please visit <http://www.igi-global.com/book-series/advances-digital-crime-forensics-cyber/73676>. Postmaster: Send all address changes to above address. Copyright © 2021 IGI Global. All rights, including translation in other languages reserved by the publisher. No part of this series may be reproduced or used in any form or by any means – graphics, electronic, or mechanical, including photocopying, recording, taping, or information and retrieval systems – without written permission from the publisher, except for non commercial, educational use, including classroom teaching purposes. The views expressed in this series are those of the authors, but not necessarily of IGI Global.

Titles in this Series

For a list of additional titles in this series, please visit:

<http://www.igi-global.com/book-series/advances-digital-crime-forensics-cyber/73676>

Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM

Regner Sabillon (Universitat Oberta de Catalunya, Spain)

Information Science Reference • © 2021 • 260pp • H/C (ISBN: 9781799841623) • US \$195.00

Social Engineering and Information Warfare Operations Emerging Research and Opportunities

Rhonda L. Johnson (Upper Iowa University, USA)

Information Science Reference • © 2021 • 150pp • H/C (ISBN: 9781799842705) • US \$145.00

Critical Concepts, Standards, and Techniques in Cyber Forensics

Mohammad Shahid Husain (Ministry of Higher Education, Oman) and Mohammad Zunnun Khan (Integral University, India)

Information Science Reference • © 2020 • 292pp • H/C (ISBN: 9781799815587) • US \$225.00

Utilization of New Technologies in Global Terror Emerging Research and Opportunities

Emily B. Stacey (Swansea University, UK)

Information Science Reference • © 2019 • 141pp • H/C (ISBN: 9781522588764) • US \$135.00

Applying Methods of Scientific Inquiry Into Intelligence, Security, and Counterterrorism

Arif Sari (Girne American University Canterbury, UK)

Information Science Reference • © 2019 • 396pp • H/C (ISBN: 9781522589761) • US \$195.00

Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems

S. Geetha (VIT Chennai, India) and Asnath Victy Phamila (VIT Chennai, India)

Information Science Reference • © 2019 • 334pp • H/C (ISBN: 9781522582410) • US \$225.00

For an entire list of titles in this series, please visit:

<http://www.igi-global.com/book-series/advances-digital-crime-forensics-cyber/73676>



701 East Chocolate Avenue, Hershey, PA 17033, USA

Tel: 717-533-8845 x100 • Fax: 717-533-8661

E-Mail: cust@igi-global.com • www.igi-global.com

Table of Contents

Preface	xv
Acknowledgment	xix
Chapter 1	
A Comprehensive Perspective on Mobile Forensics: Process, Tools, and Future Trends	1
<i>Aju D., Vellore Institute of Technology, Vellore, India</i>	
<i>Anil Kumar Kakelli, Vellore Institute of Technology, Vellore, India</i>	
<i>Ashwin Suresh Varma, Vellore Institute of Technology, Vellore, India</i>	
<i>Kishore Rajendiran, Sri Sivasubramaniya Nadar College of Engineering, India</i>	
Chapter 2	
Applications of Machine Learning in Cyber Forensics	29
<i>Kishore Rajendiran, Sri Sivasubramaniya Nadar College of Engineering, India</i>	
<i>Kumar Kannan, Vellore Institute of Technology, Vellore, India</i>	
<i>Yongbin Yu, University of Electronic Science and Technology of China, China</i>	
Chapter 3	
Machine Learning Forensics: A New Branch of Digital Forensics	47
<i>Angad Gupta, 3Tier R&D India Pvt Ltd, India</i>	
<i>Ruchika Gupta, Bharat Electronics Limited, India</i>	
<i>A. Sankaran, Manakula Vinayagar Institute of Technology, India</i>	

Chapter 4

Crucial Role of Data Analytics in the Prevention and Detection of Cyber Security Attacks67

Charulatha B. S., Rajalakshmi Engineering College, India

A. Neela Madheswari, Mahendra Engineering College, India

Shanthi K., Dr. M. G. R. Engineering College, India

Chamundeswari Arumugam, Sri Sivasubramaniya Nadar College of Engineering, India

Chapter 5

Deep Learning Approaches to Overcome Challenges in Forensics81

Kiruthigha M., Anna University, Chennai, India

Senthil Velan S., Amity University, Dubai, UAE

Chapter 6

Deep Learning-Based Malware Detection and Classification93

Mirnalinee T. T., Sri Sivasubramaniya Nadar College of Engineering, India

Bhuvana J., Sri Sivasubramaniya Nadar College of Engineering, India

Arul Thileeban S., Sri Sivasubramaniya Nadar College of Engineering, India

Daniel Jeswin Nallathambi, Sri Sivasubramaniya Nadar College of Engineering, India

Anirudh Muthukumar, Sri Sivasubramaniya Nadar College of Engineering, India

Chapter 7

Detecting Fake News Using Deep Learning and NLP117

Uma Maheswari Sadasivam, BITS Pilani (Off Campus), India

Nitin Ganesan, Madras Christian College, India

Chapter 8

Impediments in Mobile Forensics134

Vani Thangapandian, R. V. Government College, University of Madras, India

Chapter 9

Use-Case of Blockchain in Cybercrime and Cyberattack145

Karthika Veeramani, Sri Sivasubramaniya Nadar College of Engineering, India

Suresh Jaganathan, Sri Sivasubramaniya Nadar College of Engineering, India

Chapter 10

Motivational Quotes-Based Intelligent Insider Threat Prediction Model..... 164

*Sunita Vikrant Dhavale, Defence Institute of Advanced Technology,
India*

Chapter 11

Challenges of Developing AI Applications in the Evolving Digital World and
Recommendations to Mitigate Such Challenges: A Conceptual View 177

*Srinivasan Vaidyanathan, Cognizant, India
Madhumitha Sivakumar, Sri Sivasubramaniya Nadar College of
Engineering, India
Baskaran Kaliamourthy, Atto Technology Solutions LLC, Dallas, USA*

Chapter 12

Challenges in Developing Software in Today’s Scenario: An Analysis at
Developmental Stage Level 199

*Srinivasan Vaidyanathan, Cognizant, India
Lakshmi Priya B., Sri Sivasubramaniya Nadar College of Engineering,
India*

Compilation of References 223

About the Contributors 242

Index..... 246

Detailed Table of Contents

Preface	xv
----------------------	----

Acknowledgment	xix
-----------------------------	-----

Chapter 1

A Comprehensive Perspective on Mobile Forensics: Process, Tools, and Future Trends	1
--	---

Aju D., Vellore Institute of Technology, Vellore, India

Anil Kumar Kakelli, Vellore Institute of Technology, Vellore, India

Ashwin Suresh Varma, Vellore Institute of Technology, Vellore, India

Kishore Rajendiran, Sri Sivasubramaniya Nadar College of Engineering, India

The modern-day smartphones are the result of the technological progression that is happening in this digital world. This technological advancement has brought an incremental augmentation where these were not perceived as critical by the smartphone users. Also, the computational capability and networking competence has been dragooned constantly to maintain the momentum with the ever-expanding workload demands. This scenario has endorsed the smart gadgets such as smartphones and tablets to accomplish the growing complex challenges. In this digital era, the next generation users are substituting the conventional way of preference such as the personal computers and laptops with smartphone for the social connectedness, e-commerce, financial transaction, market updates, latest news, or even editing images. Users willingly install various mobile apps on to their smartphone and consequently providing their valuable and sensitive personal information to their service providers without thinking and knowing the security lapses and repercussions. Considering the fact, the smartphones' size and its portability, these devices are much more susceptible of being stolen, becoming jeopardized, or being exploited for various cyber-attacks and other malevolent activities. Essentially, the hackers look forward to the new mobile vulnerabilities so that they exploit the revealed vulnerability once a newer edition of the respective mobile operating system is released. In view of the fact that the smartphones are too vulnerable to various exploits, the necessity for a

digital investigation entrained to establish a separate domain named mobile forensics. This established forensic domain is specialized in acquiring, extracting, analyzing, and reporting the evidence that is obtained from the smartphone devices so that the exploiting artifacts and its respective actions are determined and located. This chapter puts forward the various processes involved with the mobile forensics that can be employed for examining the evidences of various cyber incidents. Furthermore, it discusses the various vulnerabilities with the iOS and Android mobile operating systems and how they are being exploited in detail. The chapter also discusses the various approaches of data extraction and the respective industry standard for the tools that are being utilized for the same.

Chapter 2

Applications of Machine Learning in Cyber Forensics29

*Kishore Rajendiran, Sri Sivasubramaniya Nadar College of
Engineering, India*

Kumar Kannan, Vellore Institute of Technology, Vellore, India

*Yongbin Yu, University of Electronic Science and Technology of China,
China*

Nowadays, individuals and organizations experience an increase in cyber-attacks. Combating such cybercrimes has become the greatest struggle for individual persons and organizations. Furthermore, the battle has heightened as cybercriminals have gone a step ahead, employing the complicated cyber-attack technique. These techniques are minute and unobtrusive in nature and habitually disguised as authentic requests and commands. The cyber-secure professionals and digital forensic investigators enforce by collecting large and complex pools of data to reveal the potential digital evidence (PDE) to combat these attacks and helps investigators to arrive at particular conclusions and/or decisions. In cyber forensics, the challenging issue is hard for the investigators to make conclusions as the big data often comes from multiple sources and in different file formats. The objective is to explore the possible applications of machine learning (ML) in cyber forensics and to discuss the various research issues, the solutions of which will serve out to provide better predictions for cyber forensics.

Chapter 3

Machine Learning Forensics: A New Branch of Digital Forensics47

Angad Gupta, 3Tier R&D India Pvt Ltd, India

Ruchika Gupta, Bharat Electronics Limited, India

A. Sankaran, Manakula Vinayagar Institute of Technology, India

Machine learning (without human interference) can collect, analyze, and process data. In the case of cyber security, this technology helps to better analyze previous cyber-attacks and develop respective defense responses. This approach enables an automated cyber defense system with a minimum-skilled cyber security force. There

are high expectations for machine learning (ML) in cyber security, and for good reasons. With the help of ML algorithms, we can sift through massive amounts of security events looking for anomalies, deviations from normal behavior that are often indicative of malicious activity. These findings are then presented to the analyst for review and vetting, and the results of his determination fed back into the system for training. As we process more and more data through the system, it evolves: it learns to recognize similar events and, eventually, the underlying traits of malicious behavior that we're trying to detect. This chapter explores machine learning forensics.

Chapter 4

Crucial Role of Data Analytics in the Prevention and Detection of Cyber Security Attacks67

Charulatha B. S., Rajalakshmi Engineering College, India

A. Neela Madheswari, Mahendra Engineering College, India

Shanthi K., Dr. M. G. R. Engineering College, India

Chamundeswari Arumugam, Sri Sivasubramaniya Nadar College of Engineering, India

Data analytics plays a major role in retrieving relevant information in addition to avoiding unwanted data, missed values, good visualization and interpretation, decision making in any business, or social needs. Many organizations are affected by cyber-attacks in their business at a greater frequency when they get exposure to the internet. Cyber-attacks are plenty, and tracking them is really difficult work. The entry of cyber-attack may be through different events in the business process. Detecting the attack is laborious and collecting the data is still a hard task. The detection of the source of attack for the various events in the business process as well as the tracking the corresponding data needs an investigation procedure. This chapter concentrates on applying machine learning algorithms to study the user behavior in the process to detect network anomalies. The data from KDD'99 data set is collected and analyzed using decision tree, isolation forest, bagging classifier, and Adaboost classifier algorithms.

Chapter 5

Deep Learning Approaches to Overcome Challenges in Forensics81

Kiruthigha M., Anna University, Chennai, India

Senthil Velan S., Amity University, Dubai, UAE

Cyber forensics deals with collecting, extracting, analysing, and finally reporting the evidence of a crime. Typically investigating a crime takes time. Involving deep learning methods in cyber forensics can speed up the investigation procedure. Deep learning incorporates areas like image classification, morphing, and behaviour analysis. Forensics happens where data is. People share their activities, pictures, videos, and locations visited on the readily available platform, social media. An abundance of

information available on social networking platforms renders them a favourite of cybercriminals. Compromising a profile, a hacker can gain access, modify, and use its data for various activities. Unscrupulous activities on such platforms include stalking, bullying, defamation, circulation of illegal or pornographic material, etc. Social network forensics is more than the application of computer investigation and analysis techniques, such as collecting information from online sources. CNNs and autoencoders can learn and obtain features from an image.

Chapter 6

Deep Learning-Based Malware Detection and Classification93

Mirnalinee T. T., Sri Sivasubramaniya Nadar College of Engineering, India

Bhuvana J., Sri Sivasubramaniya Nadar College of Engineering, India

Arul Thileeban S., Sri Sivasubramaniya Nadar College of Engineering, India

Daniel Jeswin Nallathambi, Sri Sivasubramaniya Nadar College of Engineering, India

Anirudh Muthukumar, Sri Sivasubramaniya Nadar College of Engineering, India

Malware analysis is an important aspect of cyber security and is a key component in securing systems from attackers. New malware signatures are being created continuously and detection techniques need to keep pace with them. The primary objective is to propose a solution which detects malicious files in real time by evaluating each file. Other objectives are to assess the threat level of the malware and recognize the family of malicious file. Hence, to cover all the needs and to fulfill the motivation, a deep neural network is more suitable to detect and classify the malware. Convolutional neural network-based system MalNet-D is designed to detect the presence of malware, and subsequently, to classify the detected malware into the family in which it belongs, a variation of MalNet-D termed as MalNet-C is proposed. Images of the executable files, both malignant and benign, are used as input data, which is trained by the respective MalNet. This is used to detect and classify malware into families. The system achieved 93% accuracy in malware detection and 96% accuracy in malware classification.

Chapter 7

Detecting Fake News Using Deep Learning and NLP.....117

Uma Maheswari Sadasivam, BITS Pilani (Off Campus), India

Nitin Ganesan, Madras Christian College, India

Fake news is the word making more talk these days be it election, COVID 19 pandemic, or any social unrest. Many social websites have started to fact check the news or articles posted on their websites. The reason being these fake news

creates confusion, chaos, misleading the community and society. In this cyber era, citizen journalism is happening more where citizens do the collection, reporting, dissemination, and analyse news or information. This means anyone can publish news on the social websites and lead to unreliable information from the readers' points of view as well. In order to make every nation or country safe place to live by holding a fair and square election, to stop spreading hatred on race, religion, caste, creed, also to have reliable information about COVID 19, and finally from any social unrest, we need to keep a tab on fake news. This chapter presents a way to detect fake news using deep learning technique and natural language processing.

Chapter 8

Impediments in Mobile Forensics..... 134

*Vani Thangapandian, R. V. Government College, University of Madras,
India*

In this digital era, the usage of mobile phones in daily life has become inextricable due to the facilities and the level of sophistication it offers. Proportionately, the crimes and offenses involving the mobile devices are growing in rapid speed. Whenever a crime occurs in a spot, the forensic team will arrive there to identify and locate the evidence of the criminals. If the crime involves digital equipment like computers and laptop, then digital forensic team will investigate and analyze the devices for digital evidence collection. These days, mobile phones have the capability to offer any kind of information and services digitally on top of the palm of the user. Anything is available on the hands with a single touch on the screen of the mobile devices. It also offers to the adversaries many digital services which are harmful to the societies. The fast-paced advancement in the digital front paves the way for many digital crimes. Hence, a new field, mobile forensics, emerges out to trace the evidence, but it faces many challenges due to the dynamic nature of the digital technologies.

Chapter 9

Use-Case of Blockchain in Cybercrime and Cyberattack..... 145

*Karthika Veeramani, Sri Sivasubramaniya Nadar College of
Engineering, India*

*Suresh Jaganathan, Sri Sivasubramaniya Nadar College of Engineering,
India*

Cybercrime involves unlawful activities done by the individual in cyberspace using the internet. It is cyberbullying, financial theft, code-hack, cryptojacking, hacking, etc. The main difference between cybercrime and cyberattack is that cybercrime victims are humans. The crime associated with the latter is that of a computer network, hardware or software. Cyberattack activities include ransomware, viruses, worms, SQL injection, DDoS attacks, and government and corporate are potential targets.

Cyber security provides a specialised approach to the protection of computer systems from cybercrimes and cyberattacks. As of now, no cyber defence is 100% safe. What is considered safe today may not be secure tomorrow. Blockchain enables a new way of recording transactions or any other digital interaction within the network with security, transparency, integrity, confidentiality, availability, and traceability. This chapter explains in detail about cyber risks and how blockchain can be used to avoid risks in financial and insurance frauds.

Chapter 10

Motivational Quotes-Based Intelligent Insider Threat Prediction Model..... 164

*Sunita Vikrant Dhavale, Defence Institute of Advanced Technology,
India*

Insiders are considered as the weakest link. The digital records of a person's Facebook likes against motivational quotes can be used for automatic and accurate prediction of sensitive attributes related to their personality traits depression, and their views against company/government policies, etc. Such analysis will help organization to take proactive measures against vulnerable insiders. Insiders managing their impressions differently than their basic personality traits can also be identified. Deep learning models can be utilized to learn and map the association among extracted features and insider behavioral patterns. Further, reinforcement techniques can be used to select appropriate motivational quotes in order to collect additional data required for further analysis. At the same time, the same exposed motivational messages on insider's social platform can aid to improve their psychological health over a time. However, due to implications involved in data collections related to personalization and data collection privacy, the authors have quoted their work in terms of this concept chapter only.

Chapter 11

Challenges of Developing AI Applications in the Evolving Digital World and Recommendations to Mitigate Such Challenges: A Conceptual View 177

*Srinivasan Vaidyanathan, Cognizant, India
Madhumitha Sivakumar, Sri Sivasubramaniya Nadar College of
Engineering, India
Baskaran Kaliamourthy, Atto Technology Solutions LLC, Dallas, USA*

These intelligence in the systems are not organic but programmed. In spite of being extensively used, they suffer from setbacks that are to be addressed to expand their usage and a sense of trust in humans. This chapter focuses on the different hurdles faced during the course of adopting the technology namely data privacy, data scarcity, bias, unexplainable Blackbox nature of AI, etc. Techniques like adversarial forgetting, federated learning approach are providing promising results to address various issues like bias, data privacy are being researched widely to check their competency to

mitigate these problems. Hardware advancements and the need for enhancing the skillset in the artificial intelligence domain are also elucidated. Recommendations to resolve each major challenge faced are also addressed in this chapter to give an idea about the areas that need improvement.

Chapter 12

Challenges in Developing Software in Today’s Scenario: An Analysis at Developmental Stage Level 199

Srinivasan Vaidyanathan, Cognizant, India

Lakshmi Priya B., Sri Sivasubramaniya Nadar College of Engineering, India

Software engineering emphasises to adopt a well-defined and structured approach to develop any software. Nonetheless, serious challenges exist in the software development process and these challenges are faced in developing software in today’s scenario. This is majorly to satisfy the need for developing good quality product which has the capability to meet the “volatile user requirements” in organizations. As new products are developed to tend to the current technological needs, new challenges arise inevitably. So, until a new challenge is encountered, solutions to these unknown and newly arising challenges cannot be devised. Hence, a better software development strategy would be to realise all the previously encountered, more frequent or obvious challenges, and to design an efficient solution to these known challenges beforehand so that no more extra resources and time need to be diverted during the software development cycle in order to overcome the challenges. Therefore, recognizing and addressing the challenges in software development at each and every developmental stage is extremely necessary in order for organizations to succeed. In this study, the authors have attempted to structurally and systematically reviewing the literature to arrive at the software development challenges and provided ways of addressing those challenges. The study also provided for possible solutions and recommendations and scope for future research in this area.

Compilation of References 223

About the Contributors 242

Index 246

Preface

“Sarvam Krishnarpanam”. In Bhagavad Gita, Chapter 3, Lord Krishna explains ‘karma-yoga’, is a way that frees the person from bondage of karmic reaction and leads to purification of mind. He also explains that everyone must engage in some sort of activity in this world and even to maintain the body one has to work.

OVERVIEW

This book supplies connected information related to the challenges and solutions in cyber forensics. It highlights the issues, techniques, practices applicable and pertaining to cyber forensics. The research findings contained in this book is ideal for the cyber forensics experts who desire to improve the investigation approach by adapting AI algorithms. The decision making in various investigations can be eased by getting insights of the various approaches summarized in the various chapters. The automation of the investigation can be overlooked practically by the experts to increase their support in finalizing a decision in cyber forensics investigation. A new dimension in terms of approach to AI is taken up here to showcase the relationship between AI and cyber forensics. Automation is a major theme for bringing this work.

TODAY'S SCENARIO

Due to digital era, all IT and non-IT related companies are under the pressure in resolving the cyber crime incidents. Cyber crime is a crime that is related to computer system, laptops, mobile devices, internet, etc. Cyber crimes may cover for instance, fake email, distributing copyrighted material, hacking, SQL Injections, cross-site scripting, malware, cyber stalking, data diddling, etc. Cyber crime and cyber forensics are attached to one another and they are inseparable. If there is a crime, then forensics expert becomes essential. Actually, cyber forensics cases make a way to prevent cyber crime at an appreciable level. Though cyber forensics

lays a foundation for proactive measures, still there is sharp increase in the cyber forensics' investigations. Failed or weak cyber security is another reason for cyber forensics. The comprise on the cyber security increases cyber crime and in turns pays a pay to cyber forensics.

Cyber forensics need a skilled expertise to handle the investigation in a many domain, namely mobile, network, digital image/audio/video, memory, wireless, database, malware, etc. Each investigation must follow a process and requires lot of memory space, tools, etc. to initiate an investigation. The investigation can be namely, forgery, disputes, theft, fraud, etc. Conventional investigation lacks to face the challenges that involve complex data in the last decade. More intelligent investigation techniques are the need and demand to meet the various cyber forensics investigation to mitigate the time and resources. Due to limitation of time and resources in cyber crime investigations, AI to automate the process, has been receiving attention over last few years. Through the use of multiagent system and expert's knowledge, analyzing and correlating the data during the investigation can mitigate the time. Further, AI can track the abnormal patterns in a complex data that are susceptible to threat in various investigation. This book portrays AI techniques to apply in forensics investigation that involve complex data.

TARGET AUDIENCE

This book is ideal for professionals and researchers working in the field of cyber forensics. A resource for research scholars and researchers of Computer Science and Engineering, Information Technology, Electronics and Communication Engineering, Telecommunication Engineering who wish to take up projects on cyber forensics related to AI, machine learning and deep learning. Researchers will find this book useful for their research projects and will find this book as a handy reference guide. Software and Hardware Engineers who work specifically in cyber forensics, will find this book as a useful resource. Banking, Insurance, Data centre, mobile, Networking, social media, etc. professionals can use this book as a reference to enhance their security. Cybercrime department, Cyber specialist, lawyers, company policy makers, academician, lab researchers, and many investigators who are working in cyber forensics will be benefited by this book.

ORGANIZATION OF THE CHAPTER

Twelve chapters organized in this book provide an interesting aspect of AI in cyber forensics. Chapter 1 analyses the process of mobile forensics to examine the cyber

Preface

incidents. Shares the vulnerabilities related to various mobile operating systems, and data extraction tools for mobile forensics. Chapter 2 investigate the issues in data collection for various cyber forensics investigation. Further, concisely stated the research issues and solutions pertaining to the application of machine learning in cyber forensics. In Chapter 3, discusses the machine learning adoption in developing an automated cyber defence system. Presents, how the machine learning approach aid the data collection, training events to detect the malicious behaviour. Chapter 4 portrays the role of data analytics in an investigation procedure related to cyber attack. Demonstrates and report an instance by applying machine learning algorithms with the available dataset.

Chapter 5 explores the forensics investigation using deep learning in image classification, morphing and behaviour analysis. Elaborates how by compromising a profile, the attacker gain access to the image data from social media and involve in unscrupulous activities information. Discusses the usage of CNN and Autoencoders to learn the feature of an image. Chapter 6 looks on the securing systems component via malicious files, from attacker. Assess and detect malicious files based on the threat level in each file. For detection and classification, applies CNN based system MalNet –D is applied and reports that the system achieved 93% accuracy in malware detection and 96% accuracy in malware classification. Chapter 7 views the social media to detect the fake news from hatred community. Fake news creates confusion, chaos, misleading the community and society. To avoid the spread of fake news this chapter proposes an approach to detect fake news using deep learning algorithm and natural language processing. Chapter 8 describes many challenges in mobile forensics that is dynamic in nature due to the adversary's role. Chapter 9 discusses the approach of cyber attack and crimes. Further elaborates the secure block chain technology that prevent the adversary's role in financial and insurance frauds.

Chapter 10 exposes the insider's psychological health through the various motivational messages on their social platform. Chapter 11 brings the special attention on merging techniques like adversarial forgetting, federated learning approach in mitigating the hurdles faced by adopting the AI technologies to address the data privacy issues, data scarcity, etc. Further discusses, the challenges, and various recommendation addressing the technology. Projects, the most important, need improvement areas. Chapter 12 targets the challenges in developing the software in today's scenario in software organization. Comprising the technology growth, the high-quality software as per the changing user needs in organization is expected to be produced. A better development strategy to face the challenges and at the same time with no comprise on time and resources in software development cycle is vital at this point. This chapter recognizes and addresses the challenges faced by software organization in software development and how to succeed.

CONCLUSION

This book contains research articles targeted various areas of cyber forensics like mobile forensics, forensics tools, forensics investigation, adaption of machine learning algorithm, automated defence system, data analytics, deep learning algorithm, adversarial forgetting, federated learning, software development, etc. The emergence of adversarial forgetting, and federated learning can further enhance the challenges of the forensics experts in investigation and decision making. Confluence of machine learning and deep learning play a vital and beneficial role in cyber forensics as it provides forensics expert a platform to enhance further.

Sanjay Misra

Covenant University, Nigeria

Chamundeswari Arumugam

Sri Sivasubramaniya Nadar College of Engineering, India

Suresh Jaganathan

Sri Sivasubramaniya Nadar College of Engineering, India

S. Saraswathi

Sri Sivasubramaniya Nadar College of Engineering, India

Acknowledgment

First, we would like to thank all the researchers for the complete support for the successful completion of the editorial process. Second, we would like to take the opportunity to thank the authors for their contribution in this book. Thirdly, we thank the editorial review board members for managing their time in reviewing the submitted chapters. We also take this opportunity to thank the IGI publishers and their team for their support and responses to make this project come as reality. Last but not the least, we would also like to thank whosoever have contributed to this book.

Sanjay Misra
Covenant University, Nigeria

Chamundeswari Arumugam
Sri Sivasubramaniya Nadar College of Engineering, India

Suresh Jaganathan
Sri Sivasubramaniya Nadar College of Engineering, India

S. Saraswathi
Sri Sivasubramaniya Nadar College of Engineering, India

Chapter 1

A Comprehensive Perspective on Mobile Forensics: Process, Tools, and Future Trends

Aju D.

Vellore Institute of Technology, Vellore, India

Anil Kumar Kakelli

 <https://orcid.org/0000-0002-2004-0611>

Vellore Institute of Technology, Vellore, India

Ashwin Suresh Varma

Vellore Institute of Technology, Vellore, India

Kishore Rajendiran

Sri Sivasubramaniya Nadar College of Engineering, India

ABSTRACT

The modern-day smartphones are the result of the technological progression that is happening in this digital world. This technological advancement has brought an incremental augmentation where these were not perceived as critical by the smartphone users. Also, the computational capability and networking competence has been dragooned constantly to maintain the momentum with the ever-expanding workload demands. This scenario has endorsed the smart gadgets such as smartphones and tablets to accomplish the growing complex challenges. In this digital era, the next generation users are substituting the conventional way of preference such as the personal computers and laptops with smartphone for the social connectedness, e-commerce, financial transaction, market updates, latest news, or even editing images. Users willingly install various mobile apps on to their smartphone and consequently providing their valuable and sensitive personal information to their

DOI: 10.4018/978-1-7998-4900-1.ch001

service providers without thinking and knowing the security lapses and repercussions. Considering the fact, the smartphones' size and its portability, these devices are much more susceptible of being stolen, becoming jeopardized, or being exploited for various cyber-attacks and other malevolent activities. Essentially, the hackers look forward to the new mobile vulnerabilities so that they exploit the revealed vulnerability once a newer edition of the respective mobile operating system is released. In view of the fact that the smartphones are too vulnerable to various exploits, the necessity for a digital investigation entrained to establish a separate domain named mobile forensics. This established forensic domain is specialized in acquiring, extracting, analyzing, and reporting the evidence that is obtained from the smartphone devices so that the exploiting artifacts and its respective actions are determined and located. This chapter puts forward the various processes involved with the mobile forensics that can be employed for examining the evidences of various cyber incidents. Furthermore, it discusses the various vulnerabilities with the iOS and Android mobile operating systems and how they are being exploited in detail. The chapter also discusses the various approaches of data extraction and the respective industry standard for the tools that are being utilized for the same.

INTRODUCTION

Computers in all its glory have slowly progressed from the size of a big hall to that of a grain of rice. It is quite evident how big of a role technology plays in the 21st century. It's quite indisputable that the most common and accessible form of reliable technology lies in mobile phones and handheld devices.

Technology being a coin that encompasses a huge responsibility often tends to reveal its dark side after much integration into the human lifestyle. Cyber Crime is at an all-time high and Cyber Criminals tend to come up with innovative ways to infiltrate into its victim's network; be it through Social Engineering or brute force attacks. These days the often go-to evidence for any Crime Investigator would be the stakeholder's mobile phones. Hence it can be concluded that the part played by Digital Forensics and its applications in the various sub-domains of Cyber Security is irrefutable.

In a world that is dominated by the power of data, the science of discovering, safe retrieval and analysis of digital evidence from mobile phones is generally categorized under the umbrella term of mobile forensics. Any information that passes through a mobile phone, be it generated or received by it, comes under digital evidence and it plays a substantial role in solving crime.

BACKGROUND

Mobile Forensics generally follows the same principles that are religiously followed in Digital Forensics. As valuable and portable as digital data goes, it's equally considered volatile and vulnerable to corruption. Data Authentication comes as a primary foundation to any digital evidence collection as the context and verdict of any crime can change with the minute variations in data which could be either due to human error during evidence collection or sabotage.

During evidence collection, data is seen as a volatile commodity that should be handled with as much care as possible to prevent any sort of change from its original state. This task becomes particularly difficult as the technology advances, criminals tend to encrypt their devices to prevent an external source from accessing its data and provide contingency measures in case of a breach such as wiping the system clean of any evidence, hence rendering the device useless.

It's considered as an unspoken rule of evidence collection to not turn the device off, keep it for charging, etc. to prevent any sort of data corruption. Unfortunately, this is not the case every time as it might be required to physically open the device or change settings to force our way into the system due to their state when discovered. In these circumstances, logs are maintained meticulously regarding the initial and final stages of the device. Chain of custody is another important aspect as more the people the device has passed onto, the higher than chances of data corruption or sabotage.

Collection and Transport of evidence are also given prime importance as any electromagnetic anomaly can trigger the device to render its data useless. Cords and cables are disconnected, their pictures taken, digital evidence (Mobile phones and its associated peripherals) are sealed in an electronic evidence bag and stored in a location that won't be subjected to extreme temperatures.

Any form of evidence collection must be in accordance with the regulations set up by the judiciary of that region/country. Failure of which, the data can even be considered inadmissible by the court even if it has information that can acquit/incriminate the suspect.

Nowadays, variety of mobile phones are commercially available that uses diverse operating systems, files systems, applications and peripherals. In recent times, due to the increased use of smart phones, digital forensic examiners have come across increasing requests to examine data in the handheld devices. With the advancement and evolution of mobile technology at a faster pace, the variety of data available with such mobile devices and the way they are utilized are also evolving. In current scenario, each of these devices may or may not be supported by the available forensic tools. Henceforth, there would always be a delay before the latest mobile phones are supported by the forensic tools. More importantly, it is not adequate to document

the phonebook, call logs, messages, photos and videos from the mobile devices because the devices currently used are miniature computers. The data from variety of applications installed in such devices may contain appropriate information that may not be automatically analysed by the existing forensic solutions, thereby posing a greater challenge in terms of digital forensic skills requirements for mobile device examinations. During the investigation, few cases would require only partial data whereas in other cases a comprehensive and full data extraction from the phone is required for effective examination as well as for the latent recovery of erased data. All these details put forward a need for the development of a proper guidelines and processes for extraction and documentation of pertinent and significant data from mobile phones. This should be followed by required updation along with the evolution of mobile phone technology (Murphy, C. A., 2009). In this article, the author emphasise the selection of consistent examination processes for the extraction and documentation of relevant data from mobile devices by the investigators that best fits their scenario and requirements.

The rapid development of technology with respect to mobile phones has led to advanced cybercrimes (Chernyshev, M., Zeadally, S., Baig, Z., and Woodward, A., 2017). The advancements, challenges faced and the research opportunities with respect to mobile device forensics were discussed. The article also focusses upon the important criteria for evaluating the soundness of digital forensic process, integrated digital forensic process model with related soundness criteria, smart phone features, evidence sources and also the comparison of data extraction processes. It also, emphasises on providing an introduction to few of the commercially available forensic tools for mobile devices. The authors also identified few research directions that need to be explored towards the evolution of efficient mobile forensic techniques and technologies.

The transition from computers to smart phones poses great challenge to forensic professionals while analysing the seized device (Herrera, L.A., 2020). Challenges of acquiring smart phones while minimizing the loss of viable forensics data were focussed. In the article, the authors have discussed potential types of acquisition, possible issues around unlocking the hardware and extracting information followed by probable issues around unlocked devices.

When the smartphones are exposed to water, the electro-chemical reactions (Fukami, A., & Nishimura, K, 2019) that happen inside the smartphones were examined to recover or restore the contents from the damaged mobile. Also, the normal diagnoses of the water affected devices are discussed along with its respective repair methodologies. A study of the JPEG header details of Apple smartphones (Mullan, P., Riess, C., & Freiling, F, 2019) are examined and analysed to a larger extent to examine the impact of the prospects of performing the source identification. Through the analysis, its been identified that the concrete hardware is harder for the

mobile phones when compared to the conventional cameras. An understanding of the operational mechanism (Shaheen, J. A., Asghar, M. A., & Hussain, A, 2017) of the android applications is provided as a guidance to explore and develop android based applications. Also, the working of Dalvik virtual machine is explicated and further the kernel of the android operating system is elaborated.

A digital forensic device named SEAKER (Storage Evaluator and Knowledge Extraction Reader) (Gentry, E., & Soltys, M, 2019) that provides faster and targeted feedback for immediate incident or crime evidence assessment through Raspberry Pi is presented. Primarily, this system is developed for the on-scene and time-sensitive investigations thereby reducing the large backlogs at the forensics laboratories. The issues related to the Call Detailed Records storage (CDR) (Abba, E., Aibinu, A. M., & Alhassan, J. K, 2019) is dealt with in this article and thereby solving respective issues by identifying and modelling six new artifacts through communication activities. The identified new artifacts are incorporated with the existing CDR for better forensics analysis. The forensics analysis were conducted on three different social media applications such as Facebook, Twitter, and MySpace (Al Mutawa, N., Baggili, I., & Marrington, A, 2012) through smartphones such as BlackBerrys, iPhones, and Android phones. The respective analyses were primarily aimed at determining whether the conducted activities will be stored in the internal memory. It is observed that no traces could be found out from the BlackBerry devices. But, iPhones and Android phones did store significant amount of sensitive information that can be recovered and utilized by the forensic experts to solve the case.

A fully automated mobile forensic tool named, Fordroid (Lin, X., Chen, T., Zhu, T., Yang, K., & Wei, F, 2018) is proposed to analyse the mobile applications on android devices. The main purpose of this mobile tools is to find out what and where the sensitive data will be written in the local storage. The respective mobile forensic tool was able to locate the sensitive information with 98% efficiency. The accuracy of steps and distances registered by the health app (van Zandwijk, J. P., & Boztas, A, 2019) is examined and investigated with three different models of iPhone such as iPhone 6, iPhone 7 and iPhone 8 under empirical conditions. It is observed that the health properties can be taken into consideration and can be utilised as an evidence for digital investigations.

Smartphones plays a significant role in each and every one's life in today's digital world. This research article mainly analyze the snapchat artifacts (Alyahya, T., & Kausar, F, 2017) that is stored inside any android smartphones thereby identifying the implications and importance of a digital forensic investigative process. An emphasis on how the digital forensic tools (Wilson, R., & Chi, H, 2017) aids or assists the forensics investigators is presented. It assists the forensic experts in acquiring the evidences, specifically with the messages that are stored inside the iOS smartphones. Also, a framework has been suggested to verify the data integrity of any forensics

tools. The technical issues as well as the challenges encountered (Ninawe, P. N., & Ardhapurkar, S. B, 2014) in the cloud with respect to the android mobile forensics has been exemplified. The smartphones have significant data that can be connected towards an individual per byte. The information stored inside the smartphones are extremely useful for an investigation.

It is a significant challenge (Faheem, M., Le-Khac, N. A., & Kechadi, T, 2014) for each and every digital forensic investigator to really acquire and extract the sensitive data from a smartphone for the investigation purpose which later on would be utilized in the court of law as evidences. Here, a demonstration on how to obtain and access the Samsung S3 root is shown in order to create extract and create disc images and verify it. The vulnerabilities found in android smartphones (Hur, J. B., & Shamsi, J. A, 2017) are described here in this article. Also, the attacks such as privilege escalation, privacy attacks and other threats with respect to smartphones are presented. A discussion on the possible countermeasures against the said vulnerabilities or attacks on android phones are presented here. This survey article presents the research carried out within the mobile forensics ecosystem (Barnpatsalou, K., Cruz, T., Monteiro, E., & Simoes, P, 2018) for the past seven years since the year 2018. The respective survey finds out the drawbacks and projects the differences of the past research directions and addresses the challenges involved with the research. A comparative overview between android operating system and iOS operating system (Singh, A. J., & Bhardwaj, A, 2014) is presented highlighting the security aspects of these two operating systems.

An open source methodology to access the iOS device through SSH shell (Hyndavi Koganti & Siva Nageswara Rao G, 2019) is proposed. The respective method can be utilized to acquire the sensitive data from the iOS device securely for performing forensic analysis. A discussion on smartphone characteristics (Lohiya, R., John, P., & Shah, P, 2015) for carrying out the mobile forensic analysis and investigation utilizing various mobile forensic tool is been presented. Also, empirical results on investigation utilizing Molekit Lite and Autopsy 3.1.2 are presented. Factors influencing the security issues in iOS and android smartphones (Hayran, A., İğdeli, M., YILMAZ, A., & Gemci, C) with respect to its technologies are examined and presented. Various factors that influence the security issues of both the smartphones are reduced attack surface, privilege separation, permission-based access control, sandboxing, data encryption, data execution prevention and address space layout randomization, geo-location and auto-erase.

Once the new launches happen with the smartphones, hackers look forward to exploit the newer versions and therefore new vulnerabilities in smartphones (Kataria, A., Anjali, T., & Venkat, R, 2014) are found out. Here, the various versions of Google android as well as the iOS operating systems are analysed and compared for its vulnerabilities. An approach for mobile forensics domain based on meta-modeling

(Ali, A., Abd Razak, S., Othman, S. H., Mohammed, A., & Saeed, F, 2017) has been developed. The developed methodology identifies the common ideas in mobile forensics through Mobile Forensics Meta-model. The significance of this method is to capture and reuse the digital forensic knowledge in turn supporting the forensic training as well as the management activities. A layered framework (Goel, M., & Kumar, V, 2019) for mobile forensic analysis is presented here. Extracting the digital data and preserving the respective data in a proper step by step process from the smartphone device is a huge challenge and is of great significance pertaining to the investigation. This article focuses on documenting each and every activity carried out in the forensic investigative process.

A database driven methodology (Baggili, I. M., Mislán, R., & Rogers, M, 2007) that is used to store the data pertaining to the smartphone acquisition examination process is discussed. Later on the respective data can be utilized to measure or calculate the error rates of the tools used. The error rates can be used to validate the smartphone acquisition tools. This article talks about motive the behind the processes that preserves any kind of digital evidences (Srivastava, A., & Vatsal, P, 2016) in its original form or format. Along with the evidence preservation, it has to perform the planned analysis by identifying, collecting and validating the respective evidence data to reconstruct the past incidents. The article presents the adaptability of the existing network forensic frameworks (Khan, S., Shiraz, M., Abdul Wahab, A. W., Gani, A., Han, Q., & Bin Abdul Rahman, Z, 2014) for quantitative analysis when applied to the mobile cloud computing. A classification to help understand the anatomy of network forensic framework is proposed.

An examination of the popular digital wallet applications (Montanez, A, 2014) is performed for the cryptocurrencies Bitcoin, Litecoin and Darkcoin for its respective potential mobile device artifacts. The article presents a thorough knowledge (Sachdev, H., Wimmer, H., Chen, L., Abdul-Al, C. F., & Powell, L. M, 2018) with respect to the digital forensic tool such as the evidence extraction process as well as the type of the evidence recovered. An automated system to perform a live memory forensic analysis (Thing, V. L., Ng, K. Y., & Chang, E. C, 2010) for smartphones is proposed. The dynamic behaviour of the volatile memory is examined and it is observed that the analysis is particularly useful for the realtime evidence acquisition analysis. It is noted that the acquisition consistency ranged from 75% to 100%.

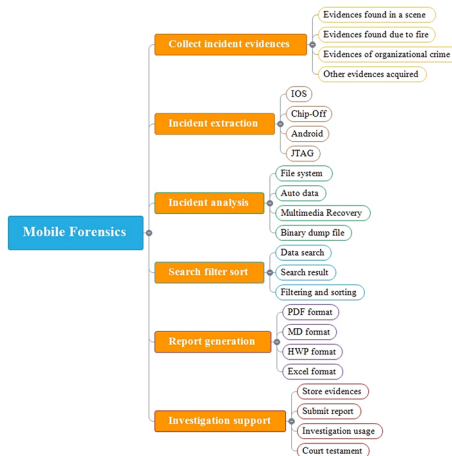
The methodology utilized to investigate the mobile devices (Sai, D. M., Prasad, N. R. G. K., & Dekka, S, 2015) for critical evidences to security investigation is presented. The method encompasses the various tools, methods and the respective procedures required to collect evidences from a variety of common mobile devices. In this article, the literatures related to the mobile forensics that focusses on the architecture of the mobile operating system and anti-forensics method (Al-Hadadi, M., & AlShidhani, A, 2013) is focussed and presented. Here, a true case study

that underwent empirical experiments which identifies the sources for the digital evidence from Oman is presented. With the available forensic tools, experiments are carried out with the NIST (National Institute of Standards and Technology) forensic method to extract the Whatsapp artifacts (Umar, R., Riadi, I., & Zamroni, G. M, 2018). Also, the respective forensic tool is been compared and evaluated based upon its strengths and weakness.

PHASES INVOLVED WITH MOBILE FORENSICS

Mobile device forensics and investigation has turn out to be a substantial and vital part of digital forensics. The paramount amount of data that is gushing into the smartphone will persist to rise rapidly since the mobile devices increase to gravitate among the personal and professional users. The primary purpose of this mobile forensics is to recuperate and preserve all the digital evidences from the respective mobile devices in forensically perfect condition. To accomplish the said primary purpose, a standard mobile forensic process has to be framed and practiced. This standard process will enable any forensic expert to collect, extract, analyze, search filter, generate report and provide investigation support from the digital evidences obtained originally for the respective mobile devices.

Figure 1. Phases of Mobile Forensics



TYPES OF MOBILE OPERATING SYSTEM

Mobile Operating Systems are specific operating systems that are designed for handheld use with special emphasis given to telephony as well as to all the features of a personal computing system. These operating systems are configured to function with a modem that is placed inside the device and a port for SIM card(s).

Smart Mobile devices generally are said to contain a two phased operating system. The primary mobile software platform is complemented by a low-level operating system which is unique to the device that runs it. There are multiple security vulnerabilities that are found in the lower rung of these mobile operating systems that are exploited by criminals to take control of the device and to escalate their access privilege.

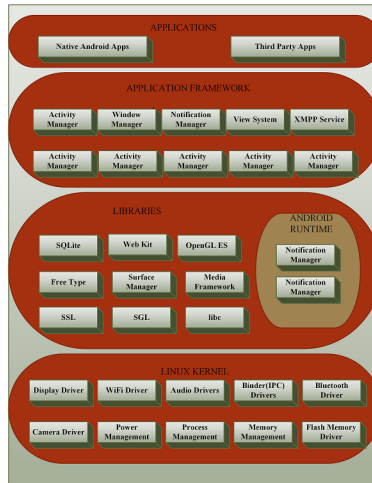
Multiple Mobile Operating Systems have come and gone throughout the Smartphone revolution but some of the most common OS's that are popular along with their developing organizations are Android OS (Google Inc.), iPhone OS / iOS (Apple), BlackBerry OS (Research In Motion), Symbian OS (Nokia), Windows Mobile (Windows Phone) and so on.

Android Operating System

The Android software development kit is primarily utilized to develop and demonstrate the android based application through the Java programming language. For a particular domain, the regular structures of the programs are determined by the application framework. Fundamentally, an application structure is a constituent in its framework that can be recycled. The respective framework sets the applications architecture and integrates a variety of abstract classes and the collaboration of the respective instances. Basically, android based mobile devices are energized with its respective batteries and the device operating system is intended to administer the processes to maintain the energy intake to the lowest. In the android mobile devices, when a specific mobile application is not in usage currently, the operating system racks up its activities. Also, at the same time, it will be available for immediate use for the user rather than closing down the respective application. During the whole activity, the application does not utilize the energy from the device battery or from the device CPU resources. When the memory in the device is low, automatically android manages and balances the respective applications stored in the memory due to which all the inactive processes will be terminated starting from the longest inactive application. Android, primarily is an extensive layered operating environment that is in accordance with the Linux kernel with different versions. The architecture of the android system is depicted in figure 2 which constitutes different layers of the android system such as Application layer, Application frame work layer, Library

layer, Android Run time layer and Kernel layer. Android mobile operating system is a heap of software components which is grossly segregated into five parts as well as four primary layers. Here, each and every layer in the architecture is associated with one another and all the respective layers will be discussed in this chapter.

Figure 2. Architecture of an Android system



Application Library

All the users access and interact with the mobile application only through the application layer. And also, once applications is installed in the mobile device and begin using that application, that particular application is used from the application layer. Moreover, applications like chrome browser, gmail, facebook, youtube and so on works on the application layer.

Since GNU 'C' library, glibc is intricate and too much big, android executes its own libc version such as bionic libc which is 200k in size. But the disadvantage with the bionic libc library is that it does not fully endorse the Portable Operating System Interface and also it is not compatible with the glibc library. The library layers in the android architecture comprises of a set of C/C++ libraries that are utilized by variety of components of the android operating system and thus offers assistance to the application framework.

Linux Kernel

Basically, the Linux kernel is the primary element of a Linux operating system and is the core interface between a computer system's hardware and its respective processes. The linux kernel is placed at the bottom of all the layers in the android architecture where the Linux 2.6 variant has 115 patches approximately. These patches provide basic system capability such as device management, memory management and process management. Furthermore, the kernel takes care and manages everything that the Linux is really worthy, such as like device drivers and networking.

Dalvik Virtual Machine

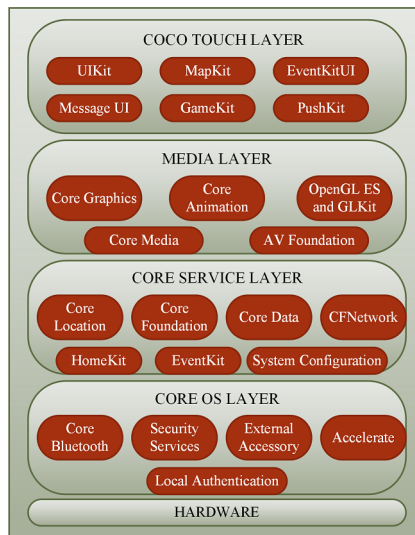
Primarily Java programming language is utilized to develop the entire android mobile applications and its elemental frameworks. Android systems use its own developed virtual machines rather than utilizing a standard Java virtual machine. The standard virtual machine Java ME is not compatible with the existing virtual machine since it is optimized for small systems. The respective small systems usually offer diminutive Random Access Memory, a slower Central Processing Unit. Furthermore, the personal computer offers no swap space to redress the small amount of memory where the android application is been run over the Linux kernel. Due to the disadvantage of the existing mechanism, the android applications are been run on a Java virtual machine called the Dalvik virtual machine. Later on Google went on to revamp and optimize the Dalvik virtual machine for its hardware characteristics of the mobile devices. The bytecode interpreter utilized in the virtual machine is named as Dalvik where it is been used as a distribution format. Dalvik has its own bytecode format instead of using the existing bytecode where it adjusts itself to the requirement of the android target devices. When compared to the regular Java bytecode, the Dalvik bytecode is much more compact and the .dex files generated are small comparatively. The tool named .dex in the android system which is a part of android SDK transforms the Java class files into the .dex format. The Java class files are compiled by the regular Java compiler. From every Java class files, the .dex format files will integrate all the Java class files and deletes the duplicate information.

iOS Operating System

The real game changer for Apple is its iOS which is the operating system that runs on all iPhones. The iOS went on with several changes and adaptations in its evolutionary process. The iOS operating system was first unveiled and introduced by 2007 with the launch of its first ever iPhone and later on it went on to be referred to as OSX. A year later by 2010, the name of OSX is changed to iPhone OS with the

launch of the iPad and subsequently, for the last time iPhone OS is changed to iOS. Henceforth, iOS represents the backbone of the Apple mobile platform and thus controlling all the various facets of the Apples' hardware. Apple offers a complete experience, bringing the best ever performance through their hardware by ingenious amalgamation of its software thereby controlling the whole iPhone ecosystem. The accomplishment of iOS has heavily swayed away the other Apples' platforms such as Apple Watch, WatchOS and TVOS.

Figure 3. Layered architecture of iOS



Each and every application in iOS is composed of at least one thread that depicts a single path of execution. The application's main function is run through a single thread that is started by every application. The specific functions will be executed by the applications that can have additional threads. When the said application creates a new thread, it turns into an autonomous entity inside the process space. Every thread in the application has its own implementation stack and the kernel schedules its run-time independently. The threads can convey each other with other threads and processes, since the respective threads are in the same process space. Here, as the processes itself, every threads in the respective applications share the similar VM spaces and also have the similar kind of access rights. Each and every memory needs the memory allocation space in both the kernel memory space as well as the program memory space. Basically, the core structures required to manage the thread of an application and coordinate is called scheduling.

The program's memory space stored the heap space of a thread and the per-thread data. Primarily, most of the structures are generated and initialized when the first thread is been generated. A method to perform as the primary entry point for the thread is required in order to generate the low-level thread. Subsequently, one of the obtained thread routines is utilized to start the thread. By utilizing the different methods such as NSThread, POSIX thread or NSObjec, the threads can be generated to spawn the thread. Once a thread is generated, several thread environments is required to be configured. The respective configuration can be performed by the configuration of thread stack size and its local storage as well as setting up the detached state of a thread and its priority.

VULNERABILITIES: ANDROID

WebView Vulnerability

WebViews is a vulnerability that happens with the android devices. The android devices are made vulnerable just by embedding a specific webpage within an application whereby the native application code with JavaScript and HTML web content is integrated seamlessly in to the android device. The WebView can be loaded by the developers through the API in different ways. One way is to load the web content through either by http or https protocols. Another way is by loading files from the file system through 'file://'. The third way is to load the html pages through 'data:/'. Normally, a basic WebView will neither be active nor execute the respective JavaScript unless the user clicks the respective hyperlink that lies within the WebView. The two different types of vulnerability that causes the damage is excess authorization and file-based cross-zone scripting. Once authorization is bestowed to any user to many web contents than what is intended, then this is called the excess authorization attack. If a file is loaded thereby permitting any script to run within the application and also, when the loaded script is considered to be of same source as the running application, then this attack is called file based cross zone scripting. When a third-party JavaScript which is not trusted is loaded, it gains access to the file system to read all the files. Consequently, due to the untrusted access by the JavaScript, the system will be affected and vulnerable to the Man-in-the-Middle (MiM) attack.

Repackaging

It is a very ordinary android device attack where the attackers alter or manipulate any well-known application downloaded from any app market. Subsequently, the

attackers reverse-engineer the downloaded app, add few malicious payloads and later on the respective manipulated app is uploaded to the app markets. Henceforth, the users can be fooled up very easily since it is very much difficult to differentiate between the original app and the manipulated file. And now once the manipulated app is been installed, the malicious code in the modified app can carry out the attacks in the background.

Predominantly, the respective proneness is noticed in business applications that run on any android based smartphones. Any user could register who registers as an android developer can very easily decompile any app and modify and repackage it. Mostly, the vulnerability results owing the bytecode structural properties. Since the android app is written in Java bytecode, the respective code can be modified and repackaged with the attacker private key and subsequently, upload it in the market with self-sign.

Dirty Unstructured Supplementary Service Data

The Dirty Unstructured Supplementary Service Data (USSD) is a type of vulnerability that happens in the android mobile. The said USSD vulnerability is revealed by September 2012. Mainly, this attack allows the hacker to reset and wipe out all the contents remotely from the android smartphones especially with Android 4.1 Jelly bean. Here, the attacker or the hacker explores and discover the vulnerability that is located in the dialer. Usually, the dialer is utilized by the user to send commands to the mobile operator. During the operation, the attacker utilizes the USSD code to execute the attack. The respective attack can be performed through malicious url, Near Field Communication (NFC) or Quick Response (QR) code to remotely exploit the vulnerability of the android device without any user permission.

Android SSL/TLS

The Secured Sockets Layer (SSL) / Transport Layer Security (TLS) vulnerability attack happen owing the poor SSL/TLS implementation that is identified by a German researcher. The SSL/TLS utilizes one or more cipher suite to provide secure data transfer. A mixture of encryption, authentication and message authentication code algorithms is called a cipher suite. This cipher suite is utilized during the security setting negotiations for a SSL/TLS connection data transfer. Basically, the customized SSL code implementation is more tolerant than the default android setting which made it vulnerable. One should understand that the outdated cipher suites are often and much more vulnerable to attacks. By any chance if the user is using the outdated cipher suite, then the hacker can very easily attack and manipulate the respective data in the transit itself.

Social and Sharing Authentication Flaws

The various social applications such as LinkedIn, Twitter, Facebook and various other social applications that are accessed through the android smartphones saves the authentication password of each and every application in an unencrypted plaintext thereby making it very much vulnerable. The hacker or the attacker intrudes into your smartphone and installs any malware into it, then he will be able to access and transfer these unencrypted plaintexts to any of the remote server. Subsequently, the hacker will be able to very easily get your valuable credentials. Thus most of the social application might be having a real threat due to this kind of vulnerability.

Zygote socket vulnerability is a threat that happens in an android mobile device. A zygote process consumes all the smartphone's resources through flooding causing Denial of Service (DoS) attack. Subsequently, due to the DoS attack, the android phone gets rebooted. The steps involved with the Zygote process are,

1. Each and every android APKs are started off by the zygote process.
2. The init process starts the zygote.
3. It is pre-loaded with Dalvik/ART virtual machine.
4. Requests to spawn off applications on a socket.
5. The Activity manager service writes commands to the zygote socket.

Zitmo

Zitmo is considered to be the most successful trojans of all time named as Zeus especially for banking vulnerability. Actually, said trojan was part of personal computers and subsequently jumped to the smartphones. The vulnerability that is performed through this type of attack is called as Zeus-in-the-mobile (Zitmo) spyware application. Predominantly, this attack is prevalent in android devices as a bank activation application. This attack eavesdrops on the SMS messages on the smartphones for the mobile transaction authentication number (mTAN) that will be sent through the text messages as a second authentication process.

VULNERABILITIES: iOS

Passing Passcode from a Trusted Computer

A trusted connection is established between the iPhone device and the respective personal computer when a user connects between them for installing any apps or downloading the desired music. At the same time, a pairing operation also happens

within seconds between these two devices. Pairing between devices is the process of creating and interchanging few digital certificates and its respective keys that sets up an encrypted channel to communicate between them. The passcode is the only credential that is required to initiate the respective connection for the first time. But unfortunately, it is really not required any longer for the future connections with the same computer even if the already provided passcode is modified or changed. The same personal computer can be connected and accessed with the already provided passcode unless and otherwise the iPhone is rebooted. With respect to the user, it may be convenient to the user since each and every time he need not provide the passcode for the connection. But alarmingly, this state of affairs inflicts a possible security threat on the user's private confidential data.

Since the control is with the passcode and once the pairing of iPhone and another personal computer happens, all the privileges are granted. With the obtained privileges, the iPhone grants the paired personal computer to access and extract the private data, install or uninstall any apps from the iPhone. The said digital certificates as well as the keys are stored in a file containing both the iPhone and the paired personal computer. The credentials of the paired record file will be stored with the default address in the Windows operating system. The default address is C:\ProgramData\Apple\Lockdown or \private\var\db\lockdown.

Backup Files on a Computer

Data backup is a crucial and important process where all the important data is copied or archived for being able to restore them in case of any loss of data or theft. Most of the iPhone users backup their valuable data on to the personal computers or laptops in case if they want to restore the respective data in the future. The main reason for iPhone backup is being the limited storage existing in the iPhone device. Nevertheless, this process of backing up is OS vulnerable, especially when few users do not set or have an encrypted passcode for the backup files or folders. In a Windows based operating system, the backup files are stored in the default address: user\AppData\Roaming\AppleComputer\MobileSync\Backup\6fca6cabb5271e539d6fa650b2c83e63fe0d41f8.

Using iCloud

The iCloud services are being provided to the user by Apple to help them to efficiently and securely backup their personal or media data or files over cloud. This allows the user to share their media data such as photographs, videos to their family members and friends with ease. Despite all these benefits and services, this would pose some potential threat or risk to the user's private and confidential data.

The hackers or intruders may illegally intrude into the iCloud servers and obtain the iCloud private data. For example, in the year 2014, malicious intruders or hackers intruded into many of the celebrities' iCloud accounts and were able to steal their sexual explicit photographs. Most importantly, based on the request from Apple to the law enforcement, it was able to get the warrants to access the users' private data that is stored in the iCloud.

Fingerprint Forging Vulnerability to Touch ID Sensor

In the recent years, the fingerprint forging attack which is vulnerable with iPhone has drawn great attention throughout the world. Basically, a user's fingerprint can be utilized to get access with an iPhone. At the same time, the same fingerprint is left on almost every object the user touches that includes the user's iPhone itself. Considering this said scenario, if a high quality fingerprint is found out by a hacker or a malicious user, he can easily unlock the iPhone device just by fabricating the fingerprint. In an empirical process conducted by the Chaos Compute Club (CCC), a researcher created a mould through a circuit-board kit once he lifted a potential fingerprint from the iPhone screen. Later on, the art glue was used to fill the mould to create a rubber based finger film that can be fully used to fool around the iPhone Touch ID sensor.

Trustjacking

Principally, the worst nightmare with an iPhone user is that when someone gain a constant control over his iPhone device. This constant control includes the capability of recording and controlling all the activity without even present in the same room or same space. It's all about trusting one another. Once the user is connecting his iPhone to a new laptop, the respective user will be asked whether they trust the connected laptop or not. Only when the user chooses to trust the respective laptop, it allows communicating with the iPhone device through the iTunes APIs.

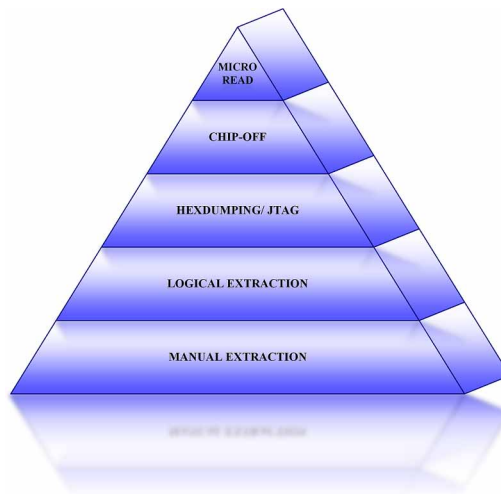
Once the trust is formed, the connected laptop will be permitted to access the photographs from the device, install apps, and perform backups and various other trusted activities especially without needing any other confirmation from the user. Moreover, as long as the laptop and the iPhone devices are connected to the same network, it permits to enable the iTunes Wi-Fi sync feature so that it makes possible to remain this type of communication with the device even after it has been disconnected from the laptop. It is quite interesting and alarming to note that the sync feature does not demand the victim's approval. It is significant to note that there is no notification mechanism to notify the users that once the laptop is been

authorized they permit access to their respective devices even after the USB cable is disconnected.

MOBILE FORENSICS TOOLS CLASSIFICATION SYSTEM

The mobile forensics tools classification that was formed by Sam Brothers is primarily used to provide mobile forensic investigators an outline of the available means to carry out the digital investigation in a better way. The overview of the available resources is presented from the least complex to the most complicated with respect to mobile evidence collection. It is very much important and significant for the digital forensic analyst to understand and make use of the different mobile forensic tools to perform the investigation in an effective and efficient manner. The respective mobile forensic tools classification system provides a proper framework to compare and contrast the various acquisition methods to capture the valuable evidences.

Figure 4. Mobile Device Classification System



Level 1: Manual Extraction

The manual extraction or acquisition is a process that manually browsing through the mobile device data and also examining the phone device documentation that can be used for investigation. The extraction process can be achieved through keypads or through touch panels. This manual acquisition method is one of the faster

methods to acquire the evidences from the suspect mobile device. For extracting the respective data, no specific cable is required to acquire the evidence data and also it works fine with almost all mobile devices. Once the data required is obtained, the respective data is evidentially documented. To err is human. As it is told, the manual extraction process is also an error prone process where all the data in the device cannot be retrieved. The main disadvantage with this manual method is that the deleted files cannot be recovered due to human intervention and also it is time consuming comparatively. Few well-known tools that can be utilized to extract evidences manually are Project-A-Phone, Fernico ZRT, EDEC Eclipse.

Level 2: Logical Extraction

The logical acquisition or extraction process helps in accessing the suspect's or users important files by connecting with the suspect's mobile device. The respective connection can be performed by physically connecting to the suspect's device through a data cable. Once the respective device is been connected, with the help of the AT commands the evidences can be acquired. Basically, this method is a faster and easier method to use that supports foreign language. In this logical method, huge amount of data based on research is available that can be utilized for the investigation very effectively. And also, the reporting features are obtainable in this method. One of the main disadvantages with this method is that the deleted files cannot be accessed. The different prominent tools that can be utilized for this type of method include Lantern, Oxygen Forensics Suite and XRY Logical.

Level 3: Physical Acquisition - Hex Dump / JTAG

This physical acquisition process aids in acquiring the details of a mobile device's file system. The respective acquisition process is performed either through a cable connectivity along with its drivers or by demounting the respective chips from the printed circuit boards. The chips will have the dump contents that could be used as evidence. Here, the data that is been extracted needs to be interpreted since the obtained data would be in RAW format. One of the primary advantages of this acquisition method is that it offers access to the deleted data that is stored in the device internal memory. One has to understand that the overwritten data cannot be retrieved or reconstructed back again at any point of time. Also, the hidden data can be extracted for the respective suspect's mobile device. The disadvantage of this method is that since it provides the data in the RAW format, it has to be converted or interpreted. Another limitation is its inconsistency in dealing with the report formats. This method is restricted to only specific manufacturers and it is tough to use. This method is cost-effective and delivers more significant information to the

digital forensic experts. Few well-known tools that can be used for this extraction purpose is Pandora's Box, XACT and Cellebrite's UFED Physical Analyzer.

Level 4: Physical Acquisition – Chip-Off

This Chip-Off method helps in un-mounting of memory chips from the mobile device and access the contents. Subsequently, the binary image of the mobile device is created which becomes costly. Also, a good amount of knowledge is required to perform these operations. Inadequate treatment of the mobile device may cause serious physical damages to the un-mounted chip and therefore, the data in the chip would be impossible to be retrieved. To carry out the investigation it read through either the secondary phone device or EEPROM reader to extract the respective information. Basically, it is a costly method that is capable of extracting all the data from the mobile device memory. This kind of data extraction provides the forensic expert a better understanding of what is happening in the mobile device comprehensively. The primary demerit of this method is that the data extracted is not continuous where it is difficult to convert and interpret. Prominent tools and equipments that can be utilized for the chip-off purpose is Circuit Board Holder, iSeasamo Phone Opening Tool, Xytronic 988D Solder Rework Station and SD Flash Doctor.

Level 5: Physical Acquisition - Micro Read

Micro Read is a physical acquisition process that offers a physical view of the electronic circuitry of the mobile device memory through the high-performance microscope. This respective microscope is utilized to examine the physical gates on the chips in the mobile device. Subsequently, the gate level information that is been extracted is converted to 1's and 0's thereby figuring out the consequent ASCII code. If the memory chip in the mobile device is impaired physically, then this type of acquisition process is most effective for data extraction. But, this method of data acquisition is a high-priced method. Once the required data is extracted from the mobile device memory, then all the respective data is verified and is considered to be forensically very stable (Kömmerling, O., & Kuhn, M. G, 1999). This acquisition process requires abundant knowledge of the hardware and the file systems to process and extract the data in an efficient manner. It is observed that there is no better tool available to read and extract the data through Micro Read. Also, it is noted that the whole process of data extraction is expensive and time intensive.

The below mentioned table consolidates all the different types of classification tools available for extracting the valuable evidences from the mobile devices. The various processes involved with all the five different type of tools are briefed up in the table. To better understand the five different tools, the advantages and

A Comprehensive Perspective on Mobile Forensics

disadvantages of each and every tools are summarized here. Also, the various tools that can be utilized for acquiring the mobile device data with respect to all the five level classification type is tabulated here for reference.

Table 1. Merits and De-merits of different mobile tool classifications.

Sl. No	Type	Process	Merits	De-Merits	Tools
1	Manual Extraction	<ul style="list-style-type: none"> → Utilize the tools and record the data manually. → Review the documentation 	<ul style="list-style-type: none"> → Manually works on all devices. → Ease of use. 	<ul style="list-style-type: none"> → Difficult to get all data. → Time consuming. → No access to deleted files. 	<ul style="list-style-type: none"> → Project-A-Phone. → Fernic ZRT → EDEC Eclipse
2	Logical Extraction	<ul style="list-style-type: none"> → Connection via data cable. → Data extraction using AT commands. 	<ul style="list-style-type: none"> → Ease of use. → Standard report format. → Plenty of data available. → The process can be repeated. 	<ul style="list-style-type: none"> → Data may change. → Minimal log access. → No deleted files. 	<ul style="list-style-type: none"> → Lantern → Oxygen Forensics Suite → XRY Logical
3	Physical Extraction (Hex Dumping / JTAG)	<ul style="list-style-type: none"> → Usage of JTAG data extraction. → Boot loader to extract phone and dump memory. 	<ul style="list-style-type: none"> → Can access deleted files. → Hidden data extraction. → Can bypass Password. 	<ul style="list-style-type: none"> → Data conversion. → Inconsistent report format. → Difficult to work on. → Cables are customized. 	<ul style="list-style-type: none"> → Pandora's Box → XACT → Cellebrite's UFED Physical Analyzer
4	Physical Extraction (Chip-Off)	<ul style="list-style-type: none"> → Remove memory from devices. → Reads in EEPROM. 	<ul style="list-style-type: none"> → Extracts all the data. → Clarity on what is been performed. → Respective Trainings. 	<ul style="list-style-type: none"> → No Continuous data. → Multiple report format. → Chip may damage while extracting. 	<ul style="list-style-type: none"> → iSeasamo Phone Opening Tool. → Xytronic 988D Solder Rework Station → SD Flash Doctor.
5	Physical Extraction (Micro Read)	<ul style="list-style-type: none"> → High power microscope is used to see the memory status. 	<ul style="list-style-type: none"> → Capable of extracting and verifying all data. → Good clarity on what is been performed. 	<ul style="list-style-type: none"> → Time consuming. → Difficult to interpret. → No specific report format. → Too expensive. 	<ul style="list-style-type: none"> → High power digital microscope.

RECENT TRENDS AND ISSUES WITH MOBILE FORENSICS

The current trends and the different issues related to the mobile forensics are the data-related issues, Device and Operating Systems Diversity, Security Aspects, and Cloud-related Issues.

Mobile Data-Related Issues

The anonymity that surrounds over the World Wide Web leads to a number of new trends and issues to the researchers in this domain. Additional problems and challenges are created inadvertently due to the employment of incognito web browsers so that the convallescening the true identity of any user becomes too much complicated. In the view of the fact that the web browsers are employed in incognito mode, deliberate IP and MAC address spoofing attack is employed.

The considerable amount of data that is extracted during an investigation is one of the perpetual challenges these days. These huge amounts of data may create management problems, increased cost and more processing time. In this scenario, while the respective large volume of data needs to be accessed more than once, the real storage issue arises when training the datasets or performing behavioral analysis. Due to the constantly increasing storage capacity with the mobile devices and also the cloud storage services support, the problem with the storage exacerbates further. The full disk encryption helps the user to secure their sensitive data. But, it is also a major hindrance to the law enforcement agency especially when dealing with crimes and investigation. Now, the digital forensic experts or investigators will not be able to easily acquire and access the mobile device data as in the past. Separate digital forensic tools have to be adapted to handle or manage the newer operating system versions so that they can find a way to access the mobile data.

Mobile Device and Operating Systems Diversity

The major challenge during the digital forensics investigation is the huge variety and models of mobile devices, its hardware components and the respective operating systems. This enormous variation affects and changes the roadmap towards the data collection and analysis with respect to the digital investigation. Various technologies incorporated in the mobile phones increases the discrepancy among the mobile forensics tools with respect to its functionality and presentation. Furthermore, these discrepancies cause the compatibility problems even between the similar family mobile devices.

Mobile Security Aspects

The new challenges that occur to the digital forensic ecosystem are the unremitting evolution of the newer and also the zero-day malicious software (malware). The mobile forensic category plays a crucial and significant role in environments such as Public Protection and Disaster Relief (PPDR) systems. In this scenario, the agencies in the PPDR system are prompted to work in tandem with the unforeseen disasters and emergency situations of any scale. Also, depend on the infrastructure and its respective support so that they will be having place to work for their daily operations. It is also significant and important to observe that the data collected by the PPDR devices serves as valuable and significant evidence. Also, it also acts as a system for recognition and detection of malicious activity.

Cloud-Related Services

Largely, organizations are migrating towards remote, virtual and on-demand service called as the Cloud services. The reason behind this migration is due to the increased requirement for a flexible computing power and the significant storage ability so as to reduce the infrastructure cost. The cloud services offer unlimited and dynamic resources for computation, storage and services virtually. Each and every organization can scale up their infrastructure with respect to agility, efficiency and flexibility through the cloud services.

The cloud forensic investigation includes the forensic activities both in the cloud and in the mobile device side that necessitates the usage of mobile forensics methods. For a digital forensics investigation, the methodologies and tools applied to the mobile forensics cannot be applied towards the digital investigation that is carried out with the cloud services. Most of the digital forensics tools has very limited capabilities and functionalities over the cloud-hosted data since the users rely on the cloud services thereby decreasing the amount of relevant data hosted on to a mobile device. This scenario poses a threat and establishes a challenge to the digital forensic domain. Another serious concern for the mobile cloud forensics is the need to guarantee the network connectivity which really drives the investigative process. The real challenge is how to safeguard the data being remotely wiped off or prevent data alteration from a compromised cloud server. The mobile cloud forensics should have a whole new perspective with respective to the investigative process model. The data storage in the remote virtual machines and their respective availability affects the investigative process since it has to be dealt with both mobile device and the cloud.

Most of the existing mobile forensic tools do not consider and does not have the capability to work in cloud environment. Also, it is observed and noted that the

forensic tools that has the cloud support will require different service models such as Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).

CONCLUSION

The security and the protection mechanism are the two weak positions in a mobile application. The number of vulnerabilities has decreased to a larger extent with every new version or variants are launched. The impacts of vulnerabilities on the mobile operating system have reduced and this can be realized through the Open Web Application Security Project (OWASP) scores. Also, it doesn't mean that the hackers are not going to attack the mobile operating system. We should understand that there will always be someone somewhere to hack into the system.

With regard to smartphones, android application has vital vulnerabilities which is slightly more than those of iOS. It is noted that the android applications iOS is affected by 43% vulnerabilities whereas the iOS is been affected by 38% of vulnerabilities. And it is observed that the one third of the android devices emanates from the configuration flaws. 8% of iOS users have jailbroken their mobile devices whereas 27% of the android devices runs with root privileges. These type of mobile devices with such root privileges are at higher threat since those privileges can be attacked by a malicious software. In todays digital super highway, cyber criminals are too much active doing illegal activities in the cyber world. Therefore, Google as well as Apple takes active steps to combat these cyber criminals. Google provides Google play protect to keep safe the mobile device by scanning all the applications that is been installed in the android device. Likewise, to prevent the malware being disseminating App store, Apple accomplishes manual analysis of all the developer apps before making them obtainable in the App store for download.

The moderate to heavy utilization of cloud service should be seriously taken into consideration because of the new contextualization of mobile device security and its services. This particular fact of contextualization provides a whole new dimension through which the jurisdictional incidents take place. It has to explicate how the investigations for various components of digital forensics concerns are performed. The industry as well as the academia has to observe and follow the specific plan for incorporating the cloud principles and ideas into their future implementation and realization.

REFERENCES

- Abba, E., Aibinu, A. M., & Alhassan, J. K. (2019). Development of multiple mobile networks call detailed records and its forensic analysis. *Digital Communications and Networks*, 5(4), 256–265. doi:10.1016/j.dcan.2019.10.005
- Al-Hadadi, M., & AlShidhani, A. (2013). Smartphone forensics analysis: A case study. *International Journal of Computer and Electrical Engineering*, 5(6), 576–580. doi:10.7763/IJCEE.2013.V5.776
- Al Mutawa, N., Baggili, I., & Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. *Digital Investigation*, 9, S24–S33. doi:10.1016/j.diin.2012.05.007
- Ali, A., Abd Razak, S., Othman, S. H., Mohammed, A., & Saeed, F. (2017). A metamodel for mobile forensics investigation domain. *PLoS One*, 12(4), e0176223. doi:10.1371/journal.pone.0176223 PMID:28445486
- Alyahya, T., & Kausar, F. (2017). Snapchat analysis to discover digital forensic artifacts on android smartphone. *Procedia Computer Science*, 109, 1035–1040. doi:10.1016/j.procs.2017.05.421
- Baggili, I. M., Mislán, R., & Rogers, M. (2007). Mobile phone forensics tool testing: A database driven approach. *International Journal of Digital Evidence*, 6(2), 168–178.
- Barmpatsalou, K., Cruz, T., Monteiro, E., & Simoes, P. (2018). Current and future trends in mobile device forensics: A survey. *ACM Computing Surveys*, 51(3), 1–31. doi:10.1145/3177847
- Chernyshev, M., Zeadally, S., Baig, Z., & Woodward, A. (2017). Mobile Forensics: Advances, Challenges, and Research Opportunities. *IEEE Security and Privacy*, 15(6), 42–51. doi:10.1109/MSP.2017.4251107
- Faheem, M., Le-Khac, N. A., & Kechadi, T. (2014). Smartphone forensic analysis: A case study for obtaining root access of an android samsung s3 device and analyse the image without an expensive commercial tool. *Journal of Information Security*, 5(03), 83–90. doi:10.4236/jis.2014.53009
- Fukami, A., & Nishimura, K. (2019). Forensic Analysis of Water Damaged Mobile Devices. *Digital Investigation*, 29, S71–S79. doi:10.1016/j.diin.2019.04.009
- Gentry, E., & Soltys, M. (2019). SEAKER: A mobile digital forensics triage device. *Procedia Computer Science*, 159, 1652–1661. doi:10.1016/j.procs.2019.09.335

Goel, M., & Kumar, V. (2019, March). Layered Framework for Mobile Forensics Analysis. *Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE)*.

Herrera, L. A. (2020). Challenges of acquiring mobile devices while minimizing the loss of usable forensics data. *Proceedings of 2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 1-5.

Hur, J. B., & Shamsi, J. A. (2017, December). A survey on security issues, vulnerabilities and attacks in Android based smartphone. In *Proceedings of 2017 International Conference on Information and Communication Technologies (ICICT)* (pp. 40-46). IEEE.

Kataria, A., Anjali, T., & Venkat, R. (2014, February). Quantifying smartphone vulnerabilities. In *Proceedings of 2014 International Conference on Signal Processing and Integrated Networks (SPIN)* (pp. 645-649). IEEE.

Khan, S., Shiraz, M., Abdul Wahab, A. W., Gani, A., Han, Q., & Bin Abdul Rahman, Z. (2014). A comprehensive review on adaptability of network forensics frameworks for mobile cloud computing. *The Scientific World Journal*.

Koganti & G. (2019). Forensic Acquisition of IOS Devices. *International Journal of Recent Technology and Engineering*, 8(4), 10847–10855. doi:10.35940/ijrte.D4374.118419

Kömmerling, O., & Kuhn, M. G. (1999). Design Principles for Tamper-Resistant Smartcard Processors. *Smartcard*, 99, 9–20.

Lin, X., Chen, T., Zhu, T., Yang, K., & Wei, F. (2018). Automated forensic analysis of mobile applications on Android devices. *Digital Investigation*, 26, S59–S66. doi:10.1016/j.diin.2018.04.012

Lohiya, R., John, P., & Shah, P. (2015). Survey on mobile forensics. *International Journal of Computers and Applications*, 118(16).

Montanez, A. (2014). Investigation of cryptocurrency wallets on iOS and Android mobile devices for potential forensic artifacts. Dept. Forensic Sci., Marshall Univ.

Mullan, P., Riess, C., & Freiling, F. (2019). Forensic source identification using JPEG image headers: The case of smartphones. *Digital Investigation*, 28, S68–S76. doi:10.1016/j.diin.2019.01.016

Murphy, C. A. (2009). *Developing process for mobile device forensics*. Madison. Retrieved, October 03, 2020 from <https://digital-forensics.sans.org/media/mobile-device-forensic-process-v3.pdf>

A Comprehensive Perspective on Mobile Forensics

- Ninawe, P. N., & Ardhapurkar, S. B. (2014). Forensic-as-a-service for mobile devices (literature survey). *Int. J. Comput. Sci. Inform. Technol*, 5(6), 7776–7778.
- Sachdev, H., Wimmer, H., Chen, L., Abdul-Al, C. F., & Powell, L. M. (2018). A Digital Forensic Tool for Mobile Devices: Paraben. ToKnowPress.
- Sai, D. M., Prasad, N. R. G. K., & Dekka, S. (2015). The Forensic Process Analysis of Mobile Device. *Int. J. Comput. Sci. Inf. Technol*, 6(5), 4847–4850.
- Shaheen, J. A., Asghar, M. A., & Hussain, A. (2017). Android OS with its Architecture and Android Application with Dalvik Virtual Machine Review. *International Journal of Multimedia and Ubiquitous Engineering*, 12(7), 19–30. doi:10.14257/ijmue.2017.12.7.03
- Singh, A. J., & Bhardwaj, A. (2014). Android vs. IOS: An Architectural Perspective. *International Journal of Innovative Research and Development*, 3(1), 82–90.
- Srivastava, A., & Vatsal, P. (2016). Forensic importance of SIM cards as a digital evidence. *Journal of Forensics Research*, 7(322), 2. doi:10.4172/2157-7145.1000322
- Thing, V. L., Ng, K. Y., & Chang, E. C. (2010). Live memory forensics of mobile phones. *Digital Investigation*, 7, S74–S82. doi:10.1016/j.diin.2010.05.010
- Umar, R., Riadi, I., & Zamroni, G. M. (2018). Mobile forensic tools evaluation for digital crime investigation. *Int. J. Adv. Sci. Eng. Inf. Technol*, 8(3), 949. doi:10.18517/ijaseit.8.3.3591
- Van Zandwijk, J. P., & Boztas, A. (2019). The iPhone Health App from a forensic perspective: Can steps and distances registered during walking and running be used as digital evidence? *Digital Investigation*, 28, S126–S133. doi:10.1016/j.diin.2019.01.021
- Wilson, R., & Chi, H. (2017, April). A case study for mobile device forensics tools. In *Proceedings of the SouthEast Conference* (pp. 154-157). 10.1145/3077286.3077564

KEY TERMS AND DEFINITIONS

Android: Android is a mobile operating system developed by Google that lets users to manipulate the mobile devices intuitively, with finger movements that mirror common motions, such as pinching, swiping, and tapping.

Data Extraction: Data extraction is a process that involves retrieval of data from various sources for further data processing, storage, or analysis elsewhere.

Digital Evidence: Digital evidence is any significant information stored or transmitted in digital form that a party to a court case may use at trial.

iOS: iOS is a mobile operating system for Apple-manufactured devices such as iPhone, iPad, iPod Touch and Apple TV that allows iPhone users to interact with their phones using gestures such as swiping, tapping, and pinching.

Mobile Forensics: Mobile phone forensics is the science of retrieving data from a mobile phone under forensically sound conditions. This includes full data retrieval and examinations of data found on the SIM/USIM, the phone itself and the optional memory cards. Data retrieved and examined can include images, videos, text or SMS messages, call times and contact numbers.

Smart Phones: A smartphone is a mobile device that combines cellular and mobile computing functions such as web browsing and the ability to run software applications into one unit.

Vulnerability: Vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Chapter 2

Applications of Machine Learning in Cyber Forensics

Kishore Rajendiran

Sri Sivasubramaniya Nadar College of Engineering, India

Kumar Kannan

 <https://orcid.org/0000-0002-7501-8745>
Vellore Institute of Technology, Vellore, India

Yongbin Yu

University of Electronic Science and Technology of China, China

ABSTRACT

Nowadays, individuals and organizations experience an increase in cyber-attacks. Combating such cybercrimes has become the greatest struggle for individual persons and organizations. Furthermore, the battle has heightened as cybercriminals have gone a step ahead, employing the complicated cyber-attack technique. These techniques are minute and unobtrusive in nature and habitually disguised as authentic requests and commands. The cyber-secure professionals and digital forensic investigators enforce by collecting large and complex pools of data to reveal the potential digital evidence (PDE) to combat these attacks and helps investigators to arrive at particular conclusions and/or decisions. In cyber forensics, the challenging issue is hard for the investigators to make conclusions as the big data often comes from multiple sources and in different file formats. The objective is to explore the possible applications of machine learning (ML) in cyber forensics and to discuss the various research issues, the solutions of which will serve out to provide better predictions for cyber forensics.

DOI: 10.4018/978-1-7998-4900-1.ch002

INTRODUCTION

Cybercrime has drastically increased since the 1970s with the widespread use of technology that led to various criminal activities. This, in turn, emphasized the need for efficient investigations over the past few years. Cyber forensics, also termed as digital or computer forensics, turns around the scientific and authorized extraction of evidence in the digital form. This field examines, analyzes, and reports the digital evidence given cyber/digital criminal activity (Baggili, I., & Behzadan, V. 2019). In human life, digitization has become dominant, occupying most of the day-to-day activities, either in professional or personal life. As a result, people are in and around a device that leads to digitization in most of their routine work. For example, a smartphone can provide access to various sensitive data (e.g., transaction, email, and messages) that can provide user-related information and their social connectivity (Rohmeyer, P. 2010). Mainly, digitization evolves at the cost of financial frauds; Intellectual Property Rights (IPR) infringements, malware, and terrorist communication are among the few to show the originality of cybercrime and its behavior.

Cyber forensics needs a structured efficient mode of inquiry about forensic pieces of evidence found in the crime space (Atlam, H., Walters, R., & Wills, G. 2018). By 2025, the expected number of Internet of things (IoT) devices may reach 21.5 billion worldwide, increasing the amount of data to be handled. Thereby, increasing the possibilities of cybercrime in a huge scale and providing preventive measures pose a great challenge (Statista Research Department. 2016). The development of Internet and data communication technologies can provide space for intruders to inject security attacks, cybercrimes, and malware (Atlam, H. F., et. al. 2017). Malicious attacks in the networks are common, and hackers can intrude into the network, which can be identified with an effective cyber security mechanism with artificial intelligence (AI). So there is a need for data handling with huge IoT data and predictive intelligence with the help of AI (Atlam, H. F., & Wills, G. B. 2020).

In order to handle the analysis of large amounts of complex data for forensic purposes, investigators frequently handle the increased demand with less time and low-priced measures. This is the reason why AI is being used in the field of cyber forensics; besides, even many traditional investigators might argue that it is not an incomparable solution, as they agree that AI can help improve the battle against cybercrime (Karie, N. M., et. al. 2019).

This chapter proposes a suitable framework in which machine learning (ML) concepts and techniques are integrated with digital forensic activities (e.g., evidence collection, analysis, and correlation). In this framework, forensic expert decides upon the prediction results of ML to move towards report generation.

Background

In this section, the authors provide a background study of cyber forensics in terms of state of the art, cybercrimes with forensics, and applications of cyber forensics. Finally, they discuss the critical challenges of digital/cyber forensics.

State of the Art

Using biochemistry, psychology, and current technology in cyber forensic is developing along with standard techniques to identify cybercrimes. Consistency in digital/cyber forensic direct analysis procedure is synonymous with reliability and trustworthiness; such behaviour is regular with repeatable performance and deriving dependable results. The investigatory process in the context of cyber forensics requires consistency to achieve quality. Any evidential explanations which show inconsistency may lead to the unsafe process. Consistency in all aspects is the focus to determine the state of the art in cyber forensics, which uses small scale digital/cyber devices (SSDDs) and deep learning. SSDDs are a new growing field which falls behind in terms of analysis and procedures (Backer, 2009). In SDDD forensics, smartphone, drone, gaming consoles, wearable technologies, and smart toys are playing a significant role (Al Hosani et al., 2020. Meffert et al. (2017) proposed a real-time forensic state acquisition controller to provide the solution which uses IoT data obtained from the cloud. Chhabra et al. (2020) devised a traffic framework to address forensics data in huge size with the MapReduce model to analyze the traffic features which have dynamic nature.

The process of finding acceptable cyber evidence for submission in the court is challenging because of diversity, ubiquitous, heterogeneous, and rapid development. The evidence collection requires an intelligent way to predict about the updated data with current details. Deep learning is the subset of AI that can focus on real-time analysis of evidence data for prediction.

Cybercrimes and Forensics

Cybercrime contains details about illegal activities conducted on a computer. Traditional crimes are committed while using a piece of manual/human evidence, but cybercrime includes more specific varieties of criminal offences, such as phishing schemes and infections. Digital/cybercrime initially started with hackers who accessed a computer network anonymously. Few crack the security networks for the thrill, while others do it to get classified information and gain sensitive details. Finally, lawbreakers can bring the computer system into their control by viruses which can destroy personal and business operations. System/computer viruses are

varieties of code or adware and spyware programs that can copy themselves and damage or destroy data and systems.

In some cases, computer infections are widely used on a big scale (e.g., with a bank, government or hospital networks); these actions may be categorised as cyber terrorism. Computer hackers also take part in phishing frauds, such as asking for bank account amounts, and credit card theft. Cybercrime can be classified as Type I and Type II cybercrime. Type I is mostly technical, while Type II has a more prominent human element. On the other hand, digital/cyber forensics has the process of preservation, identification, extraction, and documentation of digital evidence that can be submitted based on the court of law. It is a technology of finding proof from cybercrime committed using a computer, cell phone, server or network. It provides the forensic team with the best techniques and tools to solve complicated digital/cyber-related cases.

The purpose of computer forensics techniques is to research, preserve, and analyze home elevators computer systems to find possible evidence for a trial. Many of the methods investigators use in crime scene investigations have digital/cyber counterparts, but there are also some unique aspects to computer investigations.

Learning Over Forensics

The most famous research area in ML, deep learning has come out as a technological field that can offer fast processing of vast amounts of data during system training using a neural network. In general, cybercrime has more data, which motivated the concept of bringing learning cognitive computing techniques into cyber forensics as a way to aid in the analysis of the enormous amount of data during a forensic investigation process. Wang and Pei (2017) also highlighted that a deep neural network could be able to unearth visual patterns through robust learning and even a considerable amount of data models. The above discussion states that deep learning has the ability when used in digital/cyber forensics, to unearth relevant digital/cyber evidence from big data as and when required by investigators.

Applications of Cyber Forensics

Digital/cyber forensics is the branch of the forensic science that offers digital/cyber evidence in solving the crime underneath the rules of law. With the usage of different digital/cyber media devices and social media, several branches are associated with digital/cyber forensics, for example, mobile forensics, system forensics, database forensics, and email forensics. With increasing digital/cybercrime in every branch, digital/cyber forensics has broad applicability.

Applications of Machine Learning in Cyber Forensics

Most of the applications of digital/cyber forensics can address crime detection, prevention, analysis, preservation, identification, extraction, documentation, and interpretation (Wachter, 2018) in different areas (e.g., health care and traffic management):

- **Crime Detection:** Phishing, spoofing, and ransomware over digital/cyber networks can lead to malicious activity and malware.
- **Crime Prevention:** It allows mitigating the crime well ahead, such as zero-day vulnerability. For example, in the healthcare system to protect the sensitive information of the patient and protect with blockchain or any other security technology.
- **Crime Analysis:** The IoT data of an intelligent transport system can predict required information based on the features extracted from the evidence.
- **Preservation:** It consists in the protection of digital/cyber evidence such as a photo or video of crime for future use. This process contains secured access to the evidence to whom assigned with the investigation using the ledger system.
- **Identification:** It consists in digital media information and the devices used in the crime scenes identified and recorded as evidence of the cybercrime.
- **Extraction:** From the crime scene, the investigators maintain and manage the first evidence during the investigation.
- **Documentation:** All the evidence about crime scenes is noted with a chain of custody details. A blockchain framework is used to ensure user anonymity in the cybersecurity threats.
- **Interpretation:** In a report generation, the forensic expert can use imaging and mounting the evidence with different tools (e.g., Sleuth kit and Autopsy) represented in the court of law. Data fragments are reconstructed based on the evidence the forensic expert collected and analyzed in the forensic report.

KEY CHALLENGES

However, the research on cyber forensics is still at an early stage and implies many challenges over technology, resources, and legal aspects. In this section, the authors address the critical challenges in cyber forensics. Additionally, a few recent studies (Yampolskiy, 2019) discussed the use of ML techniques in cyber forensics and the challenges faced over time. Zoya (2020) divided these challenges into technical, resource, and legal-related challenges; the authors discuss them below.

Technical Challenges

The technology which is adopted in cyber forensics is not enough to address all the solutions in IoT and forensics (Singh et al., 2018). Thus, technical challenges arise during real-time analysis, steganography, and evidence collection. The authors focused on the following technical challenges:

- Hackers may adopt anti-forensics techniques and manipulate the evidence of forensic investigation with the help of AI.
- Most of the organizations have a denial syndrome over cyber forensics, which affects the security system inside the organization. The same visionless way towards cybercrime may lead to the failure of the technical process inside the organisation.
- There is a need for policy based on the technical process of control and auditing. A process model is required to address the audit and control process.
- Safety and security of the evidence management against the malware or intruders is a challenge.
- An intruder possibly trains the AI models via backdoors to corrupt the system to act maliciously.
- To use technology which has its inherent drawbacks noted with action taken report.

Resource Challenges

The cybercrime investigation requires many resources such as the volume of evidence, communication network, media, and SSDs, which are managed based on the nature of the crime. The list below indicates some of the challenges for the future:

- There is a need to devise a mechanism to identify the resources of the dark Web, whereas it is necessary to trace tools for deep Web and surface Web accessing persons.
- Providing training on prevention and awareness over the dark Web is not adequate for capacity building over criminality (Safjański & James, 2020).
- In recent days, data resources are stored in online storage spaces (i.e., cloud) which pose a new challenge in retrieving an image of such vast data that may require service interruption.
- Digital/cyber resources come with various versions, which might have different features. This creates confusion for the expert who is involved in the investigation.

Applications of Machine Learning in Cyber Forensics

- Using network resources to capture specific packets out of millions transmitted in the network requires individual devices that may reduce the transmission time.
- IoT device-generated personal data are unstructured and may be spoofed; this is a challenge for the legal process, which requires more analysis based on resources.

Legal Challenges

There is always a need for legal systems that permit to sustain the legal reliability of the resultant forensic analyses. Cyber judicial challenges are in standards, international legislations, reconstructions or simulation, scrutiny, and possible issues. Some of the problems in the legal aspect are as follows:

- There is a need for appropriate information management policies in the international arena.
- The use of AI over the forensic investigation and its policy are not at a mature level, because there is no legal provision to allow intelligent experts and forensic experts to work (Baggili & Behzadan, 2019).
- There is a lack of awareness to understand global standards in cyber forensics administered in corporate policies, which needs realization for a successful forensic workout.
- Guidelines in traditional cyber forensics might not be best suited for IoT, edge, and cloud computing with wearable sensor technologies.
- Policies for privacy and data protection are limited to data, storage, confidentiality, and integrity (Sanchez et al., 2019).

MACHINE LEARNING RELATED WORK AND RESEARCH CONTRIBUTIONS

The Internet brings into many more applications which increase vast volumes of data, and digital/cyber storage poses a need for investigations and examination of massive data. Presently, cyber forensics does not have specialized tools to analyze and correlate such a considerable volume of data. Thus, there is a need for tools, and techniques result to bring AI as Hoelz et al. (2009) proposed. Wand and Pei (2007) argued the importance of ML over cyber forensics and the areas where learning techniques are used. Consequently, modern forensic systems are exploiting the advantage of ML techniques to study and compute the code and files having malware information, which can predict the behavior of malware and ensure security against new threats.

Rughani and Bhat (2017) researched the use of ML in cybercrime while training the environment with artificial neural networks to analyze and predict the artefacts which can be helpful in the investigation. All these works emphasize the adoption of AI and related techniques to address intrusions and other threats in cyber forensic systems. Finally, Karie et al. (2019) proposed a novel framework which integrated deep learning and cognitive computing into cyber forensics. This approach aimed to recognize the usefulness of forensic inquiry using ML. As network devices and humans are not enough to monitor the intrusions and threats, a generic framework is necessary to address sophisticated systems that need to defend, detect, adapt, and strengthen to make intelligent decisions.

Research Contributions

This work contributes the following points as research deliverables:

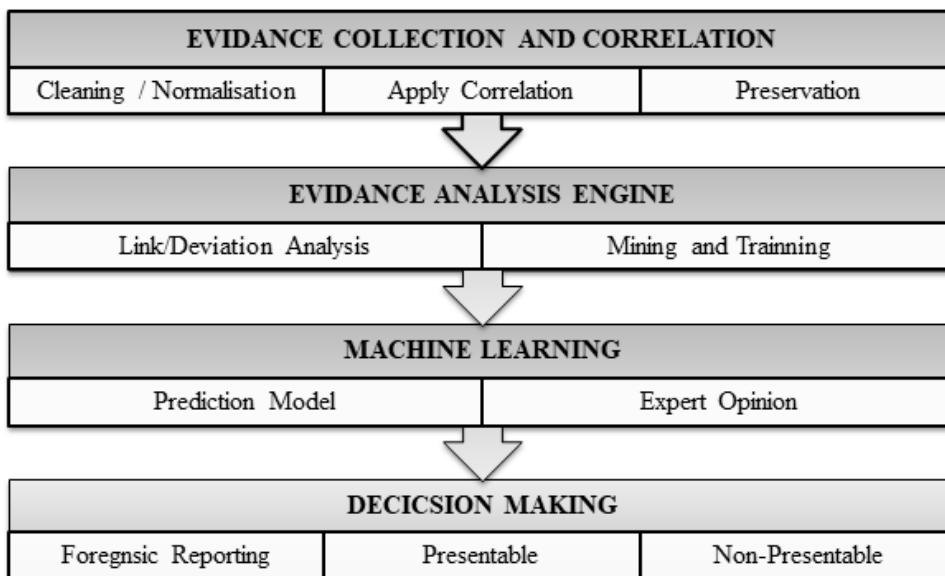
- Addressing cyber forensics in a generic framework, with all the required analysis steps.
- Using an ML algorithm to predict a threat and allow the experts to clearly establish if it is malicious or not.
- Validating the results and generating the report of cyber forensics with a proper approach.
- Providing a case study for verifying the proposed framework.

The Cyber Forensics Machine Learning (CyFML) Framework

The authors' contribution to support cyber forensics consists in the cyber forensics machine learning (CyFML) framework, which includes ML and mining techniques to provide better predictions. Figure 1 illustrates the CyFML framework by a high-level contextual diagram which shows the framework with the generic functional flow, provides the details of ML algorithms, and addresses specific scenarios.

Applications of Machine Learning in Cyber Forensics

Figure 1. The cyber forensics machine learning framework



The CyFML framework is characterized by the following functional steps:

Step 1: In order to select the forensics domain, the digital/cyber information is normalized, and correlation is applied to it. Below, Equation [1] represents the nonempty set of domains involved in the cyber forensics domain of reference:

$$D = \{D_1, \dots, D_n\}, D_i; 1 \leq i \leq n \quad [1]$$

where D is a finite nonempty set.

Step 2: In the evidence analysis, the key issues are identified; they are difficulties in the preservation of records with the assistance of link/deviation analysis. Mining techniques to separate problems and match the training are set to the scenario of reference. Below, Equation [2] represents the set of files in the selected forensic domain:

$$R = \{R_1, \dots, R_n\}, R_i; 1 \leq i \leq n \quad [2]$$

where a D_i can contain R_i from R .

Step 3: The prediction model is identified based on the earlier analysis. A set of nonempty prediction states is determined using ML techniques, and expert opinion is considered for the predicted results, as Equation [3] shows below:

$$P = \{p_0, \dots, p_n\} \quad [3]$$

where P is a finite non empty set of predictions.

Step 4: Finally, forensic decision making is addressed for cyber data. Forensic reporting with presentable data and nonpresentable data informs the policy. The reporting can be shared through the procedure and bring criticalities such as a failure, malfunction, error or defect. Below, Equation [4] shows the process:

$$R_i : P_i \xrightarrow{\text{input}} P_j \xrightarrow{\text{Output}} \Delta \quad [4]$$

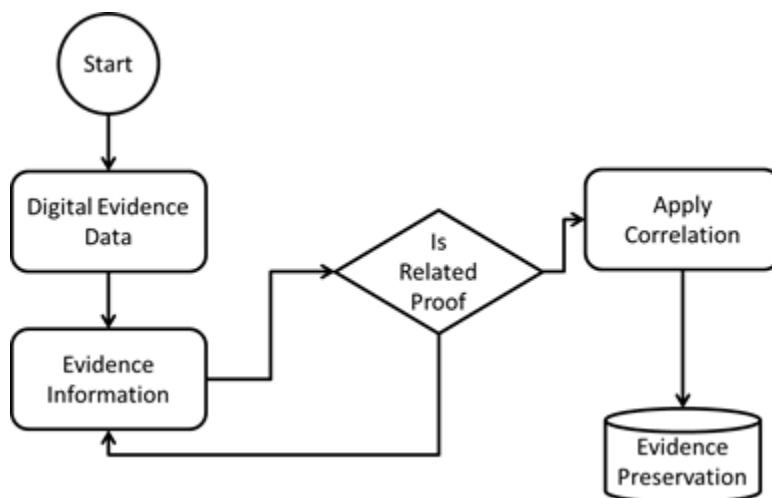
where reporting R_i can read the prediction input P_i and goes to P_j producing some output Δ .

Step 5: Expected action taken based on the defined policy behavior. There is a need for predicting the behaviour of actors involved in the context scenario.

Evidence Collection and Correlation

Digital/cyber evidence is a proof from physical or electronic devices or digital/cyber proof from a hard disk file, email, SMS, image, video, logs or content. The disclosure of evidence is an electronic proof which becomes progressively significant as the specialists complete their assessment. At present, verification is information directly related to the data the inspector requires in the assessment technique. In this phase of the CyFML framework (Figure 2), the authors propose to collect the evidence and correlate it to store the preserved data of digital/cyber forensics.

Figure 2. Evidence acquisition process



Evidence Analysis with Machine Learning and Deep Learning

In this phase of the CyFML framework, each evidence item is recorded with date and time. Elements which are considered for evidence are tagged with description. Many categories of evidence exist, but the authors believe the most focused cyber forensics is Internet-based and stand-alone computers or devices and mobile devices. Evidence analysis distinguishes the key issues, which identify difficulties in the preservation records with the assistance of link/deviation analysis. Mining techniques to separate problems and match the training are set to the scenario of reference. Data mining is used to extract or “mine” information from a massive volume of Internet data. Clustering, regression, predictive models, and neural network can be used to handle cyber forensic data. Based on the problem requirements, supervised learning or unsupervised learning are taken into consideration.

Forensic Reporting

During the reporting, a few steps have to be completed, such as identifying the data based on the events, gathering all relevant details in an objective report, and listing the events leading to the solution of the investigation (Baror et al., 2020). Finally, all the sources of evidence are collected. The reporting of cyber forensics can be done based on the phases of the proposed CyFML framework, namely from evidence collection to decision making, with ML techniques.

Prediction and Decision Making

In digital/cyber forensics, the usage of AI is called ML forensics, which recognizes patterns of the crime and predicts the malicious activity or gets a clue from the history of a similar kind of crime. It requires a framework to analyze the data on the Internet or many other ways associated with links. In this regard, many techniques and technologies in ML have been successfully adopted in cyber forensic. One such way is link analysis, which finds the association based on relatives by, for example, blood, friends, spouse, employees, and neighbours. Finally, decision making with the help of experts is explained via reporting in digital/cyber forensics, along with AI to ensure completeness (Mena, 2003).

Closure of the Case

Finally, the cyber report to close the case is submitted based on the following elements (Qadir & Varol, 2020):

- List the components of the data related to fraud.
- Investigator details and evidence storage details.
- Ways to access the evidence data by the investigator to create detection models.
- An analysis model and a description of how clustering techniques can be used and visualised.
- Usage of ML and rule engine for cyber forensic analysis.
- Possible generation of reactive rules to address the prevention and security of a fraudulent transaction.
- Experts' findings and relevant notes in the report.

SCENARIOS

In this section, the authors report the findings of the adoption of their CyFML framework in a case study they developed on two scenarios.

Scenario 1: Banking Fraud

In the last few years, a vast number of transactions occurred in the bank. The auditor charged a few of the employees who might indulge with suspect activity during the loan approval, but who are not able to fix it. Thus, the accounting firm appointed an expert to audit activities connected to loans and their authorization by the employees

of the bank. During the audit, the expert examined several computer systems the employee of the bank used. The digital/cyber forensic inspectors arranged straight away to do the forensic analysis over the computing devices which were used in the bank (Global Digital Forensics, 2020).

In this scenario, the investigator might not have the necessary details to fetch manual documents, and looking for any file in the system can be taken as evidence to file a case against the concerned employee.

Scenario 2: Forensic Prediction Analysis of Glass (Evidence)

As per the digital/cyber forensic examination report (Rayan, 2017), the investigator found that stalking had occurred over social media and the accused had stabbed a victim using a glass piece. In this scenario, the investigator used linkage analysis to trace the suspects, but the investigator needed to know the type of glass the aggressor used to stab the victim. The data set to predict the kind of glass is Glass Identification (German, 2017). This data set allows studying the type of glass using a deep learning algorithm to predict and help the investigator decide upon the victim. This data set consists of 105 instances with eight critical features of glass and finally provides the type of glass as output. Highlighted features of the data set are: Id number; RI: refractive index; Na: Sodium; Mg: Magnesium; Al: Aluminum; Si: Silicon; K: Potassium; Ca: Calcium; type of glass: 1- Glass, 2- Bottle, and 3-others.

Using this data set, the authors worked with Google Colab to test over the Keras API for deep learning algorithm with ReLu function and two hidden layers having 8 and 1 neurons, respectively. Figure 3 shows the efficiency of the given data set; the authors required more data instances to get a better efficiency graph.

Figure 3. Efficiency of the given data set

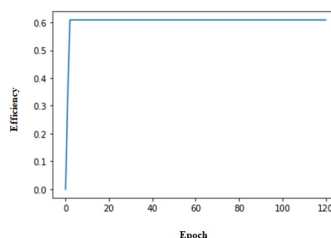


Figure 4 illustrates the TensorFlow simulation of scenario 2, which is a classification function (3 hidden layers with 8,4, and 1 neurons, respectively) with epoch count of 121 and block size 10.

Figure 4. TensorFlow simulation of scenario 2



FUTURE RESEARCH DIRECTIONS

Future work can focus on evidence management against malware, and on how to block the intruder who can enter through backdoors and train the system to act maliciously. The future enhancement should be focused on the prototype model, rather than on a scenario-based approach, and also consider the need for legal policies in the international arena.

CONCLUSION

The authors proposed the CyFML framework in order to integrate deep learning techniques into digital/cyber forensics. The authors provided a CyFML generic framework with current learning technology. This framework is made up of the following phases: Evidence collection and correlation, evidence analysis, forensic reporting, and prediction and decision. Cyber forensics and its challenges were the authors' focus in this study. Deep learning is used in prediction analysis to help the investigator. Finally, the authors reported the results of the implementation of their framework in a case study with two scenarios, which allowed understanding the different aspects of the method and its usage.

REFERENCES

- Al Hosani, H., Yousef, M., Al Shouq, S., & Iqbal, F. (2020). State of the art in digital forensics for small scale digital devices. In *Proceedings of 11th International Conference on Information and Communication Systems (ICICS)* (pp. 72-78). Academic Press.
- Atlam, H., Walters, R., & Wills, G. (2018). Internet of things: State-of-the-art, challenges, applications, and open issues. *International Journal of Intelligent Computing Research*, 9(3), 928–938. doi:10.20533/ijicr.2042.4655.2018.0112
- Atlam, H. F., Alenezi, A., Walters, R. J., Wills, G. B., & Daniel, J. (2017). Developing an adaptive risk-based access control model for the Internet of things. In *Proceedings of IEEE International Conference on Internet of Things (iThings), IEEE Green Computing and Communications (GreenCom), IEEE Cyber, Physical, and Social Computing (CPSCom), and IEEE Smart Data (SmartData)* (pp. 655-661). 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.103
- Atlam, H. F., & Wills, G. B. (2020). IoT security, privacy, safety, and ethics. In M. Farsi, A. Daneshkhah, A. Hosseinian-Far, & H. Jahankhani (Eds.), *Digital Twin Technologies and Smart Cities. Internet of Things (Technology, Communications and Computing)* (pp. 123–149). Springer. doi:10.1007/978-3-030-18732-3_8
- Backer, C. (2009). *Digital forensics on small scale digital devices. Seminar Topic: Covert channels and Embedded Forensics, Ruhr-University Bochum*. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.392.8017&rep=rep1&type=pdf>
- Baggili, I., & Behzadan, V. (2019). Founding the domain of AI forensics. In *Proceedings of the Workshop on Artificial Intelligence Safety (SafeAI 2020)* (pp. 31-35). Academic Press.
- Baror, S. O., Ikuesan, R. A., & Venter, H. S. (2020). A defined digital forensic criteria for cybercrime reporting. In *Proceedings of International Conference on Cyber Warfare and Security* (pp. 617-XVIII). Academic Conferences International Limited.
- Chhabra, G. S., Singh, V. P., & Singh, M. (2020). Cyber forensics framework for big data analytics in IoT environment using machine learning. *Multimedia Tools and Applications*, 79(23), 15881–15900. doi:10.1007/11042-018-6338-1
- German, B. (2017). *Glass classification: Can you correctly identify glass type?* <https://www.kaggle.com/uciml/glass/data>

Global Digital Forensics. (2020). *Case study: Banking industry executive level financial fraud*. <https://einvestigate.com/case-study/banking-industry-executive-level-financial-fraud/>

Hoelz, B. W., Ralha, C. G., & Geeverghese, R. (2009). Artificial intelligence applied to computer forensics. In *Proceedings of the 2009 ACM symposium on Applied Computing (SAC '09)* (pp. 883-888). Association for Computing Machinery. 10.1145/1529282.1529471

Karie, N. M., KEBANDE, V. R., & Venter, H. S. (2019). Diverging deep learning cognitive computing techniques into cyber forensics. *Forensic Science International: Synergy, 1*, 61–67. PMID:32411955

Meffert, C., Clark, D., Baggili, I., & Breitingner, F. (2017). Forensic state acquisition from Internet of things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition. In *Proceedings of the 12th International Conference on Availability, Reliability, and Security (ARES '17)* (pp. 1-11). Association for Computing Machinery. 10.1145/3098954.3104053

Mena, J. (2003). *Investigative data mining for security and criminal detection*. Butterworth-Heinemann.

President's Council of Advisors on Science and Technology (U.S.). (2016). *Report to the president, forensic science in criminal courts: Ensuring scientific validity of feature-comparison methods*. Executive Office of the President of the United States, President's Council of Advisors on Science and Technology.

Qadir, A. M., & Varol, A. (2020). The role of machine learning in digital forensics. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-5). IEEE. 10.1109/ISDFS49300.2020.9116298

Rayan, N. (2017). *Digital forensics report*. http://www.rnyte-cyber.com/uploads/9/8/5/9/98595764/exampledigiforensicsrprt_by_ryan_nye.pdf

Rohmeyer, P. (2010). Technology malpractice. In J. Bayuk (Ed.), *CyberForensics. Springer's Forensic Laboratory Science Series* (pp. 141–148). Humana Press.

Rughani, P. H., & Bhatt, P. (2017). Machine learning forensics: A new branch of digital forensics. *International Journal of Advanced Research in Computer Science*, 8(8), 217–222. doi:10.26483/ijarcs.v8i8.4613

Safjański, T., & James, A. (2020). Europol's crime analysis system—Practical determinants of its success. *Policing. Journal of Policy Practice*, 14(2), 469–478.

Applications of Machine Learning in Cyber Forensics

Sanchez, L., Grajeda, C., Baggili, I., & Hall, C. (2019). A practitioner survey exploring the value of forensic tools, AI, filtering, and safer presentation for investigating child sexual abuse material (CSAM). *Digital Investigation*, 29, S124–S142. doi:10.1016/j.diin.2019.04.005

Singh, J., Millard, C., Reed, C., Cobbe, J., & Crowcroft, J. (2018). Accountability in the IoT: Systems, law, and ways forward. *Computer*, 51(7), 54–65. doi:10.1109/MC.2018.3011052

Statista Research Department. (2016). *Internet of things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)*. Retrieved August 10, 2020, from <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>

Wachter, S. (2018). Normative challenges of identification in the Internet of things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review*, 34(3), 436–449. doi:10.1016/j.clsr.2018.02.002

Wang, J., & Pei, D. (2017). Kernel-based deep learning for intelligent data analysis. In *Proceedings of 2017 First International Conference on Electronics Instrumentation & Information Systems (EIIS)* (pp. 1-5). IEEE. 10.1109/EIIS.2017.8298716

Yampolskiy, R. V. (2019). Unexplainability and incomprehensibility of artificial intelligence. *Journal of Artificial Intelligence and Consciousness*, 07(02), 277–291. doi:10.1142/S2705078520500150

Zoya, K. (2020). *Digital forensics: Applications and challenges*. Retrieved June 13, 2020, from <https://legaldesire.com/digital-forensics-applications-and-challenges/4>

KEY TERMS AND DEFINITIONS

Blockchain: List of blocks distributed and linked via cryptography such as a digital ledger.

Correlation: Two variables are related when, if one variable increases, the other increases, too.

Digital Evidence: Information or data stored on devices or transmitted during the crime and acquired when electronic devices are detained and protected for investigation.

Digital Resource: It is made up of media such as images, text, video, and sound.

Internet of Things (IoT): The Internet of things (IoT) allows to transfer data between sensors and network to reach storage.

Applications of Machine Learning in Cyber Forensics

Keras API: It allows to reduce cognitive load with best practices such as deep learning.

Prediction: It is an information forecasting; it is quantitative when there is a specific condition.

Chapter 3

Machine Learning Forensics: A New Branch of Digital Forensics

Angad Gupta

3Tier R&D India Pvt Ltd, India

Ruchika Gupta

Bharat Electronics Limited, India

A. Sankaran

Manakula Vinayagar Institute of Technology, India

ABSTRACT

Machine learning (without human interference) can collect, analyze, and process data. In the case of cyber security, this technology helps to better analyze previous cyber-attacks and develop respective defense responses. This approach enables an automated cyber defense system with a minimum-skilled cyber security force. There are high expectations for machine learning (ML) in cyber security, and for good reasons. With the help of ML algorithms, we can sift through massive amounts of security events looking for anomalies, deviations from normal behavior that are often indicative of malicious activity. These findings are then presented to the analyst for review and vetting, and the results of his determination fed back into the system for training. As we process more and more data through the system, it evolves: it learns to recognize similar events and, eventually, the underlying traits of malicious behavior that we're trying to detect. This chapter explores machine learning forensics.

INTRODUCTION

DOI: 10.4018/978-1-7998-4900-1.ch003

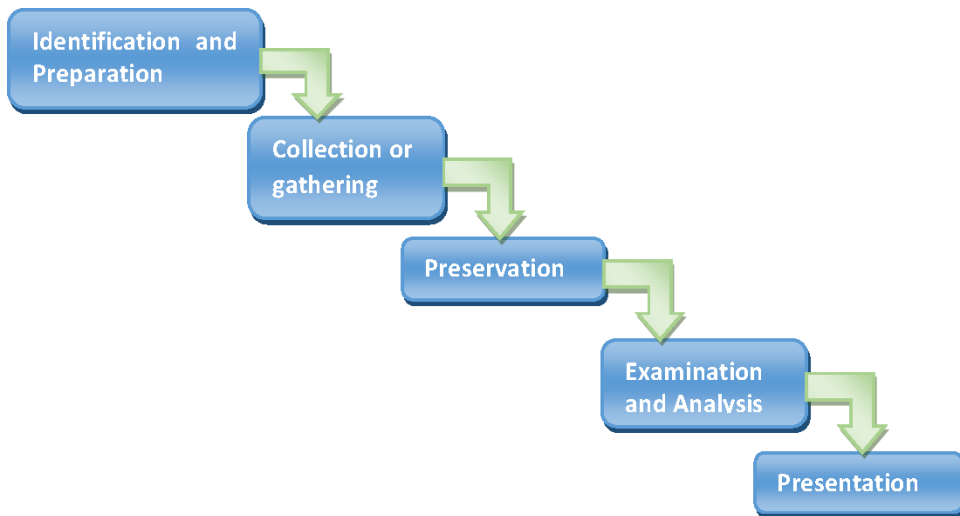
Machine learning techniques have been applied in many areas of science due to their unique properties like adaptability, scalability, and potential to rapidly adjust to new and unknown challenges. Cyber security is a fast-growing field demanding a great deal of attention because of remarkable progresses in social networks, cloud web technologies, online banking, mobile environment, smart grid, etc. Diverse machine learning methods have been successfully deployed to address such wide-ranging problems in computer security. It covers phishing detection, network intrusion detection, testing security properties of protocols, authentication with keystroke dynamics, cryptography, human interaction proofs, spam detection in social network, smart meter energy consumption profiling, and issues in security of machine learning techniques itself.

ML models have to be periodically updated to address concept drift “means change in underlying relationships and to incorporate new data points”. The frequency of updates depends on the rate of data change, the magnitude of concept drift, accuracy requirements, as well as the size of the model and your computational capacity. User behavior for example fluid and profiles have to be updated at least daily to capture new trends and reduce false positives.

Supervised models that capture analyst feedback might require even more frequent updates- preferably near real-time, to prevent the analyst from having to review many similar cases. These requirements and volume of data to be analyzed are likely to push you from the comfort zone of batch learning to streaming analytics and online learning models.

Digital Forensics Processes and Procedures

Figure 1. Digital Forensics Processes and Procedures



1. Identification and Preparation

Forensics Examiner or Investigator must have prepare before conducting case. The preparation consists of tools and equipment's for that investigation. Also they have to think in all aspects like a person, group of people “obtaining personal information which include accommodation, job and travelling records etc.” or targeting PC, laptop, note book, hand phone etc.”.

2. Collection or gathering

After target identified next to collect necessary data and information used for analysis and examination.The information collected may be from device, such as PC hard drive, USB drive etc or ongoing data from LAN or WAN in a network.

3. Preservation, Imaging and Duplication

This is for further analysis or future use if the data is affected it can be used from this session.

4. Examination and Analysis

The investigator will analyze obtained data which is used for further processing or investigation.

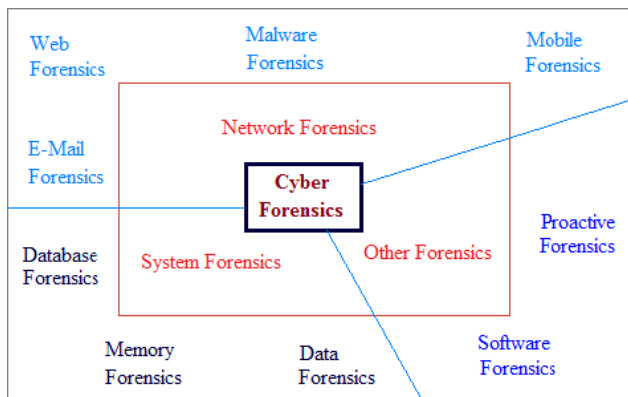
5. Presentation

This is the final stage of the digital forensics which is to be reported according to law in court. This will be readable format.

Application of Machine Learning in Cyber Forensics:

In Cyber Forensics using Machine Learning many applications are available. In that some of them are mentioned below

Figure 2. Applications of ML in Cyber Forensics



1. **Memory Forensics:** Memory forensics is a vital form of cyber investigation that allows an investigator to identify unauthorized and anomalous activity on a target computer or server. This is usually achieved by running special software that captures the current state of the system’s memory as a snapshot file also known as memory dump. This file can then be taken offsite and searched by the investigator.
2. **Email Forensics:** Email communication is also often exposed to abuse. As one of the most utilized way of online communication for both businesses and individuals, emails are amongst the critical system’s list for any organization, being used for the most simple information exchange, such as scheduling meetings, to the distribution of documents and even sensitive information.

3. **Network forensics:** Unsurprisingly refers to the investigation and analysis of all traffic going across a network suspected use in cyber crime, which say the spread of data-stealing malware or the analysis of cyber attacks.
4. **Database forensics:** Database servers store sensitive information. Database forensics refers to the branch of digital forensic science specifically related to the study of databases and the data they keep. Database forensics look at who access the database and what actions are performed. Large data security breaches are large problem and related information in search of criminal investigators.
5. **Mobile Device Forensics:** Mobile device forensics refers to that branch of digital forensics that involves evidence found on mobile devices such as personal digital assistants “PDAs”, mobile phones and any computing device with communication facility.
6. **Software Forensics:** Software forensics determines whether software has been stolen. This is performed by analyzing and comparing a source code and detecting any possible correlation. Over the past few years, software forensics has been used in several high-profile intellectual property “IP” litigations.
7. **Proactive Forensics:** Proactive Digital Forensic Component has the ability to proactively collect data, protect it, detect dubious events, gather facts, carry out the research and build a case against any questionable activities. Furthermore, an automated article is made for later use in the reactive aspect. The evidence gathered in this element is the proactive information that relates to a particular event or incident as it occurs. As opposed to the reactive aspect the collection stage in this part comes before preservation since, no event has been recognized yet. Phases under the proactive component are defined as follows:
 - I. **Proactive Collection:** Programmed live assortment of predefined data in the order of volatility and priority and related to a specific requirement of an organization or event.
 - II. **Proactive Preservation:** Computerized preservation, via hashing, of the evidence and the proactively gathered data related to the dubious event.
 - III. **Proactive Event Diagnosis:** Recognition of dubious event via an intrusion detection system or a crime-prevention alert.
 - IV. **Proactive Examination:** Automated live research of the evidence, which can use forensics techniques such as data mining and outlier recognition to subplot and construct the initial hypothesis of the occurrence.
 - V. **Report:** automated statement made from the proactive aspect analysis. This statement is also very important to the reactive part and can serve as the starting point of the reactive analysis.
8. **Reactive Digital Forensics:** It the original or post-mortem strategy of investigating an electronic crime after an incident has occurred. This calls for

identifying, conserving, collecting, inspecting, and generating the final survey.

Two types of evidence are collected under this component:

Active: Active proof refers to collecting all live “dynamic” evidence that is present after an occurrence. A good example of such information is processes working in memory space.

Reactive: Identifies collecting all the static evidence remaining, such as graphic of a hard drive.

9. **Web Forensics:** Web forensics relates to cyber-crime on the Internet. Some criminal activities like child pornography, hacking, and identity theft can be traced and the criminals can be punished if proper evidence is found against them.

Web forensic analysis is details obtained like when and what sequence the webpage was accessed. Attackers also force the browser victims by cross-site forgery for search and illegal actions. And this was accessed by inappropriate users in the system. Attack performed through internet is false URLs, malicious site redirection, web browser, database and application servers.

Memory Forensics

The two architectural features misused namely physical address layout and secure containers lead memory access to either physical memory or I/O devices. To overcome, this is not used in I/O space which is used to help CPU register to make the physical address layout to completely hide the memory. This is I/O shadowing technique to mask memory for the user to use. To step up this black box write and TLB camouflage are used to protect access memory for attackers. The second architectural feature is hardware-aided secure execution technology. More Important, hardware-enforced memory encryption in Intel secure guard extension is used in *malicious enclosed software* “*Malclaveware*” to prevent introspection and memory forensics.

- **Misusing Physical Address Layout-HIveS**

The first architectural feature we preview is the physical address layout. Physical address space on x86 platform is shared in physical memory and I/O devices. Memory used to a physical address were transverse to either the memory controller or the I/O bus were linked to location in the address space layout. This physical address layout is also used in memory forensics tools that used to understand the physical memory regions are mentioned. Memory forensic tools obtain this layout information by transferring with the operating system or BIOS, and they considered in this layout is absolute and updated. This can be violated by HIveS presenting. HIveS is used to

correct the layout machine's physical when system is operational state by verifying registers in the processor. With this control address layout difference, HIveS can prevent a memory region called HIveS memory from being seen and acquired by memory forensics tools.

The basic intelligences of HIveS is to lock memory into the I/O space, so that any performance on the physical memory address will be restored to the I/O bus alternative space of the memory controller. When the HIveS memory is locked, its memory content cannot be obtained by any processor, including the once controlled by the attacker. When the attacker wants to obtain the HIveS memory, He would first unlock the memory part by target it back into the memory address space. To protect the unlocked HIveS memory against memory forensics, we should use two novel techniques: Black box Write and TLB Camouflage. Black box enabling write allows obtaining HIveS memory creating asymmetric read / writing point within the memory and I/O space. TLB Camouflage exploits TLB which creates incoherency among multi-core processors to providing exclusive read and writes access for a single processor core to the HIveS memory.

HIveS is operating system agnostic which convert the system hardware configurations. We should make a prototype of HIveS on an x86 desktop with an AMD FX processor maintaining the both Windows and Linux. Therefore HIveS hides the malware without converting hypervisor or OS kernel, system software, including BIOS. It is randomly most developed software-based memory gaining tools on both Windows and Linux. Further, we extend HIveS with several considering anti-forensic techniques, such as RAM-less encryption and Cache-based I/O storage, to defeat hardware-based memory acquisition approaches.

- **Misusing Secure Computing-Malclaveware**

The second architectural feature is we recently widely used secure execution technology. Strong hardware-assisted execution equipments are capable of protecting applications even from the traditional highest-privilege software, the operating system. This property often used for security-critical tasks, such protection can also be mishandled by attackers to deny forensic memory acquisition.

- To demonstrate the potential threat, we used the secure enclave technology of Intel SGX in malware, and call the new family Malclaveware. Transparent, hardware-based CPU bound memory encryption of SGX is used in Malclaveware to deny forensic examiner access to plaintext memory. Using the remote attestation, the malware will execute only in the designated environment, effectively evading most of the current sandbox-based detections. Lastly, by protecting the malware execution in the secure enclave,

it would be impossible for the host-based protection to introspect the malware internals. We apply the design to ransomware and build a highly equipped ransomware prototype that exploits the protection of SGX.

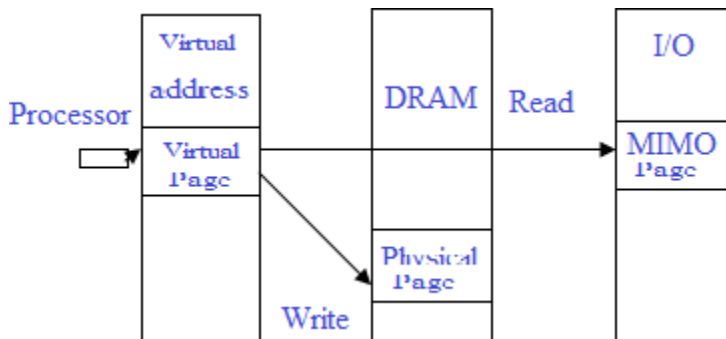
- Instead of observing only the attacks, we reflex on the root causes of nonprotected and provide discussion on the countermeasures.

We proceeding several countermeasures for detecting and mitigating HIveS and Malclaveware. One approach to see HIveS is to directly observed the CPU registers. Mainly, it remains a challenge to destory proper configurations from malicious usages. We find application whitelisting to be an mainly used step towards maintain securing container misuses. To summarize, we make the following contributions:

- We identify a general class of anti-memory-forensic technique that exploits hardware architectural features and present two attacks within the class, HIveS and Malclaveware.
- We present HIveS, an OS agnostic system that exploits hardware features on x86 platform to conceal memory in I/O space, effectively subverting the foundation of memory acquisition. We develop two novel techniques, Blockbox Write and TLB Camouflage to enable covert operations on the unlocked HIveS memory against memory forensics. A prototype of HIveS is built on the x86 platform to demonstrate its capability for concealing the HIveS memory against several of the most updated memory forensic tools on both Windows and Linux.
- We present Malclaveware, which takes advantage of hardware-assisted secure execution technology to prevent memory forensics and system introspection. We apply the concept of Malclaveware to ransomware to create a new breed of ransomware that is highly targeted and able to hide the file encryption key-even in the presence of a higher-privilege forensics subsystem. Experiments on our prototype show little performance impact.
- We provide discussion on the countermeasures and limitations of the newly presented attacks to fuel development of future system defense.

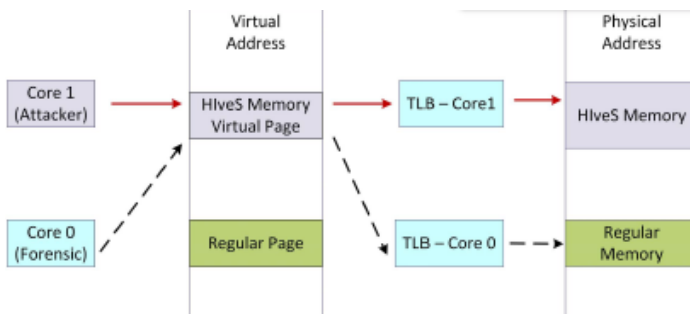
HiveS Memory Access Property

Figure 3. Blackbox write - asymmetric read/write destination for memory access.



When the HIveS memory is in the locked state by applying the I/O shadowing technique, none of processor cores can read or write the HIveS memory. Most of the time, the attacker does not need to access the HIveS memory at all, so it can lock the memory for better protection. However, the attacker has to unlock the memory eventually to access it. When the attacker only needs to write to the HIveS memory, she can use the Blackbox Write technique in Fig. 3. Moreover, if the attacker also needs to frequently read the memory content, she can use the TLB Camouflage technique. Table I shows the different access privileges to the HIveS memory for both attackers and forensic examiners when applying different antifoensic techniques.

Figure 4. TLB camouflage - core specific memory address mapping.



HIveS is operating system agnostic, so the HIveS memory can be concealed on x86 platforms for both Windows and Linux. However, we need to develop a kernel

module on Linux or a device driver on Windows with the root privilege to set the hardware registers. Contrary to current root kits that modify kernel data structures or routines in the operating system, HIveS does not leave any trace in the memory or hard disk, so it cannot be detected by checking the integrity of the OS image in the memory and the hard disk.

HIveS Extension

HIveS is mainly developed to defeat software-based memory acquisition methods that really on a trusted software module in the operating system to acquire the physical memory through the processor-to-memory path. Both I/O Shadowing and Black box Write rely on modifying the IORR registers, and TLB Camouflage creates an incoherent page translation in TLB caches of multiple processor cores. All the modifications are made on the processor, and thus only affect processing of memory requests originated from the processor. On the other hand, hardware-based memory acquisition solutions can detect HIveS, since a dedicated I/O device can capture physical memory images via direct memory access, which totally bypasses the processor hardware configurations made by HIveS. Moreover, the Cold Boot technique exploits the physical remanence property of memory chips to directly extract sensitive data from the chips. The Cold Boot technique resets the system and invalidates all configurations prior to system reset. To enhance the capability of HIveS against the hardware-based forensics tools, we propose to retrofit several existing techniques in HIveS, including IOMMU, RAM-less encryption, and Cache-based I/O storage.

- 1) **Hiding From I/O Devices:** We propose to use IOMMU to evade physical memory forensics by I/O devices via DMA. Similar to the translation from virtual memory addresses to physical memory addresses performed by the MMU, IOMMU is a hardware device that translates device DMA addresses into proper physical memory addresses. Each I/O device is assigned a protected domain with a set of I/O page tables that define the corresponding memory addresses. During a DMA transfer, the IOMMU intercepts the access message from the I/O bus and checks its cache “IOTLB” for the I/O-to-memory address translation along with the access right. IOMMU is controlled with in-memory tables and memory-mapped registers. Once a DMA request passes IOMMU, it is then processed by the northbridge. The northbridge then forwards the request either to the I/O hub or the DRAM controller base on the ranges defined by DRAM Base/Limit and MMIO Base/Limit registers. Therefore, HIveS can set the IOMMU to only allow a peripheral device to perform DMA into assigned regions, thus preventing a full system memory acquisition with

DMA. When the IOMMU is not available on some old systems, the DMA can also be redirected by manipulating the northbridge using MMIO Base/Limit registers. The main idea is to modify the MMIO Base/Limit registers to bounce DMA reads back to the I/O hub.

- 2) **Hiding From Cold Boot:** There are two solutions to evade Cold Boot-based memory acquisition mechanisms: RAM-less encryption and Cache based I/O storage. The basic idea of RAM-less encryption is to encrypt all the memory content in the HIveS memory with a secret key stored in CPU registers [30], [31]. Since operating systems do not use all the MTRR and IORR register pairs all the time, HIveS can encrypt the HIveS memory using AES and store the encryption key in unused MTRR or IORR registers. Thus, even if the physical memory is completely acquired through Cold Boot, the content of HIveS is still being protected, because the encryption key in the CPU registers is lost forever due to the system reset. The basic idea of cache-based I/O storage is to save HIveS memory only in the CPU cache [32]–[34] and then mask it with I/O Shadowing technique. When the memory address is set to cacheable in the page table entry and both RdMem and WrMem bits in the IORR base register are set to 1, any write to that location will trigger a cache line fill if the memory content is not yet loaded in the cache. When the HIveS system is unlocked, the attacker can simply write data into memory, as usual. When the HIveS system is locked, the HIveS memory is cached and masked by I/O shadowing. Therefore, neither I/O devices nor the processor can read out the HIveS memory in the cache. It will maintain the content in the cache considering the limited cache control.

Email Forensics

Email Access Protocols

Email offers the exchange of electronically stored messages by using the Internet. There are two standard methods that can be employed to transmit emails namely, the web-based standard and client-server based standard. The email communication, messages are encoded in ASCII format and non-textfiles such as sound and images can be attached and transmitted in binary streams format. Application protocols developed for email includes Internet Message Access Protocol “IMAP”, Simple Mail Transfer Protocol “SMTP”, Post Office Protocol “POP”, UNIX-to-UNIX Copy Protocol “UUCP”, and Mail Transfer Protocol “MTP” [5]. However, these protocols were developed in the late 1980s and some are considered obsolete. Currently, the most common protocols in use for sending and receiving emails are the SMTP, POP and, IMAP. Below we highlight prominent email access protocols in use today. This

includes the SMTP, POP, and IMAP. Whereas the SMTP is used to send emails from client to the server the other two protocols are used to retrieve emails from the server to the client.

Evidence Gathering

Email forensic is the emerging area of study in the digital forensic discipline. The process of collecting digital evidence by using forensic tools and forensically sound methodology is very fundamental in the digital forensic discipline. As email moves from one server to another server over the Internet it adds information of the servers it passes through to the email header. Notwithstanding the possibility of being forged, the email header is still very potential to email investigators because it provides credible information. Therefore, in order to investigate and prove the authenticity of the disputed email, an investigator needs to collect the email header of the disputed email and the mail server log form the mail servers involved in transmitting the email. In order to collect email header and email server logs, the investigator can use subpoenas depending on the legal requirement. Furthermore,

an investigator needs to get images of all computers of the accused and the victim for investigation purpose. Moreover, the image of the email server and its back-up should also be acquired. Investigator can collect email header from the disputed email directly. Evidence gathering tools are available in numbers, some are freely available while others are for sale. Common digital forensic evidence acquisition tools are En Case Forensic, X-Ways Forensics and Access Data Forensic Tool Kit“FTK”.

1. Email Data Collection

The email data collection stage includes collecting email data of suspicious email ids. We collect email data from several mail clients. As standardization of different mail storage file format and protocols becomes common among nations, it becomes simpler to collect email data from several mail clients. We must separate out every single email from one email account. Thus, we can collect all the user message data.

2. Attribute identification

From each email, we can extract certain attributes necessary for email forensics. Common attributes include from address, to address, cc, subject, received, date, etc. From these attributes, we can identify the relationship between several email accounts. Also, a large amount of evidences can be concluded from this.

3. Network Graph generation

From the data and attributes that have been collected, we can create network communication graph. Nodes in the graph represent email accounts and edges between them represent the relationship or communication between them. The from address and the to address acts as the two endpoints of the edge. The value of corresponding edge is the number of emails between from address and to address.

From this email communication network graph, we can further study the criminal organizations and their core members.

4. Traffic filtering

After creating network graph, we apply filtering on the resultant graph. For traffic filtering, we use the weight of each edge. Based on the applications and criminal cases, we set a threshold value. If the value of an edge is higher than the threshold value, it indicates that the relationship between those two accounts is close. If the value of the threshold is less than the specified threshold, we delete those edges. After filtering, we get some nodes and edges from the initial network graph. This may form into several clusters.

5. Email Header Analysis

Following evidence gathering the immediate actions to be taken by the investigator is to analyze the email header in order to ascertain if the email spoofed. Currently, the SMTP is the rudimentary protocol for transmitting emails from one device to another device. However, it is important to note that every line of the email's header can be forged. The received lines found in the email header provide details of the servers that the email passed through as it moves from the sender to the receiver. Therefore, this field should be analyzed carefully in order to determine if the email is genuine or not. Thus, when reading email header only the received line of the device you trust should be considered trustworthy. The common received line in the email header provides information in the following format:

- “i” receiver's device name and IP address
- “ii” sender's device name and IP address
- “iii” message ID and
- “iv” date and time.

However, each SMTP server adds the received line in a different way. The investigator needs to acquaint with the different formats in order to conduct email header analysis more efficiently. In practice as email moves from one server to another, the SMTP adds the new received line to the email header. The correct way to interpret

the received lines in the email header is to read them from the bottom to the top. The topmost received line is added to the email header by the email recipient's server.

6. Email Server Logs Analysis

Email server logs analysis can be yield credible results in email forensic, in particular when the email header has been compromised. The acquisition of email server logs may require issuing a subpoena to the service provider. However, this is limited by the data retention policy of the company. Usually, service providers store data for short time to avoid storage cost. In practice, email servers store email logs based on email accounts, IP address from which they are sent, date and time. Therefore, the investigator should pay attention to these details during email server logs analysis. Moreover, during email server analysis it is important to keep in mind the clock drift in order achieve desired results. A comparison of details obtained from email header analysis and details found on the email server can substantiate the credibility of the email. This includes comparing details such as message ID, received and transmitted time. For client-server based application, many servers keep copies of emails.

7. Analysis of local device

The devices of the victim or the suspect can be a source of potential evidence of email related crimes and disputes. The image of these devices should be taken for further investigation in case other means fail to prove the genuine sender of the email. In this case, the image of the devices should be taken and further analysis should be conducted on the image. Observe that in order to retain the integrity of the evidence, image acquisition and analysis should be conducted using forensic tools and forensically sound methodologies. In this context, forensic image acquisition tools such as EnCaseForensic, and Access Data's Forensic Tool Kit“FTK” can be used. During analysis of local device's image, the investigator should focus on analyzing the browsing history and saved emails.

Network Forensics

The idea of network forensics deals with the data found across a network connection mostly incoming and outgoing traffic within the host in the Network. Network forensics analyzes the traffic data logged through firewalls or IDS or at network devices like routers. The goal is to trace the source of the attack so that the cyber criminals are prosecuted.

Machine Learning Forensics

Network forensics is defined as *“The use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities”*. Network investigation includes the reformation and analysis of data from computer networks associated with having been alternated or got to in an unauthorized manner. Its purpose is to permit specialists to reason about the circumstances or reasons for the activity under investigation and to give proof in front of court of law.

Network forensics comprehends:

Detecting, acknowledge and allotting responsibility for attacks against our frameworks.

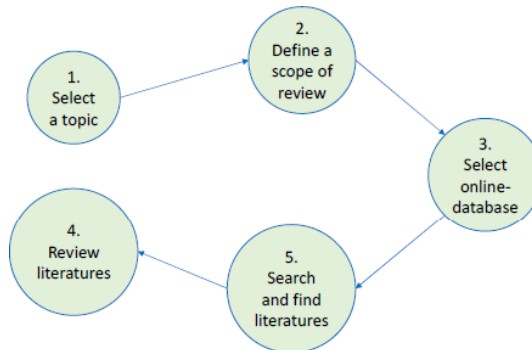
The utilization of security gadgets and their review data for evidentiary information. Using networks for static information gathering during the investigation. Usually, network forensic investigations will utilize event log investigations and outline to determine the following:

- Who: is to blame for the action?
- What: has the attacker done.
- When: each event happened.
- Where: identify the location or host that the attack took place from.
- Why: why did the crime happened, what were their motives of culprit.
- How: which source were used, or vulnerabilities abused. With numerous unlawful activities including network advances, these sorts of investigations are developing in number and structure imperative component computer forensics.

Database Forensics

It consists of five stages:

Figure 5. Stages of Database Forensics



The topic selection process initiated by seeking questions relating to this topic or what background is related to this topic. For this we use randomized query planning “RQP” algorithm which search by random related query used for searching. There are two fundamental questions that become the reference of this research that is; what database forensic and how-to analysis database is forensic. At this stage of decide on the scope of your review, we will search related some phrases to find a collection of libraries related to DFA. There are two methods used in the Phrase used by using without quotation marks between phrases and using quotation marks between phrases. Phrases used in this search contents: Database Forensic Analysis; Carving Database; Forensic Database.

The process use RQP for select databases to conduct searches that occurs at this current stage is to select a search database that will be used to gather the data in accordance with the phrase that has been determined in the previous stage. The database search on both sources consists of two methods i.e. without the use of quotation marks and using quotes. This will categorize the search results by source and extract data from each selected article. This stage we called conducts searches and find literature. The final stage is previewing the literature. At this stage, the discussion related data that has been obtained by title and year on each article. The methods or techniques used for the DFA process found in the article’s discussion are the results of an analysis to discover new methods that address the purpose of this article.

Mobile Device Forensics

Modern phone is like a minicomputer. This implies the need for an OS, which is suitable for portability demands. Mobile phones that deploy an open source OS enable their users to freely customize them. Such a feature makes these OSs

incredibly attractive to many smartphone vendors. Android is the most popular open source mobile OS. Android OS accounts for 84.8% of the smartphone market share. Therefore, in this review, the discussion is restricted to the influential studies on Android OS forensics.

Lee et al. proposed the implementation of onsite Android smartphone forensics based on the regulations set by the National Institute of Standards and Technology “NIST”. A tool, with some useful capabilities, was created in this study for Android-based mobile phone forensics. The implemented tool was developed by Java and it could assist in capturing any potential evidence in a timing manner. The developed tool offered a list of useful elementary digital forensics capabilities including the available information on SIM card number, SIM manufacturer, SIM card status, as well as capturing logs of browsers, calls, available SMSs and contacts. The study is considered one of the initiatives in the field of Android forensics, and the provided features could improve the digital forensics procedure, considering the possibility of not having the required forensic tools onsite, and the drainage of the phone battery. However, a very elementary design testing, which can never be considered sufficient, was only provided in this study. In addition, the developed tool did not exactly consider the presentation of evidence, which is a major challenge for any forensic analysis tool.

In the same year, 2009, Lessard and Kessler deployed an HTC Hero smartphone for Android forensics purpose. In their study, they mainly focused on testing several memory imaging and data analysis tools to classify their outcomes. For device imaging, the AccessData Forensic Tool Kit “FTK” Imager version 2.5.1 was used. In addition, FTK for data examination was used, where Access Data FTK version 1.81 was deployed for this purpose. Moreover, CelleBrite was used in analyzing the same captured memory images for further classification. The logical examination was not employed in this study to produce better outcomes as the results obtained from FTK were not sufficient. The main study results show that conducting Android forensics using FTK could recover some of the deleted messages, contacts and easy passwords. However, the main problem with FTK was the required time, which was very long. Apart from FTK, the conducted logical analysis could recover much more than what was recovered by FTK. In fact, it could recover nearly everything that matters for Android forensics including browsing history, emails, voicemails, and different types of messages, images and various passwords. However, the main disadvantage of logical analysis is the necessity for the root access, which is, as mentioned earlier, a source of trouble for mobile device forensics.

Finally, their experiment with CelleBrite could recover different types of messages, video, ontacts, call logs and photos. However, this was done directly using logical extraction without the need for imaging. In addition, the used tool could not recover especially important information relevant to emails and browsing history. One of

the early books of Android forensics published in 2011 was written by Hoog. This book is an extremely useful reference in mobile forensics, especially for Android forensics. Hoog's book offers a wide range of topics covering both software and hardware sides of smartphones that operate on Android. The main advantage of Hoog's book is being, up to the author's knowledge, the first milestone in the field of Android forensics. This reference addressed critical issues such as setting up the hardware to bind by digital forensics rules, suggesting techniques for bypassing locking up passwords and leveraging switched-off phones.

Further, the author presented a detailed explanation for the possible phone isolation ways, ensuring that the phone is not connected to any network during the forensic process. In addition, Hoog suggested the concepts of modern applicable acquisition categorization, i.e. logical and physical acquisitions, which have been adopted ever since. He also provided a detailed description of physical acquisition techniques, which are still popular until today, such as the deployment of Joint Test Action Group "JTAG" and physical extraction. In addition, he described possible ways for forensically examining micro SDs and similar memory attachments. Maus et al. proposed a complete implementation of their approach, which is called Android Forensic Toolkit. The developed tool was installed and tested in an HTC Desire phone with Android version 2.2 OS. Another advantage presented in this study is that it was possible using the standard map services, such as Google Maps, and with a proper Application Programming Interface "API" to present the acquired data in the form of an approximated map route of the mobile phone. Nevertheless, the presented approach can be faced by two main challenges: ensuring that the GPS is kept on as well as gaining the required permissions. These two setbacks can possibly jeopardize any attempt for using the tool in any mobile forensics' procedure.

CONCLUSION

"Data is the new oil" for this modern and adventures world, we are growing in terms of the data points and data centers day by day. In the same fashion we also growing with many advancement techniques in the forensic science. More the advancement and more the risk involved all the work, to cover up all the risk we need the modern and latest models/data techniques to handle all these issues. Here is the machine learning is played the important role in the forensic science in the various field. Some of the useful techniques and fields are discussed above in the chapter. Now a days in this modern world without data science and machine learning techniques to control and established the controlled measured instruments are exceedingly difficult. Email/Mobile/network forensic are playing the important role to make the

life measurable and secure. Machine learning highly recommended into the forensic science with the variety of the advantages.

REFERENCES

- Al-Dhaqm, A., Razak, S., Othman, S. H., Ngadi, A., Ahmed, M. N., & Mohammed, A. A. (2017). Development and validation of a database forensic metamodel “DBFM”. *PLoS One*, 12(2), e0170793. doi:10.1371/journal.pone.0170793 PMID:28146585
- Appavu, S., Rajaram, R., Muthupandian, M., Athiappan, G., & Kashmcera, K. S. (2009, July). Data mining based intelligent analysis of threatening email. *Knowledge-Based Systems*, 22(5), 392–393. doi:10.1016/j.knosys.2009.02.002
- González-López, J., Ventura, S., & Cano, A. (n.d.). Distributed selection of continuous features in utilabelclassi_cation using mutual information. *IEEE Trans. Neural Netw. Learn. Syst.* Available: <https://ieeexplore.ieee.org/document/8877992>
- Hauger, W. K., & Olivier, M. S. (2015). The state of database forensic research. *2015 Information Security for South Africa ISSA 2015 Conf.* 10.1109/ISSA.2015.7335071
- Kim, S., & Kim, H. (2016). A new metric of absolute percentage error for intermittent demand forecasts. *Int. J. Forecasting*, 32(3), 669-679. Available: <https://linkinghub.elsevier.com/retrieve/pii/S0169207016000121>
- Ali, K. M. (2012). Digital Forensics Best Practices and Managerial Implications. *Fourth International Conference on Computational Intelligence, Communication Systems and Networks*, 196-199. 10.1109/CICSyN.2012.44
- Labiche, Y., Kolbah, B., & Mehrfard, H. (2013). Combining Static and Dynamic Analyses to Reverse- Engineer Scenario Diagrams. *IEEE Int. Conf. Softw. Maintenance*, 10.
- Nemetz, S., Schmitt, S., & Freiling, F. (2018). A standardized corpus for SQLite database forensics. *Digital Investigation*, 24(Supplement), S121–S130. doi:10.1016/j.diin.2018.01.015
- Peyre, G. (2019). *Mathematical Foundations of Data Sciences*. CNRS and DMA, Ecole Normale Supérieure. Available: <https://mathematical-tours.github.io>
- Hadjidj, R., Debbabi, M., Lounis, H., Iqbal, F., Szporer, A., & Benredjem, D. (2009, March). Towards an integrated e-mail forensic analysis framework. *Digital Investigation*, 5(3-4), 124–137. doi:10.1016/j.diin.2009.01.004

Wang, L., Zhang, R., & Zhang, S. (1892). A Model of Computer Live Forensics based on Physical Memory Analysis. *Proceedings of 1st International Conference on Information Science*.
J. Clerk Maxwell, *A Treatise on Electricity and Magnetism*, 68–73.

Chapter 4

Crucial Role of Data Analytics in the Prevention and Detection of Cyber Security Attacks


Charulatha B. S.

*Rajalakshmi Engineering College,
India*

Shanthi K.

*Dr. M. G. R. Engineering College,
India*

A. Neela Madheswari

 <https://orcid.org/0000-0001-8213-7155>

Mahendra Engineering College, India

Chamundeswari Arumugam

*Sri Sivasubramaniya Nadar College of
Engineering, India*

ABSTRACT

Data analytics plays a major role in retrieving relevant information in addition to avoiding unwanted data, missed values, good visualization and interpretation, decision making in any business, or social needs. Many organizations are affected by cyber-attacks in their business at a greater frequency when they get exposure to the internet. Cyber-attacks are plenty, and tracking them is really difficult work. The entry of cyber-attack may be through different events in the business process. Detecting the attack is laborious and collecting the data is still a hard task. The detection of the source of attack for the various events in the business process as well as the tracking the corresponding data needs an investigation procedure. This chapter concentrates on applying machine learning algorithms to study the user behavior in the process to detect network anomalies. The data from KDD'99 data set is collected and analyzed using decision tree, isolation forest, bagging classifier, and Adaboost classifier algorithms.

DOI: 10.4018/978-1-7998-4900-1.ch004

INTRODUCTION

Data Analysis can be applied in many disciplines of data mining, cyber security to study the behavior of data for anomaly detection. In anomaly detection a profile of the normal data is developed and then data that does not agree with it as an anomaly (Dimitar et al., 2017). Broadly speaking, dataset used in various analyses can be split into two subdomains, inliers and outliers, in which the outlier's data behaves abnormally (Fabrizio et al., 2016). Using the outlier's data, it is possible to detect the anomalous behavior at a certain point of time in an application. Outlier detection can belong to three families, namely supervised, semi-supervised, and unsupervised. Mostly the outlier dataset is analyzed using the unsupervised methods based on statistical, deviation, distance based, density based, angle based, isolation based, concept based, cluster size/density based, etc.

The application where the data behave anomalously can be fields of Data mining (Zhangyu Cheng, 2019), sensor technology (Yu HsuanKuo et al., 2018), Cyber-attack (Simon D.Duque Anton et al., 2019) (Filipe Falcão et al., 2019), HTTP/HTTPS protocol (Hieu Mac et al., 2018) (Ya-Lin Zhang et al., 2018), weather data (Tadesse Zemicheal et al., 2019) Network Intrusion Detection System (Zouhair Chiba et al., 2019) etc. Normally, outlier detection methods can detect the outliers accurately. In many cases, they end up with non-outliers as outliers and outliers as non-outliers. So a biased method will do this task well efficiently to detect the anomalous behavior of the data.

The main idea behind the work is to do the network traffic analysis. Using this analysis, the network administrator can have a watch on the traffic pattern to identify anomalous traffic. In order to have familiarity with the analysis, historical data is used to develop mathematical model. For the development of the model the data set available from Kaggle is used which is freely available to the public.

The objective of this paper is to detect network based anomalies using the publicly available dataset. All the parameters are cautiously considered and class required for this analysis is tracked. The training and testing data splitting was conveniently decided in applying the decision tree, random forest and bagging classifier algorithms. Python is used in this research work to detect the network anomalies and accuracy was also evaluated. The contribution that was emphasized in this chapter is as follows:

- To detect network-based anomaly detection systems
- Apply the decision tree, isolation forest, random forest, Ada Boost and bagging classifier on data set
- Study the performance accuracy of these methods in detecting the anomalies

The organization of the paper is as follows. Background Section details the literature survey and the Intrusion Detection Section discusses the anomaly detection used in this paper. The methods used for analysis are decision trees, random forest, isolation forest, bagging classifier, and Ada Boost classifier are discussed. The Methodology section details the applicability of the unsupervised anomaly detection algorithm used in this work, and the results obtained by applying these methods using the dataset KDD'99. Conclusion section provides the summary of the work done and future work of this proposed chapter.

BACKGROUND

(Zhangyu Cheng et al, 2019) applied anomaly detection methods to detect the local and global outliers using Isolation forest and local outlier factor with low complexity to prune the data set. Also applied ensemble method to improve pruning accuracy and improve the outlier detection rate. (Yu-HsuanKuo et al, 2018) proposed a regression model to fit the sensor data to detect the outliers using contextual outlier detection methods. (Filipe Falcão et al, 2019) used 12 types of detection methods that belong to a family of algorithms for the dataset that is prone to system and network intrusion detection. (Hieu et al, 2018) targeting the web attack of SQL Injection, Cross-site Scripting(XSS), XPath Injection, Local File Inclusion(LFI), Server-side Template Injection, Code Injection, OS command Injection, Server side Request Forgery, and Others. They analyzed and detected malicious patterns in the HTTP/HTTPS requests using regularized deep autoencoders. (Ya-Lin et al, 2018) proposed the Anomaly Detection with partial Observed Anomalies using the three methods, isolation forest unsupervised method, support vector machine supervised method, and the cost sensitive strategy PU learning based method on the different datasets. Also the problem of malicious URL detection was also demonstrated.

(Tadesse et al, 2019) used benchmark weather data sets to handle the missing values by applying the five strategies of mean imputation, MAP imputation, reduction, marginalization, and proportional distribution with IF, LODA and EGMM unsupervised anomaly detection algorithms. (Simon et al, 2019) adapted the three algorithms, one class support vector machines, Isolation Forests and time series Matrix Profiles algorithms to detect the process behavior in industrial enterprise dataset. Out of which Matrix profile was able to detect the attack that occurs multiple times. (Dimitar NikolaevKarev et al, 2017) used unsupervised machine learning algorithm Isolation Forests to identify intrusion models using HTTP log data. (Qing et al, 2018) applied anomaly detection in spatio-temporal data to investigate multiple types of traffic data. (Xing Yang et al, 2019) applied a density-based local outlier

factory detection algorithm to determine the outlier in network flow data streams, and also used the LSTM model for prediction.

(Timofey et al, 2018) used code vector representation to detect the kotlin code fragments in the programming language community that is available in the GitHub repository. In this analysis, Local Outlier Factor, Isolation Forest, and Autoencoder neural network methods were used to detect the code anomalies. (Zouhair Chiba et al, 2019) combined the suricata signature based detection and anomaly detection isolation forest methods in Network Intrusion Detection System to detect and protect from intruder's network attacks in the network environment by monitoring network traffic. (Degang et al, 2019) studied the anomaly detection of abnormal signals in wireless devices based on four dataset using isolation forest algorithm.

OUTLIER ALGORITHMS USED FOR ANOMALY DETECTION

This section provides the significance of outlier methods in cyber security related applications, intrusion detection systems. As per Hawkins, Outlier is an observation which deviates so much from the other observations as to arouse suspicions that it was generated by a different mechanism (Hawkins, 1980). There are a lot of areas in which these kinds of outliers exist or are created and the need of study arises. For example, The birth of a child to Mrs.Hadlum happened 349 days after Mr.Hadlum left for military service. Average human gestation period is only 280 days. Here 349 days is observed which is an outlier (Barnett, 1978). Some of the sample applications of outlier detection are in Health Care, Finance Domain, Sports arena etc.

Outlier detection distinguishes outlier data from normal data using either: abnormality detection which compares new data to a model of normality or outlier classification which classifies new data as either normal or abnormal. Outlier detection can also use time-series or sequence analysis to detect changes in temporal patterns (John Wang, 2014).

INTRUSION DETECTION

An intrusion is a series of activities in computer network systems that compromise security of the system. An intrusion can be an external attack or internal misuse of the system. An intrusion can compromise confidentiality, integrity, availability and also other security aspects in various ways (Xiangyang, 2003).

The classifier will consume time to detect intrusion and this in turn will have impact on the accuracy. (Kajal Rai et al, 2016). Accuracy and time estimate are considered as a major factor to evaluate the intrusion detection algorithms. Accuracy

can be defined as the number of correct predictions. It can be computed as shown in Equation(1)

$$\frac{(TP + TN)}{(TP + TN + FP + FN)} \quad (1)$$

Where TP is True Positive, TN is True Negative, FP is False Positive and FN is False Negative

METHODOLOGY

Decision trees can detect the malicious activities for a large set of data as they provide rules that can be understood easily. (Kajal Rai et al, 2016). Random forest classifier is very effective in classifying the attack since it is an ensemble algorithm. (Nabila Farnaaz and M A Jabbar, 2016).

Few data points will be identified as anomalies which is susceptible to a process called isolation. Isolation forest detects anomalies by following the process of isolation differs basically from other methods of anomaly or intrusion detection (Fei, T. L, 2008).

Neural network, rule learning, statistical models and ensemble methods are some machine learning algorithms to detect intrusion. Ensemble methods performs well during training process. One advantage of bagging classifier is that it takes less time to build the model and provides low false positives when compared with algorithms of similar kind. (Gaikwad, et al, 2015). Detections of false positives and the minimization of the false negatives can be achieved using AdaBoost (ArifYulianto, et al, 2019). Due to these various advantages of machine learning algorithms, the following is applied in this proposed work: i) Decision tree, ii) Random forest, iii) Isolation forest, iv) Bagging classifier, and v) Adaboost classifier.

Data Set

For the study the data set is taken from Kaggle repository. The URL of the data source is present in the reference. The data has 42 columns and 125974 rows. 100,780 records are used to train the model and the remaining 25194 used for testing the models. The 41 fields are attributes and the 42nd field is the class label normal, dos, probe etc. The preprocessing is a pre requisite for the machine learning algorithms. The machine learning data set should be tuned to suit our needs. This is done by preprocessing.

Preprocessing

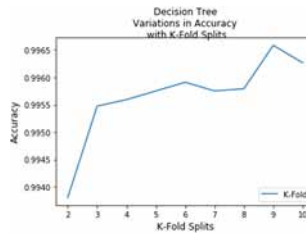
The categorical data are converted to discrete values. The data is normalized using min max normalization. The attributes of the data set are like that of Duration, Protocol, Type of service, Source Bytes, Destination Bytes, Type of the message, Login details, Login type owner or guest, Error rates, Type of attack. Using the above data set the algorithms are analyzed.

- i) **Decision tree:** A decision tree is represented by a tree like graph having nodes and edges. The root and the intermittent nodes represent the test attribute and the leaf represents the class label. (Kajal Rai et al, 2016). Decision tree is the well-known classification method for data mining. The reasons for it are: i) Decision tree is very fast to train and test the data, ii) Its results are very easy to understand for human operators and visualize, iii) Its results are used to mine rules (Atilla Ozgur et al., 2012).

In proposed decision tree the target variable is the class label which indicates the type of attack. The predictor variables used in the study to name a few are protocol, type of service, length of the data etc. During training, the decision tree technique partitions examples of data records in the training data recursively until a stopping criterion is met. After each partition, the set of training examples falling in a branch of the decision tree has less loss inconsistency with respect to the target class. A typical stopping criterion for not further partitioning a branch is that all the examples are of the same target class, and the branch becomes a leaf in the decision tree.

The structure of a decision tree shows the correspondence between the predictor variables and the target variable for the proposed problem. The decision tree divides the problem space into a number of sub-regions with all the training examples in one sub-region having the same target value. The sub-regions can then be used to classify the target value of real test data. Each path from the root node of a decision tree to a leaf node of the decision tree represents a pattern of the predictor variables or a sub-region that is useful in predicting the value of the target variable (Xiangyang, 2001). The accuracy is estimated and is given in Figure 1. The average accuracy score is calculated as 0.9956.

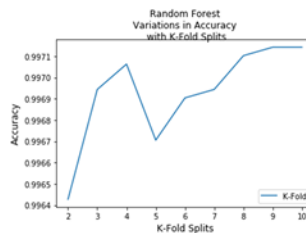
Figure 1. Accuracy using Decision Tree K-fold splits whereas K=10



- ii) **Random Forest:** Random forest method is used for prediction type of problems. The performance in Random forests is high due to ensemble. The ensemble is achieved with a set of decision trees that are generated using subspaces of data selected randomly. Let D be a training dataset in an M -dimensional space X , and Y be the class feature with a total number of c distinct classes. The method for building a random forest follows the steps as taken from (Bharathidason, 2014)

The accuracy is estimated and is given in Figure 2.

Figure 2. Accuracy using Random Forest with K-fold splits where as K=10



- iii) **Isolation forest:** The Isolation forest also belongs to the family of ensemble learning algorithm. The algorithm builds a group of isolation trees using a recursive and randomized tree partitioning procedure. An isolation tree belongs to a family of binary tree. The trees represent a nested collection of partitions of the finite dimensional feature space, grown iteratively in a top-down fashion, where the cuts are axis perpendicular and random (Guillaume Staerman, 2019). Isolation forest has high degree of adaptability and highly efficient. Due to these merits it can be used in parallel computing algorithms. Due to these merits it is very helpful in detecting the anomalies. (Sahand Hariri

et al, 2019). In Isolation forest the observations are selected by the random selection of features. The algorithm uses the split value used to split the tree. The split value is selected between the two extremes of the selected feature. The number of splits depends upon the path length from the root to the leaf (Fei, T. L, 2008), (Fei, T.L, 2012). The maximum depth for the tree is varied and for each varied value, accuracy is calculated and is given in Figure 3. Also by varying the number of trees, accuracy is calculated and is given in Figure 4.

Figure 3. Accuracy in Isolation Forest by varying Number of Trees

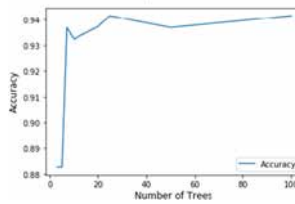
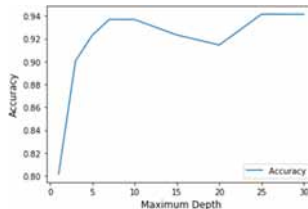


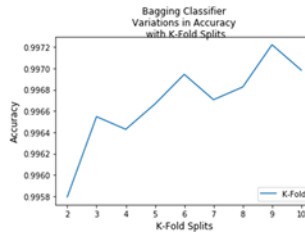
Figure 4. Accuracy in Isolation Forest by varying Maximum Depth



- iv) **Bagging classifier:** Bagging gets its name from Bootstrap Aggregating. This method follows ensemble learning. The underlying principle of bagging is to create different classifier and to ensemble them parallel. This method also distributes the training data randomly among the classifiers (Xiao-Dong et al, 2010). The accuracy is estimated and is given in Figure 5.

Crucial Role of Data Analytics in the Prevention and Detection of Cyber Security Attacks

Figure 5. Accuracy using Bagging classifier with K-fold splits where as K=10



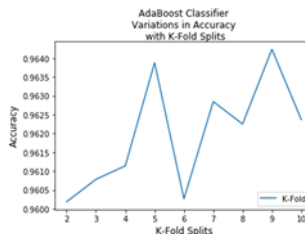
- v) **Ada Boost Classifier:** The aim of Ada Boost is to improve the accuracy of the classification by combining several weak learning algorithms. The training is done to each weak learning algorithm using a set of training data. The training is done by adjusting the weights of all the samples iteratively. Let us consider N training samples $X = \{(X_1, Y_1), (X_2, Y_2), \dots, (X_N, Y_N)\}$ where X_i denote the i^{th} sample and Y_i the class label for the sample can be -1 or +1. Initializations are done to the parameters, the number of iterations, the weak classifier count, weights of the data instance (Freund et al, 1999).

The Ada Boost algorithm has the following main steps:

- Step 1: Sampling step:** In this step, some samples (D_t) are selected from the training set, where D_t is the set of samples in the iteration t .
- Step 2: Training step:** In this step, different classifiers are trained using D_t , and the error rates (ϵ_t) for each classifier are calculated.
- Step 3: Combination step:** Here all trained models are combined.

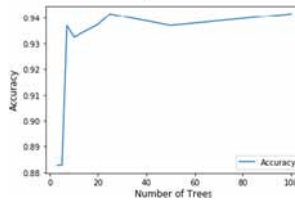
The accuracy is estimated and is given in Figure 6. The average accuracy score is 0.9619.

Figure 6. Accuracy using Ada Boost Classifier with K-fold splits whereas K=10



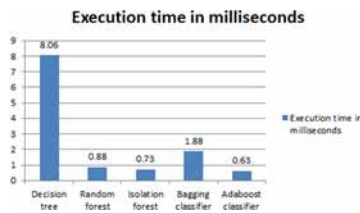
Crucial Role of Data Analytics in the Prevention and Detection of Cyber Security Attacks

Figure 7. Accuracy using Ada Boost Classifier when the trees are varied



The execution time for finding accuracy is given in Figure 8 for various algorithms.

Figure 8 Execution time of the various algorithms in millisecond



Accuracy for each of the algorithms as per above analysis are summarized and presented in Table 1.

Table 1. Accuracy values by applying confusion Matrix

Algorithm	Accuracy in %
Decision tree	33
Random forest	100
Bagging classifier	100
Adaboost classifier	67
Isolation Forest	100

As per figure 8, execution time for each of the algorithms in seconds are presented in Table 2.

Table 2. Execution time estimates

Algorithm	Execution time in seconds
Decision tree	0.00806
Random forest	0.00088
Isolation forest	0.00073
Bagging classifier	0.00188
Adaboost classifier	0.00063

The contribution of this work is as follows.

- Decision tree, random forest, isolation forest, bagging classifier, Ada Boost was applied to detect the network based anomalies.
- Applied decision tree, the split of training and testing aided to know that the class distribution was true. Since it is large set of data, 10-fold cross validation was used to reduce the overfitting. Prediction accuracy obtained is 33%.
- Isolation forest was applied to identify the anomalies by locating the split point in the data distribution. Prediction accuracy calculated by varying number of Trees and maximum depth is 94%.
- Bagging classifier with 10 fold splits was used to reduce the overfitting and error. Prediction accuracy obtained with 10-fold split is 99.72%
- Ada Boost classifier was used to tally the prediction made from decision tree to decide on the final classification. Prediction accuracy computed with 10-fold split and varied trees is 99%
- Detection was effective to identify the anomalies in the data set.
- 7.Mitigation in detecting network based anomalies

Using the mathematical equation of the models derived, one can do proactive analysis. One can apply the real time traffic data to the model classify whether this data will be classified as attack or not. If the data traffic details end up in classifying as attack then the network administrator can block the traffic from the IP address or the protocol used, setup a firewall to avoid attack. Hence such analysis will help to analyze the traffic and derive a conclusion based upon the outcome of the models

CONCLUSION

Three records are taken as a sample for testing the model generated using the various classifiers. The same three records are subjected to each of the models. When comparing the accuracy value of each algorithm, it was observed that decision tree needs more training to increase the accuracy level. Ensemble methods of learning give better performance. In the case of the decision tree the result indicates that the training is to be increased to improve the performance. In this data set Ada Boost classifier is performing to a lesser extent. When comparing the execution time for different algorithms, it is clearly seen that Ada Boost classifier performs better than other algorithms.

FUTURE RESEARCH DIRECTIONS

To evaluate the performance of intrusion detection, some of the metrics like F1 score, precision, recall can also be studied further. Various other machine learning algorithms can also be implemented and be studied for intrusion detection. The results discussed made use of the open data set available but to check with realistic data from a live website will be still interesting.

REFERENCES

- Atilla O., Hamit, E. (2012). *An Application of Decision Trees in Intrusion Detection*. Academic Press.
- Barnett, V. (1978). The study of outliers: Purpose and model. *Applied Statistics*, 27(3), 242–250.
- Bharathidason & Venkataeswaran. (2014). Improving Classification Accuracy based on Random Forest Model with Uncorrelated High Performing Trees. *International Journal of Computers and Applications*, 101(13).
- Degang, S., Yulan, H., Zhixin, S., Guokun, X., & Wei, Z. (2019). An Efficient Anomaly Detection Framework for Electromagnetic Streaming Data. *ACMICBDC*, 151-155.
- Dimitar, N. K., Christopher, M., & Ruslan, V. (2017). Cyber Threat Hunting Through the use of an isolation Forest. *International Conference on Computer Systems and Technologies, ACM CompSys*, 163-170.

Crucial Role of Data Analytics in the Prevention and Detection of Cyber Security Attacks

Fabrizio, A., Fabio, F. (2016). Toward Generalizing the Unification with Statistical Outliers: The Gradient Outlier Factor Measure. *ACM Transactions on Knowledge Discovery from Data*, 10(3), 1–26.

Farnaaz & Jabbar. (2016). Random Forest Modeling for Network Intrusion Detection System. *Procedia Computer Science*, 89(213-217).

Fei, T. L., Kai, M. T., & Zhi-Hua, Z. (2008). Isolation Forest. *Eighth IEEE International Conference on Data Mining*, 413–422.

Fei, T. L., Kai, M. T., & Zhi-Hua, Z. (2012). Isolation-based Anomaly Detection. *ACM Transactions on Knowledge Discovery from Data*, 3, 1–39.

Filipe, F., Tommaso, Z., Caio, B. V. S., & Anderson, S. (2019). Quantitative comparison of unsupervised anomaly detection algorithms for intrusion detection. *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, 318–327.

Freund, Schapire, & Abe. (1999). A short introduction to Boosting. *Jinkō Chinō Gakkaishi*, 14, 771–780.

Gaikwad, D. P., & Ravindra, C. (2015). Intrusion Detection System using Bagging Ensemble method of Machine Learning. *Proceedings of the International Conference on Computing Communication Control and Automation*, 291-295. 10.1109/ICCUBEA.2015.61

Hawkins, D. (1980). *Identification of Outliers*. Chapman and Hall.

Hieu, M., Dung, T., Lam, N., Hoa, H. N., Hai, A. T., & Duc, T. (2018). Detecting Attacks on Web Applications using Autoencoder. *Proceedings of the Ninth International Symposium on Information and Communication Technology*, 416–421.

John, W. (2014). *Encyclopedia of Business Analytics and Optimization*. IGI Global Publication.

Li, X., & Ye, N. (2001). Decision tree classifiers for computer intrusion detection. *Parallel and Distributed Computing Practices*, 4(2), 179–190.

Qing, W., Weifeng, L., & Bowen, D. (2018). Spatio-temporal Anomaly Detection in Traffic Data. *Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control*, 46, 1–5.

Rai, K., Devi, M. S., & Guleria, A. (2016). Decision tree based Algorithm for Intrusion Detection. *International Journal of Advanced Networking and Applications*, 7(4), 2828–2834.

Simon, D. D. A., Anna, P. L., Christoph, G., & Hans, D. S. (2019). Security in Process: Detecting Attacks in Industrial Process Data. *Proceedings of the Third Central European Cybersecurity Conference*, 5, 1–6.

- Staerman, G., & Forest, F. I. (2019). Article. *Proceedings of Machine Learning Research*, 101, 332–347.
- Tadesse, Z., & Thomas, G. D. (2019). Anomaly detection in the presence of missing values for weather data quality control. *Proceedings of the 2nd ACM SIGCAS Conference on Computing and Sustainable Societies*, 65–73.
- Timofey, B., Victor, P., Kirill, S., Nikita, P. (2018). Detecting anomalies in Kotlin code. *Companion Proceedings for the ISSTA/ECOOP 2018 Workshops*, 10–12.
- Train_data.csv. (n.d.). <https://www.kaggle.com/what0919/intrusion-detection/>
- Xiangyang, L., Nong, Y. (2003). Decision tree classifiers for computer intrusion detection. *Real-Time System Security*, 77–93.
- Xing, Y., Wenli, Z., Nanfei, S., & Hao, Z. (2019). A Fast and Efficient Local Outlier Detection in Data Streams. *Proceedings of the 2019 International Conference on Image, Video and Signal Processing*, 111–116.
- Ya-Lin, Z., Longfei, L., Jun, Z., Xiaolong, L., & Zhi-Hua, Z. (2018). Anomaly Detection with Partially Observed Anomalies. *Companion Proceedings of the The Web Conference*, 639–646.
- Yu-Hsuan, K., Zhenhui, L., & Daniel, K. (2018). Detecting Outliers in Data with Correlated Measures. *Proceedings of the 27th ACM International Conference on Information and Knowledge Management*, 287–296.
- Yulianto, Sukarno, & Suwastika. (2019). Improving AdaBoost-based Intrusion Detection System (IDS) Performance on CIC IDS 2017 Dataset. *Proceedings of the 2nd International Conference on Data and Information Science, Journal of Physics*, 1192.
- Zeng, X.-D., Chao, S., & Wong, F. (2010). Optimization of Bagging Classifiers based on SBCB Algorithm, *Proceedings of the Ninth International Conference on Machine Learning and Cybernetics*.
- Zhangyu, C., Chengming, Z., & Jianwei, D. (2019). Outlier detection using isolation forest and local outlier factor. *Proceedings of the Conference on Research in Adaptive and Convergent Systems*, 161–168.
- Zouhair, C., Noreddine, A., Khalid, M., Amina, E. O., & Mohamed, R. (2019). Newest collaborative and hybrid network intrusion detection framework based on suricata and isolation forest algorithm. *Proceedings of the 4th International Conference on Smart City Applications*, 77, 1–11.

Chapter 5

Deep Learning Approaches to Overcome Challenges in Forensics

Kiruthigha M.

Anna University, Chennai, India

Senthil Velan S.

Amity University, Dubai, UAE

ABSTRACT

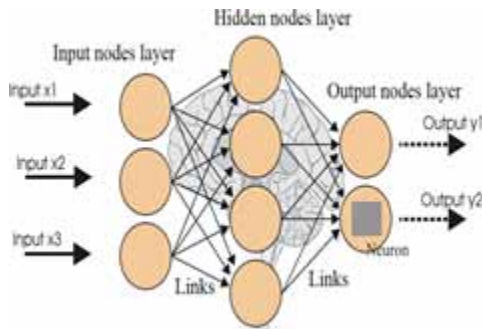
Cyber forensics deals with collecting, extracting, analysing, and finally reporting the evidence of a crime. Typically investigating a crime takes time. Involving deep learning methods in cyber forensics can speed up the investigation procedure. Deep learning incorporates areas like image classification, morphing, and behaviour analysis. Forensics happens where data is. People share their activities, pictures, videos, and locations visited on the readily available platform, social media. An abundance of information available on social networking platforms renders them a favourite of cybercriminals. Compromising a profile, a hacker can gain access, modify, and use its data for various activities. Unscrupulous activities on such platforms include stalking, bullying, defamation, circulation of illegal or pornographic material, etc. Social network forensics is more than the application of computer investigation and analysis techniques, such as collecting information from online sources. CNNs and autoencoders can learn and obtain features from an image.

DOI: 10.4018/978-1-7998-4900-1.ch005

INTRODUCTION TO DEEP LEARNING:

Deep learning is a part of machine learning technique that enables the computer to learn by example. Deep learning consists of Artificial Neural network (ANN). ANN consists of layers of nodes as how a human brain has. Each node in a layer is connected to the adjacent layer. Signals are transmitted between nodes as they are between neurons in brain and corresponding weights are assigned. A heavier weighted node will contribute more effect on the next layer. System that learns through deep learning will be in similar to how a toddler does. Each learning model applies non-linear transformation to its input and uses the learning to build a statistical output. The learning is iterated until a level of accuracy is reached. The term deep represents the number of layers the input has to pass through.

Figure 1. Artificial Neural Networks



DEEP LEARNING MODELS

Deep learning algorithms perform self-learning representations. In training process, they use unknown input distributions to learn features, group them and find some useful pattern. No single architecture is perfect, they work better for specific tasks. Deep learning models can be classified as supervised (CNN, RNN) and Supervised (AE, RBM, GAN).

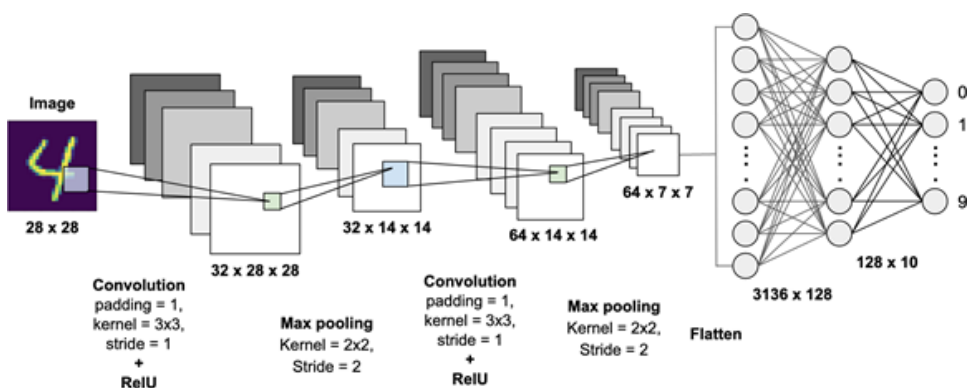
CONVOLUTIONAL NEURAL NETWORKS (CNN)

CNN has proven its efficiency in image classification and processing. Though ideal for image data, works better for non-image data too. CNN can be explained in four steps

Deep Learning Approaches to Overcome Challenges in Forensics

1. Convolution: It helps with feature detection with the help of kernels (filters). Feature Maps are created
2. Apply the ReLu (Rectified Linear Unit): increase the non-linearity of the image
3. Pooling: Helps CNN to detect features in various images irrespective of lighting, position, angle etc. Max pooling helps to preserve important features of the image.
4. Flattening: Feature map matrix is flattened to single column and fed to neural network

Figure 2. Convolutional Neural Networks



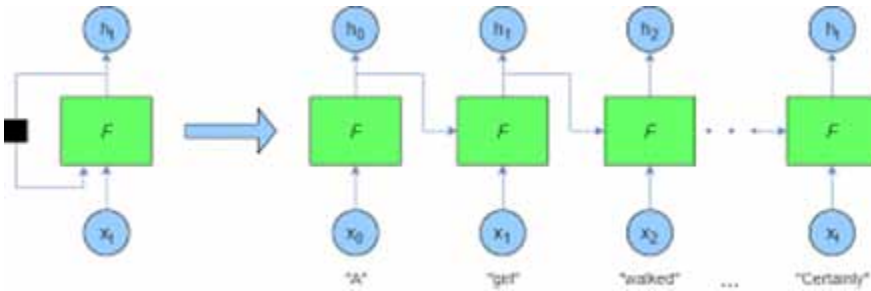
RECURRENT NEURAL NETWORKS (RNN)

In RNN nodes are connected to form a directed graph along temporal sequence. RNN has memory which remembers all things calculated. It remembers every information through time. This feature makes RNN efficient in time series prediction. RNN are also called LSTM (Long Short Term Memory)

How a RNN works:

1. A single temporal input is provided
2. Calculate current state using current input and previous state
3. It can be iterated through any number of time steps
4. Once all time steps are over, current state is used to calculate output

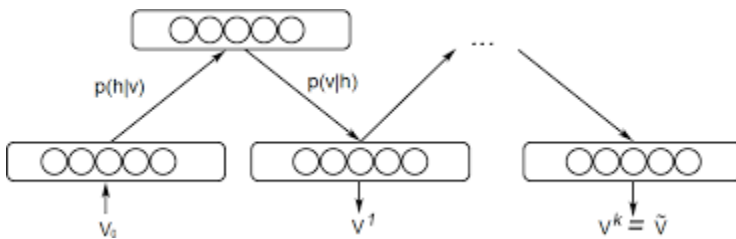
Figure 3. Recurrent Neural Networks



BOLTZMANN MACHINE (BM)

Boltzmann Machine are stochastic deep learning models which consist of only hidden and visible nodes. They don't contain output node. The input nodes activate certain nodes in hidden layer. The activated nodes in the hidden layer reconstruct the hidden nodes. Boltzmann machine are generative models. They produce activation of hidden nodes in the forward pass and in the backward pass they perform reconstruction of input.

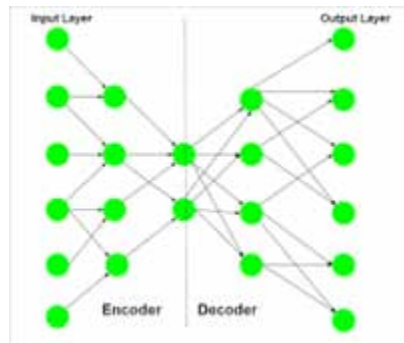
Figure 4. Boltzmann Machine



AUTO ENCODERS (AE)

Auto encoders work by encoding the input data, then performing activation function and finally decoding the data for output. Auto encoders are generative networks that learn the features themselves and extract the important features. They are used in dimensionality reduction.

Figure 5. Auto Encoders



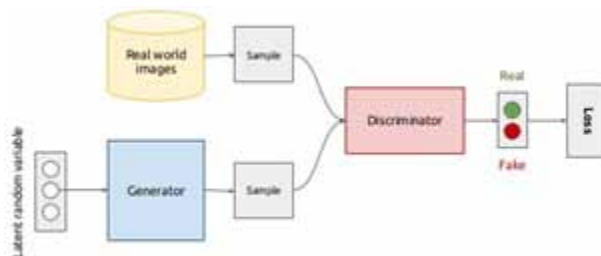
GENERATIVE ADVERSARIAL NETWORKS (GAN)

GANs are generative modelling that involves two tasks

1. Generator: Generate new examples
2. Discriminator: Discriminate example either true or fake

GANs are exciting with their ability to generate new examples in any problem domain that are realistic.

Figure 6. Generative Adversarial Networks



DEEP LEARNING AND CYBER FORENSICS

Cyber forensics is a sub domain of cyber security that uses software tools to investigate various components of the system. It requires analysis of large amount of data to provide evidence of a crime. Cyber security professionals need to examine large and complex pool of data to disclose Potential Digital Evidence (PDE) used to support

lawsuit. This could not be achieved manually as it might lead to errors (Tan and Yu, 2017). Here comes the use of Deep learning techniques which could analyse and identify data about the attack. Deep learning techniques have proven to deliver accurate results by their computational capabilities. Various techniques like Auto encoders, Boltzmann machines and Convolutional neural networks have been good in learning data. Deep learning provides better processing capabilities with large amount of data which makes it better computational technique for cyber forensics. Deep learning techniques can be used to mine visual patterns from large datasets.

Digital forensics becomes more crucial when it comes to issues about: Author of documents (characteristics such as age, identity, gender etc) and their motive behind the unauthorised evidence. The Digital Forensic Research Workshop (DFRWS) has defined digital forensics (DF) as “The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations”. The challenge falls on how to recover the digital evidences that are of interest to the investigator. It is quite tedious for the forensic experts to perform data analysis and cross check each machine’s data individually.

CHILD PORNOGRAPHY

The evolution of internet has facilitated distributing contents faster through anonymous file sharing services and cryptographic services which makes it difficult to identify the content and its author. Though digital era has made our lives easier, but it also fuelled a prodigious surge in online abuse of children. Social media has been the other mode of distribution among groups or individuals. Though we would refuse “I haven’t seen any such image” does not mean it’s not available. Facebook has declared that they have removed 8.7 million pieces of content that violates child nudity or exploitation of children. With the help of AI and Machine learning 99% of contents were removed before anyone reported it (Mirjalili and Ross, 2017). WhatsApp has flagged off millions of accounts that shared child pornographic contents. Though the contents cannot be decoded they were identified using their profile pictures or group profile information.

An ensemble of CNN’s can be used in classifying whether an image in pornographic or not. They can be further used in face detection and age estimation (G. Wang et al., 2019). Though skin exposure alone cannot be a factor since most of videos of sumo players, swimming etc. have exposed skin. So deep learning models are trained

in identifying important features in video like difference in age group, position of child, etc.

CYBER STALKING AND BULLYING

Cyber stalking is repeated use of digital communication to annoy or threaten an individual or a group by continuous posting of the off topic, unflattering and unwanted comments on social network, email or chat room. Cyber bullying is harassment when both culprit and the victim are adolescent. Cyber bullying is becoming a significant issue in social networking. Cyber stalking or cyber bullying can lead to sexual harassment, hostile environment, or suicidal ideation. Cyber stalking or cyber bullying is a repetitive activity over time rather than once. It is often discussed as a persistent and repetitive activity. Cyber stalking is often personalised. Bare words highly intentional provides fear and trauma only to victim. Most social platforms teenagers use have safety centres like YouTube safety centre.

Deep learning models like Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), Bidirectional LSTM (BLSTM) and Attention Network model can be used in detection of Cyber bullying. CNN's can be used for image and text classification and sentiment analysis. LSTM is used in determining long term dependencies for text classification. BLSTM for bidirectional purpose and BLSTM with attention, for identifying temporal dependencies (D. Halpern et al., 2017). Pronunciation based CNN's (PCNN) are used in correcting the spelling errors that do not alter the pronunciation, thus making detection of cyber bullying easier.

In a survey by anti-bullying charity, it was found that more than 40% of 10,000 UK youth aged between 12 to 25 found Instagram as most bullied platform, where 37% by Facebook and 9% by Twitter. Facebook has incorporated a Deep Neural network called DeepText since 2016. DeepText works as how human perceive a word's meaning context. DeepText uses deep learning algorithms for text classification and for understanding slang and word-sense ambiguity. Deep Text has a state of art understanding of human language as it understands intent, entities and sentiments. It sifts through thousands of post to estimate its user and provide a personalised experience. DeepText uses BRNN to capture context dependencies through recurrence and semantic dependencies through convolution. Instagram has also started using DeepText to block offensive comments.

Twitter uses IBM Watson to detect text containing harassment before it is reported. IBM Watson uses cognitive computing platform to find abusive words in the language. User who is found bullying in twitter will lose some of his privileges.

FACE SPOOFING

Face spoofing is cheating a face recognition using a substitute like photo video recording or 3D mask. If the attack succeeds, the attacker gains access rights of authorised person. Deep learning models using CNNs lack in extracting features from image and live face, when various filters are applied we may lose information like edges, texture etc. This makes CNN difficult to classify between live and spoof faces. One improvement could be adding temporal features like blinking of eye or movement of lips and mouth. This works better for paper images, but if the attacker replays a captured video, then the problem still sustains. Remote photoplethysmography (rPPG) a technique to track signals like heart rate without contact with human skin can be a good choice. rPPG signals are used to detect 3D mask attacks. Now CNN combined with RNN can be used in detecting face spoofs.

FAKE FACE

Face swapping is replacing face of one person with the other in a photo or video without affecting the realism. Deep learning models like Generative Adversarial Networks (GAN) help in wrong hand for this purpose. This technology helped attackers creating pornographic or sexually compromising videos of innocent victims and circulate in social media (Liu et al., 2017). Many digital forensic tools fail to detect them as they are progressively built as a single image.

FAKE NEWS

Perceiving news from social media is double edged sword. On one side it is easily accessible, socially relevant, and easily conveyable and see from different perspectives. But on the other side they are easy to manipulate based on interest or opinion (Kai Shu et al., 2019). It is specifically a manipulated news spread in social media to degrade a person or organisation. Detection of fake news can be anyone of the following methods

1. **Content Based:** Rely on text content to identify truthfulness of the message. Various text characteristics like TF-IDF, topic features, language styles, writing styles, consistency, social emotions etc. (uses RNN)
2. **User Based:** Model traits of users who respond to the news. They extract user account information's like gender, hometown, and number of followers. (CRNN -CNN combined with RNN)

3. Structure Based: Supports propagation structure in social media. Implicit information's like hashtags and URL to communicate information to users who does not own a social media account. This information can improve the performance of rumour identification (graph based NN)

CREDIT CARD FRAUD

Cashless transactions like digital banking, credit card, debit card, online payment is becoming more popular today as well as fraudulent activities. Credit card fraud happens when an unauthorised person uses credit card or account details for unauthorised purpose or fund transfer. Fraud can be identified by the deviation in spending behaviour of customer. Fraud detection is essential for the banks as fraudulent activities may lead to incline in the reputation of the banks. Identity theft includes use of name, account details, card no etc to use card accounts. Credit card fraud can happen anytime even card is safe with us.

Employing auto encoders in fraud detection can help a lot with dimensionality reduction. They use only important features to detect a fraudulent activity. Any abnormality in behaviour can lead to high reconstruction error. Restricted Boltzmann Machine, Deep Belief networks can also be used for fraud detection. Deep Belief Network is a series of RBM's.

PHISHING

Phishing is a cybercrime in which victims are reached through mail, text messages or telephone by offender who enacts as a legitimate person to cajole sensitive data like account details, passwords etc.

E-mails act as main form of communication from banks regarding account details, login details and credit reports. Phishing emails or messages may lead the customer to click on a link that leads them to a webpage where they provide their details. A massive phishing attack happened in 2017 where a hacker gained access of millions of Gmail user's mail history. Anti-phishing aims in detecting phishing contents from text messages.

Machine learning algorithm normally use key features of a mail to identify whether it is phishing or not. But using deep learning we could detail the structure of mail to classify it. We could use functional words and subject line. Deep learning models like RNN and Auto encoders can help in finding salient features to classify an email efficiently. The spread of phishing is not an end with email and sms. To the development of digital world phishing happens even through QR code, spear

phishing, spoof mobile apps, URL etc. Some attacks are even held on websites that possess HTTPS and SSL certificates. Deep learning models including CNN to extract local features of URL and LSTM to extract context semantic features for better classification of URL (Jeeva and Rajsingh, 2017). Deep Boltzmann machines can also be used in collecting features from phishing URL which could be used in further recommendations.

MALWARE

Malware is a malicious software used to invade secured information's from the system. To protect legible users, many organisations use signature-based malware detection methods. But due to advancement of technology the attackers evade them easily by polymorphism and obfuscation. Machine learning algorithms like decision trees, KNN, Naive Bayes and SVM can be used in malware detection through extracted features. But they under perform in identifying behaviour features of malware (Sun et al., 2017). Deep learning has the ability of feature learning through multi-layer deep architecture, it is possible to learn higher conceptual features based on local feature representations (Alhanahnah et al., 2018). Behaviour based deep learning models along with machine learning algorithms can work better. When it comes to learning features, it is auto encoders or RBM in the scene.

The actions in behaviour-based malware detection considers only security-oriented operations. Operating system related operations include more effectiveness to detection system. Monitoring API and their corresponding parameters to find malicious behaviour identifies hostile attacks (Sharmeen et al., 2018). Stacked Auto encoders can be used to identify one hot feature for every API call. SAEs follow a greedy layer wise unsupervised learning and supervised parameter fine tuning. To the end of SAEs we could add classifiers for detecting malicious activity.

DDoS

Distributed denial of service is a form of denial of service attack, where attackers use multiple distributed resource to launch a DoS attack. It results in unavailability of network services by flooding the servers with undesirable traffic. DDoS attacks are of three types: Volumetric (catch the bandwidth of the server), Protocol based (capture the resources of the target server) and Application level (using application level vulnerabilities to crash the target). Convolutional systems monitor the system and identify attacks based on statistical divergence. The deep learning model should be capable of learning patterns from sequence of network traffic and trace attack

activities (Han et al., 2017). Deep learning models like Boltzmann machine and Auto encoders can be used to perform feature extraction through unsupervised learning. Boltzmann machine has proved to provide better accuracy in Intrusion Detection Systems. Multi-channel CNNs used as CNNs that have higher classification performance.

REFERENCES

- Alhanahnah, M., Lin, Q., Yan, Q., Zhang, N., & Chen, Z. (2018). Efficient signature generation for classifying cross-architecture IoT malware. *Proceedings of the 6th IEEE Conference on Communications and Network Security*. 10.1109/CNS.2018.8433203
- Halpern, D., Piña, M., & Vásquez, J. (2017). Loneliness, personal and social well-being: towards a conceptualization of the effects of cyberbullying/Soledad, bienestar social e individual: hacia una conceptualización de los efectos del cyberbullying. *Cult. y Educ.*, 29(4), 703–727. doi:10.1080/11356405.2017.1370818
- Han, Y. H., Yuan, X., Li, C., & Li, X. (2017). DeepDefense: Identifying DDoS Attack via Deep Learning. *IEEE International Conference on Smart Computing (SMARTCOMP) IEEE*, 1-8.
- Jeeva, S. C., & Rajsingh, E. B. (2017). Phishing URL detection-based feature selection to classifiers. *Int. J. Electron. Secur. Digit. Forensics.*, 9(2), 116–131. doi:10.1504/IJESDF.2017.083979
- Liu, Y., Jourabloo, A., Ren, W., & Liu, X. (2017). *Dense face alignment*. ICCVW. doi:10.1109/ICCVW.2017.190
- Mirjalili, V., & Ross, A. (2017). *Soft biometric privacy: Retaining biometric utility of face images while perturbing gender*. ICB.
- Sharmeen, S., Huda, S., Abawajy, J. H., Ismail, W. N., & Hassan, M. M. (2018). Malware threats and detection for industrial mobile IoT networks. *IEEE Access: Practical Innovations, Open Solutions*, 6, 15941–15957. doi:10.1109/ACCESS.2018.2815660
- Shu, Zhou, Wang, Zafarani, & Liu. (2019). *The role of user profile for fake news detection*. CoRR, abs/1904.13355
- Shu, K., Cui, L., & Wang, S. (2019). defend: Explainable fake news detection. *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, KDD*, 395–405.

Sun, H., Wang, X., Buyya, R., & Su, J. (2017). CloudEyes: Cloud based malware detection with reversible sketch for resource constrained internet of things (IoT) devices. *Software, Practice & Experience*, 47(3), 421–441. doi:10.1002/pe.2420


Tan, X., & Yu, H. (2017). Effective small interfering RNA design based on convolutional neural network. *IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, 16-21.

Wang, G., Li, W., Aertsen, M., Deprest, J., Ourselin, S., & Vercauteren, T. (2019). Aleatoric uncertainty estimation with test-time augmentation for medical image segmentation with convolutional neural networks. *Neurocomputing*, 338, 34–45. doi:10.1016/j.neucom.2019.01.103 PMID:31595105

Chapter 6


Deep Learning–Based Malware Detection and Classification

Mirnalinee T. T.

 <https://orcid.org/0000-0001-6403-3520>

Sri Sivasubramaniya Nadar College of Engineering, India

Bhuvana J.

 <https://orcid.org/0000-0002-9328-6989>

Sri Sivasubramaniya Nadar College of Engineering, India

Arul Thileeban S.

Sri Sivasubramaniya Nadar College of Engineering, India

Daniel Jeswin Nallathambi

Sri Sivasubramaniya Nadar College of Engineering, India

Anirudh Muthukumar

Sri Sivasubramaniya Nadar College of Engineering, India

ABSTRACT

Malware analysis is an important aspect of cyber security and is a key component in securing systems from attackers. New malware signatures are being created continuously and detection techniques need to keep pace with them. The primary objective is to propose a solution which detects malicious files in real time by evaluating each file. Other objectives are to assess the threat level of the malware and recognize the family of malicious file. Hence, to cover all the needs and to fulfill the motivation, a deep neural network is more suitable to detect and classify the malware. Convolutional neural network-based system MalNet-D is designed to detect the presence of malware, and subsequently, to classify the detected malware into the family in which it belongs, a variation of MalNet-D termed as MalNet-C is proposed. Images of the executable files, both malignant and benign, are used as input data, which is trained by the respective MalNet. This is used to detect and classify malware into families. The system achieved 93% accuracy in malware detection and 96% accuracy in malware classification.

DOI: 10.4018/978-1-7998-4900-1.ch006

INTRODUCTION

Malware analysis is an important aspect of cyber security and is a key component in securing systems from attackers. Attacks are directed in form of malware as attack vectors. They are primarily in executable formats bound to benign exe files to fool people. In this case, a separate malware analysis tool is required to detect the malwares. Typically, Antivirus software are used for detection of malwares. Behind the screen, analysis is done by antivirus establishments and the virus signatures are uploaded into database from which detection is done. There are two major methods available namely static and dynamic analysis, both consume time and not feasible to be done in real time. Static analysis evaluates the code piece by piece for viral signatures. Dynamic analysis is typically done by running the executable in sandbox and detecting viral nature if any.

Malware is a software which purposefully damage the computer resources and takes the form of executable code. Such codes are referred to as virus, worms, Trojans, etc. Malware's intent is to act against the computer user but not by exploiting some deficiency in the system. Major business faces a loss of \$12 million, annually due to the virus attacks revealed by an FBI survey (Computer crime, 2013). The role of antivirus software is to detect and eliminate the viruses in computer software and hence it is called so. During 2009, a survey by Symantec stated that 80% of home user had installed antivirus software though most of them had not used the antivirus software for protecting their system (Internet Security, 2013).

In a world where effects of malware infection are fatal, real time analysis is needed to block them before they spread like "WannaCry" did. Beyond the monetary losses, this also helps to invade privacy, a skeptical key point with many users. Added to these defects, there is loss of data which is highly critical for major operations. These major issues clearly serve as motivation for real time detection of malware. With the current available tools, they don't seem feasible due to the latency involved with detection by anti-virus software.

New malware signatures are being created continuously and detection techniques need to keep pace with them. The nature of malware analysis has been typically passive. In passive analysis the analyst analyses executable files by running a traceback on the operations executed in them. This is tedious and time consuming in nature. Such methods cannot be used to detect malware or infected files in real time. Detecting and blocking malware in real time greatly increases defense mechanisms against new types of malware created each year. Panda Labs annual report for the year 2017 suggests that over 15 million of the malware files that were seen that year were infected with newly created malware (PandaLabs, 2017). Moreover, these statistics were gathered only for clients serviced by Panda Labs. Therefore, to combat the proliferation of malware there is a need to analyze and identify them in real time.

Our primary objective is to propose a solution which detects malicious files in real time by evaluating each file. Beyond this, we also want to classify the type of malware family the malicious file belongs with, to assess the threat level of the malware. Hence, to cover all the needs and to fulfil the motivation, a deep neural network is more suitable to detect and classify the malware. we propose a solution using deep learning networks for detection of malware in real time. This work proposes the usage of a Convolutional Neural Network to perform this analysis of malware. We utilize images of files, both malign and benign as input data which is trained on a Convolutional Neural Network (CNN) where it is used to both detect and classify malware into families.

The proposed system of malware detection takes as input an executable file and performs binary classification to predict whether the executable is a malware or not. Hence the input dataset consists of both malware executables and benign executables. These input executables are fed to 8-bit encoding module which converts the executable files into grayscale images of high dimensions.

After this, the generated grayscale image is passed through a bilinear interpolation module for down sampling its size. This module also makes sure all the images are of fixed sizes before being fed into convolutional neural networks as input tensors. The output of this module would be binary classification to predict whether the input executable file is a malware or benign file. For malware classification the input undergoes similar pre-processing steps before they are fed to CNN as input tensors for training. CNN will now predict the malware family to which the file belongs to through multi-class classification. The observed results shown that the deep neural network is more appropriate to analyze the malware.

BACKGROUND

Malware

The program or software that are malicious and harmful to a computer will be a malware whose intentions will be stealing, monitoring, manipulating sensitive information available in the system. system is affected by malware through internet whenever the user visits a malicious website or through downloads, USB drives, emails, etc., to spread their malicious code to infect the devices. Once the system is infected with malware, then nowadays with sophisticated attacks continue to communicate with the system, also monitors and extracts sensitive information from the system. New strains of malware often try to fool both the users and also the antimalware programs most often by using web proxies for these evasive actions. Some of the new malware behaviors include changing forms and only residing in system's RAM

in order to get avoided from detection by signature-based mechanisms and from being exposed. Various categories of malware reported in the community were:

Virus: Program that copies itself and cause adverse effect by corrupting, deleting the files and are usually look like executable files.

Trojans: This kind of malware disguises itself as legitimate software, and make backdoors through which the other malicious software may enter.

Spyware: As the name suggests they spy for passwords, user's surfing nature, etc., by hiding behind at the background.

Worms: These programs will contaminate the entire devices in network locally or in the whole network through the network interfaces. Each infected system will in turn infect other connected systems.

Ransomware: This is otherwise referred as scareware which may stop the operation of the infected system and will threaten to delete all information available in the system unless a ransom is paid.

Adware: These are not most harmful in nature nevertheless they will be more aggressive in advertising and may weaken the security of the system.

Botnets: It's the cluster of infected systems that are still under the control of the attacker. Malware are evolving day by day, making the process tedious to protect our data. Clop is one of the most dangerous recent ransoms which is a variant of CryptoMix ransomware, Raas which is Ransomware as a Service is also growing threat that hires professional hackers to implement the attack. Zeus Gameover is a sort of Trojan malware that masquerades itself that cannot be traced because it by passes centralized servers (Safety Detectives, 2020).

Cryptojacking malwares are used to mine cryptocurrencies, the impact of these have seen a rise since the cost of cryptocurrencies tend to increase over years.

Malware Analysis

Malware analysis is done to determine the behavior, intent of the malware, to assess the extent of damage caused. Malware Analysis can be either static or dynamic. Static analysis is done without executing the code and by analyzing the signature of the binary file. Signature is generated by the applying cryptographic hash on the file in order to understand the components of file. Advanced approaches will apply reverse engineering on the malware binary converting them into assembly code to understand the nature of it.

Dynamic analysis is done by allowing the infected system to run in a controlled and isolated setup to perceive the nature of the damage inflicted. Acquisition of the memory and analyzing are the steps involved in the dynamic analysis of malware.

Deep Learning for Classification

The most commonly used deep learning architecture is the convolutional neural network (CNN, or ConvNet) used for analyzing images. CNN architecture requires no or minimum pre-processing which is one of space invariant artificial neural networks (SIANN) and known for sharing the weights and invariant to translations. CNN is a network inspired by biological processes that divides the image into several receptive fields and applies the filters over them to extract features automatically. CNN find its applications in several fields such as natural language processing, recommender systems, video recognition, image analysis, image classification, object detection, segmentation, face recognition, Self-driving cars that use CNN based vision systems, classification of crystal structures etc. Any CNN architectures is a layered architecture with three basic components Convolutional layer, pooling layer and Fully Connected Layer.

Convolutional layers apply convolution operation over the receptive fields of the image and passes the extracted features to the next layer in the architecture. Convolutional networks may have local or global pooling layers, that are used to reduce the quantum of trainable parameters. Most commonly used pooling are average and max which takes the average or maximum value of features extracted by the previous convolutional layer. The fully connected layer will have connections with every other neuron and the final layer will have the number of node equivalent to the number of classes in the classification problem. The loss function in this layer will compute the error in the prediction of classes. This will get back propagated in order to update the weights and biases to optimize the loss.

State of Art Malware Detection technologies

Malware is a program whose intentions are to perform unauthorized access to data present in the system without the knowledge of system administrator (Sikorski et al., 2012). This will help the attacker

With simpler words malware is a software that helps an attacker complete and fulfills his malicious and crime intentions.

Malware detection and classification has been categorized as static and dynamic, authors (Sikorski et al., 2012) state that, static analysis report whether a file is malicious or not based on few signatures, whereas dynamic analysis check the behavior during run time, processes of the system and erase the infection as well.

Before looking into the prior research work let's see the classification of malware analysis techniques. The malware analysis techniques can be widely classified into two categories:

- **Analysis using dynamic methods:** In dynamic malware analysis the suspicious software is made to run in a safe environment usually referred to as a sandbox to study the intention of the software (Bailey et al., 2007). This process will help in investigating the behavior of the software and its attributes can be analyzed. Dynamic analysis provides a deeper insight on the behavior of the software such that one could observe how it will behave when it is made to run in the actual system. There are few tools such as Process Monitor, Process Explorer are available for this purpose.
- **Analysis using static methods:** Static analysis involves the probing the executable files instead of the instructions made up the executables. This is like identifying any patterns and studying their behavior (Liu et al., 2011). The intends and capabilities are analyzed in static methods (AV-test, 2014). Following are few of the types of static malware analysis techniques for detection:
 1. Machine code can be disassembled into assembly level instructions in order to learn the intentions.
 2. Antivirus can be used to detect the presence of malware.
 3. Hash of the suspicious malware can be computed and can be treated as a fingerprint for analysis
 4. The output of the software can be examined for any pattern of strings
 5. The file format can be investigated for its rationale and intention.

Due to the availability of huge malware samples, researchers focused on automatic classification techniques for malware detection. Also unsupervised learning techniques such as clustering is employed for malware detection, by grouping the unusual information as an outlier. In 2014 Microsoft recorded and registered in its database more than 236 malware families. Machine learning algorithms were explored in detail by the research community in detecting and identifying the malware. Authors (Rad et al., 2018) used Artificial Neural Network to detect the presence of malware in an unseen file as a binary classifier with a good performance (Rad et al., 2018). Kwon et al. (2018) also addressed the same issue of detecting malware using learning-based approach. They have evaluated their approach with only 220 samples with dynamic behavior. To effectively apply any supervised learning for detecting the presence of malware huge samples are required.

95% of detection was achieved through a deep learning-based malware detection in (Saxe et al., 2015) with a 0.1% false positive rate. This was observed over a dataset of 400,000 instances of software binaries.

Mohaisen et al. (2015) proposed a system AMAL(AutoMal), an automated and behavior-based malware analysis and labeling system. This system could able to collect behavioral artifacts, then extract features for building classifiers. For

certain families of malware this system is performing well. Kinable et al. (2011) explored various clustering algorithms for grouping the similar behavior patterns as clusters. Identifying number of clusters is a major issue in detecting the families of malware. Need a good learning model to represent the exact features to identify the presence of malware along with the detection of the families of malware. Thus, deep learning-based framework is proposed in this research to improve the performance in detecting malware. Rieck et al. (2008) proposed a combination of both supervised and unsupervised learning method to identify the malware category based on the behavior.

Explored deep learning framework for detecting the presence of malware and classification (Marín et al., 2019), compared with conventional machine learning methods. However, for certain category of malware their framework reported very low accuracy. Kolosnjaji et al. (2016) explored the potential of deep learning in detecting malware. Convolutional neural Network along with LSTM is used for classifying the malware. The performance is much better when compared with using only CNN. Liu et al. (2017) proposed a machine learning based system to classify the malware classes. They trained the model for 9 classes and after classification clustering algorithm is used to identify the unknown malware class.

Kolter et al. (2006) uses n-grams of bytecodes of the files of features. The most relevant features from each file are selected and a variety of classification algorithms like support vector machines, naive Bayes classifier, decision trees were trained on this data. Ultimately, it was found that boosted decision trees outperformed all other classification machine learning algorithms. Deep learning techniques were used on features extracted from files in (Gavrilu et al., 2009) . Another approach is the usage of LSTMs or other RNNs to classify the files using the sequence of operations performed within the files as data. However, as it has been (Gavrilu et al., 2009) pointed this process is time consuming. It requires execution of entire files which is time consuming. Moreover, training of RNNs is computationally intensive in general. LSTM based techniques have been proposed for anomaly detection in (Mirza et al., 2018; Vinayakumar et al., 2017; Malhotra et al., 2015). These techniques can easily be adapted for classification of malicious files as well as the underlying framework and intuition behind the methods is the same. Analysis of the code in the executable files could also be done to generate control flow graphs. From such graphs any sequence of calls that could indicate presence of malware could be found out. However, this method would not work if the code in the infected file has been obfuscated. Table 1 has listed the related works in this domain.

Microsoft Malware Classification Challenge dataset used in this paper has served as a benchmark dataset for more than 50 research papers.

Table 1. Review on malware detection

Author & Year,	Techniques Used	Remarks
Bailey et al., 2007	Behavioural based attributes are collected during execution for dynamic analysis. To collect the behavioral fingerprint of the activities of malware, they are executed in a virtualized environment. These finger prints are clustered for automatic classification and analysis	Running in a Virtual environment, anti VM evasive techniques may not behave as malicious
Liu et al., 2011	A complex Boolean expression built using the malicious behavior features to detect the malware	Limitation is the dynamic analysis is of the malware behaviors. The features collected were static.
Rieck et al., 2008	Monitors the behavior of malware using sandbox, classifies them with respect to a corpus using SVM into 14 families	Benign binaries classified as malware. Not capable of classifying the malware families that are not exposed during learning
Rad et al., 2018	Implemented a binary malware classifier using a neural network that can classify a file as malicious or benign on Windows Portable Executable (PE) files	Not implemented to consider multiple classes of malware
Saxe et al., 2015	A deep forward neural network classifies whether the file is malware or not.	Very a smaller number of benign binaries led to inaccurate performance
Kinable et al. (2011)	Malwares are represented as call graphs, similar graphs are clustered using k-medoids clustering, DBSCAN to detect the types of malwares	Requires the number of clusters to be identified first before clustering
Kwon et al. (2018)	3 CNN models were used to classify the network anomaly	Found to be less performing than LSTM model

The authors (Hassen et al., 2017) proposed automated call graph-based techniques using to analyze and categorize incoming samples are needed. Machine learning features are collected to perform a static analysis, in order to classify them into malware categories. The main limitation of the call graph-based techniques is that it incurs performance overhead due to graph comparison operations.

Ahmadi et al. (2016) combined various features through investigating the byte code and the disassembled code together. In (Burnaev et al., 2016), authors propose a technique called One-Class SVM to classify the malwares by exploiting the closeness to origin of coordinates in a feature space. The authors combine two concepts (SVMs and learning using privileged information) to define a hyperplane that is used for distinguishing malwares hence has limitations when it comes to detecting complex malware structures.

Yuxin et al. (2019) represent the malicious software as opcode and the same is detected by using a deep belief network (DBN), an autoencoder to extract the feature vectors of binary executables. Autoencoder helps in reducing the dimensions of the

features extracted and can get the insight of the data better than other methods. The works (Zhang et al., 2017; Kim et al., 2016) use opcode sequences, segment counts, asm operators, file ID and file size, symbol counts, size of different sections and entropy extraction as features for classification and which again incurs significant time in extracting the features from the executable files which are in the order of gigabytes. The authors of (Bailey et al., 2007) proposed an ensemble model on deep neural network to detect the malware by stacking up various features such as PE body, headers and structure of the malware files using n-grams which defines the behavior of the malware again requires significant amount of time for extraction of their feature components.

Though the prior research work has shown that machine learning approaches are becoming more popular for classifying malware, however, most of the machine learning methods for the classifying and detecting malware use shallow learning algorithms (e.g. SVM). Further research work (Bailey et al., 2007; Kim et al., 2016; Yuxin et al., 2019; Zhang et al., 2017) have shown that deep neural network has superior performance compared to traditional learning algorithms. When we have a very large dataset the the feature extraction will become tedious. For example, the 2-gram category in n-gram method has more than 65,000 features in a normal executable file which takes up to 10,300 seconds for feature extraction alone while the k-nearest neighbor algorithm takes more than 300 seconds when the value of k equals 5.

Also, many others (Ahmadi et al., 2016; Bailey et al., 2007) have specifically designed to target higher performance on specific datasets such as Microsoft Malware Classification Dataset or Malign. To tackle this problem, we propose a deep convolutional neural network called Malnet for addressing two problem statements: malware detection and malware classification. In both the problems, the model converts the executable files into grayscale images of fixed size using bilinear interpolation transformation technique in the first phase and performs image classification in the next phase using deep convolutional neural net to achieve the target. Experiments conducted on the dataset that was curated from various anti-virus software vendors and the Microsoft Malware Classification Challenge dataset demonstrate that our model achieves high accuracy with much lesser training time compared to the other models.

Existing methods were not sufficient enough because millions of new malwares keep on reporting dynamically, Artificial intelligence-based solutions to detect these new signatures were the need of the day in the cyber security domain.

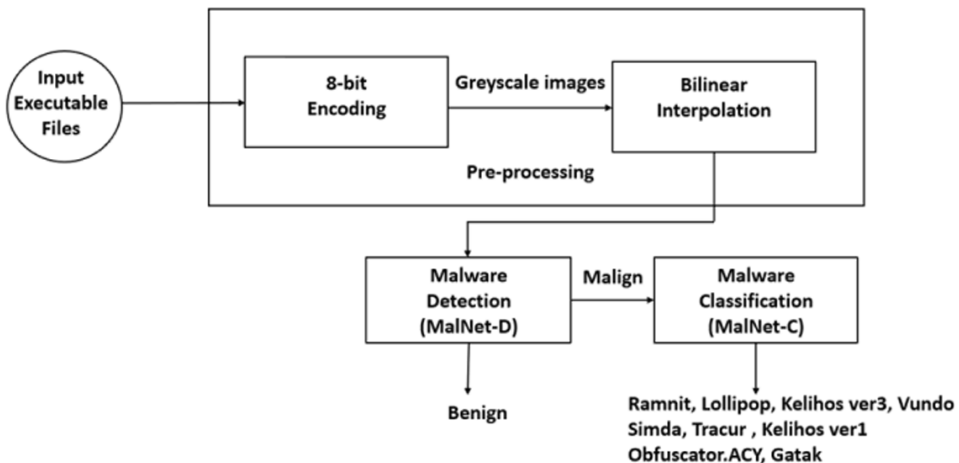
PROPOSED METHODOLOGY

System Overview

A Deep learning based system is proposed to detect the presence of malware and to identify the class. The proposed system shown in Figure 1, uses the Convolutional Neural Network based architecture to detect the malware from executable files automatically and termed as MalNet. To identify the classes of malware using MalNet the executable files need to be converted into images. Proposed system explores the various encoding techniques for representing executable files as images and the best technique is 8-bit encoding which is illustrated in section Preprocessing.

The size of the images thus obtained is very large which in turn increases the number of parameters of MalNet. To address this issue various image resizing methodologies were exploited and proposed bi-linear interpolation image resizing method as the suitable one and elaborated in section Resizing.

Figure 1. Proposed System Architecture



The process of identifying the malware class is formulated as a hierarchical method. Initially for a given executable file the presence of malware is detected using a proposed Convolutional Neural Network based architecture MalNet -D. Once the system detects the presence of malware, the family to which this belongs to, need to be identified. MalNet -C is proposed as a second level Convolutional Neural Network based multi class classification task which is illustrated in section Malware Detection and Classification.

PREPROCESSING

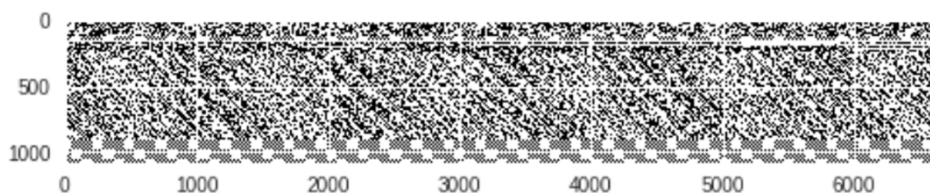
Encoding

The executables are in binary raw format. Analyzing these files to identify the presence of malware is a tedious task. In order to identify the pattern associated with the normal and malicious information, the raw data is converted to image files using encoding technique. Two encoding techniques namely, 1-bit encoding and 8-bit encoding were explored and in this work 8-bit encoding is applied to convert the raw executables into digital images.

1-Bit Encoding

In 1-bit encoding scheme each single bit of the input file, taking on a value of either 0 or 1 is mapped to either 0 or 255 resulting in a gray scale image. The output of this encoding scheme is showed in Figure 2. However, the drawback of this scheme is that the images generated are too large in size. Secondly the images contain only 2 values for pixels i.e. 0 and 255 making them highly inefficient and reducing the amount of information that can be extracted to identify features.

Figure 2. 1-Bit Encoding



8-Bit Encoding

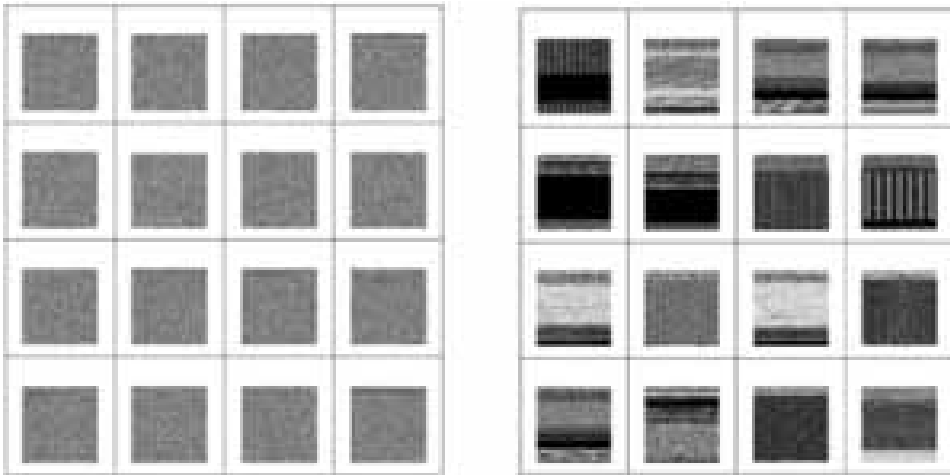
An efficient encoding scheme to overcome the difficulties in the 1-bit encoding is 8-bit encoding. In this scheme pixel values 0 to 255 is assigned to a sequence of 8 contiguous bits from the executable file. These 8 bits can represent any value in the range [0, 255]. Since this is also the range of a single pixel in a gray scale image, the sequence of 8 bits are encoded as a single pixel. This method does not have any data loss as all the bits of the file are represented and is also space efficient. The image obtained from this encoding scheme is shown in Figure 3.

Figure 3. 8-Bit Encoding



With 8-bit encoding scheme, the correspondence between code and patterns in the image are high. This would enable more efficient and accurate feature extractions improving accuracy. Thus the 8-bit encoding scheme would suit the classification tasks better. Sample images of benign and malign executable after 8-bit encoding are shown in Figure 4. (a) and (b) respectively. These patterns give rise to features that can be detected by the CNN architectures in modules further down the pipeline for classification tasks.

Figure 4. a. Sample images of benign executables b. Sample images of malware executables



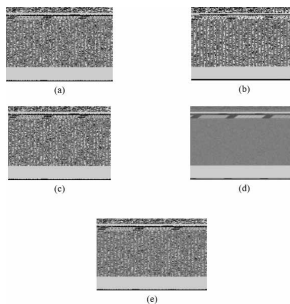
Bilinear Interpolation

The images generated after encoding are of various sizes with respect to executable files and also the size is very large. In order to the size and equalize the sizes of all the images the images are all down sampled to a fixed size for feature representation using Deep Learning Networks. In order to do this, first the pixel values are constructed

as an array and then resized into a near perfect square matrix. This matrix is then shrunk to a size of 64*64 using the bilinear interpolation algorithm. This algorithm basically interpolates the value of a pixel using the values of 4 nearby pixels. It is an extension of linear interpolation for interpolating two variables in a rectangular 2-D grid. The key idea is to perform linear interpolation in both the directions. Although each step is linear in the sampled values and in the position, the interpolation as a whole is quadratic in sample location. The image obtained from the application of bilinear interpolation algorithm is shown in Figure 5. (e). Various image resizing algorithms such as lanczos interpolation, nearest neighbor interpolation, bicubic interpolation, and pixel area relation algorithms are displayed in Figure 5. (a), (b), (c), (d) and (e).

Considering performance, only nearest neighbor, pixel area relation and bilinear interpolation algorithms are viable for real time detection. Among the three algorithms bilinear interpolation performs well and generated better quality images compared to other techniques. Thus this technique is employed to resize the images to the required size for further processing.

Figure 5. Output of resizing algorithms for the image shown in Figure 4: (a) Lanczos algorithm (b) Nearest algorithm (c) Bicubic algorithm (d) Pixel Area Relation algorithm (e) Bilinear algorithm



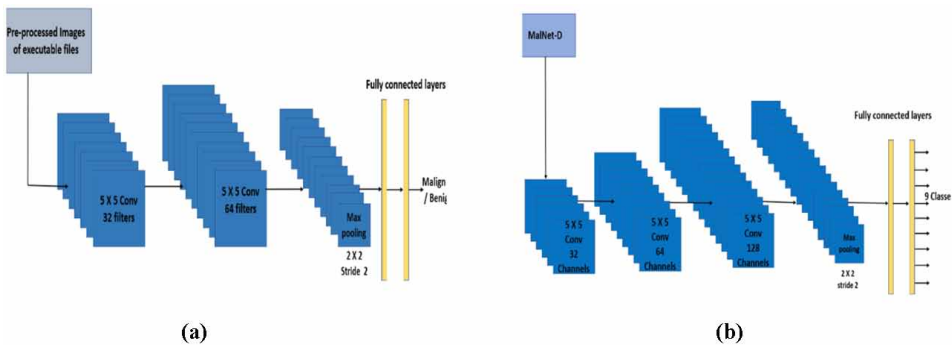
Deep Neural Network Based Malware Detection (MalNet –D)

Convolutional Neural Network is the most popular deep learning based approach for image classification. Malware detection is modeled as a binary image classification problem to detect the presence and absence of malware in given file. A novel Convolutional Neural Network based architecture termed as MalNet -D is proposed to detect the presence of malware. The lower part of the architecture has two convolutional layers in order to reduce spectral variation and to capture the dependencies in terms of spatial and temporal. The first convolutional layers has 32 kernels each of size

5x5, where in the second has 64 kernels of the size 5x5 to extract the features from the images. Max pooling layers follow the two convolutional layers in order to down sample the convoluted feature maps. These two pooling layers have the filters of size 2x2 with stride 2. To avoid overfitting dropout layers are also introduced after the max pooling layers with rate 0.2. The extracted high-level features are fed to the classification part of the MalNet- D architecture, which has two fully connected layers. The first fully connected layer is designed to have 1024 nodes with softmax activation function, while the second fully connected layer has 1 output node since this MalNet-D is a binary classifier and hence with the sigmoid activation function. The architecture of MalNet-D is shown Figure 6. (a).

This architecture is trained with Microsoft Malware Challenge dataset and the model is created. This model could able to predict the presence of malware for the unknown executable files. Further the detected file needs to be classified as to which family it belongs to.

Figure 6. a. MalNet –D b. MalNet – C



The proposed system takes as input an executable file and performs binary classification to predict whether the executable is a malware or not. So, the input dataset consists of both malware executables and benign executables. These input executables are fed to 8-bit encoding module which converts the executable files into grayscale images of high dimensions. These images are down sampled to fixed size (64 x 64) by the bilinear interpolation transformation scheme while preserving the important characteristics and patterns present in the original image. Once the grayscale images are down sampled, it is fed into the neural net for training/testing phase to detect the presence of malware. The detected files are classified into 9 categories by the classification module. The proposed CNN, MalNet-D tailored for requirements of malware detection are trained with the images generated after encoding and resizing.

Deep Neural Network Based Malware Classification: MalNet-C

The detected malware needs to be classified under any one of the 9 families as described in Table 2. A Convolutional Neural Network based architecture termed as MalNet-C is proposed for classification. The proposed MalNet-C has 4 convolutional layers with 32, 64, 64 and 128 kernels of size 5x5 each. The convoluted feature maps are down sampled by the maxpooling layers after the first and last convolutional layers whose filter size 2x2 with stride of 2. The architecture also employs dropout layer with rate 0.2. The first of two fully connected layers have 1024 nodes with Relu activation function. The final discrimination layer has the nodes equivalent to the number of families of malware, 9 with softmax activation function. This MalNet-C is trained with images of three different sizes namely, 32x32, 64x64 and 128x128. For malware classification, the system takes as input an executable file and predicts the malware family to which the file belongs to through multi-class classification. The input dataset for training the model consists of only malware executable and no benign files. The malware executable files represent a mix of 9 different malware families. These executables files are fed to 8-bit encoding module for being converted into images of high dimensions, where each image represents the characteristics and behavior of the malware family it belongs to. These high dimensional images are down sampled to fixed size using bilinear interpolation transformations scheme without losing important discriminating characteristics and patterns of different malware families. Once the images are down-sampled, the images are fed into MalNet-C as input tensors for training/testing phase. The architecture of MalNet-C is shown Figure 6. (b).

The output of this multi-class classification would be an integer denoting the class number of the malware family to which the executable file belongs.

EXPERIMENTAL RESULTS AND DISCUSSION

Dataset Description

The dataset used for the classification tasks comes from a variety of sources. Microsoft's dataset released as part of the Malware Classification Challenge on Kaggle (BIG 2015) provides the malware files for use in both the malware detection and malware classification modules. It contains 20000 malware files having a collection of 9 different families of file size 1/2 TB when uncompressed. Each malware file has an identifier, (Ronen et al., 2008) which is hash value of 20 character that identifies uniquely the file and an integer referring to the class label,

which is out of the 9 family names of malware. The names of the 9 families and its type are listed in Table 2.

Table 2. Malware families in the dataset

Family Name	Samples	Type
Ramnit	1541	Worm
Lollipop	2478	Adware
Kelihos ver3	2942	Backdoor
Vundo	475	Trojan
Simda	42	Simda Backdoor
Tracur	751	TrojanDownloader
Kelihos ver1	398	Backdoor
Obfuscator.ACY	1228	Obfuscated malware
Gatak	1013	Backdoor

For the malware detection module, in addition to the Microsoft Dataset, benign files have been sourced from online software centers, system boot files and other application software. A total of 2500 benign files were obtained and to avoid bias in classification the distribution of malware and benign files in the train and test dataset is uniform. The train and test split for this module is 80:20.

Implementation Stack

The encoding, preprocessing modules and the malware classification module were implemented in Python 3. The various libraries used in the implementation of this module were as follows.

- OpenCV - Framework for handling images
- Numpy - Utility library
- BeautifulSoup - Automate downloading benign files.
- GoogleDrive Library - Access Google drive to store and retrieve dataset.

As with the rest of the project, the malware classification module was completely implemented in Python 3. The various libraries used in the implementation of this module were as follows:

- Keras - Framework for implementing NN

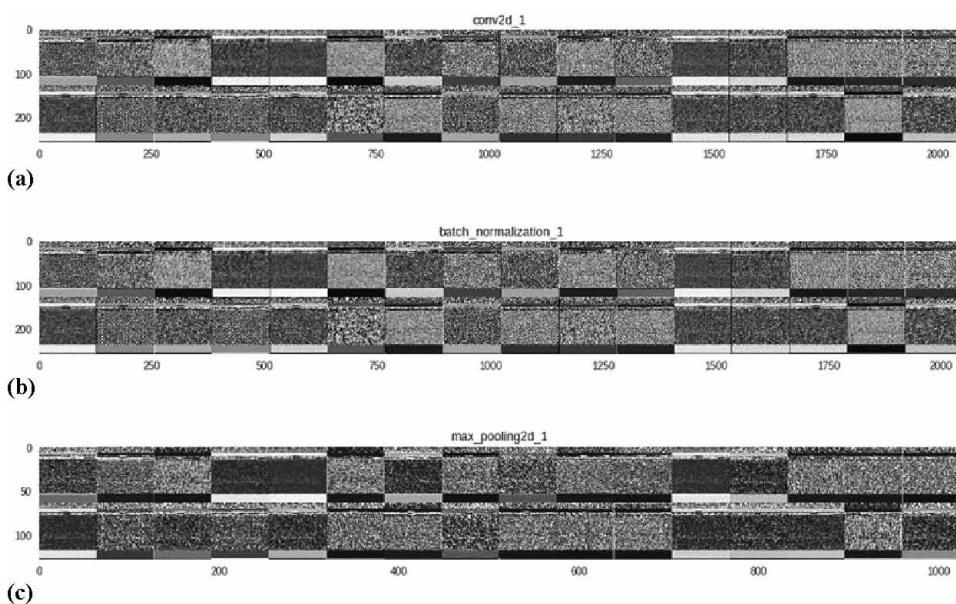
Deep Learning-Based Malware Detection and Classification

- Tensorflow (Backend).

MalNet –D

The features learned at first convolution layer and after normalization layer and max pooling layer during training are visualized as shown in Figure 7. (a), (b) and (c). The optimizing algorithm used here is Adam Optimizer with a learning rate of 0.001 and binary logarithmic cross entropy is used to compute loss. The Malware detection performance of MalNet D for the (BIG2015) dataset is shown in Table 2. for the image size of 64x64. To prove the efficiency of the proposed system, compared with the well-known standard architectures proposed by researchers in the past - the VGGNet and ResNet. VGG16 is a convolutional neural network model proposed by Simonyan et al. (2014). VGG16 is the classification model trained with 14 million images for 1000 classes. This model comprises 13 convolutional layers and 3 dense layers. Convolutional layers were trained with images of sizes 224x224 for feature representation. The learned features were trained for classification using dense layer with ReLu as activation function and the output layer uses softmax as activation layer.

Figure 7 a. Output of first convolutional layer b. first batch normalization layer c. first maxpooling layer



The hyperparameters of these architectures have been modified to make them compatible with the size of the input images. The modifications for the VGGNet are as follows. The input layer now takes in 64*64*1 input tensor instead of the 224*224*3 in the original VGGNet architecture. To compensate for the reduced input size, the number of trainable parameters is reduced by reducing the number of filters in the subsequent layers and reducing the overall number of layers as well. In particular, the first layer starts with 16 filters instead of 64. After the first down sampling with the Maxpooling Layer, the filters are doubled to 32. Finally, after another round of down sampling, the Fully Connected Layer is introduced with 1024 neurons instead of 4096 in the original architecture. The final output layer is a sigmoid activation layer instead of the 1000-unit softmax activation layer as binary classification is being done here. The 3*3 filters used for the convolutional layers in the original architecture have been preserved.

Similarly, the architecture of the ResNet (He et al., 2016) has also been modified and a much shallower network compared to standard ResNet is being used.

Table 3. Detection results

Model	Image size	Accuracy (%)	Loss	Training Time (sec)	Trainable Params
VGGnet	64x64	49.6	8.0342	12925	39,891,649
ResNet	64x64	49.6	8.0342	100	4,945
MalNet-D (Proposed)	64x64	93.5	0.3269	175	16,831,361

The accuracy reported by the standard architectures were low when compared with the proposed system as reported Table 3. Even though the computational time and the associated hyper parameters were on the better side for ResNet architecture, accuracy is very low.

MalNet-C

The final module of the pipeline is the malware classification module. This module classifies the files being designated as 'malware' into one of the 9 malware families. Similar to the previous module, the encoded images are trained on three architectures including the two standard architectures - VGGNet and ResNet. The modifications made to the two architectures to ensure compatibility with the inputs being fed in here, are similar to those made for the malware detection module as well. The one exception is the final output layer where instead of a sigmoid activation layer a

Deep Learning-Based Malware Detection and Classification

softmax activation layer is used as there are nine classes here instead of the two in the previous module. Additionally, for classification, inputs images of sizes 32*32, 64*64 and 128*128 are used for training three architectures.

As shown in the Table 5, the MalNet-C slightly outperforms the VGGNet for various input sizes, performing best on the 128*128 size input. The optimizing algorithm used here is Adam Optimizer and logarithmic cross entropy is used to compute loss. The confusion matrix is shown in Table 4. This shows that the incorrect predictions for families is low using the MalNet-C architecture.

Table 4. Confusion Matrix for MalNet-C

	Ramnit	Lollipop	Kelihos ver3	Vundo	Simda	Tracur	Kelihos ver1	Obfuscator. ACY	Gatak
Ramnit	449	1	0	0	0	1	3	8	1
Lollipop	1	734	0	0	0	2	0	1	6
Kelihos ver3	0	0	880	2	0	0	1	0	0
Vundo	1	0	0	142	0	0	0	0	0
Simda	1	1	0	1	10	0	0	0	0
Tracur	5	3	0	0	1	213	0	4	0
Kelihos ver1	2	0	0	0	0	0	117	0	1
Obfuscator. ACY	5	1	1	0	0	1	0	360	1
Gatak	0	0	0	0	0	2	3	2	297

MalNet-C is devised based on the shortcomings of the existent architectures like VGGNet and ResNet. The images in our dataset contain very less features compared to the images in ImageNet towards which the existent architectures are targeted. By tuning the layers and reducing the parameters involved, MalNet-C provides better results compared to the existent architectures which are deep in nature and hence contain more parameters.

For malware detection, VGGNet performs poorly. This is due to the intricate features which are present as differences between multiple malware classes as compared to major feature differences between malware and benign images. Intricate feature differences are detected more easily due to the deep nature of VGGNet. With respect to the differences between classification and detection in ResNet, it is due to lack of generalization of trend i.e. underfitting. This has occurred due to the minimal dataset which is worsened by the lack of trainable parameters in the architecture.

Table 5. Classification results

Model	Image size	Accuracy (%)	Loss	Training Time (sec)	Trainable Params
ResNet	64x64	65.05	1.16	1980	5,081
MalNet-C	64x64	95.86	0.23	2550	16,839,561
VGGNet	64x64	94.64	0.22	12400	39,851,169
ResNet	32x32	66.06	1.03	470	5,081
MalNet-C	32x32	93.69	0.29	730	4,256,649
VGGNet	32x32	92.52	0.29	10925	39,751,649
ResNet	128x128	71.88	1.01	6800	5,081
MalNet-C	128x128	96.11	0.24	14800	33,924,169
VGGNet	128x128	94.51	0.28	16850	39,979,993

CONCLUSION

Real time detection of malware has been a predominant problem that required solution in the Cyber Security field. Exploiting the underlying structure of malware files, a convolutional neural network to train on encoded images of executable files were explored, both of benign and malign classes for detection. In addition to this, classification of malware families was experimented using deep learning network. Utilizing the detection model, any application can be encoded and classified as a malware or benign file. For further analysis into the type of malware, the classification model could be utilized for classifying into specific malware type. Primarily, we would like to increase the accuracy as high as possible since false classification could lead to potential data and monetary losses. Variants of deep learning architecture is designed for detection and classification. MalNet-D system detects the presence of malware. Once detected, MalNet-C identifies the category of the malware. Results show this technique performs well in terms of improving accuracy and reducing the loss. To prove the efficiency of this method, compared the results with the standard deep learning architectures namely VGGNet and ResNet. This method outperforms both VGGNet and ResNet.

As the extension of this work, a machine learning algorithm can be devised to detect the category of malware that changes time to time, the results can be further improved in terms of accuracy and a web application can be developed to act as a user interface for ease of usage.

REFERENCES

- Ahmadi, M., Ulyanov, D., Semenov, S., Trofimov, M., & Giacinto, G. (2016, March). Novel feature extraction, selection and fusion for effective malware family classification. In *Proceedings of the sixth ACM conference on data and application security and privacy* (pp. 183-194). 10.1145/2857705.2857713
- Antivirus software. (n.d.). https://en.wikipedia.org/wiki/Antivirus_software
- AV-test, Malware, The Independent IT-Security Institute. (2014), Retrieved from <http://www.av-test.org/en/statistics/malware>
- Bailey, M., Oberheide, J., Andersen, J., Mao, Z. M., Jahanian, F., & Nazario, J. (2007, September). Automated classification and analysis of internet malware. In *International Workshop on Recent Advances in Intrusion Detection* (pp. 178-197). Springer. 10.1007/978-3-540-74320-0_10
- Burnaev, E., & Smolyakov, D. (2016, December). One-class SVM with privileged information and its application to malware detection. In *2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)* (pp. 273-280). IEEE. 10.1109/ICDMW.2016.0046
- Computer crime costs \$67 billion, FBI says – CNET. (n.d.). https://www.insight.com/content/dam/insight/en_US/pdfs/symantec/symantec-corp-internet-security-threat-report-volume-18.pdf
- Gavriluț, D., Cimpoeșu, M., Anton, D., & Ciortuz, L. (2009, October). Malware detection using machine learning. In *2009 International Multiconference on Computer Science and Information Technology* (pp. 735-741). IEEE. 10.1109/IMCSIT.2009.5352759
- Hassen, M., Carvalho, M. M., & Chan, P. K. (2017, November). Malware classification using static analysis based features. In *2017 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1-7). IEEE. 10.1109/SSCI.2017.8285426
- He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 770-778). 10.1109/CVPR.2016.90
- Internet Security Threats Report. Symantec. (n.d.). <http://www.symantec.com/threatreport/>
- Kim, Kim, & Lee. (2016). Performance analysis of the malware classification method in accordance with the changes in assembly code. *Journal of the Korean Institute of Communication Sciences*, 885-886.

- Kinable, J., & Kostakis, O. (2011). Malware classification based on call graph clustering. *Journal in Computer Virology*, 7(4), 233-245.
- Kolosnjaji, B., Zarras, A., Webster, G., & Eckert, C. (2016, December). Deep learning for classification of malware system call sequences. In *Australasian Joint Conference on Artificial Intelligence* (pp. 137-149). Springer. 10.1007/978-3-319-50127-7_11
- Kolter, J. Z., & Maloof, M. A. (2006). Learning to detect and classify malicious executables in the wild. *Journal of Machine Learning Research*, 7(Dec), 2721–2744.
- Kwon, D., Natarajan, K., Suh, S. C., Kim, H., & Kim, J. (2018, July). An empirical study on network anomaly detection using convolutional neural networks. In *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)* (pp. 1595-1598). IEEE. 10.1109/ICDCS.2018.00178
- Liu, L., Wang, B. S., Yu, B., & Zhong, Q. X. (2017). Automatic malware classification and new malware detection using machine learning. *Frontiers of Information Technology & Electronic Engineering*, 18(9), 1336–1347. doi:10.1631/FITEE.1601325
- Liu, W., Ren, P., Liu, K., & Duan, H. X. (2011, September). Behavior-based malware analysis and detection. In *2011 first international workshop on complexity and data mining* (pp. 39-42). IEEE. 10.1109/IWCDM.2011.17
- Malhotra, P., Vig, L., Shroff, G., & Agarwal, P. (2015, April). Long short term memory networks for anomaly detection in time series. In *Proceedings* (Vol. 89). Presses universitaires de Louvain.
- Marín, G., Casas, P., & Capdehourat, G. (2019, May). Deep in the Dark-Deep Learning-Based Malware Traffic Detection Without Expert Knowledge. In *2019 IEEE Security and Privacy Workshops (SPW)* (pp. 36-42). IEEE. doi:10.1109/SPW.2019.00019
- Mirza, A. H., & Cosan, S. (2018, May). Computer network intrusion detection using sequential LSTM neural networks autoencoders. In *2018 26th Signal Processing and Communications Applications Conference (SIU)* (pp. 1-4). IEEE. 10.1109/SIU.2018.8404689
- Mohaisen, A., Alrawi, O., & Mohaisen, M. (2015). Amal: High-fidelity, behavior-based automated malware analysis and classification. *Computers & Security*, 52, 251-266.
- PandaLabs Annual Report. (2017). *Panda Security*. https://www.pandasecurity.com/mediacenter/src/uploads/2017/11/PandaLabs_Annual_Report_2017.pdf

Deep Learning-Based Malware Detection and Classification

Rad, B. B., Nejad, M. K. H., & Shahpasand, M. A. R. Y. A. M. (2018). Malware classification and detection using artificial neural network. *Journal of Engineering Science and Technology*, 13, 14–23.

Rieck, K., Holz, T., Willems, C., Düssel, P., & Laskov, P. (2008, July). Learning and classification of malware behavior. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 108-125). Springer. 10.1007/978-3-540-70542-0_6

Ronen, R., Radu, M., Feuerstein, C., Yom-Tov, E., & Ahmadi, M. (2018). *Microsoft malware classification challenge*. arXiv preprint arXiv:1802.10135

Safety Detectives. (n.d.). <https://www.safetydetectives.com/blog/most-dangerous-new-malware-and-security-threats/>

Saxe, J., & Berlin, K. (2015, October). Deep neural network based malware detection using two dimensional binary program features. In *2015 10th International Conference on Malicious and Unwanted Software (MALWARE)* (pp. 11-20). IEEE. 10.1109/MALWARE.2015.7413680

Sikorski, M., & Honig, A. (2012). *Practical malware analysis: the hands-on guide to dissecting malicious software*. No Starch Press.

Simonyan, K., & Zisserman, A. (2014). *Very deep convolutional networks for large-scale image recognition*. arXiv preprint arXiv:1409.1556

Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017, September). Long short-term memory based operation log anomaly detection. In *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 236-242). IEEE. 10.1109/ICACCI.2017.8125846

Yuxin, D., & Siyi, Z. (2019). Malware detection based on deep learning algorithm. *Neural Computing & Applications*, 31(2), 461–472. doi:10.1007/00521-017-3077-6

Zhang, Y., Rong, C., Huang, Q., Wu, Y., Yang, Z., & Jiang, J. (2017, August). *Based on multi-features and clustering ensemble method for automatic malware categorization*. In *2017 IEEE Trustcom/BigDataSE/ICSS*. IEEE.

ADDITIONAL READING

- Barak, L. (2020). Preventive medicine is the best method for computer hygiene. *Computer Fraud & Security*, 2020(1), 9–11. doi:10.1016/S1361-3723(20)30007-5
- Bishop, C. M. (2006). *Pattern recognition and machine learning*. springer.
- Fox, S. R., Flack, J. C., & Harman, P. V. (2009). *U.S. Patent No. 7,489,812*. Washington, DC: U.S. Patent and Trademark Office.
- Genge, N. E. (2002). *The forensic casebook*. Ballantine Books.
- Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT press.
- Hassoun, M. H. (1995). *Fundamentals of artificial neural networks*. MIT press.
- Malyshev, A., Biyachuev, T., & Ilin, D. (2014). *U.S. Patent No. 8,635,694*. Washington, DC: U.S. Patent and Trademark Office.
- Prasad, R., & Rohokale, V. (2020). Malware. In *Cyber Security: The Lifeline of Information and Communication Technology* (pp. 67–81). Springer. doi:10.1007/978-3-030-31703-4_5
- Szegedy, C., Ioffe, S., Vanhoucke, V., & Alemi, A. A. (2017, February). Inception-v4, inception-resnet and the impact of residual connections on learning. In *Thirty-first AAAI conference on artificial intelligence*.

Chapter 7

Detecting Fake News Using Deep Learning and NLP

Uma Maheswari Sadasivam
BITS Pilani (Off Campus), India

Nitin Ganesan
Madras Christian College, India

ABSTRACT

Fake news is the word making more talk these days be it election, COVID 19 pandemic, or any social unrest. Many social websites have started to fact check the news or articles posted on their websites. The reason being these fake news creates confusion, chaos, misleading the community and society. In this cyber era, citizen journalism is happening more where citizens do the collection, reporting, dissemination, and analyse news or information. This means anyone can publish news on the social websites and lead to unreliable information from the readers' points of view as well. In order to make every nation or country safe place to live by holding a fair and square election, to stop spreading hatred on race, religion, caste, creed, also to have reliable information about COVID 19, and finally from any social unrest, we need to keep a tab on fake news. This chapter presents a way to detect fake news using deep learning technique and natural language processing.

INTRODUCTION

The news is a fake news when the information posted on a web site cannot be verified as its source is not clear. Fake news could cause chaos or misguiding people about a whole situation or topic and also have a negative impact on society and community

DOI: 10.4018/978-1-7998-4900-1.ch007

(Schetinger et al., 2017). These fake news could have been done intentionally to bring in chaos at work place (Murphy, 2017) targeting society or community or individuals. Detecting such fake news and alerting the users about the same could avert confusion among the users across the globe. In the current political crisis especially when countries go for polls to select their country head, global economic crisis, discrimination of races and the COVID 19 crisis happening all round the world the researchers see many fake news being circulated on the web. In reality these Fake news (Allcott, Gentzkow, 2017) can be different forms like deliberate misguiding information, headlines is false, hate spreading, sharing misinformation on social media and including the satirical ones. (Lazer et al., 2018) (Wallace, 2013). Detecting fake news is now equally challenging and very important in this cyber age to make the world a better safe place for one and all. This paper uses NLP and Deep learning techniques to detect fake news on web. The deep learning are sophisticated as it can deal with complex pattern to classify the News as Fake or not while other Machine learning algorithms cannot handle complex patterns.

FAKE NEWS DETECTION USING NLP AND DEEP LEARNING

Detecting fake news in media like TV,radio, print where one can easily find out a real news from a fake news if knowledge about media and how publishing is done. Sometimes these news are biased as well which is really confusing the users and misguiding them.

The fake news evaluations are done once the information about sender who sent the message or the news creator or the author details, their background, organization, URL details. Also exploring into the message, its content, date of story, experts in the report and update frequency of the website throws more information to decide if its a fake news or not. The sources of the story is further scrutinised to check if it is from anonymous person, biased or not and for other vital clues as well. These parameters along with why the message was created, if their intension was for profit or an advertisement also helps to detect if it's a fake news or not.

There are huge volume of information which may be unstructured data that are related to specific news or topic to be processed on the web. Natural Language Processing or NLP combined with text analytics is used to unlock huge data sets available on web[(Wondeflow, 2019) (Oshikawa et. al., 2020)]. NLP is used to convert huge volume of unstructured data in the websites to a normalized form and can be stored into data file. The obtained structured data stored in a file will be used by the smart software or model to determine if the news or message is fake or not. There are two models possible which are machine learning and deep learning models. In this paper deep learning model is the one going to decide and fake news

is detected. The structured data has fake news parameters also called features. Using these features deep learning model is trained and the obtained model fit is deployed into the application.

ANALYSIS: HOW TO DETERMINE FAKE NEWS

There are many factors that determine if the news is fake or not and are discussed in detail as follows. In this paper a benchmark for the dataset is set and is also the highlight of the work.

i. Checking on the authority of the news

The news published should be checked for authority. There are several ways to do the check on authority. In data mining phase the web page linkages could be used to determine the authority. The authority is hidden in Web page linkages and can be scrutinized to get better picture of news or information on web page. The Web consists not only of pages but it also has hyperlinks of other web pages as well. These hyperlinks can throw more information on authority of news or information published. When a Web page is created by a hyperlink pointing to another web page then it guarantees the author's endorsement of the other page. These collective endorsement of a given web page by different authors on the web may indicate the importance of the page and may naturally lead to the discovery of authoritative Web pages (Botafogo et. al.,1992). This information about Webpage linkage provides us with news relevance, its quality and also the contents of the web page that can be analysed for further anomalies.

Other notable ways to detect web page authority is using Hubs called HITS or Hyperlink Induced Topic Search which rates webpages using the web link structures and rank those webpages of specified topic or news. HITS uses hubs and authorities. When you search for specific news or topics the search engine returns set of relevant web pages called roots which are the authorities and pages that aren't relevant are called hubs. These hubs and authorities defines the recursive relationship between webpages and a page that has many hubs link as authority while a Hub is a page that links to many authorities (Raluca, Remus). Then a weight-propagation phase is initiated which is an iterative process that determines numerical estimates of hub and authority weights. Thus the links between two pages with the same Web domain (i.e., sharing the same first level in their URLs) often serve as a navigation function and thus do not confer authority(Allan B. et. al., 2001).

Google's Page Rank computes based on the quality and quantity of links to a webpage, prescribing a rank number as a result (Allan B. et. al., 2001). On a page if

a website A is linked to another website B then Google notes this as an endorsement of authority and quality of your website. This gives a higher rank for website A as its original for that given search.

Any of the method below can be used to determine authority of news.

ii. Subject

The subject of the news that is mentioned as in the news contents and its a short line describing news content.

iii. Visual assessment of website or web page

Based on the visuals of website that hosts the news, helps us to decide if its fake or not. Check the visuals on the website or web page if it has any annoying advertisements, images that are amateurish as they are possibly stolen from other sources. Finally check for the image quality (Sophie J. N, et. al., 2017) and if the image is not of high quality or stolen or not professional then the website could be a FAKE.

iv. News source, article source and trustworthy

The news source or outlet can be investigated to check if it is a genuine news source or not. A news source is trustworthy if all respected the news. Trustworthy feature information can help us decide if news is fake or not. If the news source is well known among users then considering all of the other factors helps us decide if news is fake or not. If the news or article source is mentioned as unknown or anonymous then the article or news is unreliable and can be inferred that news or article is probably Fake.

v. Domain name and legitimate

The domain name can be checked if its legitimate or not. If the domain name is not a well known news domain like CNN, BBC, ABC, MSNBC, TOI and other news websites then its not a legitimate source. Every country has its own local print media and TV media that has a domain name or website providing legitimate news (Allcott, Gentzkow, 2017). If the domain name is not legitimate then news is probably fake.

vi. Background check of contacts.

Detecting Fake News Using Deep Learning and NLP

The contacts mentioned in the website can be checked to find if they are legitimate team. If contacts are not clearly mentioned or their emails or identities are not clear then it can be a fake news with a bad intention (Allcott, Gentzkow, 2017).

i. Check the author of news.

The author of the news can be checked by doing a background check on the author. If the author is not genuine then news can be fake.

ii. Hatred or angry message in the news.

If the news has any signs of malicious intent or spreading hatred or anger in society or in community then investigation is needed. Most of such hatred or anger message are with an intent of damaging the peace within a society or in a community. A hatred or anger message may be a fake news as its not balanced. A news that is biased and not fair in its content is definitely not with good intention. A sentiment Analysis (Jakub et al., 2017) helps to determine if contents are hatred or anger or a negative sentiment which might instigate violence or any bad trend in the community or society.

iii. Check the writing style and mistakes.

Do a spell, grammar and punctuations check. If there are many mistakes in spelling, grammar and punctuations then its a possibly a fake News (Kai et. al., 2017). Normally a professional news editor or an author would not make so many mistakes and leave us an unreliable content. There are many ways to do spelling, punctuation or grammar check one way is using NLP (Oshikawa et. al., 2020) and other is to move contents to word processing software where spell, grammar and punctuation checks can be done on it.

iv. Check if similar article or news exists.

The web can be searched using search engines like google.com for similar article or news and if we find such an article or news then we can infer that news or article is not FAKE.

v. Do a Fact check.

A fact check can be done using website like factcheck.org, politicoFact.org, snopes.org. These websites help us with if the news or article is true or not. These

fact check websites has a database of websites which are fakes. Truth of news or an article means news or article scrutinised is not FAKE (Schetinger et. al., 2017). Recently as this work was carried, TWITTER came up with a fact check feature to stop FAKE or misinformation among users of twitter. The website snopes.org was used to do factcheck on news in this paper work.

vi. Do a check on published date of news or article

The date of news published can give us a clue if the news was fake or not. The date of publication if was suspicious or does not add up then we can conclude that news is FAKE.

vii. Impersonation

Check for impersonation in the news. If the news depicts any celebrity or any person then it could be a FAKE.

These are the different features considered to find out if the news is FAKE or not. The outcome Fake or not Fake is called the target value (Leskovec, Rajaraman, Ullman,2016).

In this paper, all these features are used to determine if the news is FAKE or not. There is no dataset available on the web that meets all these details or features or input values. This lead to set a benchmark on the dataset. Using this dataset the prediction of Fake or not with a higher accuracy was obtained.

NLP TO CREATE THE TRAINING SET AND TEST SET DATA WITH A BENCHMARK

The previous section explained all the data that can be used to detect if the news is fake or not. First the raw data is obtained from web using web scrapping techniques which gives us unstructured data. The unstructured data is read and a data extraction using NLP (Traylor et al., 2019) is done to get all the features for the detecting news is fake or not. The process of extraction and obtain useful features about news from the raw data is called feature extraction(Leskovec, Rajaraman, Ullman,2016) (Kai et. al., 2017). LSTM or Long Short Term Memory (Jakub, Ahmet, Rafal, 2017) is used for extracting data without losing the sequence of words as its important in the sentimental analysis column 9 of the dataset. This feature extraction has a benchmark set to the dataset used in this paper and is as follows:

Column 1: Authority of news

Detecting Fake News Using Deep Learning and NLP

Column 2: Subject
Column 3: Visual assessment of webpage
Column 4: News source
Column 5: Trustworthy news
Column 6: Domain name legit
Column 7: Background check of contacts
Column 8: Author of news
Column 9: Sentiment analysis of news
Column 10: writing style of news
Column 11: Mistakes in writeup
Column 12: similar news existence
Column 13: Status of fact check
Column 14: date of publication
Column 15: Impersonation in news
Column 16: FAKE or NOT.

Where the column 16 is target.

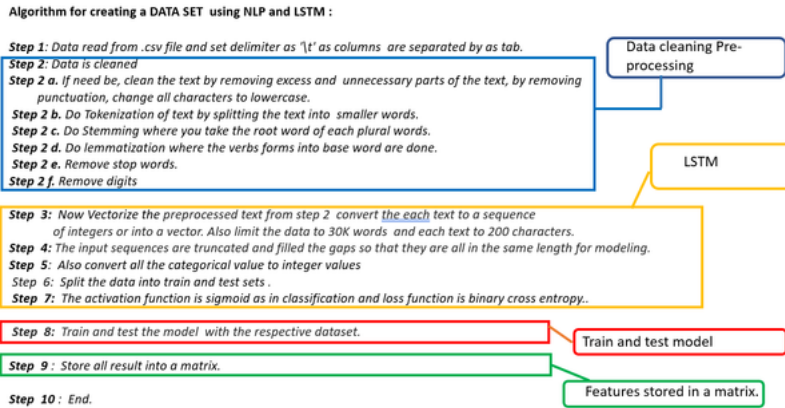
The data above is stored in a .csv file. The data should be read from the .csv file and prepare an input feature matrix. As the Machine learning or Deep learning models use math models which means models work on numeric data. These math models can be trained with a proper input feature matrix. To prepare an input matrix, conversion of text to numbers while numerical values stays same. NLP can be used to do data pre-processing and data transformation as well (Jiahao, 2019). The NLP algorithm uses LSTM for feature extraction and is as follows:

The numerical data cleaning involves removing null values, handling missing, duplicate values and outlier removal (Wondeflow, 2019) (Meiryum, 2019). While with pre-processing of text like converting all characters to lower case, removing numerical values in text, removing punctuations and finally removing all stop words is done. The NLP can help with extracting all features from raw data and write it into a .csv file. Again NLP is also used to do the pre-processing of data in.csv file as it has text and numbers. Now a dataset with the benchmark is obtained which is very important part in this work. This dataset is used by models of Deep learning as these models works on numbers only.

The dataset is divided into a training set and a test set data (Jason B., 2017). The training data set would be 70 to 80% of total data while the test set data is 20 to 30% of total data. While testing for accuracy of the LSTM model, keep a tab on if the model is neither overfit and nor an underfit (Wondeflow, 2019) (Meiryum, 2019). A model is “Overfit” if it has not learned anything, though it may look that it has learnt as the train accuracy and test accuracy is a high score. If model has not learned anything at all as the test and train accuracy score is less and so the model

declared “Underfit”. Using a underfit or overfit model doesn’t predict with high accuracy and also gives a bizarre results (Kai et. al., 2017).

Figure 1. Data set creation using NLP and LSTM.



Learning Models Used in Detecting Fake

Machine learning or Deep learning models learns pattern from the data that is feed to it during the learning phase. Machine learning models can be used when there is a less commonality between the different input values or features. While Deep learning models are used when input values have more commonality between them and also it captures the more minute details or patterns. For example deep learning is like “To recognize a black cat in a dark night” and commonality here is colour of night while the colour of cat is a real challenge to differentiate. Deep learning models are based on Neural network. Using Neural networks with multiple layers helps to do a better prediction. This paper uses Deep learning models to find if it’s a deceptive news or not using models like Simple Neural network SNN and Deep neural network DNN.

Neural Network is a network of neurons. Each Neural Network has 3 layers and they are input layer, hidden layer and output layer as shown in Figure 2. Neural network with one hidden layer is called Simple Neural Network or SNN. Each layer has multiple neurons.

Detecting Fake News Using Deep Learning and NLP

Figure 2. Simple Neural Network

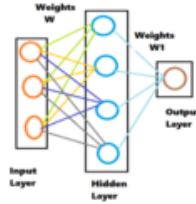
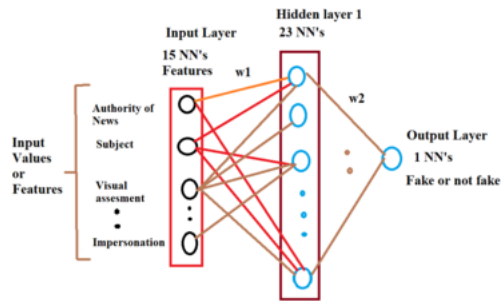


Figure 3. Number of neural networks at each layer of SNN.



At the input layer, it takes input from source and forms a matrix say X . The number of neurons at this layer is equal to number of features or input data as in figure 2. This layer applies weights to each element of matrix (ie., dot product) and represented as $X \cdot W$.

At the hidden layer as in figure 2, it takes $X \cdot W$ from input layer and does some action or processes it using an activation function f . The activation function could be predicting or classifying. There are many types of activation functions like Threshold (binary), Sigmoid (continuous), Rectifier (binary), Hyperbolic Tangent (continuous), SoftMax (Sigmoid for more than 1 output layers) (Michael, 2018). The number of neurons at this layer is 1.5 times the number of features or input values. The function is represented as $F(X \cdot W)$ and the hidden layer applies its weights say $W2$ to $F(X \cdot W)$ which gives matrix Z as output.

Finally at the output layer as in figure 2, it takes Z matrix which is the output of hidden layer and activates some function and gives the final output say Y . It has only 1 neuron as it a classifier in this work, as we predict if news is FAKE or not Fake (Mohamed at. AI., 2019)

This way Neural network or Artificial Neural network ANN can have one or more hidden layers which is respectively called SNN and DNN models. These models demand excessive computing power as it handles more computations at each layer, accordingly we need to use GPU instead of CPU especially for very large dataset.

Figure 4. Algorithm for SNN



There are 15 features of input data used to predict if the news is FAKE or NOT FAKE. The Neural network needs 15 NN at input layer, while 23 NNs at hidden layer and 1 NN at output layer as shown in Figure 3.

a. Simple neural networks

Simple neural networks or SNN are learning any nonlinear function as in Figure 2. These learn weights and maps any input to an output value. SNN has an activation functions to help learn any complex relationship between input and output values. It is during a feed forward propagation the inputs are processed. This process continues until the accuracy is reached or when the max number of iterations is reached. Then we do a testing on the model (Oshikawa et. al.,2020)

SNN Algorithm

The training phase is followed by testing phase to generate the model fit. There is a feed forward and backward propagation in SNN. The forward feed propagation executes activation functions while the backward propagation adjusts the weights. Divide the data set into 80% for training phase and 20% of dataset for testing phase.

The SNN algorithm uses input features and apply weights to it. The output of input layer goes to the hidden layer. At the hidden layer where weights are applied to the input arriving at the hidden layer and many activation functions are used as the input is processed. The output of hidden layer then goes to the output layer of

Detecting Fake News Using Deep Learning and NLP

SNN. At the output layer the news considered is classified as Fake or not. There are 15 input features used by SNN as shown in figure 3. The SNN algorithm as shown in figure 4.

b. Deep Neural Networks, DNN

Deep Neural Networks are very similar to ordinary Neural Networks as they are also made up of neurons that have learnable weights and biases (Grégoire, 2018). A DNN has a single input layer, more than one hidden layer and an output layer. Though many hidden layers can be used but only 2 hidden layers are used in this model as shown figure 5. The figure 6 shows the numbers of neurons in each layer in this Fake news detection work.

Figure 5. Deep Neural networks

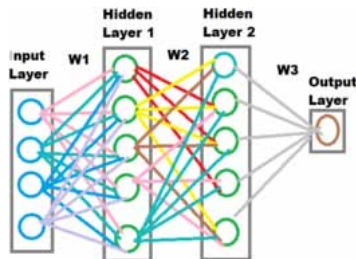
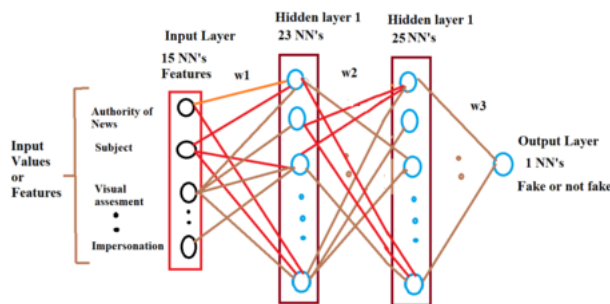


Figure 6. Number of neural networks at each layer of DNN.



DNN Algorithm

The training phase is followed by testing phase to generate the model fit. There is a feed forward and a backward propagation as well. The feed propagation executes

activation functions while the backward propagation adjusts the weights. The dataset is divided as 80% for training phase and 20% of dataset for testing phase.

The DNN algorithm uses input features and applies weights to it. The output of input layer goes to the hidden layer1. The hidden layer1 then applies its weights to the input arriving at the hidden layer1 and using many we activation functions while processing the input. The output of hidden layer1 then goes to the hidden layer2 and same happens as in hidden layer1 (Grégoire, 2018) (Crescenzio, 2015). Now output of hidden layer2 goes to output layer of DNN. At the output layer the news considered is classified as Fake or not. The algorithm for DNN is as in figure 7.

Figure 7. Algorithm for DNN



Results

The two deep learning models SNN and DNN using the same data sets are as follows. The results of each model predicting if the news is Fake or not is discussed .

We compute the training accuracy and test accuracy of both models for each dataset taken and tabulate the results.

The size of dataset taken and the model is as follows:

Case 1. Dataset has 7 rows of data as shown in figure 8.

Figure 8. Dataset for case 1.

Detecting Fake News Using Deep Learning and NLP

The figure 8 shows green colored text used for training which is 80% of dataset and red colored text used for testing which is 20% of dataset.

Table 1.

MODELS	Training accuracy % obtained	Test accuracy % obtained
SNN	100	1 out of 2 rows correct = 50%
DNN	100	1 out of 2 rows correct = 50%

Results of SNN and DNN models for above dataset are tabulated as follows:

Figure 9. Dataset for case 2.

Case 2. Dataset has 10 rows of data as in figure 9.

Table 2.

MODELS	Training accuracy % obtained	Test accuracy % obtained
SNN	100	1 out of 2 rows correct = 50%
DNN	100	1 out of 2 rows correct = 50%

Figure 10. Dataset for case 3.

The figure 9 shows green colored text used for training which is 80% of dataset and red colored text used for testing which is 20% of dataset.

Results of SNN and DNN models for above dataset are tabulated as follows:

Case 3. Dataset has 14 rows of data as shown figure 10.

The figure 10 shows green colored text used for training which is 80% of dataset and red colored text used for testing which is 20% of dataset.

Results of SNN and DNN models for above dataset are tabulated as follows:

Table 3.

MODELS	Training accuracy % obtained	Test accuracy % obtained
SNN	100	3 out of 3 rows correct = 50%
DNN	100	3 out of 3 rows correct = 50%

The work shows that SNN had 100% training accuracy and when tested it gave 100% accuracy as in case 3. While the DNN touched a 100% accuracy during training and its test accuracy was 100% as well as in case 3. So conclusion is that as the dataset size is increased the model's prediction with higher accuracy was obtained. This work highlights that both models SNN and DNN could be used, as 100% test accuracy is obtained in both models. The inference is that SNN would be better than DNN model. Its that SNN has one hidden layer therefore less number of computations as compared to DNN which has 2 hidden layer and conclusion is SNN would be the Model Fit that could be deployed in the application.

CONCLUSION

The news that people consume from various sources of media need to be scrutinized for fake or not. The impact of Fake news is costing peace and harmony of society, community as well. In this paper we explored the basics of all features that are needed to determine a fake news and second part was to benchmark a data set which meets the features needed. A raw data was obtained from web using web scrapping techniques. Then a feature matrix was created by extracting features from raw data using NLP and LSTM. The models used this feature matrix to train the model with labelled targets. There were two models Simple neural network and Deep neural network used. The results of training accuracy and testing accuracy suggested

Detecting Fake News Using Deep Learning and NLP

that SNN and DNN are equally having higher accuracy, but considering number of hidden layers, the number of computations involved in the hidden layers which could be expensive when very large dataset is used suggests that SNN would be better than DNN.

FUTURE WORK

This basic work in future will be extended to improve the dataset and implement other models of deep learning. Work will find out better metrics that would be adopted to improve the quality of datasets as they are the basics for obtaining a higher test accuracy. The work would also be extended to try different models like Convolution neural networks, Reinforcement neural networks and others as well to improve the training and test accuracy of predicting a news if a fake or not.

REFERENCES

- Allan, B., Gareth, O. R., Jeffrey, S. R., & Panayiotis, T. (2001, April). Finding Authorities and Hubs From Link Structures on the World Wide Web. *Proceedings of the 10th international conference on WWW*, 415-429.
- Allcott, H., & Gentzkow, M. (2017, May). Social media and fake news in the 2016 election. *The Journal of Economic Perspectives*, 31(2), 211–236. doi:10.1257/jep.31.2.211
- Botafogo, R., Rivlin, E., & Shneiderman, B. (1992). Structural analysis of hypertext: Identifying hierarchies and useful metrics. *ACM Transactions on Information Systems*, 10, 142–180. doi:10.1145/146802.146826
- Gallo. (2015, Jan). Artificial Neural Networks: tutorial. In *Encyclopedia of Information Science and Technology* (3rd ed.). IGI Global.
- Dataflair. (2020). *Advanced Python Project – Detecting Fake News with Python*. <https://data-flair.training/blogs/advanced-python-project-detecting-fake-news>
- Grégoire, M., Wojciech, S., & Klaus-Robert, M. (2018, February). Methods for interpreting and understanding deep neural networks. *Digital Signal Processing*, 73, 1–15. doi:10.1016/j.dsp.2017.10.011
- Jakub, N., Ahmet, T., & Rafal, S. (2017, May). LSTM Recurrent Neural Networks for Short Text and Sentiment Classification. *International Conference on Artificial Intelligence and Soft Computing CAISC 2017*, 553-562.

- Jason, B. (2017). *Datasets in NLP*. <https://machinelearningmastery.com/datasets-natural-language-processing/>
- Jiahao, W. (2019). *NLP Text Preprocessing: A Practical Guide and Template*. <https://towardsdatascience.com/nlp-text-preprocessing-a-practical-guide-and-template-d80874676e79>
- Kim, A., & Dennis, A. R. (2018). Says who? The effects of presentation format and source rating on fake news in social media. *Proceedings of the 51st Hawaii International Conference on System Sciences*. 10.24251/HICSS.2018.497
- Shu, K., Sliva, A., Wang, S., Tang, J., & Liu, H. (2017, September). Fake News Detection on Social Media: A Data Mining Perspective. *SIGKDD Explorations*, 19(1), 22–36. doi:10.1145/3137597.3137600
- Kotteti, C. M. M., Dong, X., Li, N., & Qian, L. (2018). Fake news detection enhancement with data imputation. *IEEE 16th Int. Conf. on Dependable Autonomic and Secure Comp.*, 187-192.
- Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., Metzger, M. J., Nyhan, B., Pennycook, G., Rothschild, D., Schudson, M., Sloman, S. A., Sunstein, C. R., Thorson, E. A., Watts, D. J., & Zittrain, J. L. (2018, March). The science of fake news. *Science*, 359(6380), 1094–1096. doi:10.1126/science.aao2998 PMID:29590025
- Leskovec, J., Rajaraman, A., & Ullman, J.D. (2016). *Mining of Massive Datasets* (2nd ed.). Cambridge University Press.
- Kantardzic, M. (2011). *Data Mining: Concepts, Models, Methods, and Algorithms*. Wiley publishers, IEEE press. doi:10.1002/9781118029145
- Ali, M. (2019, July). *The 25 Best Datasets for Natural Language Processing*. <https://lionbridge.ai/datasets/the-best-25-datasets-for-natural-language-processing/>
- Michael, J. G. (2018). *How to Create a Simple Neural Network in Python*. <https://www.kdnuggets.com/2018/10/simple-neural-network-python.html>
- Elhadad, Li, & Gebali. (2019). Fake News Detection on Social Media: A Systematic Survey. *Communications Computers and Signal Processing (PACRIM) IEEE Pacific Rim Conference on*, 1-8.
- Murphy, M. (2017). Study: Fake news hits the workplace. *Leadership IQ*. <https://www.leadershipiq.com/blogs/leadershipiq/study-fake-news-hits-the-workplace>

Detecting Fake News Using Deep Learning and NLP

Oshikawa, R., Qian, J., & Wang, W. Y. (2020). A survey on natural language processing for fake news detection. *Proceedings of the 12th Conference on Language Resources and Evaluation (LREC 2020)*, 6086–6093.

Raluca, T., & Remus, R. (n.d.). *HITS Algorithm - Hubs and Authorities on the internet*. <http://pi.math.cornell.edu/~mec/Winter2009/RalucaRemus/Lecture4/lecture4.html>

Schetinger, V., & Manuel, M. O. (2017). Humans Are Easily Fooled by Digital Images. *Computers & Graphics*, 70, 142–151. doi:10.1016/j.cag.2017.08.010

Gupta, S., Thirukovalluru, R., Sinha, M., & Mannarswamy, S. (2018). CIMTDetect: A Community Infused Matrix-Tensor Coupled Factorization Based Method for Fake News Detection. *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*. 10.1109/ASONAM.2018.8508408

Sophie, Wade, & Watson. (2017, July). Can people identify original and manipulated photos of real-world scenes? *Cognitive Research: Principles and Implications*, 30.

Traylor, T., Straub, J., & Snell, N. (2019). Classifying fake news articles using natural language processing to identify in-article attribution as a supervised learning estimator. *IEEE 13th Int. Conf. on Semantic Comp.*, 445–449.

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146–1151.


Wallace, S. (2013). Impartiality in the news. In *Journalism: New Challenges*. CJCR: Centre for Journalism & Communication Research, Bournemouth University.

Wondflow. (2019). *Natural Language processing examples*. <https://www.wonderflow.co/blog/natural-language-processing-examples>

Chapter 8

Impediments in Mobile Forensics

Vani Thangapandian

 <https://orcid.org/0000-0001-5928-7331>

R. V. Government College, University of Madras, India

ABSTRACT

In this digital era, the usage of mobile phones in daily life has become inextricable due to the facilities and the level of sophistication it offers. Proportionately, the crimes and offenses involving the mobile devices are growing in rapid speed. Whenever a crime occurs in a spot, the forensic team will arrive there to identify and locate the evidence of the criminals. If the crime involves digital equipment like computers and laptop, then digital forensic team will investigate and analyze the devices for digital evidence collection. These days, mobile phones have the capability to offer any kind of information and services digitally on top of the palm of the user. Anything is available on the hands with a single touch on the screen of the mobile devices. It also offers to the adversaries many digital services which are harmful to the societies. The fast-paced advancement in the digital front paves the way for many digital crimes. Hence, a new field, mobile forensics, emerges out to trace the evidence, but it faces many challenges due to the dynamic nature of the digital technologies.

INTRODUCTION

The mobile devices are ubiquitous in nature due to its abundant availability in the market. The mobile device is an umbrella term that comprises of Smartphones, Tablets, Handheld devices, Drones, and other wearable devices. The device has

DOI: 10.4018/978-1-7998-4900-1.ch008

Impediments in Mobile Forensics

faced exponential growth since the past decades, both in technological and usage in personal space. The data stored in these devices also proportionately grow along with the technological outburst. Since the device is intertwined with the everyday life of a common man, it attracts many evils to the owner of the device and evidently to the society in the form of cyber attacks, cybercrimes, and other forms of criminal activities. It paves the way to Mobile Forensics, the new branch of Cyber Forensics. Mobile forensics is a multidisciplinary field which comprises of Computer Science, criminology, and Cyber Forensics. This field applies the strategies and procedures for evidence collection, which are useful for law enforcement people. Unlike digital forensics, mobile forensics faces many hardships due to the dynamic nature and exponential growth of the underlying technology. The following sections elaborate on the various factors due to which the mobile forensics process becomes a challenging one.

BACKGROUND

In this paper, the author (Sundar Krishnan, 2019) discusses smartphone devices' extensive use, the transmission of enormous volumes of data, and the difficulty in extracting digital evidence. They outlined the constraints and difficulties while dealing with the devices (Krishnan S., 2014) discusses the legal challenges in retrieving the data from the apps connected with cloud storage. The author (James J. I., 2013) lists out the challenges in forensic automation. The author (Harichandran, 2015) conducted a survey on tools/technology for the improvement of mobile forensics. The authors (Irons A. D., 2009) discussed giving training to the respective investigators by emphasizing the importance of digital pieces of evidence. The authors (James J. I., 2013) described the existing integrated set of tool and their shortcomings.

SOURCES OF EVIDENCE FOR MOBILE FORENSICS

The mobile devices are flooded with information due to the availability of enhanced memory devices with huge storage capacity. The valuable evidence can be found in the form of the following data: Contacts list, Documents, Messages (SMS, MMS, and Email), History (Browsing and Call), Locations Details (GPS and Maps), Apps Usage (Social Media Apps, personal Apps, etc.), Reminders (Calendar and sticky notes), Data collection (Photos, Videos, and Music files), Audio files (Voice mail and other recordings), Deleted Text messages, etc.

Among these data, the browsing history, last dialed call history, and location details are of the most important and commonly acquired data. Some of the data

will be stored in ROM, and some of them are stored in the SIM module. The data stored in the SIM module are very useful and sensitive in the inspection point of view. The prime notion of an investigator is to retrieve these data without any modification, which is very tedious. Because it involves many difficult factors such as accidental reset of the device, secure wiping, accidental loss of data during the transit, obfuscation of data, falsified data dynamic nature of data, data hiding, data overwriting, etc. Some data may be erased due to the volatile nature of the memory. These kinds of data need to be recovered with utmost care before the device restarts.

The UICC (Universal Integrated Circuit Card) component must be carefully removed from the device to recover the deleted text messages. Then the device can be connected with a PC or Laptop through a card reader for the recovery of deleted messages. However, the removal of the UICC component may result in the loss of data stored in the volatile memory. HexDump method can be used for the recovery of deleted text messages. However, it involves a lengthy procedure to establish the connection interface between the mobile device and the forensic workstation.

MOBILE FORENSICS PROCESS

At the prime level, Mobile Forensics encompasses the major processes of Cyber Forensics such as Data Acquisition, Identification, Evaluation, and Report Generation. It starts with the mobile Device's Seizures as the start-up process, and it follows both invasive and non-invasive methods for data acquisition from the seized device. Among the major processes, data acquisition is the hardest process in Mobile Forensics as this field faces many impediments due to the following factors.

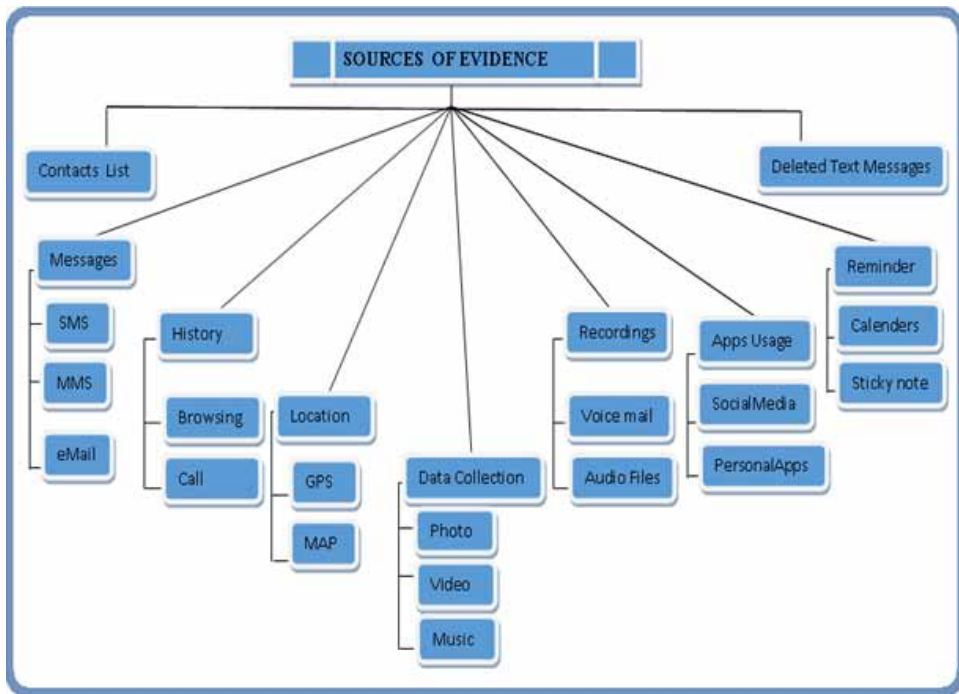
MOBILE DEVICE ARCHITECTURE

The basic components for a mobile device include a microprocessor, memory (ROM, RAM), Digital signal processor, Screen (LCD), radio device, one speaker with a microphone, and a set of keys with interfaces. There is no generic architecture for mobile devices, and each manufacturer comes with a unique set of digital components for their mobile device. The variations can be in any component, such as processor variants, memory chips, and communication modules. Some devices come with additional facilities such as expandable memory slots, replaceable battery devices, camera functionalities, a touch-sensitive screen, cell interface for supporting high-speed data, etc. Each variation needs a customized operating system, and hence the manufacturer prefers a unique operating system for their devices. The functionalities of the device vary depending on the operating system. This diverse nature poses a

Impediments in Mobile Forensics

big challenge to the forensic investigation as the investigator needs to learn about the range of products and the respective operating system's working fashion.

Figure 1. Sources of Evidential data



IMPEDIMENTS

I. Existence of Preconditions

As the forensics study is severely device dependent in Mobile forensics, the investigator must prepare a strategy appropriate to the seized device based on a correct methodology and guidelines. Before beginning the process, the device must be secured in a wireless preservation container or a Faraday Bag to preserve its data. If the device is connected in wireless mode with the internet, the data may be modified or erased by remote swiping technique. In some cases, the connectivity may leak sensitive data like location information to the adversary people. This device is isolated in a wireless preserving container to avoid all these circumstances.

II. Data is a Big Deterrent in Mobile Forensics

The data stored in the mobile device plays big havoc in Mobile Forensics. Inside the mobile device, the storage component exists in two locations: the UICC module and the Mobile Equipment component. The data may be residing either of these locations or in both. The data residing inside the UICC module include PIN (Personal Identification Number), PUK (PIN Unlocking Key), and LND (Last Numbers Dialed) and other authentication details of the subscriber. It is very hard to retrieve these data as they are encrypted using cipher Encryption Algorithms. Inside the memory component of UICC, the data is stored in a hierarchical organization, which is composed of standard and non-standard files. The standard file includes one Root or Master file, a set of Directory files, and several Elementary data files under each Directory file. The non-standard file maintains the details of the network operators and their services. Recovering these data is a big challenge due to the following reasons.

1. To manage the data in a mobile device is a big challenge as the data is also in mobile status.
2. In a mobile device, the data is constantly uploaded or downloaded over a particular instance of time, leading to loss of evidential data.
3. Nowadays, the mobile device comes with a high-end storage facility. So the device is exploded with the data stream. For example, the data stored in a 65 GB mobile device will consume almost 33500 reams of paper to be printed. To analyze such tremendous volumes of data will be time-consuming.
4. In smartphones, there is no standard location specified for storing the data. The data may be stored in any location, including volatile or non-volatile memory. The choice of location differs from version to versions of OS.
5. The data acquisition process is dependent on the design of the device.
6. The data acquisition gets tougher with a wide variety of hardware pieces of equipment for mobile devices.
7. Data preservation is also a difficult task as a technology outburst.
8. Data is dynamic in nature, and hence the data capturing accuracy is questionable.
9. There is no standard format for storing the data in Mobile devices. Hence different strategies need to be created for each format.

III. Risks in Network isolation

1. If the mobile device is shut down when captured, there is a serious risk of deleting data stored in the device's volatile memory. Hence, the Mobile Device

Impediments in Mobile Forensics

must not be shut down to prevent accidental deletion of evidential data once seized in the crime spot.

2. If the battery backup is very low, the device must be connected immediately with charging to keep the device in switched ON state. Because switching off, the device may create authentication issues and block access rights.
3. The Airplane mode must be activated in the device to disconnect the device from the networks.
4. The other networking fidelities like WIFI, GPS, and HotSpot must be switched off. If it is not turned off, some undesirable effects may occur, such as the investigators' locations details may be shared with the criminals. This may lead to the remote wiping of the sensitive data in the seized mobile Device.

IV. Safety and Security Mechanisms

There are inbuilt security mechanisms provided by the operating device for each mobile device. The mechanisms may be a software-based or hardware-based process. The software locks include pattern matching, password, passcode, SIM PIN, PUK, etc. The hardware locks include biometric locks such as fingerprint, iris lock, and face lock. All these security mechanisms undergo the encryption process for strong authentication support. Hence they are very difficult to crack. Some security mechanisms restrict time limits for the number of attempts, beyond which it goes permanently locked. So the mobile forensics investigator has to be very careful while unlocking the device. The following are some of the characteristics of security features.

1. Built-in security features are strong nowadays, such that any attempt to recovery may wipe out the data from the device.
2. The handset lock, SIM PIN, and PUK lock depend on the model of the device.
3. The handset lock is automatically activated when the device is in power-on state.
4. In GSM phones, the SIM has a small non-volatile memory with a lightweight processor chip. The chip is mainly for manipulation of the data in chip memory.

V. Software Constraints

The rapid development of various mobile devices paves the way for the release of numerous operating systems. The functionalities of all the mobile operating systems are similar. They differ in nature as per the hardware equipment they are written for implementation. They mainly depend on the size and type of storage devices, processors, and the security mechanisms incorporated in the devices. This aspect is

tough for executing a mobile forensic process as each process needs to be device-dependent. New update patches have to be released whenever there is a change in the security policies and mechanisms. The forensics strategy has to be modified based on these updates, which is very difficult for the investigators.

The user data and the application data are mostly stored in the SQLite databases in an encrypted form. To retrieve these data, the investigator has to decrypt the data from the databases. For this, the investigator must have good exposure to SQLite database functionalities. Only a smaller number of mobile applications store their data in such databases. Many applications never use the SQLite database to store their data, which will be a challenge for performing forensics. These applications and the Operating System and Cloud Storage for storing their data are more beneficial in unexpected situations such as device theft, accidental deletion of data, or broken device. It is very challenging to get the data from the cloud both in legal and technical aspects. The following are the factors that affect the forensics process.

1. The Operating Systems of smartphones are closed source systems.
2. The mobile Device Operating System vendors periodically release OS updates, making the forensic investigation a very challenging one with the existing tools.
3. Many social networking applications are accessible through computers as well as mobile devices. When it comes to mobile devices, the lightweight versions of the applications are used due to the hardware constraints. Hence the evidence collection is limited in smartphones.
4. The single forensic tool may not be sufficient for the comprehensive investigation of mobile devices, and also the collection of tools are needed for investigating a particular model. This collection cannot be used for all models.

VI. Hardware Constraints

The mobile forensics process starts with identifying the mobile device, whether it is a very old device or a damaged condition. If the device is very old, then the connecting devices must be acquired appropriate to the making year of the device, because the latest tools are not backward compatible now a day. If the device is in damaged condition, then the interface will not be functioning. In such cases, only MicroRead and ChipOFF level data extractions are possible.

If the device is good condition, then the type and make of the device must be identified. A mobile device's hardware components are diverse in type and model, as several manufacturers are mushrooming every day. So, the investigator must identify the model and type of device before beginning the forensics process. However, it is very hard to study the device by simply looking at the device. The device details can

Impediments in Mobile Forensics

be obtained from the menu of the settings of the phone. The device must be opened to get the details, which is not easy if it is locked. Then the Device unlocking mechanisms should be employed to bypass the security mechanisms. Another method to get the details of the device is to remove the UICC component from the device. The UICC component is located behind the battery to avoid unwanted removal. However, the risk in removing UICC is that the sensitive data in the volatile memory will be lost.

Many Mobile forensic toolkits are available to offer the identification facility. These toolkits are installed in a work station, and the respective device must be connected with the work station with appropriate connectors. If the physical connectivity is not possible, then wireless connectivity options such as Bluetooth, WiFi, IR can be employed. However, the wireless connection may lead to the sharing of location details to the adversary, which is part of the security mechanism implemented in the device. The following are hardware related factors that pose a threat to the mobile forensics process.

1. The exponential growth of diversified mobile devices is a big threat to the forensics investigation.
2. The forensic tools are depending on the model of the mobile device. As the specification varies, the tools have to be redesigned to accommodate the variation.
3. Smartphones are always in active mode; hence the data keeps on flowing in and out of the device.
4. Switching off the device may lead to the loss of data in volatile memory.
5. A variety of hardware is used in smartphones. So hardware knowledge is very much essential for the investigator.
6. There are several mobile device manufacturers mushrooming day by day.
7. Power and data connectors
8. There are different designs of power connectors for consuming the same power.
9. The mobile data is stored in volatile memory locations; the power drain leads to loss of shreds of evidence.

VII. Types of Carrier and Service Provider

Different types of data carriers and service providers are in existence with a different set of protocols and mechanisms. Initially, there are two types of cellular networks: GSM-based networks and CDMA based networks. In GSM-based networks, the UICC module is used for the authentication of the subscribers. In CDMA based networks, the UICC module is not present; instead, similar functionality is directly implemented into the device. The subsequent version of the CDMA system comes with an additional component CSIM (CDMA subscriber Identity Module) for

incorporating the UICC module. In recent days, the cellular systems support LTE and VOLTE functionalities to provide higher data and voice transmission rates. The forensic investigation strategy must be designed according to these protocols and mechanisms for better investigation results.

Though there are many kinds of technologies, the working organization is the same for all the cellular networks, and a network consists of many components, including RAN (Radio Access Networks), MSC (Mobile Switching Centers), RNC (Radio Network Controllers), and several nodes. The RNC and the nodes are collectively referred to as RNA. MSC maintains RNC's for network registration, call handing over, routing services, and location maintenance. The MSC controls these operations using many databases, namely HLR (Home Location Register), VLR (Visitor Location Register). The MSC stores the CDR (Call Detail Records) and SAD (Subscribers Account Data) in these registers. The CDR and SAD are very useful evidence for a crime scene investigation.

VIII. Technological Barriers

Mobile Forensics is an interdisciplinary field encompassing many fields such as Cloud Computing, Machine Learning, Artificial Intelligence, and Digital Forensics. Both Machine Learning and Mobile Forensics are in their infant stages. A long way to go against cyber threats is to become easy targets for cyber crimes and other unwanted activities.

IX. Admissibility of Electronic Evidence

The evidence gathered in the process of mobile forensics faces a challenge in legal aspects also. As the electronic evidence is prone to be hampered, it may lead to the falsification of evidence. In India, the Supreme Court refines the existing Indian Evidence Act with many amendments to accept electronic evidence under some mandatory compliance (Section 65B). This aspect will pose a big challenge for presenting the electronic evidence acquired during the mobile forensics process.

X. Design of Forensic Tool Kit

The design of an appropriate forensic tool is in the infant stage today due to the fast-paced technological advancements in mobile hardware and mobile software. The tool has to be selected for forensics based on many important factors like the device's model, the device's release date, the type of operating system used in the device, the locking mechanism. A single tool cannot be applied for comprehensive forensic analysis. Many factors affect the outcome of the mobile forensics process.

Impediments in Mobile Forensics

They depend on the type of device, application, the operating system implemented in the device, and the hardware components. The mobile forensic tool must be designed as an integrated tool to overcome the above-listed impediments.

CONCLUSION

Mobile Forensics attracts threats from all the directions ranging from software to hardware. It faces many challenges and hurdles to come up with valid evidence acceptable by the society and legal systems. The mobile forensics field has to overcome all the above barriers to emerge as a prominent field. The Investigating Officer must undergo continuous learning and training as new technological advancements are growing exponentially.

ACKNOWLEDGMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

- Dubey, V. (2017). *Admissibility of electronic evidence: an Indian perspective*. Forensic Research & Criminology International Journal.
- Harichandran, V. (2015). A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. *Computers & Security*.
- Irons, A. D., Stephens, P., & Ferguson, R. I. (2009). Digital Investigation as a distinct discipline: A pedagogic perspective. *Digital Investigation*, 6(1-2), 82–90. doi:10.1016/j.diin.2009.05.002
- James, J. I. (2013). *G. P. Challenges with Automation in Digital Forensic Investigations*.
- Krishnan, S. C. L. (2014). Legal Concerns and Challenges in Cloud Computing. *2nd International Symposium on Digital Forensics and Security (ISDFS 2014)*.
- Mellars, B. (2004). Forensic Examination of Mobile Phones. Digital Investigation. *The International Journal of Digital Forensics & Incident Response*, 1(4), 266–272.

Rizwan Ahmed, R. V. (2005). *Mobile Forensics: an Overview, Tools, Future trends and Challenges from Law Enforcement perspective*. Emerging Technologies in E-Government.

Sundar Krishnan, B. Z. (2019). Smartphone Forensic Challenges. *International Journal of Computer Science and Security*, 13(5).

Tejas Karia, A. A. (2015). The Supreme Court of India re-defines admissibility of electronic evidence in India. *Digital Evidence and Electronic Signature Law Review*, (12), 37.

KEY TERMS AND DEFINITIONS

Faraday Bag: A *Faraday Bag* or *Faraday Shield* is a closed container which is used to avoid the signals to go out or come inside. A Faraday shield is made up of conducting materials and it is named after its inventor Michael Faraday. Generally this bag is used for preventing from data theft and data leakage by blocking the signals from WiFi, Bluetooth and other radio signals.

HexDump: A *HexDump* is one of the Forensic methods used for the extraction of raw information stored in the flash memory of the device.

Chapter 9

Use–Case of Blockchain in Cybercrime and Cyberattack

Karthika Veeramani

 <https://orcid.org/0000-0002-0711-1745>

Sri Sivasubramaniya Nadar College of Engineering, India

Suresh Jaganathan

Sri Sivasubramaniya Nadar College of Engineering, India

ABSTRACT

Cybercrime involves unlawful activities done by the individual in cyberspace using the internet. It is cyberbullying, financial theft, code-hack, cryptojacking, hacking, etc. The main difference between cybercrime and cyberattack is that cybercrime victims are humans. The crime associated with the latter is that of a computer network, hardware or software. Cyberattack activities include ransomware, viruses, worms, SQL injection, DDoS attacks, and government and corporate are potential targets. Cyber security provides a specialised approach to the protection of computer systems from cybercrimes and cyberattacks. As of now, no cyber defence is 100% safe. What is considered safe today may not be secure tomorrow. Blockchain enables a new way of recording transactions or any other digital interaction within the network with security, transparency, integrity, confidentiality, availability, and traceability. This chapter explains in detail about cyber risks and how blockchain can be used to avoid risks in financial and insurance frauds.

DOI: 10.4018/978-1-7998-4900-1.ch009

INTRODUCTION

Cyber Crime (Broadhurst & Chang, 2012) makes use of digital technologies in committing a crime. In other words, the latest techniques with the application of internet access private data through unlawful activity and thereby doing a crime. It includes attacks on data center, child pornography, financial and e-Commerce data. Cybersecurity (Ahmad, 2019) prevents cybercrime with cryptographic techniques, virtual private networks(VPN) and firewall. VPN provides a means to access personal information over public network internet. Cybercrime broadly classified into three groups.

1. Crime against individuals, such as Computer Vandalism, transmitting a virus, unauthorised access/control over a computer system (Chattopadhyay & Mitra, 2018, 2020), intellectual property thefts.
2. Crime against an organisation, such as unauthorised access to its computer, cyber terrorism on the government, spreading illegal information (Chelliah et al., 2019) and usage of pirated software.
3. Crime against society, such as uploading child pornography, indecent activities in the public places, sale of banned articles and gambling online.

Common Types of Cyberattacks

1. Denial of service (DoS) and distributed denial of service (DDoS) attacks: These attacks overwhelm the system resources, thereby prevents it from servicing the request. It dramatically reduces the system ability to respond to the service request. Some of Dos and DDoS includes Transmission Control Protocol (TCP), synchronous (SYN) flooding or SYN attack, Ping-of-death attack (PoD) or long ICMP attack, Smurf attack, Botnets or bots and Teardrop attack.
2. Man-in-the-middle attack: A malicious actor eavesdrops the conversation between sender and receiver and then access information that they are trying to send one another. The attacker sends and receives data meant for someone else without the sender and receiver knowing until it is too late. He works to fork the TCP connection into two connections, one is between the sender and attacker, and the other is between attacker and receiver.
 - a. IP spoofing attack: The attacker modifies the IP address field on a packet with a fake address instead of the sender's correct IP address.
 - b. Replay attack or playback attack: The attacker catches and preserves past communications, and then he attempts to repeat or delay it.

Use-Case of Blockchain in Cybercrime and Cyberattack

3. Phishing attack: The attacker sends malicious emails pretending that it comes from the trusted source.
 - a. Spear phishing attack: It is similar to a phishing attack where an attacker uses email spoofing or cloned websites.
4. Drive-by download attack: This attack installs spyware, adware, malware and even an unwanted program that are not of interest to the end-user.
5. Password attack or password cracking: This attack aims to steal the user's password and relevant login credentials and also called a brute force attack or cracking.
6. Structured Query Language (SQL) injection attack: Attacks on database-driven sites.
7. Cross-site scripting (XSS) attack: This attack embeds malicious code into the script of a genuine website to get information of users in that site.
8. Eavesdropping attack: Listens to others conversation by intercepting the communication link between them without being identified. There are two types of eavesdropping attack, namely passive and active.
9. Birthday attacks: Cryptographic cyber-attacks that are done against hash algorithms used for verifying the integrity of a message.
10. Malware attack: An unwanted software is being installed on the victim's computer without his/her consent. Though the effects of the malware may not be immediate, it ends in bringing harm to the victim's computer. Some malware includes macro virus, file injector virus, system infectors, stealth virus, polymorphic virus, trojan horse, ransomware, spyware and worm.

Blockchain

A blockchain is a distributed decentralized ledger (Karthika & Jaganathan, 2019) that records all the transactions that take place on the peer to peer network. It provides an immutable source of truth that can be accessed by users in the network. In simple words, it is a one way linked list of groups of transactions. It offers greater transparency by making the ledger available to anyone in the network. The users are identified with their public key, and hence they stay anonymous in the blockchain network. The transactions within the Blockchain cannot tamper as it links with the hash value of the forthcoming blocks. For example, if a hacker wants to tamper a transaction in the n^{th} block, he has to persuade all the successive blocks in Blockchain to change the hash value. Hence, immutability is one such major security feature of blockchain technology. There are two types of Blockchain, such as public Blockchain and private Blockchain.

- **Public Blockchain:** Anyone can connect to the public Blockchain with no access restrictions. It offers incentives for those who secure the Blockchain by correctly adding the blocks to it. Bitcoin and Ethereum are the most known public blockchains.
- **Private Blockchain:** Only the administrator has the right to add the user to the private Blockchain with access restrictions. Both the participant and validator access are restricted. Hyperledger fabric is the most known private Blockchain.

BACKGROUND: CYBERSECURITY TECHNOLOGIES

Cyber Security technologies deal with protecting computer systems and preventing illegal access to data. It protects hardware, software, networks and its data. It is mandatory for any computer system or network to have cybersecurity technology where sensitive information is being stored and transferred. As no cybersecurity technology is foolproof, there is a need to identify and adopt new technologies to strengthen cybersecurity steadily. Some of the existing cybersecurity technologies include Machine Learning and Deep Learning, Behavioral Analytics, Embedded Hardware Authentication and Zero-Trust Model.

Machine Learning and Deep Learning

Machine learning plays a vital part to provide cybersecurity. It pre-emptively detects cyber threats and strengthens security infrastructure through penetration testing, real-time cybercrime mapping and pattern detection. Moreover, Deep learning helps in analysing data such as transaction, real-time communications and logs to identify threats or unwarranted activities.

Cyber-attack named “WannaCry” attacked nearly 2 lakh computers over 150 countries in May 2017. It encrypts the files on the computer and makes them unreadable. The target of the attack was to acquire special decryption software. Another attack called “ransomware” targets individuals and large organisations, including the U.K.’s National Health Service, Spanish telecom giant Telefonica, Chinese schools, U.S.-based delivery service FedEx, and Russian banks. The total losses of this attack estimate to approximately \$4 billion. There were about 10.5 billion malware attacks in 2018 alone. Humans cannot handle these large volumes of attacks. Machine learning helps in identifying attacks. It applies algorithms on previous datasets and makes a statistical analysis to get assumptions about a computer’s behaviour.

Use-Case of Blockchain in Cybercrime and Cyberattack

Machine Learning can uncover threats and automatically suppress them before they cause severe damage to the system. Microsoft in early 2018 has identified a Trojan malware with its window defender anti-virus software that employs various layers of machine learning to detect recognised threats. Here are some lists of companies that use machine learning to reinforce cybersecurity. These include Microsoft, Chronicle, Splunk, Sqrrl, Blackberry and Demisto. Machine learning in cybersecurity provides solutions for threat detection and response, data protection and application security. The following examples show how machine learning helps in cybersecurity.

- Phishing and spam filtering: ML helps in filtering phishing and spam using classification algorithms, thereby detecting malicious activity with predefined parameters.
- Forensic analysis: Clustering benefits forensic analysis (Karie et al., 2019) where it throws some light on the type of attacks and how data are compromised.
- Incident response and risk management: Association rule learning presents recommendations to mitigate risks and how to respond to incidents.
- Prevention and threat modelling: ML algorithms support to predict fraudulent activity before it evolves into a costly data theft or breach.

Though ML contributes to cybersecurity with its classification and clustering models, it's likely to act maliciously pretending the threat as a normal.

Behavioural Analytics

Behaviour Analysis considers improving advanced cybersecurity technologies. It helps in determining patterns on network activities to identify real-time cyber threats. For example, an unusual rise in data transmission pattern from a specified user could probably indicate a cyber-attack. One of the benefits of using Behaviour Analysis is to detect insider threats. The behavioural analysis finds out the following types of anomalies within an organisation:

- Schedules: A potential threat exists if an employee logs into the network outside his regular working hours. It may trigger further inquiry or needs an extra layer of security.
- Applications: The risks associated with using unauthorised or different application than using a typical application, especially browser may indicate a threat in accessing the network.

- Geography: When an employee logs onto the network from different geological location, it could indicate some risks to cybersecurity.
- Devices: Employee accessing the network from a computer with different machine ID rather than his regular machine ID can be a reason for the alert.

Even though each of the above methods can give details about cyber risks, behaviour analysis becomes more effective when an organisation considers all of these factors concurrently.

Embedded Hardware Authentication

A password/PIN is no longer sufficient to offer foolproof identity verification. It can be stolen by anyone to have illegal access to the system. One of the emerging technologies for confirming a user's identity is embedded hardware authentication. It relies on a dedicated physical device held by an authorised user, offers a way to gain access to the computer system in addition to the password. The device generates a unique key that must be used with the password for user authentication. Intel has launched the Sixth generation vPro Chips, and hardware enabled multifactor authentication solution, designed to establish identity protection. Intel Authenticate tries to address the issue of data breaches originating from stolen user credentials with the help of new security technology. It checks identity by combining three factors such as personal identification number, mobile phone and fingerprint. One issue with hardware-based authentication is that legitimate users cannot log in to the system if the hardware device is stolen or lost.

Zero-Trust Model

Zero Trust cybersecurity model does not automatically trust anything inside or outside the network. It must verify everything trying to connect onto the network before granting any access. It allows only authenticated users and devices can access applications and data and also protects it from advanced threats on the internet. Some of the issues when using a zero-trust model for cybersecurity are

- Reduced data compromise and malware propagation
- Lateral movement restriction and hiding in unmanaged network communication pathways.
- Software vulnerability exploits have less impact
- Phished credentials lose value
- Declining deployment of shadow IT

Blockchain Cybersecurity

Blockchain cybersecurity (Piscini et al., 2019; Mathew, 2019) is one of the latest cybersecurity technologies that's gaining attention nowadays. It works based on blockchain technology's decentralized peer-to-peer network concepts (Sowmiya & Poovammal, 2019). Every user in the network holds the responsibility to ensure the authenticity of newly added data. The blockchain technology safeguards the data from attackers with their impenetrable network. Moreover, the application of blockchain with Artificial Intelligence can bring a better system for cyber threat detection.

Blockchain in Cybercrime

The new battle by the companies is cybercrime. Cybercrimes can slither in any business, medical care, university, government, or military system to gather information and record data. Prevention of cyber-crime will be an important priority for financial firms, notably as the volume of data is growing enormously and would be increasingly high in the near future. Distributed ledger technology and artificial intelligence have a great potential to revolutionise the storage and exchange of financial data, and this could be the solution to overcome the risk of cyber-criminality in financial organisations. This technology may not have been fully developed yet, and financial firms will have to snap it up prior to diverse implementation.

Technology alone would never be a remedy for the effective fight against cybercrime; the observation of systems and suspicious activity requires human experience and expertise. But it is critical to overcome cybercrime (Taylor et al., 2019) that the right systems be implemented to manage data most securely and to provide experts with the most effective tools to operate, which is a pending issue for Blockchain.

According to Lone (2019), Digital evidence (Graham & Smith, 2020) plays a vital role in investigating digital crimes due to criminal activities done by the persons. While investigating cybercrimes, extreme care should take for these parameters, i) guarantee integrity, ii) authenticity and iii) auditability of digital evidence (Tian et al., 2019). Blockchain technology assures capability for enabling a secured and transparency of transactions (events/actions). According to Lone (2019), cyber forensics should implement this technology for these reasons, i) improved transactional efficiency, ii) the reduction of fraud, and iii) reduced costs of transactions due to increased transparency and absence of third-party validation. Below are some of the promising use cases of Blockchain Technology in Cyber Forensic (Gopalan et al., 2019) and how the department of cybercrime wing collaborates for betterment in tracking, monitoring and capturing the cybercriminals.

1. Digital Forensics Chain

Forensic Chain (Lone & Mir, 2019) is a blockchain-based solution to keep and trace digital crimes. Blockchain is a type of data structure that facilitates the creation and storage of transactions done and shares it across all participating peers in a distributed computer network. Blockchain uses cryptography to secure and build an indispensable audit trail to record and store transactions occurring within the network. Forensic-Chain consists of blocks made up of details like location, time-stamp with date, and these details are hashed and recorded in the chain by a smart contract.

2. Hotel Chain

A new product named as HotelChain using Blockchain Technology is developed by a start-up company Zebi for the Department of Law Enforcement, Andhra Pradesh to track criminals and missing persons in that state. It combines Blockchain and AI to store information about hotel guests. HotelChain stores the daily transactions that happened in the hotel and is shared with the local police station. Both the parties (Hotel authorities and Police) get benefited due to reduced paper documents, online data, and less difficult process for legal obligation. Data available in HotelChain can be compared with the police database for finding criminals and any missing persons. Currently, it is implemented in Vishakhapatnam city and is encouraged in other countries, like Japan and Singapore.

CASE STUDY 1: FINANCIAL FRAUDS

Financial fraud (Hyvärinen et al., 2017) occurs when someone denies cash or capital and damages the pre-planned budget employing tricky plans. Individual persons can be misdirected, or other unlawful practices that lead to wholesale fraud or extortion of speculation is also termed as financial fraud. Forthcoming sections give a significant clarification of Financial Frauds and examine how Blockchain Technology helps in forestalling this sort of tricks.

Tax evasion and money related cheats have become the most recent subject of conversation as this has influenced the monetary divisions a ton. Somebody could utilise your data and access your records and complete exchanges. The end client needs to store his insight with the goal that he/she can't be an injured individual for such sort of digital assaults. In the present market, blockchain is an enthusiastically prescribed procedure that assists with checking these defects in the framework and secure the electronic instalments in monetary associations.

Frauds impact association of assorted types and sizes over a broad scope of enterprises and geologies. Results can be immediate, through money related misfortunes, or aberrant, through fines and reputational aftermath. In 2018, firms overall lost more than \$7 billion to inward misrepresentation plans, as per a 2018 Report to Nations by the Association of Certified Fraud Examiners (ACFE) - which broke down 2,600 genuine instances of word related extortion from organisations across 125 regions and 23 ventures. Tending to the danger of misrepresentation is a critical test for all associations.

Types of Financial Fraud in Businesses

Too often, an entrepreneur discovers the point of no return that even the most faithful worker may commit money related frauds. The worker may steal organisation information when circumstances arise or if the worker is in severe monetary problem and needs quick money. The four basic types of financial fraud are:

1. *Misappropriation*, also called robbery, which is the illicit utilisation of assets by an individual who controls those assets. For instance, an accountant may utilise organisation cash for his own needs. Commonly, misappropriation stories don't make it into the paper since specialists are humiliated to such an extent that they decide to keep the undertaking calm. They usually settle secretly with the thief as opposed to confronting open investigation.
2. *Inner robbery*, which is the taking of organisation resources by workers, for example, taking office supplies or items the organisation sells without paying for them. Interior burglary is regularly the guilty party behind stock shrinkage.
3. *Adjustments and payoffs*, which are circumstances in which representatives acknowledge money or different advantages in return for access to the organisation's the same old thing. The employee makes a situation to pay more for the merchandise or items than would generally be appropriate. That additional cash discovers its way into the employee's pocket who encouraged the entrance. As a general rule, settlements and payoffs are a type of pay off, yet not many organisations report or dispute this issue and take severe actions against the committers.
4. *Skimming* is a process performed by the workers by making deceitful receipts and takes cash without making any passage in income book.

Why Fraud Takes Place and How Is It Tackled

An absence of interior oversight joined with a high-pressure workplace gives the perfect conditions to hierarchical extortion to happen. A review by PwC, a worldwide

evaluator, presents that 52% of internal on-screen characters include in such tricks, 24% are from top-level on-screen characters. As indicated by PwC's "Worldwide Economic Crime and Fraud Survey 2018" - which assembled information from 7,200 respondents across 123 unique regions - utilisation of a blockchain-improved framework for data trade may assist with diminishing the dangers and expenses to the notoriety of ranking directors perpetrating misrepresentation. Right now, associations address extortion by building up an implicit rule, drawing in with outer evaluators and giving the position to interior review groups. The utilisation of information observing instruments and examination additionally adds to bring down misfortunes and quicker recognition of misrepresentation cases, as announced by the ACFE. The ACFE report additionally referred to the most well-known technique for starting extortion discovery. It didn't depend on innovation by any stretch of the imagination, however, through worker tips and whistleblowing, speaking to 40% of cases.

If Blockchain technology screens the exchanges and records of the bank, cheats could have been forestalled or identified at the beginning period. Lately, numerous exponential budgetary tricks surfaced out in the open and private banks. As revealed by the Reserve Bank of India, noting an RTI, state-run banks have said upwards of 8,670 "credit extortion" cases totalling nearly thousands of crores throughout the last five monetary years.

Digital tackles and information altering issues have presented extreme dangers. Blockchain is an energetically prescribed procedure to check these ailments. Indeed, according to Juniper Research, \$290 million was put into the improvement of the worldwide blockchain industry in the central portion of 2016. Money related associations were the first to ensure their electronic instalments utilising Blockchain.

Blockchain as a Solution

Blockchain stores the record of transactions that are time-stamped and each block is linked with its previous block by hash pointer. Blockchain innovation gives a close to continuous review trail of data. Along these lines, regardless of whether deceitful action occurs, there is a primary method to distinguish and label the related exchanges. With regards to advanced digital wallets, it is practically challenging to find a fake transaction. The money sent starting with one digital wallet then onto the next can't surpass the sum recorded in the sender's wallet. It is extremely hard for employees in the organization to alter digital records.

For organisations that don't yet deal with direct instalments in digital monetary forms, they can, in any case, influence the advantages of blockchain innovation to disincentivise extortion. For instance, when archiving budget reports, expectations sheets or some other computerised record inclined to alter, put away, traded or crushed, such exercises can be naturally "logged" on a blockchain.

Use-Case of Blockchain in Cybercrime and Cyberattack

The way toward logging these exchanges to open blockchains is known as tying down, where just the hash of that movement is recorded as exchange and kept in a chain. These blockchain exchanges would then be able to be perceptible to anybody, for full open responsibility, or just to those conceded consents to view or access the first documents for assessment, for example, outer evaluators or controllers. At present, it could help to manage fiscal report misrepresentation plans, which include exaggerating resources, incomes and benefits, and downplaying liabilities, costs and misfortunes. Potential fraudsters who know about this discernibility and the lastingness of these records are thus improbable to complete their ideal plans.

Blockchain doesn't comprehend a wide range of extortion, particularly when the exchanges occurring is disconnected. The innovation's primary role is to serve a critical misrepresentation investigator and uprightness implementation to handle genuine issues like degenerate work and altering land records.

How does the Blockchain Technique Help to Fight Fraud?

In Blockchain, the computerised records consolidate into blocks, and such blocks make a chain cryptographically and sequentially interfacing system with one another through cutting edge numerical calculations. Each block has an unusual arrangement of records with an association with the past one. The hashing is performed by 'n' quantities of PCs over the system. Each block registers the equivalent computerised count and has its one of a kind advanced mark. When another block is enrolled, the member gets notice of the equivalent. The data on this block can't be changed or adjusted. The members can just enhance the current old data.

Blockchain For Avoiding Identity Fraud

Character extortion makes a potential hazard to Mastercard organisations and money related establishments. Such organisations become caution and send alarms to their clients if a character misrepresentation happens. Despite strict principles and different consents laid, crooks gain admittance to classified information. Such criminals take essential data and use it without due endorsements. Blockchain has made it conceivable to make a sealed computerised character of people. If all the personality data are placed in a blockchain with consents, just allowed gatherings would have the option to confirm exchanges while approved groups appreciate restricted access.

CASE STUDY 2: INSURANCE FRAUDS

The banking and insurance industries have open arms Blockchain. The insurance industry understands that it needs to remain competitive, thus simplifying processes and meeting the demands of digitally knowledgeable clients. Blockchain technology can help insurance firms overcome the challenges of today and create transparent and credible operations (Raikwar et al., 2018). The authors will outline several of the challenges facing organisations and how Blockchain can mitigate these problems in future, to understand the current insurance industry landscape fully.

Challenges Within the Insurance Industry

Insurance companies face several challenges in the context of complex compliance issues, limited mature market growth, fraudulent claim activity, payment transactions for external parties and the handling of vast quantities of data. Insurers should also develop from the emphasis on compensating for financial losses to physical risk prevention to compete effectively with disruptors by increasing their data visibility. Furthermore, many insurers have asked how to streamline processes and secure sensitive information due to their move to digital transactions. There are growing concerns about the high costs and safety of using digital valets.

Blockchain to the Rescue

Although Blockchain may not be at the end of the day with the insurer's problems, it provides underlying technology which encourages confidence, transparency and stability. However, insurers have already employed a few ways to mitigate the above challenges by using the technology: i) security; (ii) big data; (iii) third-party transactions; (iv) intelligent contracting and (v) reinsurance. But, there are never-ending opportunities and insurance companies and start-ups are exploring fully-fledged technology insurance applications, which includes (i) detection and prevention of fraud, (ii) insurance for property and casualties, (iii) Health and (iv) Reinsurance.

1) Fraud Detection and Risk Prevention

Blockchain technology stores insurance claims in immutable ledger that helps to eliminate common insurance frauds.

Key points

Use-Case of Blockchain in Cybercrime and Cyberattack

- a. The cost of insurance fraud goes over \$40B per year, and standard methods are hard to detect.
- b. By fusing claims data between insurers, Blockchain's distributed ledger technology can move forward fraud detection.
- c. Blockchain technology can save insurers the cost of paying for governmental and subscription data to avoid fraud by facilitating better data sharing.

Fraud Detection Using Blockchain Technology

Insurers could record permanent transactions on a distributed directory, with granular access controls for data security protection. Storing claims information on a shared list would help insurers work together and find suspicious behaviour. Blockchain technology would take a considerable amount of coordination between insurers to stop fraud, but in the long term, it would prove extremely beneficial. An effort to counter fraud based on a blockchain could begin with fraudulent claims being shared to help us find bad behaviour patterns. Applying this technology, insurers can reap the following three benefits: (i) removing or dealing with multiple accident complaints; (ii) owning and reducing counterfeiting through digital certificates; and (iii) reducing premium diversions, e.g. for unlicensed brokers selling insurance and pocketing premiums.

ii). Property and Casualty (P&C) insurance

A joint lead and insurance contracts can improve the efficiency of property and casualty insurance to achieve smart contracts.

Key points

- a. P&C reports that data has been dispersed through several places controlled by various parties, making it a challenge to resolve claims.
- b. Blockchain technology allows automated data collection, analysis and possibly up to 3x quicker and 5x cheaper than currently, some types of P&C claims.
- c. Applications processing and payments are accelerated by automated "smart contracts," which spares insurers more than € 200b per year.

P&C Insurance on a Blockchain

Blockchain technology can codify business rules and automate claims management using intelligent contracts while offering a permanent trail of audit, allowing

policyholders and insurers to scan and manage physical assets digitally. Intelligent agreements using blockchain technology can transform paper contracts into programmable code that automates the processing of claims and calculates insurance liabilities for all concerned.

For example, when the accident occurs, the insurer informs immediately by linking the intelligent contract with the sensors in a vehicle. The smart contract can inform medical teams and towing services, start the process of insurance claims and inform the insured person that the assistance is being provided. New information such as police reports and crash photos can be added to the claim by the Smart Contract, thus simplifying the payout process by minimising human intervention.

iii) Health Insurance

It improves interoperability and keeps the medical records secure by adopting blockchain technology into the ecosystem of health insurance industry.

Key points

- a. The demand for patient confidentiality results in insurers often not having full access to the medical history of their patients.
- b. The lack of information may lead to denials of insurance claims.
- c. Patient information can be encoded with Blockchain technology, facilitating information transmission while maintaining patient privacy.

Healthcare Using Blockchain Technology

An industry-wide, synchronised repository of health care data can maintain patient privacy while saving billions each year from the industry. Checking the medical data of patients can be returned and shared case-by-case by Blockchain Technology. The blockchain system maintains the distributed ledger with a cryptographic signature for every record rather than forcing insurance providers to accumulate data from different databases. The signature cryptographically indexes the contents of each document and sets the time signature without saving sensitive blockchain information. Due to the shared ledger, medical data can be checked by insurers and suppliers whenever the document is modified. In the meantime, the Blockchain could provide permissions to comply with regulations, while anonymising and sharing data for research.

iv). Reinsurance

Blockchain technology facilitates the flow of information and payments between insurers and reinsurers by ensuring reinsurance contracts through smart contracts.

Key points

- a. Reinsurance protects insurers, for example, during a natural disaster, when a large number of claims occur at once.
- b. Blockchain technology can reduce risk in information sharing with smart contract's automation process.
- c. Insurance helps people dissipate the risk of natural disasters and alleviates unforeseen events.

Reinsurance Using Blockchain Technology

Blockchain technology has the potential to improve current reinsurance processes. With the use of blockchain techniques, complete premium transactions can occur on the computer systems of insurers and reinsurers, ending the need for book reconciliations for every claim between institutions. Reinsurers can be better able to assign capital for claims almost in real-time with data shared in an immutable directory and enable them to both processes and settle claims more instantly without relying on primary insurers for the data surrounding each claim.

Use-Cases (Insurance)

I. Blockchain Use Case: Etherisc (Fraud Detection – Insurance)

Blockchain start-up technology Etherisc has built up an insurance product with a blockchain capacity, which was openly tested in October 2017. The flight delay program based on crypto-currency permitted passengers to buy flight insure using either cryptocurrency or fiat money like USD and Euro. Other development products include insurance for hurricanes, and crop insurance.

Smart contracts power Etherisc's products. A contract is a paper agreement that can be enforced by law between two or more parties, but an intelligent contract is an agreement between two or more parties which can be enforced by code. With multiple 'oracles' or data sources, the Etherisc smart contract can independently verify claims. Etherisc may, for example, drone videos, compare satellite images, and weather station to the pictures provided by the insured when processing a crop insurance claim. This automatic examination can detect fraudulent claims before the

human review. Blockchain should be more commonly used as a tool for preventing fraud.

II. Blockchain Use Case: Insurwave (P&C Insurance)

The blockchain-powered marine hull insurance platform Insurwave was launched by a collaboration of organisations— including EY, ACORD, Guardtime, Microsoft, and A.P. Møller-Maersk. The platform is now commercial and is planned to deal in its first 12 months of operation with the risks of over 1,000 commercial ships and 500,000 automated transactions. In the future, the group plans to implement its platform in other types of business insurance such as freight, aviation and logistics.

The Insurwave platform provides ship location and safety conditions information in real-time to both insurers and insureds. The establishment of marine insurance premiums is, as the blockchain company R3 puts it, “notoriously complex.” Products such as Insurwave are designed to make the audit trail impossible to change more accessible to this complexity.

The process of making claims can be speeded up with reliable information stored on a vessel. It can also contribute to increasing access to data for shipowners and insurance agents. Information such as shipping, geographic location can help insurers analyses the risk they take and help ship owners to assess better the type of insurance they require.

III. Blockchain Use Case: MedRec (Health Insurance)

MedRec is a collaborative MIT Health Content Management Program. It indexes medical documents on the Blockchain instead of stored medical data directly in the chain, enabling providers with permission to access reports. This helps ensure patient confidentiality while creating a trail that facilitates patient information finding and verification in the Blockchain. While MedRec is still a proof of concept academic project, it provides a model to understand the secureness of medical data using blockchain technology. Today, Blockchain companies have essential regulatory and compliance obstacles to deal with the insurance industry to be successful.

IV. Blockchain Use Case: B3i (Reinsurance)

In October 2016, B3i is a consortium formed to explore blockchain technology by some of the most notable names in the insurance and reinsurance industries. AIG, Allianz, Aegon and Swiss Re are among the members. In 2017, B3i launched the Smart Contract Management System, a type of disaster reinsurance system for Property Cat XOL contracts. Each platform reinsurance contract is written as smart

Use-Case of Blockchain in Cybercrime and Cyberattack

contracts on the same shared infrastructure with executable code. If an event such as an earthquake or a hurricane occurs, the smart contract evaluates participants' data and automatically calculates their payments. After testing and reception of feedback by 40 companies, the B3i pilot program concluded in September 2018 and is scheduled to launch live at the start of 2019.

Running blockchain technology-based reinsurance policies helps in allocating capital and undertaking insurance policies to bring the insurance industry greater stability. Instead of relying on primary insurers for data loss, reinsurers can directly request coverage from the Blockchain.

Moving Towards a Blockchain-Powered Insurance Industry

Although blockchain technology is still in its early stages, it is already in the insurance industry with various promising use cases and applications. Both giant insurance carriers such as Allianz and Swiss Re and small blockchain technology start-ups are alike leveraging solutions. However, despite this overwhelming interest in blockchain technology, there is a large amount of room to cover before the insurance industry can make a significant impact.

Insurance companies must align themselves from an industry viewpoint to blockchain technology standards and processes. Although blockchain technology can help insurers collaborate and share information more efficiently, the insurers themselves have to be ready to work with each other. It is also necessary to further develop the technology itself. Public blockchains where anyone gains access to the ledger, because of privacy and security concerns, are not feasible for the insurance industry. Blockchains still under active development is private, permissible.

Finally, it is highly regulated in the insurance sector to protect consumers against abuse and insurance companies against excessive risk and bankruptcy. Legal and regulatory insurance frameworks must evolve and provide clear guidance for the success of blockchain technology.

CONCLUSION

Ginni Rometty, Chairman, President and CEO of IBM, said, "Cybercrime, is the greatest threat to every profession, every industry, every company in the world". Blockchain Technology, a shared distributed ledger, is a better answer for encountering cybersecurity threats. In this chapter, the authors discussed various cybersecurity threats and detailed two such scenarios, financial and insurance. Blockchain Technology can lend a helping hand for preventing, finding, and eradicating cyber threats. Due to the properties like immutability, transparency and security, the above

said technology would play a vital role in building effective solutions for handling cybercrimes. At this stage, Blockchain Technology is in its infancy stage, and the authors have to consider the parameters such as scalability, time taken for completing a transaction (writing a block in chain), and domain where the chain is implemented.

REFERENCES

- Ahmad, T. (2019). Technology Convergence and Cybersecurity: A Critical Analysis of Cybercrime Trends in India. *27th Convergence India Pragati Maidan*, 29-31. Available at SSRN: <https://ssrn.com/abstract=3326232>
- Broadhurst, R., & Chang, Y. (2012). *Cybercrime in Asia: Trends and Challenges*. SSRN Electronic Journal. doi:10.2139/ssrn.2118322
- Chattopadhyay, A., & Mitra, U. (2018). Attack detection and secure estimation under false data injection attack in cyber-physical systems. *2018 52nd Annual Conference on Information Sciences and Systems (CISS)*, 1-6. doi:10.1109/ciss.2018.8362307
- Chattopadhyay, A., & Mitra, U. (2020). Security Against False Data-Injection Attack in Cyber-Physical Systems. *IEEE Transactions on Control of Network Systems*, 7(2), 1015–1027. doi:10.1109/TCNS.2019.2927594
- Chelliah, J. B., Ajith, P. A., Samtani, G. C., Paul, D., & Bachhav, C. (2019). Security Implications in Cyber Physical Systems. *International Journal of Innovative Technology and Exploring Engineering*, 8(6S), 85–88.
- Gopalan, H. S., Suba, A. S., Ashmithashree, C., Gayathri, A., & Andrews, J. V. (2019). Digital Forensics using Blockchain. *International Journal of Recent Technology and Engineering (IJRTE)*, 8(2S11), 182–184. doi:10.35940/ijrte.b1030.0982s1119
- Graham, S. R., & Smith, K. S. (2020). *Cybercrime and Digital Deviance*. Published by Routledge., doi:10.4324/9781351238090
- Hyvärinen, H., Risius, M., & Friis, G. (2017). A Blockchain-Based Approach Towards Overcoming Financial Fraud in Public Sector Services. *Business & Information Systems Engineering*, 59(6), 441–456. doi:10.1007/12599-017-0502-4
- Karie, N. M., Kebande, V. R., Venter, H., & Choo, K. R. (2019). On the importance of standardising the process of generating digital forensic reports. *Forensic Science International: Reports*, 1, 100008. doi:10.1016/j.fsir.2019.100008

Use-Case of Blockchain in Cybercrime and Cyberattack

Karthika, V., & Jaganathan, S. (2019). A quick synopsis of blockchain technology. *International Journal of Blockchains and Cryptocurrencies*, 1(1), 54–66. doi:10.1504/IJBC.2019.101852

Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. *Digital Investigation*, 28, 44–55. doi:10.1016/j.diin.2019.01.002

Mathew, A. (2019). Cyber Security through Blockchain Technology. *International Journal of Engineering and Advanced Technology*, 9(1), 3821–3824. doi:10.35940/ijeat.A9836.109119

Piscini, E., Dalton, D., & Kehoe, L. (2019). *Blockchain & Cyber Security - An assessment of the security of blockchain technology*. Retrieved September 13, 2020 from <https://www2.deloitte.com/tr/en/pages/technology-media-and-telecommunications/articles/blockchain-and-cyber.html>

Raikwar, M., Mazumdar, S., Ruj, S., Gupta, S. S., Chattopadhyay, A., & Lam, K. (2018). A Blockchain Framework for Insurance Processes. *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. doi:10.1109/ntms.2018.8328731

Sowmiya, B., & Poovammal, E. (2019). Blockchain Technology Is a Boost to Cyber Security. In *Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems*. IGI-Global. doi: . doi:10.4018/978-1-5225-8241-0.ch013

Taylor, J. P., Dargahi, T., Dehghantanha, A., Parizi, M. R., & Choo, R. K. (2019). A Systematic Literature Review of Blockchain Cybersecurity. *Digital Communications and Networks*., 6(2), 147–156. doi:10.1016/j.dcan.2019.01.005

Tian, Z., Li, M., Qiu, M., Sun, Y., & Su, S. (2019). Block-DEF: A secure digital evidence framework using blockchain. *Information Sciences*, 491, 151–165. doi:10.1016/j.ins.2019.04.011

Chapter 10

Motivational Quotes– Based Intelligent Insider Threat Prediction Model

Sunita Vikrant Dhavale

Defence Institute of Advanced Technology, India

ABSTRACT

Insiders are considered as the weakest link. The digital records of a person's Facebook likes against motivational quotes can be used for automatic and accurate prediction of sensitive attributes related to their personality traits depression, and their views against company/government policies, etc. Such analysis will help organization to take proactive measures against vulnerable insiders. Insiders managing their impressions differently than their basic personality traits can also be identified. Deep learning models can be utilized to learn and map the association among extracted features and insider behavioral patterns. Further, reinforcement techniques can be used to select appropriate motivational quotes in order to collect additional data required for further analysis. At the same time, the same exposed motivational messages on insider's social platform can aid to improve their psychological health over a time. However, due to implications involved in data collections related to personalization and data collection privacy, the authors have quoted their work in terms of this concept chapter only.

INTRODUCTION

Many commercial applications exist in current digital markets that try to predict personal information to improve their products or services by invasions of user's

DOI: 10.4018/978-1-7998-4900-1.ch010

privacy. Individual traits can also be predicted from written texts or answers to a psychometric test. Similarly, employee behaviors on social media like Facebook, Instagram or Twitter can be analyzed; although such analysis presents serious challenges considering data privacy norms (Michal, David, & Thore, 2013). David Stillwell in 2007 (Michal, Tadesse, Bo, & Liang, 2018) created myPersonality, a Facebook App in his psychological research. In 2013, publicly available Facebook Page Likes of all users restricted by Facebook by implementing strict privacy policies. However, organizations; especially critical government agencies which are responsible for tackling national security issues; can send motivational messages or quotes daily to their employees to collect their likes and analyze their psychological behavior in order to predict any insider related threats in advance. Here, an insider can be any employee who has access to the critical information systems of an organization and can pose threats for organizational security (Miltiadis, Alexios, Nikos, Marianthi, & Dimitris, 2010, & Sunita, 2018).

Several insider threat prediction models have been proposed in the literature (Michal, Tadesse, Bo, & Liang, 2018). The authors in (Miltiadis, Alexios, Nikos, Marianthi, & Dimitris, 2010) captured the user's technological trait (using IDS, honeypot etc.) augmented with data from psychometric tests in order to analyze insider's tendency to malicious acts and the stress level. The authors categorized users in Novice, Advanced, Administrator categories based on their access level and also in Low, Medium, High user sophistication/computer skill levels. Authors in (Michal, Tadesse, Bo, & Liang, 2018) tried to predict personality traits of Facebook users using the myPersonality project dataset, where they compared performance of different machine learning models and found XGBoost classifier outperforms, with prediction accuracy of 74.2%. Authors in (Park, Youngin, & Kyungho, 2018). utilized machine learning algorithms to find the possible malicious insider using Sentiment-140 dataset and found Decision Tree and K-Means models provided highest accuracy. Authors in (Cristina, et al. 2017) tried to predict personality traits from Facebook profile pictures. In their research, they found that extroverts/agreeable individuals use warm colored pictures with many faces that showcase their socializing nature; while neurotic ones use pictures of indoor places and production of selfies associated to narcissism. Authors in (Marco, et al. 2013). utilized PsychoFlickr dataset, based on ProFlickr users for identification of personality traits and validated against user's self-assessed answers and ratings given by 12 independent assessors.

All above works have not considered impact of likes/comments against motivational messages available on social media for insider personality prediction. As insiders personality traits influences on their choice of Facebook profile pictures (Cristina, et al. 2017); similarly likes/comments to motivational messages can be based on the many personality related factors like person's thoughts/views towards life/job/colleagues, current stress level, what kind of problems currently he is facing, what

he thinks about existing challenging job conditions, any family problems if he is facing currently, his financial conditions etc. The analyses carried out in our work are aimed to examine following research questions:

- (1) Research Question 1 (RQ1): Do comments/likes against motivational messages helps to predict insider's personality?
- (2) Research Question 2 (RQ2): Do extracted deep learning features from comments/likes against motivational messages can provide valuable information related to advanced threat prediction?
- (3) Research Question 3 (RQ3): Do the same platform can be used for improving positive useful personality traits to improve employees performance during course of period?

The paper is organized as follows. In section II, Overview of the Personality Traits is given. In section III, we explain various categories of motivational quotes and we try to discover relevance of them in analyzing personality traits/stress conditions. In section IV, we propose the deep learning model that can be used for insider feature classification and prediction followed by conclusions in section V.

PERSONALITY TRAITS (MICHAL, ET AL. 2018, JOHN, & SRIVASTAVA, 1999)

Widely accepted psychological theory based Big 5 model describes five main personality traits that form the acronym OCEAN (i.e. openness to experience, conscientiousness, extraversion, agreeableness and neuroticism) (John, & Srivastava, 1999). Table 1 shows overview of the Big Five Personality Traits that could capture personality differences.

Motivational Quotes-Based Intelligent Insider Threat Prediction Model

Table 1. Big Five Personality Traits (John, & Srivastava, 1999)

Personality Trait	Description
Openness (O)	Person who are open to new experiences/think in new directions/ accept emotions/ ready to take new challenges/ curious/open-minded/creative, and tolerant
Conscientiousness (C)	Person who are prepared/pay attention/follow schedule or procedures/ self-disciplined / work hard/ do planning
Extraversion (E)	Person who are comfortable in crowd/start conversation/friendly/social, like to receive calls, spend more time talking.
Agreeableness (A)	Person who are kind/softhearted/ concerned about other’s feelings/ trustful/ help others/can make good team work
Neuroticism (N)	Person who suffers with negative emotions like get easily irritated or upset/hot tempered/ worry/suffers with phobia/ have mood swings

The score is assigned in the range of 1 to 5 for each of above personality traits based on International Personality Item Pool (IPIP) questionnaire in order to find out ones personality along each of these dimensions (John, & Srivastava, 1999, Cristina, et al. 2017).

Figure 1. Distribution of the personality traits (John, & Srivastava, 1999, Cristina, et al. 2017).

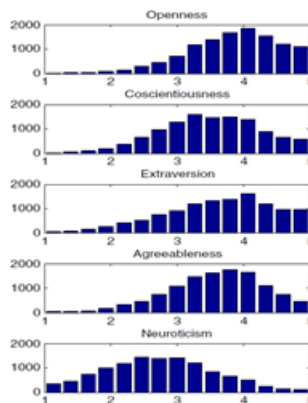


Figure 1 show the scores distribution of Neuroticism is oppositely skewed than that of remaining personality traits (John, & Srivastava, 1999). Authors in (Bachrach, et al. 2012) found that agreeableness is positively correlated with the number of tags, whereas neuroticism is negatively correlated with the number of friends. Authors in (Farnadi, et al. 2013) found that users with openness have a tendency to be more emotional in their Facebook status posts than users with neuroticism.

It is found that anxious individuals tend to be less creative, worse at problem-solving during stressful situations, and slower at learning from negative experiences (Graham, Cohen, & Shmavonlan, 1967). The studies suggest that stress negatively influences a subject's performance when they are forced into hostile environments, e.g., talking to a person with whom the subject is not comfortable with (Graham, Cohen, & Shmavonlan, 1967). Different personality types may vary considerably in how they respond to stressful events. In response to acute threats, people who are typically anxious/shy/cautious, generally adopt a flight strategy; while people who exhibit highly aggressive behavior, generally adopt a fight strategy. The authors in (Ahmed, et al., 2019) applied different machine learning based classification models for mapping personality traits (using 50-item IPIP question set) with stress scales (using Perceived Stress Scale). They found that extrovert persons tend to get moderately stressed and persons having higher score in openness-to-experience tend to perceive high stress. Students with high level stress could have direct impact on their behavior as well as on academic results (Ahmed, et al., 2019).

In addition to above traits, many additional questions and answers related to behavioral patterns can be observed and can be mapped for predicting potential malicious insider based on compliance (Park, Youngin, & Kyungho, 2018, Alisa, & Grzegorz, 2018).

- 1 Employee doesn't want to give timely critical information to the concerned people in the organization.
- 2 Employee doesn't want to contribute organization through cooperation.
- 3 Employee doesn't want to learn new things when required by an organization.
- 4 Employee doesn't want to accept things which are beneficial for existence and progress of an organization.
- 5 Employee frequently violates organizational policies and rules.
- 6 Employee is always involved in spreading lies, gossips and rumor.
- 7 Employee demoralize/demotivate colleagues/subordinates.
- 8 Employee misguide colleagues/subordinates on any issue intentionally.

MOTIVATIONAL QUOTES (Cristina et al. 2017)

Recently, many apps have been developed for dealing with anxiety/stress problems (Ref. <https://www.opencolleges.edu.au/blog/2016/05/23/mhm-best-apps-anxiety/>) as stress-related abnormalities tend to increase the risk of strokes, heart attacks, depression, and hypertension etc. These apps generally provide inspirational/motivational message quotes for overcoming anxiety/stress.

Motivational Quotes-Based Intelligent Insider Threat Prediction Model

The authors in (Cristina et al. 2017) suggested improving the self-esteem of people with chronic disorders with motivational quotes. The author suggested using motivational quotes to promote positive thinking in people with chronic disorders during digital health therapies. The authors in (Cristina et al. 2017) categorized motivational quotes as in Table 2.

People with chronic disorders feel isolated/excluded, and hence, both “Experience of Others/‘I’” and “Empowerment/‘You’” motivational quotes may help them to relate to others’ personal experiences, providing positive feedback/clear indication of social support (Cristina et al. 2017). These people will certainly send comments/likes to these motivational messages which can be studied as part of this research work. Some people may acknowledge “Reality Check” or “General Statement” quotes which expose to the negative aspects of life one is experiencing, or discuss general concepts in a passive manner. Some people who tend to accept direction from others to increase self-assurance may like “Cause-and-Effect” and “Imperative/Command” kind of motivational quotes that have capability to provide this guidance (Cristina et al. 2017). This suggests that the likes/comments against the type of motivational messages on social media like facebook can serve as an important tool to analyze/predict the behavioral trait/stress conditions of an individual etc. This in turn will help in understanding threat patterns associated with an individual employee i.e. insiders.

Due to lack of large dataset in this domain, we stated some observations based on sample IPIP survey conducted for small group with their consent. Our observations confirmed that likes towards any particular type of motivational message is highly influenced by one’s personality traits and his current depression/work pressures etc.

Motivational quotes such as “Difficult roads often lead to beautiful destinations. The best is yet to come - Zig Ziglar” can encourage a person to think differently and act against their current circumstances. This analysis also confirms that the same motivational messages can be used to improve ones performance or attitude towards work/organization by using reinforcement learning techniques.

The observations stated in (Cristina et al. 2017) also leads to think that, Person’s Facebook Likes against various motivational messages or quotes can be used for automatic prediction related to their personality traits, views against company policies, depression, and family influences. Such psychological analysis carried in advance will help any organization to take proactive measures against threats which can be imposed by vulnerable insiders. By carefully selecting motivational quote categories for particular individuals, one can also predict the state of mind of an insider and similarly can predict potential malicious insiders. However, role of same quotes can also be studied for improving the health of vulnerable employees in time and adapt into further HR policies.

Motivational Quotes-Based Intelligent Insider Threat Prediction Model

Table 2. Quote with description (Cristina et al. 2017)

Quote type	Description	Example	Our Observation – personality Trait
Choice	Presents the option of acting	“Instead of begging to be picked by others, you have the choice to pick yourself and build your brand.”— Bernard Kelvin Clive	Openness
Self-directed question	Poses a question to the individual that stimulates introspection and self-examination	“When someone tells me ‘no,’ it doesn’t mean I can’t do it, it simply means I can’t do it with them.” -- Karen E. Quinones Miller	conscientiousness
Cause-and-effect	Outlines the positive effects that may result from particular thoughts or actions	“As soon as you trust yourself, you will know how to live.” -- Johann Wolfgang von Goethe	Openness, conscientiousness, extraversion, agreeableness
Imperative/command	Provides direction and explicit commands for the individual	“Don’t waste your energy trying to change opinions ... do your thing, and don’t care if they like it.” -- Tina Fey	Openness, conscientiousness
Empowerment/“You”	Addresses the individual directly with positive statements	“Stop trying to ‘fix’ yourself; you’re NOT broken! You are perfectly imperfect and powerful beyond measure.”—Steve Maraboli	neuroticism
Experience of others/“I”	Offers the opinion or first-person account of someone else	“Why am I trying to be somebody? I am somebody.”—Eric Christopher Jackson	Openness, conscientiousness, neuroticism
Reality check	show the individual that it is natural to face pain and difficulties	“No one has it all, and no one lacks it all.”—Christopher Peterson	Openness, conscientiousness, neuroticism
General statement	Discusses general concepts or situations in life	“Surrendering is not giving up—it is gaining strength.”—Grace Sara	Openness, extraversion, agreeableness

Automated additional monitoring can be used against suspicious insiders by using reinforcement learning techniques by selecting next stages of messages/quotes for gathering likes for further accurate finer analysis.

PROPOSED MODEL

The recent development in the fields of machine learning (ML), natural language processing (NLP) and deep learning (DL) has proved to be considerable for medical diagnosis and prediction. For detecting and diagnosing stress symptoms at early stages, a medical practitioner generally asks a set of questions related to the patient’s life and reviews patient’s stress conditions on the basis of the patient’s responses/ answers. Other methods like using EEG, MEG, PET, MRI etc. are more invasive

Motivational Quotes-Based Intelligent Insider Threat Prediction Model

in nature compared to the questionnaire/response methods. Most of the time, such analysis are subjective in nature as based on human expertise and prone to errors/biases. In such cases, automated analysis using machine learning approaches may be better solution. Recently, deep learning techniques have been successfully applied for text/image/video analysis (Sunita, 2019). Features learnt by deep neural net structure have shown their great potential in various classification tasks instead of exploring different hand-crafted features as in case of traditional machine learning techniques (Sunita, 2019).

Figure 2. Proposed deep learning model for insider threat prediction

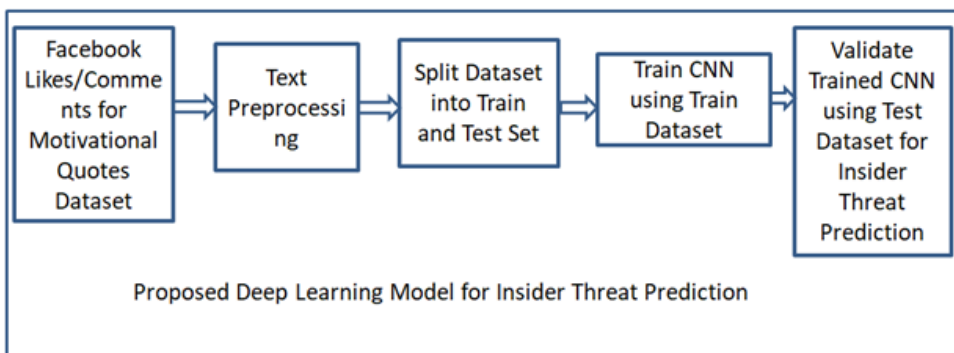


Figure 2 shows the proposed deep learning model for insider threat prediction

First the dataset will be obtained from the likes/comments written by insiders against the daily motivational messages/quotes. Such data need to be gathered over a time after taking consent of authorities and national security agencies without deviating from data privacy norms. Although some datasets like myPersonality (Michal, Tadesse, Bo, & Liang, 2018) dataset (250 users, 9917 status updates) can be used for initial studies for checking efficacy of CNN model; however new dataset from the domain will help in designing accurately predicting systems. The gathered data will be pre-processed using NLP techniques like tokenization, removing URLs/special symbols/spaces/lower cases, stemming etc.

Using the knowledge-bases such as WordNet to extract the semantic information contained in the words can improve the performance of detection. One-Dimensional CNN layers can learn invariant features present in the sequence of words and likes in the input dataset. The psychological analysis model predicts the insider threat conditions so that management can decide further actions. The dataset can be split into train and test dataset for further training and testing efficacy of CNN model (Sunita, 2019). During runtime testing, automated additional monitoring can be used

against suspicious insiders by using reinforcement learning techniques by selecting next stages of messages/quotes for gathering likes for further analysis.

Result and Analysis

We applied CNN model on myPersonality (Michal, Tadesse, Bo, & Liang, 2018) dataset containing 9917 text comments from 250 users along with OCEAN personality scores. During preprocessing, 1) the text is converted in lower case; 2) Contraction words like “ain’t” is converted to “is not” i.e. full forms; and 3) punctuation/ stop words removed. Keras Tokenizer Class is used to fit on raw text data to get 14675 unique tokens and text data is replaced by these sequence numbers. Pretrained word embedding vector based on GloVe (Global Vectors for Word Representation)(Jeffrey, Richard, & Christopher, 2014), standard dictionary of 100-dimensional vector size is used to set the weights of embedding layer of CNN. The dataset is then split into train and test dataset for further training and testing efficacy of CNN model. Table 3 gives a summary of CNN architecture used for training.

Table 3. CNN Architecture.

Layer (Type)	Output Shape	Parameters
input_1 (Input Layer)	1000	0
Embedding	1000, 100	1467500
Conv1D	996, 128	64128
max_pooling1D	199, 128	0
Conv1D_1	195, 128	82048
max_pooling1D_1	39,128	0
Conv1D_2	35,128	82048
Global_max_pooling1D	128	0
dense	128	16512
dense_1	5	645
Total Parameters		1,712,881
Trainable Parameters		245,381
Non-trainable Parameters		1,467,500

Here, the input layer is followed by embedding layer and three convolutional layers with RELU activations. Each convolutional layer consists of 128 filters with kernel size of 5x5. Final fully connected layer uses linear activation function for predicting five OCEAN scores. The CNN model is compiled by setting loss parameter to Mean

Motivational Quotes-Based Intelligent Insider Threat Prediction Model

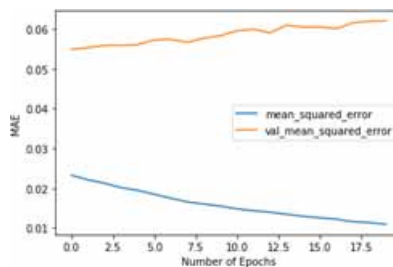
Absolute Error (MAE) and selecting Adam optimizer. The model is evaluated against final dataset containing original training and unseen test dataset.

Batch size of 16 is used for training each epoch and model is trained for total 10 epochs only. Total messages are split in ratio of 90 percent training data and 10 percent testing data. The trained CNN model is evaluated against the testing data set on laptop with containing Core-i7 CPU processor, 16 GB RAM and 6 GB NVIDIA GPU card. The algorithm is implemented in spyder anaconda python environment using Keras, Sklearn, Opencv and Tensorflow deep learning libraries.

The average MAE values for training data and test data is found to be low i.e. 0.085 and 0.191 respectively with MAE standard deviations of 0.0118 and 0.003 respectively. This confirms the high accuracy in prediction of OCEAN score values. Figure 3

shows MAE of train and test dataset per epoch. The trained model shows good accuracy in predicting the personality traits of an individual based on facebook comments given in myPersonality (Michal, Tadesse, Bo, & Liang, 2018) dataset.

Figure 3. MAE per Epoch



CONCLUSION AND FUTURE WORKS

Organizational information security and employees' privacy are two conflicting and challenging requirements while carrying out the intelligent psychological analysis for insider threat prediction. Implementing technical cyber defence controls alone do not always guarantee organizational security (Sunita, 2018), but a proactive measure that has the capability to analyze the insider behavior and predict potential malicious insiders in advance is required. Also, personality traits recognition based on the likes/comments against motivational messages is a relatively new and challenging task. Deep learning models can be utilized to learn the correlation between extracted features i.e. likes against the exposed motivational messages or quotes and insider behavioral patterns. Further, using reinforcement techniques as part of such intelligent analysis can provide next appropriate motivational quotes or messages to collect

enough data and carry out continuous analysis. There is a need to utilize a larger training dataset to increase the systems accuracy. Besides sample size, other factors like age, culture/economical or family background, physical, gender and mental fitness might pose new challenges for such analysis. People giving likes to similar motivational messages can be clustered and their personality traits can be studied from insider threats prediction point of view. Our future work will try to explore powerful application of natural language processing (NLP), behavioural analysis, sentiment analysis, and deep learning techniques for insider threat detection based on social networking data analysis. Further, contribution from specialists from various domains like computer scientists, psychologists, criminologists, and security practitioners is required for accurate mapping along with huge sample dataset for deep learning this module.

In our further studies, to get quantitative answers for research questions RQ1, RQ2 and RQ3: 1) we may perform a correlation analysis between deep learning features based on likes/comments against motivational messages and personality traits; 2) we may employ learnt model for advanced threat prediction; and 3) In future, we may analyze change in their attitudes towards work by exposing them to required set of motivational messages.

This study also opens a Pandora box of related research questions like can the same platform will be misused by the adversary for targeting key government/organizational officials as a part of psychological warfare?...

REFERENCES

- Michal, K., David, S., & Thore, G. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States of America*, 110(15), 5802–5805. doi:10.1073/pnas.1218772110 PMID:23479631
- Michal, M., Tadesse, H., Bo, X., & Liang, Y. (2018). Personality Predictions Based on User Behaviour on the Facebook Social Media Platform. *IEEE Access*.
- Miltiadis, K., Alexios, M., Nikos, V., Marianthi, T., & Dimitris, G. (2010). An Insider Threat Prediction Model. *LNCS*, 6264, 26–37.
- Sunita, D. (2018). Constructing an Ethical Hacking Knowledge Base for Threat Awareness and Prevention. IGI Global.
- Sunita, D. (2018). *Insiders Attack Analysis in Building an Effective Cyber Security for an Organization*. In *Psychological and Behavioral Examinations in Cyber Security*. IGI Global.

Motivational Quotes-Based Intelligent Insider Threat Prediction Model

John, O. P., & Srivastava, S. (1999). The big five trait taxonomy: History, measurement, and theoretical perspectives. *Handbook of personality: Theory and research*, 2(1999), 102–138.

Bachrach, Y., Kosinski, M., Graepel, T., Kohli, P., & Stillwell, D. (2012). Personality and patterns of facebook usage. *Proceedings of the 4th Annual ACM Web Science Conference*, 24–32. 10.1145/2380718.2380722

Farnadi, G., Zoghbi, S., Moens, M. F., & Cock, M. D. (2013). Recognizing personality traits using facebook status updates. *Proceedings of the workshop on computational personality recognition (WCPR13) at the 7th international AAAI conference on weblogs and social media (ICWSM13)*.

Sunita, D. (2019), C-ASFT: Convolutional Neural Networks based Anti-Spam Filtering Technique. *International Conference on Computational Science and Applications (ICCSA) 2019*.

Park, W., Youngin, Y., & Kyungho, L. (2018). Detecting Potential Insider Threat: Analyzing Insiders' Sentiment Exposed in Social Media. *Security and Communication Networks, 2018*, 1–8. doi:10.1155/2018/7243296

Alisa, B., & Grzegorz, B. (2018). Improving Self-Esteem with Motivational Quotes: Opportunities for Digital Health Technologies for People With Chronic Disorders. *Frontiers in Psychology*, 9, 2126. doi:10.3389/fpsyg.2018.02126 PMID:30450071

Cristina, S., Fabio, C., Luca, P., Michal, K., David, S., Nicu, S., Marco, C., & Bruno, L. (2017). What your Facebook Profile Picture Reveals about your Personality. *Proceedings of the 25th ACM international conference on Multimedia*, 460-468.

Marco, C., Alessandro, V., Cristina, S., & Alessandro, P. (2013). Unveiling the Multimedia Unconscious: Implicit Cognitive Processes and Multimedia Content Analysis. *Proceedings of ACM-MM*, 213–222.

Jeffrey P., Richard S., Christopher D. M. (2014). GloVe: Global Vectors for Word Representation. *Empirical Methods in Natural Language Processing (EMNLP)*, 1532-1543.

Graham, L. A., Cohen, S. J., & Shmavonlan, B. M. (1967). Some methodological approaches to the psychophysiological correlates of behavior. In *Emotional stress. Psychological and physiological reactions* (pp. 178–191). Medical, Industrial and Military Implications.

Motivational Quotes-Based Intelligent Insider Threat Prediction Model

Ahmed, A. M., & Adnan, F. (2019, August). A Machine Learning based Approach for Mapping Personality Traits and Perceived Stress Scale of Undergraduate Students. *Modern Education and Computer Science*, 8, 42–47.

Chapter 11

Challenges of Developing AI Applications in the Evolving Digital World and Recommendations to Mitigate Such Challenges: A Conceptual View

Srinivasan Vaidyanathan
Cognizant, India

Madhumitha Sivakumar
Sri Sivasubramaniya Nadar College of Engineering, India

Baskaran Kaliamourthy
Atto Technology Solutions LLC, Dallas, USA

ABSTRACT

These intelligence in the systems are not organic but programmed. In spite of being extensively used, they suffer from setbacks that are to be addressed to expand their usage and a sense of trust in humans. This chapter focuses on the different hurdles faced during the course of adopting the technology namely data privacy, data scarcity, bias, unexplainable Blackbox nature of AI, etc. Techniques like adversarial forgetting, federated learning approach are providing promising results to address various issues like bias, data privacy are being researched widely to check their competency to mitigate these problems. Hardware advancements and the need for enhancing the skillset in the artificial intelligence domain are also elucidated. Recommendations to resolve each major challenge faced are also addressed in this chapter to give an idea about the areas that need improvement.

DOI: 10.4018/978-1-7998-4900-1.ch011

INTRODUCTION

Artificial Intelligence: A Brief Introduction

In today's technology dominated world Artificial Intelligence is one of the fast developing and dynamically changing sectors. The word AI is increasingly being used everywhere right from autopilots and self-cruising cars to trivial items like toothbrush. Recent researches suggest that even AI can be used to analyse the trends of pandemics like the infamous Covid-19. This sophisticated technology comes with the ability to sweep through piles of data and analyse them effectively and bring up a conclusion thus helping us solve even the existing intractable problems. "Data is the new oil" is a paraphrase that well describes the growth rate of this technology. With the emerging technologies like Internet of Things the network is ever expanding and that requires processing lot of data and analysis of the collected data becomes a humongous task for humans. These systems have the greatest advantage that they are self-taught and always have the capability of adopting to new challenges thrown at them: the neural network which forms the building block of Artificial Intelligence, trains itself over every new data set and optimizes its predictions based on that.

The Artificial Intelligence is like a double-edged sword and it has to properly handled. The increasing connectivity between all of our technological gadgets and even entities like devices make us fragile and more vulnerable to cyberattacks from hackers who are out on the watch for sensitive data. As the AI technology is spreading its influence over a majority of the domains the hackers are also parallelly on the hunt for sophisticated methods to extract data and information from these smart devices.

Thus, adoption of AI itself should not introduce additional burden in sensitive applications. This chapter mainly focusses on the various stumbling blocks that are encountered before adopting AI for critical applications. It mainly focusses on the various setbacks that might occur while adapting to smart devices powered by AI and the various vulnerabilities of the technology that has to be addressed in future to create tightly secure software applications that can't be meddled by any potential hacker and where tracking out these malicious hackers becomes effectively easier.

BACKGROUND

Artificial Intelligence is indeed the best invention of man which has helped him ease his daily tasks and effort in any domain. Technology built to mimic human mind is indeed performing well in all domains and is being adopted by everyone. Its application ranges from chatbots, digital assistants to critical applications in the field of therapeutics and banking. Domains like Cyber security, Forensics also are

becoming quintessential in nearly all organisations due to the fear of cyber-attacks from hackers for want of some sensitive data and information that pose a great risk to the integrity of the organisation. The growing number of cyberattacks has resulted in the inaugural of Future Series: Cybercrime 2025 by the World Economic Forum and Equifax which is planned during the year 2025.

There is an increasing case of hackers adopting AI techniques to infect any system and retrieve data. According to Rajat Mohanty, CEO Paladion “if attackers can use AI then we defenders can also leverage AI’s power, speed and precision to effectively handle today’s evolved threat landscape”. But there are many hurdles to be overcome before any organisation can adopt AI (*Jawed Akhtar,2014*). Basically, the perception that AI enabled software alone can defend the organisation from attackers has to vanish. AI enabled systems are only a part of the defending system and they can only provide support in defending the information.

AI applications heavily rely upon data and thus storing and analysing huge amount of data is very important. But sensitive data must be stored with proper care and safe guarding techniques be deployed to prevent any potential breach. Data management becomes a critical task in adopting AI. In case of any data breach the results tend to be devastating as rightly said by Elon Musk, “AI is a fundamental risk to the existence of human civilisation”. There are many problems to be addressed before AI could take over the world.

Data privacy refers to the way in which any data is being shared and handled in a manner relative to its importance. Many organisations often possess sensitive data relating to their customers which they are supposed to keep private to safeguard the identities of their customers to earn trust. Any data breach may result in information landing up in the wrong hands which has to be taken care of sincerely. Data privacy is greatly questioned while adopting neural networks that process these data. As a defender there are many possible attempts that we make to defend the data but for any hacker just one loop-hole is sufficient to extricate the intimate information of any organisation. One single vulnerability is all enough for them to sneak in to the system.

Adoption of adversarial AI by hackers also pose a great risk. AI models are trained by the hackers purportedly to make a mistake in the prediction (*Marcus Comiter,2019*). Fixing this issue is difficult and this tampers with the entire system and adversely affects the performance which becomes serious in case of critical applications. This can be rightly described as “digital warfare”.

“A computer can make decision faster, but that doesn’t make it to be fair”. Bias is another issue that creeps even into the digital systems. The data being fed to train the neural networks had to be carefully looked into since the perception of the data collector can seep into the system also. Recently researches found out that many facial recognition systems that were developed identified minorities as criminals

which led to huge criticism from the people about the reliability of Artificial Intelligence driven systems. Bad data being fed into system may result in implicit bias in the result. “To build mutual trust between humans and machines there is a dire need to eradicate these implicit bias of these systems “, says a research survey conducted by IBM.

Generality of AI systems still haven’t been reached. The existing AI systems focus only on a specific application and are capable of handling only the data relevant to that application alone but to make AI systems more efficient they have to adopt to have broader use cases. Though the potential of AI is high, the dangers are also equally high.

According to a survey, companies tend to lose nearly \$5.9M each year resulting from cyberattacks, data breaches and privacy issues etc. Adopting AI without resolving its issues can result in still higher expenditures for the organisation and there is a huge void on integrating AI systems with the existing ones.

All these challenges have to be overcome before any AI system can be adopted into existence.

Research Methodology

Research methodology adopted here includes a meticulous review of existing literature and references from well established standard sites like ScienceDirect, Academicia, Research Gate, SpringerLink and other online warehouses for standard research articles. The various challenges identified here were carefully selected after going through all these research articles and filtering the prominent and impacting challenges of AI. No filtration criteria were applied with respect to the timeline or geography of any publication. The following jargons were used to further gauge the relevant articles:

- “artificial intelligence+challenges”
- “data privacy +AI”
- “bias in AI”
- “AI +data scarcity”
- “Blackbox nature +AI”
- “Artificial Intelligence+ talent crunch”
- “hardware specs+AI”
- “Federated Learning”
- “Adversarial attacks+ AI”
- “Adversarial Forgetting+ AI”
- “Neuromorphic architecture+ for AI”
- “explainable AI”

The resultant set of articles were carefully reviewed and other technological advancement related journals were also searched. Then further reduction was done on the basis of relevance of the material to the theme and topics that were analysed for the chapter.

Delineation of Challenges and Recommendations

This chapter which brings to light the myriad of challenges that are to be properly resolved before adopting AI for any critical application is majorly based on the Literature review of research articles and papers that highlighted the impacts of application of this technology at various levels for various domains. The challenges highlighted are the ones that were commonly faced before adopting AI technology into that domain. These issues are also crucial enough to influence the predictions of the AI based systems which might in turn dilute the accuracy of the prediction. Many methodologies discussed as potential resolvers of these handicaps of AI systems are those that are currently under research and have given affirmative results. Upon adoption of these solutions there has been an observed significant improvement on the performance index of the AI systems. The further research directives emphasise on Adversarial forgetting that has proven to have a significant impact over the overall decision-making process of AI and proves to enhance the process. In this way the recommendations for every challenge is presented.

CHALLENGES INVOLVED IN THE ADOPTION OF AI

Artificial Intelligence is basically based on layering the architecture in such a way that the required features are filtered at each layer so as to increase the rate of correct prediction. The so-called abstraction of neural networks consists of nodes that are connected to each other to form dense layers. The neurons in the network are usually the weighted sum (related to probability of prediction) of the inputs passed to it through various activation functions like RELU, sigmoidal function etc.

Initially the deep neural networks were tested with a single layer which then progressed into multi-layer deeply connected network to improve the predictability of the AI system. Machine learning was the key concept behind AI systems which required specialised extraction of features manually for the system to detect and meet its objectives. But later deep learning models were developed with the capability to detect the features and extract the necessary features from the input fed into the system. A Literature study anticipates that in the future AI system will be ruling nearly all the domains ranging from private to government sectors. In today's world where communication with lifeless objects is possible from a remote system using

the IoT technology integrating AI with these communicating devices can extend their functionality to mimic that of humans. Communication enables social feature and intelligence enables them to make decisions independently and also based on the communicated information from the nearby devices. These edge computing techniques can be upgraded to intelligent edge computing with Machine Learning and Artificial Intelligence. This all started with expert systems where a set of prescribed set of actions were to be taken in case of a given scenario which was programmed into the system certain set of rules.

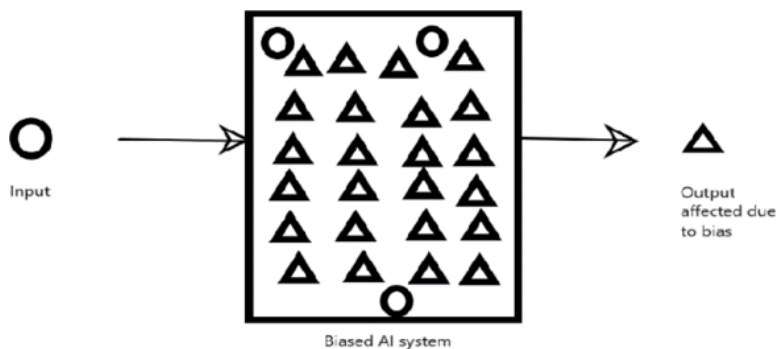
Data Privacy Issue

Though the introduction of Artificial Intelligence and Machine Learning has resulted in a huge impact on nearly all walks of life, still there exists a sense of mistrust on these technologies among the public and many industries dealing with sensitive information. The introduction of ML algorithms into these systems dealing with big data rises up the bar on the challenges that are to be faced. These algorithms work with thousands of input features and consequently they tend to compromise on the data privacy part of which the depth of exposure is unfathomable. Privacy is everyone's right in today's world and rise of any technology that violates privacy is a serious concern (*UN Global Pulse, 2012*). In today's world nearly all the online applications from health care to banking application require vulnerable personal data and given all systems being interconnected there is a high risk of data breach or misuse. Data protection doesn't merely refer to safeguarding the data but it is the fundamental right of every individual related to that data (*Joanna J. Bryson*). Any company needs to comply with the rules and regulations pertaining to personal data protection, on failure of which they end up paying the penalty. In case of using Machine Learning algorithms which are heavily dependent upon data one needs to be careful about the data flow. According to the World Economic Forum's report published in 2020, Artificial Intelligence still remains in the list of possible threats for any individual, company or industries. The WEF claims that the potential risks and threats from AI systems haven't been researched fully yet. Moreover, the average total loss from a data breach amounts to \$3.92 million, according to the 2019 Coat of Data Breach report. And this is expected to rise over by 5% in 2024 since the quantity of data that has to analysed for their sensitivity keeps increasing dynamically year after year. As the AI products keep adding additional functionality there might be a compromise in security that should not be tolerated. The data threat is basically due to the reason that the distinction between what is "personal data" and what is not is not being clearly demarcated in case of these smart systems. The existing solutions to data protection are outdated and needs improvement.

Bias in AI systems

The next big issue faced by AI is bias. Undoubtedly any technology is supposed to be impartial and their deliverables should have the same impact on every individual. But recently there was a huge chaos relating to bias found in AI enabled smart devices. Nearly AI has spread its influence over important sectors of the society like employment management, judicial system, healthcare services etc. If this technology with bias is adopted in future then the vulnerable members who are at the lowest rung of the societal ladder would become the most disadvantaged in finding jobs, acquiring fair treatment by the judicial system etc. Tackling bias needs serious efforts from the individual or from the organisational side in tracking the root of the issue (*EC-Council*). Not only racial bias but AI is also found to provoke gender bias. According to a study conducted in August 2019 by Wired and Element AI only 12% women are found be researching Machine Learning and related topics. One of the famed case studies of AI with bias is the Google Translate. It was found that while translating sentences containing word “engineer” and “nurse” from languages like Bangla and Turkish the result was found to relate female pronouns with “nurse” and male pronouns with “engineer” (*Patchen Barss,2019*). Bias in case of developing sensitive models like monthly-pay predictors might result in devastating outcome and a chaotic situation. Google photos was also recently in the news since it misclassified certain ethnic groups as “gorillas”. There is a compelling need that the creators and developers of these technology be aware of this fact and ensure that they don’t train the network on unbalanced or incorrect data. The unconsciousness of these developers results in seepage of bias into the system and which reflects in its functionality. This problem needs a more transparent approach. Mostly it is found that AI based algorithms are less traceable and that concludes one cannot trace back the working of the system when a potential bias is introduced into it. The training data is the crucial part which often acts as the gateway for bias to creep into the system(domination in training data)(*Figure.1*). The methodology adopted in collecting the training sample and the individual behind that reflects in the collected data that finally affects the outcome of the prediction system.

Figure 1. Bias in AI



Impacts of Data Scarcity

The data are the core of any AI system and data scarcity is again one of the hurdles faced during development of any Machine Learning based software. The time required to collect relevant data for that particular application slows down the pace of development. Often developers tend to underestimate the data requirements of a data-hungry system thus lowering its efficiency. Data collection process results in increasing expenditure and takes huge toll on the computational power of the system. Though effective means of processing data are available there still exists confusion relating to collecting large datasets. The Government of India announced in 2019, about setting up a National Centre for Artificial Intelligence to benefit from smart technologies. But there is a huge handicap from the researchers' side i.e. lack of enough data (Kaja Polachowska, 2019). To ensure that the developed AI systems are valid for global applications one needs to ensure that local datasets are available. There is also this one more constraint that the data collected must be feature-rich, in a manner enough to supply the system with the required information. Poorly informative data again results in ineffective prediction. This issue is mainly because Governments of developing countries often feel that maintaining and generating large volumes of data is expensive and can impact the economy of the nation. In poorly developed nations especially in the African continent many of the crucial data is missing, many births and deaths are not properly documented and there exists a serious "data deprivation". Supervised learning models require huge sets of labelled data but availability of these datasets is becoming increasingly scarce. Most of the data that is available for testing the models are often unstructured and thus they require more pre-processing before training the model on the dataset. There exist many different types of neural networks specialised for specific purposes. But lack of availability of data results in overfitting these models.

Unexplainable rationale behind decisions: Blackbox

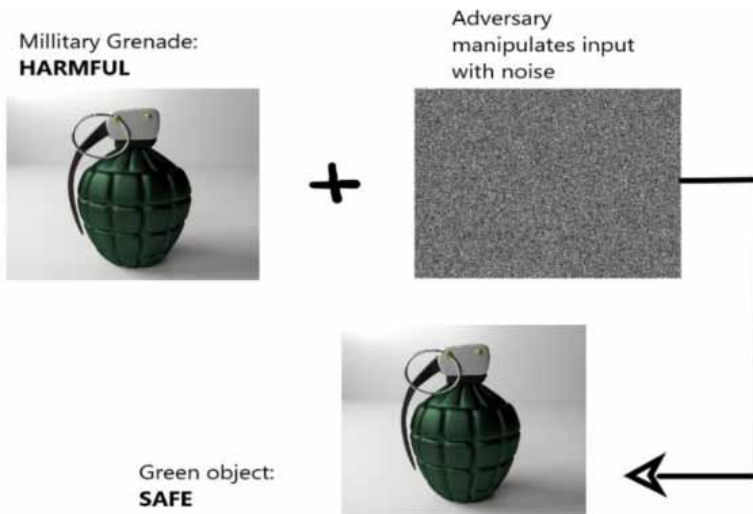
AI also suffers from another serious setback-lack of data transparency. The Machine Learning and Deep Learning implement certain algorithms like K-nearest neighbours (KNN), random forest, linear regression, logistic regression, Support Vector Machine etc. These algorithms finally end up in a conclusion but the logic behind the adoption of the concluded result is not provide (*Simon Chandler,2020*). The various factors or features that led to the conclusion is not stated explicitly resulting in ambiguity. When the rationale behind any decision is not provided with explanation there always is a feel of mistrust and question on the reliability of the system. Though there exist algorithms like linear models, rule-based algorithms and various tree-based algorithms that can be traceable but their application is limited to smaller data sets and they are handicapped to handle big data. Explanations behind the decision can result in finding discrepancies if any exist in that decision and they are a social transaction that also help in enriching the knowledge of humans (*Kaja Polachowska,2019*).

Imperceivable Adversarial attacks

Adversarial AI is the buzzword with respect to cyber-attacks. “Tit for tat” is the proverb most liked by hackers who employ AI and machine learning as a tool to destroy systems powered by the same technology. “Input attack” is one of the infamous ways used to hamper AI systems (*Marcus Comiter,2019*). Basically, machine learning algorithms are trained to identify matching patterns in the data being fed. Upon encountering a new set of data, they associate it with the previous instances and produce the result. The hackers manipulate the input dataset to increase the inconsistency in the data thus resulting in incorrect result. For example, in military applications to detect harmful objects like grenades and pistols this type of adversarial attack should be dreaded for they result in a huge impact on the system and its conclusions(*Figure.2*). These types of attacks tend to affect the reliability of the system. But there is also other type of poisoning attacks that prevent the machine learning models from detecting the patterns in the given data sets. The system is designed to malfunction according to the wishes of the attackers. These vulnerabilities in the system must be tackled properly in order to prevent the degradation of faith among the users. The inconsistencies in the dataset need not be explicit even a small change in the input vector can affect these brittle machine learning models. Many a times these attack patterns are imperceivable to the user’s eye. Attack patterns are often merged with the existing data set and often this technique of attack doesn’t require any access to the algorithm or the machine learning model (*Dr Peter Svenmarck et all,2018*). This susceptibility of these AI systems from the data-end makes necessary certain access control and restrictions while providing access to them. Another poisoning method

includes the algorithm poisoning which exploits the weakness of the algorithms of the machine learning model to hack into the system.

Figure 2. Adversarial attack resulting in misprediction



In certain critical fields like military the drones can be made to look camouflaged which subsequently cannot be detected by the smart system. This shows that the Artificial Intelligence systems have a long way to go to improve their efficiency.

The contemporary malware called the Emotet trojan is a very good example of a prototype-AI attack. The main aim of this trojan is spam-phishing this enters the system while on clicking malicious links and attachments with emails. Empowering this trojan with AI the developers have managed to create more customized and believable content that can easily trick users into clicking those links. These malwares use AI to analyse the social media content and also the email content from which they are able to customize the attack for every user. This malicious software is often trained to remain in the background without being detected and it studies the personal data and information of the victim and establishes its attack after possible survey. The AI's ability to understand the context and situation is indeed a welcoming change for positive applications but the very same can be used for operating these trojans without even being detected. The AI powered battles might even outwit and surpass the human defence strategies.

Many AI models are also being trained to possibly create a havoc. These negative AI systems also affect the security of critical applications like the military sector where the sensitive information of the military assets of the nation are at the risk

of being publicised or hacked (*Dr Peter Svenmarck et al,2018*). In the upcoming decades there is absolutely no need of any nuclear weapons or even bombs since the data are becoming powerful enough to wage a war between nations.

Rudiments of an AI system: Highly evolved Hardware

AI algorithms are programmed to run in milliseconds and are supposed to complete computations in a jiffy. This indicates that these systems are processing power intensive. This requirement forces new innovations in designing faster and robust processors that handle these algorithms and cloud computing can also help in handling large volumes of data but growing complexity of deep learning algorithms result in exponential growth in data volume. While developing AI algorithms one needs to think in different dimensions regarding the challenges that are to be faced and the problems that need to be resolved. Choosing the right algorithm for the application becomes challenging when there exists ambiguity in choosing the right data set. The existing infrastructure in companies are not capable of processing huge volumes of data, but adopting AI technology needs high-speed storage support and machine and deep learning models. There also exist integration issues while trying to integrate AI with the existing system.

Skilled Expertise: A Desir datum for any evolving field

For any technology to grow by leaps and bounds there is a requirement of good expertise and a strong knowledge base in that domain. Until today AI has been much in theory and implementation has taken speed only recently. Though there has been an explosion of interest today, still there aren't enough skilled persons. The above paradigm leads to a lack of proper human-AI interface. Certain important sectors like cyber security relating to nation's important database require persons with skill and expertise to design the AI systems so that they are fool-proof and secured and are traceable in case of any security breach helping cyber forensic investigations in future.

Though the intelligent systems make the computers more reliable and predictable and change the way they react to situations based on observation and pattern recognition that is still specific to a particular application. Generalised AI system would be the future stride for the human society to bring in more trust in the Intelligent systems.

EXPLICATION AND ANALYSIS FOR OVERCOMING THE CHALLENGES

Dealing with voluminous datasets

There have been many innovative solutions to the problems faced while working with Artificial Intelligence. The future world is predicted to heavily depend on this technology for a variety of their needs. Nearly 45% of the work could be automated by the use of AI and Machine Learning in the upcoming years. The sensitive data that fuels these machine learning models require proper protection and security so that they don't go into wrong hands and result in misuse of data that could upset any end user. Techniques like data anonymisation exist from past years (*Adkinson Orellana et al,2021*). In this process various techniques are enabled to disassociate a dataset from the identity of any individual to whom the data belongs. This ensures that the identity of the owner of the data is not revealed from any of the dataset entities. This method could satisfy the requirements of the era where the amount of data to be dealt with was low. But as the volume of datasets increased these techniques prove less effective. This technique is also identified as de-identification. There are possibilities of re-identification while using this technique. But this was used as a first line of defence against data breach or misuse. Also, the k-anonymization was one more improvement in this, instead of specifying any exact values for an attribute often a range of values was given that could be mapped to a group of k people always and not to a single individual. But in today's world the data comes from various sources like the smart phones and each dataset relating to a single individual consists of thousands of information pieces about the same person and these techniques fail to operate effectively when the dataset is highly multi-dimensional.

There has also been a growing popularity for differential privacy in which the memory capability of the Machine learning algorithm is assessed. It is evaluated in such a way that the data that it isn't supposed to remember is measured. This proves to be more efficient than compared to the k-anonymization because a certain level of noise is added to the data that prevents the re-linking or re-identification of owners.

Today many companies are adopting data access control mechanisms using several ways to ensure that any transaction with the data is being recorded in a tamper proof ledger even though the data usually is in pseudonym format (*Mac MacCarthy,2019*). There is also an increased adoption of algorithms that reduce the need of processing personal data.

Federated Learning: A novel approach to resolve Data Privacy Issue

There has also been a buzz about this new method called federated learning where the machine learning models are trained to operate on distributed data residing in devices like mobile phones which avoid the need for data sharing. The traditional machine learning model requires aggregation of data in a single machine for the model to work. This federated learning has opened up a new area of research in the field of AI since this helps in ensuring data privacy (*WeBank*). Many of the devices like smart phones and laptops generate a huge repository of data that contains sensitive information like the personal preferences of the user. The federated learning method does not have any necessitation like sharing of this personal with the machine learning model. This helps in also building personalised machine learning models. As of now AI algorithms have been operating much on the cloud and the data repositories but with federated learning these algorithms can directly operate on the data stored in the end devices. The bottleneck faced in adoption of this technique is the communication bandwidth. Mobile phones haven't advanced enough for efficient communication. There is a possibility of having a communication delay that could reduce the efficiency of the machine learning algorithm. The next important challenge faced by this method is the reliability of these devices like mobile phones. They need to be active during the entire run time and any fault might prevent the algorithm from utilising the full dataset of the device. This was first introduced by *Google* in 2017 and there have also been some discussions on the scalability and the hurdles to be faced while adopting this models that support decentralised data. There is also a significant reduction in the need to collect gigantic datasets by the companies that adopt machine learning algorithms. This is specified as a method of bringing the code to the data instead of moving the data to the algorithm. In federated learning method all the users are related to by a single identity. This facilitates in creating a virtual shared memory where the model parameters are alone exchanged between the devices that too in an encrypted manner. This solves one of the major issues in banking sector called the multi-party borrowing. This problem refers to any malicious borrower who tends to borrow money from a bank and never return and approaches another bank (*WeBank*). In this case the banks are supposed to zero on this malicious user by querying a central database after uploading all the related information of their customers which is like exposing a lot of personal data. This can be avoided in case of using federated learning mechanism.

Preventing Adversarial Attacks on Data

One more important advantage of federated learning is that since the data is never exposed, adopting this technology can seriously bring down the risk of Adversarial AI that attacks the dataset of a neural network by feeding inconsistent data that finally affects the efficiency and reliability of the system. But federated learning provides a possible escape where not only the algorithm but even the data set is made unavailable to the attacker. Poisoning the neural network becomes nearly impossible when the data resides only in the user device and is not shared to the system containing the neural network.

Cryptographic techniques help in encrypting the sensitive data that can provide a firewall kind of protection against potential hackers. Using an encrypted key that cannot be shared publicly and that can be used to infer the information from the data only to the intended user can help reduce data misuse (*Yves-Alexandre de Montjoye et al,2017*). The field of research in data privacy is ever-evolving and there are many techniques that are being experimented for potential use for AI applications and safeguarding big-data.

Uprooting bias from AI systems

As the complexity of algorithms increase there is an increasing need to develop unbiased algorithms. Understanding and measuring the extent of “fairness” of any algorithm before it is put to practical use. Leading tech giants like Google, IBM have enlisted a set of procedures that are to be adopted while developing AI systems without bias (*EC-Council*). Fact based research and testing can help identify the possibility of bias creeping into the system (*University of Southern California,2020*). Investing more time in collecting myriad data for the required application can also mitigate bias. Implementing certain algorithms that are designed to reduce the disparities in the dataset can reduce bias. Labelling the dataset for supervised learning must be done properly to ensure accurate prediction. Though some thresholds are being set to ensure fairness still human support is quintessential for any AI system to predict the result without any bias.

AI systems are often prone to amplify the bias in the dataset which can be an analogy of Bio-Magnification in species. New research has come up with the technique of adversarial forgetting approach which resides on the same line as that of selective amnesia (*University of Southern California,2020*). According to this approach the neural networks can be programmed to forget some of the inconsistent and irrelevant data in order to produce unbiased output. The computer scientists from University of Southern California have implemented this adversarial forgetting. According to them the neural networks fix the factors based on which they evaluate

Challenges of Developing AI Applications in the Evolving Digital World

the data and then filter out or ignore the data that results in a bias. Being invariant to specific aspects of the data is the key behind this technique. Statistical results have been the ones that are being depended upon till now for deciding which aspect of data to be invariant to.

Solving Data Scarcity

Proper estimation of the volume of dataset for the required application is to be calculated to ensure that there is no scarcity of data. The application of the machine learning should be considered based on which the size of the dataset can be predicted. For example, any proof of concept application requires a smaller dataset compared to any practical application like *Google Photos* that detect plants and shopping marts. Data augmentation techniques help to reduce the time and increase the efficiency in case of application like computer vision and image processing domains.

Explainability of AI becoming quintessential

Nowadays even AI is being exploited to solve the issues faced in cyber security, cyber forensics, medical diagnosis etc. Machine learning algorithms help to identify the potential attack vectors in a dataset but again there is still a huge question in the reliability of these systems. Though these technologies are prone to many other attacks but the speed and their time taken to analyse huge volumes of data is undeniably less compared to manual methods. Though the disadvantages of AI have an impact the good outweighs the bad making it a popular choice of the future tech-savvy world.

Taking an example of the emerging trend of open banking in finance sector which helps to dramatically improve the speed of transactions and help the customers access the bank services easily. The deployment of AI techniques in banking has led to open banking that allows customers to access the data held by the bank regarding them.

The need has arisen for making the algorithms more transparent and accountable for the decisions that they make especially when these decisions affect the social and cultural rights of individuals in certain applications (*Dr Peter Svenmarck et al,2018*). The dominant tech firms that adopt algorithms based on AI and ML are questioned about the correctness of the algorithm which becomes unexplainable due to the fact that these algorithms aren't transparent enough to understand their predictions. Though many researchers think of possibility of having a blockchain or ledger to keep track of the control flow of the algorithm there are several practical hurdles. According to an information science professor Byron, these algorithms are difficult to interrupt and interrogate. Machine learning models often consists of more hidden layers that explains the difficulty to track their flow. Certain cancer

detecting systems were developed to reason the cause for their decision they proved to be inefficient in the long run.

Explainable AI is an emerging trend which involves developing systems that answers the most important questions as to how the system made that decision? this technique involves the identification of certain machine learning algorithms that are inherently explain the rationale behind their decision. Decision trees, Bayesian classifiers etc are some of the examples of such algorithms. These algorithms on adoption provide a certain level of traceability and transparency that becomes increasingly essential in today's growing data scenario and they also don't compromise on the performance of the system (*Simon Chandler,2020*). Research is going to find out more algorithms that can help in providing the strong reason behind the prediction especially for medical uses and military uses. The widely used neural networks like random forest, k-nearest neighbours suffer from serious setbacks relating to their accountability. But they are the most popular algorithms that can solve nearly all the AI problems and are widely adopted but methods must evolve to make these algorithms more traceable in order to increase the sense of trust on the decision taken by these ML networks.

Sophisticated Hardware

Hardware-based acceleration is scaling up resulting directly from the advancements in AI algorithms and the need for efficient hardware. Customarily Graphic Processing Units (GPUs), Tensor Processing Units (TPUs) and CPUs chip architecture are applied in AI domain. These chip architectures fall short of a complete functionality that encompasses ability to support federated learning approach, integrate various chip architectures, multitier support etc. But neuromorphic architectures a new approach invented by Intel in 2017 is increasingly found to be effective for AI applications. The Neuromorphic architecture is modelled in view with the Central Nervous System (*James Kobielus,2020*). It can only supplement the hardware architecture for various applications and cannot replace GPUs or CPUs. They have densely connected semiconductor devices and an array of artificial neurons to facilitate AI algorithms to run effectively. This new revolution provides a promising future for further specialised hardware support for AI.

Tackling talent crunch

The empirical growth of any domain solely depends on the abundance of skill and expertise along with quality resources. The Artificial Intelligence Industry requires talented professionals with deep understanding of mathematical and computational concepts with critical thinking ability. A study brings to light that the AI professionals

Challenges of Developing AI Applications in the Evolving Digital World

have a higher probability of having a doctoral degree before they begin to develop applications (Sandeep Soni, 2017). This scenario has to be dealt with by collaborating with technical universities that can equip and train the professionals. Access to quality materials and vast datasets to experiment with can further help improve the expertise in AI industry. Idea pooling, collaboration with budding start up industries, conducting Ideathon and Hackathon events and motivating AI professionals with rewards can help to boost their in-depth knowledge of this domain and also would encourage young population to choose AI as their career path.

Table 1. Challenges and Recommendations: A review

Sl. No	Challenges faced while adoption of AI	Recommendations to abate the challenges
1.	Data Privacy	Data Anonymisation methods, K-anonymisation, de-identification and control mechanisms
2.	Bias in AI	Adversarial Forgetting and “fairness” evaluation methods
3.	Data Scarcity	Volume estimation and Data Augmentation
4.	Blackbox nature of AI	Explainable AI principles
5.	Hardware requirement	New neuromorphic architecture of processor chips
6.	Talent Crunch/ Lack of Trained professional	Specialised course training, Hackathon, Ideathon and other events to inculcate an idea of AI challenges.

These challenges are not trivial and need to be addressed appropriately (*as given in Table.1*) in order to fully automate and effectively exploit Artificial Intelligence systems for the applications in this digital era.

FUTURE RESEARCH DIRECTIONS

The further scope for this chapter could be to delve into various other issues faced while the adoption of AI technology. The challenges encountered while transforming a conventional system to a smart AI based system can also be researched further. The recommendations provided here are just in the research phase and any other possible concrete solution can be recommended in case if it is found to exhibit higher performance and cull out these drawbacks encountered.

The scope of work in this field would be to focus on to reduce the biased nature of AI algorithms. Many computer scientists have come up with explainable AI

that could possibly list out the data vectors that resulted in the predictions made by the system. But upcoming research should be focussed on removing the bias from dataset to bring AI into all sensitive applications. Though training the network on extensively large samples can increase the chance of fairness of the algorithm the learning speed is slow compared to that of humans. This factor has to be considered while developing AI systems in the future to improve their ability to handle huge data sets with varying dimensions since the future world demands such kind of systems that can be blindly relied upon.

The need of the hour is a safe and breach -proof AI that can make accurate predictions solely based on data being fed without any human-bias creeping into the system. Development of hardware powerful enough to support these power-hungry and data-hungry algorithms is also to be thrown light upon.

The current existing AI systems focus much on solving only one dimension of the problem. But the system was modelled to operate like human brain and the motivation behind AI basically is the brain. Human brains have the capability of handling and predicting multiple dimensions of a same problem but the current technology has to be extended in order to solve generic problems using Artificial Intelligence.

Effective methods of simulating the software before being practically put to use is also very critical to assess the performance of the developed AI software and check the prediction's credibility.

CONCLUSION

Artificial Intelligence is predicted to become a staple by the end of 2020 in nearly all walks of life despite being agathokakological in nature. But certain critical applications which prioritize data privacy over automation demand for more security in machine learning algorithms. There is also a dire need of data sets that are currently scarce that are to be made available to develop accurate predictions. Compatibility and cost of AI is not to be missed. These are the several road blocks that slow down the growth of the AI sector. They are to be solved and overcome before fully depending on AI for delicate applications like Cyber forensics, Medical Diagnosis, Banking, Quality Management etc that need high levels of accuracy and Explainability. All these challenges and the corresponding recommendations are discussed in this chapter with respect to developing AI applications in the evolving digital era.

REFERENCES

- Adkinson Orellana, L., Dago Casas, P., Sestelo, M., & Pintos Castro, B. (2021). A New Approach for Dynamic and Risk-Based Data Anonymization. In *13th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2020)*. Springer. 10.1007/978-3-030-57805-3_31
- Ammar, Abdelmoez & Hamdi. (2014). *Software Engineering using Artificial Intelligence Techniques: Current State and Open Problems*. Academic Press.
- Artificial Intelligence for a smarter kind of cybersecurity. (n.d.). Retrieved from <https://www.ibm.com/in-en/security/artificial-intelligence>
- Barss, P. (2019). *Eliminating Bias in AI*. Retrieved from: <https://techxplore.com/news/2019-07-bias-ai.html>
- Belani, Vukovic & Car. (2019). Requirement Engineering Challenges in building AI-based. *Complex Systems*.
- Bryson, J. J. (n.d.). *The past decade and future of AI's impact on society*. Retrieved from <https://www.bbvaopenmind.com/en/articles/the-past-decade-and-future-of-ais-impact-on-society/>
- Chandler, S. (2020). *How explainable AI is helping Algorithms avoid bias*. Retrieved from <https://www.forbes.com/sites/simonchandler/2020/02/18/how-explainable-ai-is-helping-algorithms-avoid-bias/#333c7b8f5ed3>
- Comiter, M. (2019). *Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About it*. In Belfer Center for Science and International Affairs, Harvard Kennedy School.
- de Montjoye, Farzanehar, Hendrickx, & Rocher. (2017). Solving Artificial Intelligence's Privacy Problem. *Artificial Intelligence and Robotics in the City*.
- Dixon & Eagan. (2019). 3 ways AI will change the nature of cyber attacks. Retrieved from: <https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/>
- Feldt, .de Oliveria Neto, & Torkar. (2018). *Ways of applying Artificial Intelligence in Software Engineering*. Academic Press.
- Kobielus, J. (2020). *Advancing AI with Neuromorphic Computing platform*. Retrieved from: <https://informationweek.com/big-data/ai-machine-learning/advancing-ai-with-neuromorphic-computing-platforms/a/d-id/1337587>

MacCarthy. (2019). *How to address new privacy issues raised by artificial intelligence and machine learning*. Retrieved from <https://www.brookings.edu/blog/techtank/2019/04/01/how-to-address-new-privacy-issues-raised-by-artificial-intelligence-and-machine-learning/>

Mohanty, R. (2018). *Will AI change the game for Cyber Security in 2018?* Retrieved from: <https://www.paladion.net/hubfs/Paladion--2018/resources-18/collaterals-18/will-AI-change-the-game-for-cyber-security-in-2018/Will%20AI%20Change%20the%20Game%20for%20Cyber%20Security%20in%202018%20-%20Whitepaper.pdf?hsLang=en-us>

Patridge, D. (Ed.). (1991). *Artificial Intelligence and Software Engineering*. Ablex.

Polachowska, K. (2019). *The 12 challenges of AI adoption*. Retrieved from <https://neoteric.eu/blog/12-challenges-of-ai-adoption/>

Soni, S. (2017). *Caught in the talent crunch?* Retrieved from: <https://www.magzter.com/article/Business/Entrepreneur-magazine/Caught-In-The-Talent-Crunch>

Svenmarck, D. P., & Luotsinen, D. L. (2018). *Possibilities and challenges for Artificial Intelligence in Military Applications*. Paper presented in NATO Big data and Artificial intelligence for Military Decision Making Specialists Meeting, Bordeaux, France. Retrieved from <https://blog.eccouncil.org/the-role-of-ai-in-cybersecurity/>

Tyugu, E. (2011). *Artificial Intelligence in Cyber Defense*. Paper presented at 3rd International conference on Cyber Conflict, Tallinn, Estonia.

UN Global Pulse. (2012). *Big Data for Development: Challenges and Opportunities*. Retrieved from <https://beta.unglobalpulse.org/wp-content/uploads/2012/05/BigDataforDevelopment-UNGlobalPulseMay2012.pdf>

University of Southern California. (2020). *How do we remove biases in AI systems? Start by teaching them selective amnesia*. Retrieved from: <https://techxplore.com/news/2020-02-biases-ai-amnesia.html>

WeBank. (2019). *Federated Learning*, white paper V1.0. Author.

ADDITIONAL READING

Challen, R., Denny, J., Pitt, M., Gompels, L., Edwards, T., & Tsaneva-Atanasova, K. (2019). Artificial intelligence, bias and clinical safety. *BMJ Quality & Safety*, 28(3), 231–237. doi:10.1136/bmjqs-2018-008370 PMID:30636200

Copeland, J. (1993). *Artificial Intelligence: A Philosophical Introduction*. Wiley-Blackwell.

Legg, S., & Hutter, M. (2007). Universal intelligence: A definition of machine intelligence. *Minds and Machines*, 17(4), 391–444. doi:10.1007/11023-007-9079-x

Liu, J., Kong, X., Xia, F., Bai, X., Wang, L., Qing, Q., & Lee, I. (2018). Artificial Intelligence in the 21st Century. *IEEE Access: Practical Innovations, Open Solutions*, 6(March), 34403–34421. doi:10.1109/ACCESS.2018.2819688

Singh, A. (2016). Artificial Intelligence in Various Domains of Life– A Review. *International Journal of Computer Science and Information Technologies*, 7(5), 2353–2355.

KEY TERMS AND DEFINITIONS

Adversarial AI: It is a machine learning technique that is employed to fool models by supplying them with malicious and incorrect input datasets.

Adversarial Forgetting: It is a methodology that mimics the selective amnesia in human brain applied to AI systems to remove bias.

Bias: Here bias refers to the prejudice or inclination of choice to one aspect of the decision. In AI bias refers to the prediction being made always in favour of the data set already the system has been trained with.

Blackbox: The unexplainable and opacity of the AI systems that don't reveal the rationale behind the prediction or decision taken.

Data Breach: This refers to any intentional or unintentional leak of secure or private or confidential data to any untrusted system. This is also referred to as information disclosure or data spill.

Data Privacy: It is the relationship between collection and dissemination of data. Certain companies hold sensitive data relating to their customers that they don't want to reveal to uphold the trust of their customers.

Data Scarcity: It is the unavailability of data that could possibly satisfy the need of the system to increase the accuracy and prediction dynamics.

Data Transparency: Here data transparency refers to the control flow of the data in the machine learning algorithm.

Datasets: This refers to any collection of data that holds the critical information about the current application.

Federated Learning: This is a machine learning technique that trains an algorithm on the decentralised data existing on different edge devices than compared to the traditional method of accumulating the data. This model was developed by Google and is an evolving technique that ensures data security.

Machine Learning: The study of algorithms and methods that help machines to learn implicitly without the help of instructions from the patterns in the data fed to the algorithms. This is an emerging trend of automation and is an integral part of artificial intelligence.

Chapter 12

Challenges in Developing Software in Today's Scenario: An Analysis at Developmental Stage Level

Srinivasan Vaidyanathan
Cognizant, India

Lakshmi Priya B.
Sri Sivasubramaniya Nadar College of Engineering, India

ABSTRACT

Software engineering emphasises to adopt a well-defined and structured approach to develop any software. Nonetheless, serious challenges exist in the software development process and these challenges are faced in developing software in today's scenario. This is majorly to satisfy the need for developing good quality product which has the capability to meet the "volatile user requirements" in organizations. As new products are developed to tend to the current technological needs, new challenges arise inevitably. So, until a new challenge is encountered, solutions to these unknown and newly arising challenges cannot be devised. Hence, a better software development strategy would be to realise all the previously encountered, more frequent or obvious challenges, and to design an efficient solution to these known challenges beforehand so that no more extra resources and time need to be diverted during the software development cycle in order to overcome the challenges. Therefore, recognizing and addressing the challenges in software development at each and every developmental stage is extremely necessary in order for organizations to succeed. In this study, the authors have attempted to structurally and systematically reviewing the literature to arrive at the software development challenges and provided ways of addressing those challenges. The study also provided for possible solutions and recommendations and scope for future research in this area.

DOI: 10.4018/978-1-7998-4900-1.ch012

INTRODUCTION

Planning, Analysis, Design, Implementation, Testing and Integration, and Maintenance form the stages of the software development cycle. All these stages are completed in order to develop the final product. As these stages are inter-related, the unidentified challenge at each stage might cumulate into a complex challenge at later stages which might be much more difficult to solve and demand more resources than the root challenge at an earlier stage. So, the realization of challenges faced in developing software will be of more use if the challenges faced at each stage are identified than generalizing it for the whole software development process.

The main objective of this analysis of identifying common challenges at each stage is to eliminate certain types of problems at later development stages. The risk factor in developing software would also be reduced. The wastage of resources and time can be prevented. It would also result in on-time completion of the product. This would definitely aid in creating high quality deliverables.

The chapter is organised to present the research method and delineation of challenges, to cover all the challenges at each software development stage which include challenges in planning, challenges in analysis, challenges in design, challenges in implementation, challenges in testing and integration, and challenges in maintenance. The New-Age Architectural and Management challenges in software development is also discussed. Useful solutions and recommendations for efficient software development are also suggested to overcome more frequently encountered challenges. Finally, the chapter is concluded with future scope for research in this area and an overall summary.

BACKGROUND

Research Method

Research method adopted was a systematic review of the existing literature and presenting the software development challenges and solutions. To identify the challenges and solutions, relevant set of articles were picked by searching well-known online databases such as, IEEE Xplore, ResearchGate, Elsevier, ScienceDirect, ProQuest. No filtration criteria applied for geography and publication times of articles. From the list, English is applied to reduce the list to match our choice. The following are the search strings used for finding articles.

- “Software+planning+challenges”
- “Software+Analysis+challenges”

Challenges in Developing Software in Today's Scenario

- “Software+Testing+challenges”
- “Software+programming+challenges”
- “Software+Maintenance+challenges”
- “Agile+methodology+Benefits+and+challenges”
- “Scrum+Benefits+and+challenges”
- “DevOps+Benefits+and+challenges”

Heeding only qualified papers for analysis, articles of adequate discussions on the theme of the chapter were carefully culled out from peer-reviewed and scholarly publications. List was further reduced and seminal articles of relevance covering the concepts searched for were hand-picked for further critical analysis.

Delineation of Challenges

Analysis of various renowned research papers, journals and websites have provided great clarity regarding the various challenges and difficulties in the software development lifecycle in various product development approaches such as waterfall model, agile methodology, scrum, DevOps, etc. The particular choice of one model over the other depends on various different factors such as project objectives, constraints, size of the project, etc and appropriate approach is chosen considering the benefits and challenges of that particular approach. A lot of references collected serve as proof for the fact that sequential model is less efficient for product development in the current scenario compared to iterative improvement models. Nonetheless, the specific project scenario has to be analysed well to choose the appropriate approach. Referencing research papers, journals, books, websites, etc from different geographies and publication times helped to preserve the diversity in the software development process and challenges related to the development process.

SOFTWARE DEVELOPMENT CHALLENGES

Challenges in Planning

Planning is a crucial step and foundation of any software development project. Improper planning can lead to huge loss of resources and valuable stakeholders. Therefore, at most care should be taken during planning stage. The entire project can fail if the timeline chart for software development is not properly framed. Lack of coordination amongst the team members of the project in the planning process will have catastrophic effects on the success of the project. One of the main issues is resource constraints (Seyed et al., 2011). If the required resource is limited,

then the planning process will become more complex and challenging as resource availability and optimal resource utilization should be given more emphasis than when resource is available in abundance. The objectives of a project elaborate the expected requirements of a product, that is, the goals the product is expected to achieve. These objectives are focused around project design, functionalities, content, quality and customer satisfaction. In many larger software projects, the lack of clarity in the objectives of the project can lead to many problems (Seyed et al., 2011). As any project is aimed towards satisfying all objectives, ambiguity in objectives formulation is unacceptable. The project completion can fall behind schedule if project monitoring by managers and supervisors is not properly devised during the initial planning stage. Ineffective communication and communication techniques between project planners can increase the risk involved in developing the project (Seyed et al., 2011). Optimal stakeholder involvement is necessary to build the desired deliverable. Too less or too much involvement of stakeholders may have negative side effects to project development. Failure to recognize the interdependency among systems can pave way for the failure of the project due to synchronization issues at a later software development stage. Improper prioritization of features or requirements can create instability in framework design. Planning is not a simple process as it needs intensive human expertise and skill. Therefore, skilled workforce should be employed to complete such important task (Seyed et al., 2011).

Challenges in Analysis

Complexity of the system to be developed can impact project completion. This complexity can be innate and is usually encountered in most of the larger software product development processes. Most project complexity cannot be completely eradicated but can only be made lesser complex (Seyed et al., 2011). Technical restrictions can also increase the complexity of the project. Technical constraints include the large number of technical problems and hindrances that will impact the project.

The feasibility study, technology selection and requirement analysis majorly constitute the software analysis process. Feasibility study is a detailed study of the user requirements in order to check if all the user requirements can be met or not. This lack of knowledge concerning the context may cause technical difficulties and financial problems, even a failure which could call into questioning the success of the entire work product developed (Ali Imam, 2018).

Technology selection analyses and enumerates all the technologies that are expected to be used to complete the project successfully. If old legacy systems are not completely discarded, then appropriate technology should be adopted which is compatible with old legacy systems to avoid the collapse of the project. Modern

Challenges in Developing Software in Today's Scenario

companies are not just satisfied with standalone solutions and expect third-party integration. Mostly, implementation of multiple systems in one project is expected and failure to do so will result in customer dissatisfaction. This puts the software development team under enormous pressure and makes them improve their skills and study more about other software technologies that be compatibly used with the software product that is being developed. Technologies which are suitable for use by multiple-level users from basic users to strict IT users should be adopted to serve all users instead of just one particular level of users.

Requirement analysis is taken up to list all the requirements. The requirements include human resources for developing the product, software and hardware required to accomplish the task successfully and these will be deeply analysed and enumerated out during the analysis stage. As much of development has to do with technology that's beyond the customer's expertise, customer's might not know what they actually want and so understanding and gathering the customer's mission, vision, goals, and other important parts of the project can be difficult and challenging. Changing requirements and addition of new features to existing project poses a great challenge in the process of software development. Therefore, all possible and imminent changes should be analysed and the development team should be prepared to accommodate such changes at least during initial stages in software development.

Challenges in Design

A major cause which complicates the process of software project development is the requirements volatility (Otero, 2012). Software can be altered, extended or improvised easily when it is properly designed. However, altering software can become tedious and lead to all kinds of complex problems when the software is not designed properly. The change in requirements is challenging because it has a huge impact on current and future developments efforts. This poses additional challenges to designers as they must not come up with designs that provide solutions to problems at the current instance alone but they must also anticipate future changes and should devise methods to accommodate those changes with minimal effort and cost. This necessitates that the software designers must have a strong understanding of the principles of software design concepts and must be skilled enough to manage any complex project and the changes along the software development.

Software processes involve a set of activities, actions and tasks that are required to build a high-quality software (Pressman, 2010). These also lay emphasis on a set of project-oriented or company-oriented constraints. As a result of software processes, work products are created. These activities include data/class design, architectural design, interface design, component-level design and other supporting management activities. These supporting activities include adopting a design

overview session, determining evaluation criteria for the quality of the product being developed, evaluating modularity of the design, probing reusability of the design, establishing design change management and version control procedures, design tool adoption, resource allocation and others. In a lot of scenarios, an organization's design procedure is not well realised and executed, poorly interpreted, or taken up with minimalistic expectations that do not consider the aspects that are crucial to establishing a successful design phase (Otero, 2012). This process is very challenging because necessary design process activities are many a times unnoticed, done in an ad-hoc manner, or simply not done at all.

Some product frameworks are needed to interoperate with the old legacy frameworks constructed with less established structure and older design methods. This results in software designers utilizing a bunch of design methods and innovations, all on a similar programming framework. In different cases, it is not possible to interoperate various plan models from existing code even after applying adjustments because the old legacy codes are significantly incompatible with the new code. This compatibility driven part of the design stage poses a great challenge for skilled software designers and software developers who are proficient in new technology rather in old legacy codes. The technology aspect of software design is challenging as it is always changing at a rapid rate, therefore the software designers must be familiar with the latest advancements and become well-versed in the application of these advancements while developing adequate knowledge in legacy technology as well.

It is the designers duty to enforce ethical guidelines during the design process and to thoroughly analyse the social impacts of their designs in the public domain, or in safety-critical systems; and to adhere to the appropriate professional rules and guidelines to ensure success of the product which is being developed (Otero, 2012). The ethical and professional practices aspect of software design is challenging as the software designers constantly face a number of pressures and objections from stakeholders that influence designers' decisions and reduce the clarity of the designer, most of which have consequences of social, ethical, or professional nature.

Designs are shaped by many different influences from stakeholders, the development organization, and many other factors. These influences can have cyclical effects between the system and its external influences, such that external factors affect the development of the system and the system affects its external factors (Otero, 2012). Managing these influences is essential for maximizing the throughput of the developed systems and their related influence on future business opportunities. The design inputs and influences from the system stakeholders and the developing organization is very crucial to the design process and neglection of these can result in the rejection of the software being built.

Challenges in Implementation

Lack of transparency and honesty throughout the implementation process about what product can be realistically delivered will lead to loss of valuable customers and stakeholders (Wagner, 2019). Meeting the expected outcomes from the process of implementation can become difficult if the milestones are not set and the deliverables are not realized.

Ensuring data integrity throughout the implementation process is of very high importance. By understanding the level of interoperability between the systems, data security, data consistency during data migration, and privacy standards are upheld (Wagner, 2019). If information is lost or misinterpreted during the data transfer, the data could be corrupted and not reliable.

Lack of preparedness among project team can lead to the downfall of software development cycle. The software development team must always have a clear view on the overall goals, processes and timelines. Every team member must be prepared to represent the interests of their department or team and work together to develop the implementation plan. Lack of support from the vendor and Inadequate software training tools can also ruin the software development (Wagner, 2019).

There is a high risk of failure during the implementation stage which will subsequently lead to decline in overall productivity of the company. This can decrease the self-confidence among the employees. This can also have detrimental effects on the Return On Investment (ROI) of the product being developed.

The most time-consuming activity of software implementation is the migration of data from the old legacy system to the new system (Wagner, 2019). It is absolutely necessary to find ways to make this easier and more accurate in order to adhere to the implementation timeline and minimize data errors and other issues. Lack of focus on this part early in the process can undermine training efforts and increase risk.

Programming methods, programming style and programming languages should be appropriately chosen to develop efficient and high-quality deliverables. Utmost care must be taken while selecting the data structures and devising the logic of the program. Select meaningful names for program entities and follow coding standards (Pressman, 2010). Constrain the programs by following structured programming practice (Bohl & Rynn, 2000).

Challenges in Testing and Integration

The developed software is tested to uncover the errors that were incorporated into the work product unknowingly and unintentionally. The testing methodologies include formal plan-based testing, whole testing in which the entire software is analysed and tested, partial testing in which the software is divided into parts for

testing, component-based testing which includes the process of testing when new components are added to the system. Various confusions arise as to which is the suitable testing methodology for a particular software (Pressman, 2010).

Verification is a type of static testing and validation is a type of dynamic testing. These processes contribute a significant role in testing process (Bhatt, 2017). Verification is performed to guarantee that the developed software meets all the details and is close to structural testing whereas validation is close to functional testing and is done by carrying out test cases in dynamic manner. Testing depends on practical detail and also on the code itself. Verification ensures that the work product is intended to deliver all functionality as per the client's specification. Verification is done at the beginning of the development procedure. It incorporates reviews of all client requirements and meetings, assessment to assess documents, code and specifications. Validation is to decide whether the framework consents to the prerequisites and performs all the functions for which it is built and meets the company's objectives and client requirements. Validation is done at the end of the development process and after verifications are completed. Testing is done either manually or automatically. It is discovered that computerized testing is superior to manual testing due to less effort and more accuracy.

Certain tests are difficult to be carried out manually (Bhatt, 2017). Thus, they are prone to mistakes and may be overlooked when done manually. As significantly observed, manual testing is ought to be monotonous, exhaustive, repetitive, boring and so no one wants to remain rounding about a testing strategy from time to time. Subsequently, a few testers have a tough time staying engaged during this process, and errors result in lot of doubts to arise. Automatic testing requires test data generation tools and test data validation tools which may not be technically or economically feasible by the company.

Testing is challenging as it often amounts to more project effort than any other software engineering action. A systematic strategy for testing software is indispensable and if testing is conducted haphazardly, time is wasted, unnecessary effort is expended and moreover, undetected errors sneak in through the product (Bhatt, 2017). An ineffective test plan and method will lead to the unordered construction of the software and concealment of errors at each stage in the construction process. The completeness of the test cases and testing tasks cannot be determined if the process of reviewing the Test Specification prior to testing is skipped. Ineffective technical reviews incorporate errors into the testing process even before the testing commences. The product requirements may not be specified in a quantifiable manner making them quite immeasurable for testing results. Lack of a continuous improvement approach for the testing process is also a challenge during the software testing process (Bhatt, 2017).

Challenges in Developing Software in Today's Scenario

The major challenges in developing a software is related to overcoming software integration problems that remain concealed throughout development process and surface only during the completion of a project. Extra costs, time delays and lowered software quality can be the results of incompatibilities and other integration complications. These possesses a huge threat to failure of a software project (Zafar et al., 2011). A strong and previously acknowledged integration strategy can be an effective solution to overcome integration challenges, but this requires a good understanding of what causes failure and how the failures can be mitigated. The cause of the failure can be challenging to realise for most of the software products.

Inefficiently devised module objectives and requirements disables the software developer to clearly see how the modules fit together in the combined big picture. This eventually leads to misalignment, rework and integration problems (Zafar et al., 2011). Absence of coordination between remote areas in which the software product is developed in parts prompts various technical issues which includes poorly tested segments and repetitive code. These issues cause critical problems in the testing and integration of the segments bringing about changes throughout the entire development process and at last postponing the completion of the project.

Inadequate comprehension of prerequisites and interface issues is a typical rationale behind failure of integration (Zafar et al., 2011). This issue arises when designers at one particular location have inaccurate understandings about the sub-systems developed at different destinations. This eventually results in contradictory software segments, poor structural choices, postponement of product delivery and critical integration issues. These distinctions stay covered up and show up at the hour of system integration where it is expensive to fix them compared to previous software development stages. Software integration is greatly affected when the coordination between software integrators decreases due to various factors. Diversity in procedures, systems and models at remote areas causes numerous issues particularly during the integration stage and once in a while makes it hard to build a homogenous product (Zafar et al., 2011). Communication gap between remote areas because of poor language abilities of the software developers arise. This creates issues in understanding the requirements even if they are very clearly and comprehensively explained. This is because the understanding may differ in different locations. Rapidly changing prerequisites and unexpected technical interdependencies influence the software integration process. Sometimes, the time reserved for system integration and testing is being spent on finishing the integration itself which is detrimental to on-time software completion (Zafar et al., 2011). Subsequently, the process timeline or plan gets crushed. Long-term lack of knowledge about proceedings at remote areas makes the software developers incapable to locate the opportune individual to carry out a particular task or on-time data with respect to project status, its history, data about modules created at remote areas, users of the product and integration process. This prompts

coordination issues, and an expanded likelihood of defects. Lack of a reconciliation methodology or plan with plainly appointed duties to software developers is a typical issue which leads to significant overruns in the coordination as far as time and effort is concerned. Lack of step by step prerequisites and comprehensive documentation for worldwide groups makes it hard for the designers to accurately interpret what is actually required by the client (Zafar et al., 2011).

Challenges in Maintenance

Various research studies show that product support and software maintenance consume 60% to 80% of the entire cost of the whole software development life cycle (Abran & Moore, 2014). These figures also show that the upkeep or maintenance costs are essentially because of upgrades, instead of corrections. One of the significant key issues is restorative changes since it is difficult to find the right module to do the changes and alterations amongst many available modules which are equally good choice points. It is also hard to perceive the constructed code base. A brief change in the fundamental plan may demand design changes that take a great amount of time to implement (Gupta & Sharma, 2015). Mistakes in design are hard to rectify since it requires some investment and comprehension of the whole code base and are directly connected to risks.

One of the most significant difficulties in software maintenance is to discover the impacts of a proposed change or alteration on the remaining framework (Gupta & Sharma, 2015). Impact analysis is the activity of evaluating the likely effects of an alteration on the plan without increasing unexpected side effects. The task includes monitoring the correctness of an anticipated adjustment and assessing the risks related with its completion, in addition to the appraisals of the impacts on properties, functionalities, robustness and advancement of the product. This process leads to the determination of the overall cost of implementing the changes. As the overall impact and coupling of system components is unknown or only partly known to maintenance engineers, this analysis process is difficult to adopt in practice. Versatile or adaptive changes are often difficult because of lack of data about how the product is being altered. The various realities of the new innovation or change in accordance with the existing implementation can be hard to understand and to implement. Examination and finding interfaces to the new implementation are troublesome. Issues because of uneven preliminary structure are also a matter of concern (Gupta & Sharma, 2015).

Software maintenance in firms mostly adhere to changes that are of versatile types which can be difficult to incorporate into the existing framework within the stipulated time frame. So as to accommodate any changes effectively and without any problem, the system settings and configurations need to be understood by the

Challenges in Developing Software in Today's Scenario

maintenance engineers thoroughly. Product perception is essential for any change in the system. The changes can have an impact on different segments of the framework that are interlinked, thereby causing inconsistencies somewhere else in the framework (Gupta & Sharma, 2015). Hence, this may result in additional changes to be applied to interlinked segments and has the potential of even triggering a chain of changes. This chain response is called change propagation which may make the framework to be partly inconsistent if implementation of changes or testing is incomplete.

Since the changes are done in segments of the framework during maintenance, regression testing gains more emphasis (Gupta & Sharma, 2015). The reason for regression testing is to guarantee that changes made to the product have not unfavourably influenced other existing features and functionalities of the work product. Regression testing is generally performed by undertaking a few, or all, of the test cases built to test changes made to the work product. To guarantee that all projects perform only in the intended manner, tests produced at prior stages might have to be re-run. As a program is developed, the regression test sets become bigger since old tests are subsequently included, and henceforth the expense of regression testing increases. Because of inadequate time and cost limitations, redoing all the past test cases after every minor programming correction or fix is impossible and is not done in current software practices. During maintenance, designers should make adjustments to the structure as well as information of the database interconnected to the product framework undergoing maintenance. Repetitively applying these progressions can be risky since the maintenance engineers may not be prepared to handle enormous databases. The existing quality of the framework can be a maintenance issue. The issues for the most part are quality of software and design issues such as non-compliance to various standards.

Older legacy frameworks can give rise to a few issues in maintenance process because of absence of support teams' information, item quality and developer time (Sokappadu et al., 2016). Older frameworks may require more equipment and programming changes as compared to recently deployed software systems. The older operating environments are more difficult to maintain. The documentation and software tools available for the legacy systems can be inadequate for current maintenance. A legacy software mostly requires many alterations and corrections throughout its life cycle. Also, as newer software are built, compatibility between newer software and legacy software reduces which increases the difficulty in terms of maintenance effort and cost.

A system with more interconnected components or modules can be difficult to maintain as the interdependencies amongst various components requires more time and effort to be comprehend by the maintenance engineers (Sokappadu et al., 2016). The difficulty in maintenance is directly proportional to the complexity of the system. The type of systems utilized in the development of a product can cause issues in the

maintenance of the product in the future. One of the most widely recognized reason for maintenance issue which the software development companies need to confront is that they are not able to bring in required resources and skilled personnel to maintain their software product due to poor decision on framework plan and design at the time when the software was designed and developed. During the maintenance procedure, software might need to be rebuilt when the existing architecture in the software do not support the changes which are requested by the stakeholder.

A team of maintenance engineers work on a number of projects concurrently which increases their workload and pressure. Therefore, deadline for all projects are difficult to be met which leads to customer dissatisfaction and stakeholders' drop out from the project. Clients' request for major modifications can be difficult to accommodate during the maintenance process as additional resources need to be diverted for this purpose which can highly affect other projects under development. Clients' limited expertise and absence of software training about the system adds to maintenance issues in companies (Sokappadu et al., 2016). The clients can also have exclusive requirements from the maintenance team through their change requests which can be out of the product scope or out of the limits and capabilities of the support group. Another issue due to clients' desire is that they anticipate that their requests should be executed and completed in a short time span, and this may not be plausible for the maintenance team which is already under great burden and pressure.

Clients may require drastic changes to be made in the work product even after delivery but the software development team which developed the product might be currently working with the development of other products and may presently be unavailable to carry out this extra work which will pose a huge challenge for the company and its reputation (Sokappadu et al., 2016). This increases the work and so the work should be properly assigned to different workers who have knowledge and expertise on the projects which they are assigned to. Also, this work cannot be assigned to free developers as they have no prior knowledge about the design, development and functionality of the product. If the software company hands over the responsibility of maintenance work to new developers or programmers, then the company needs to provide prior training to the programmer on the developed product, which leads to the increase in time, cost and effort for the maintenance process. Maintenance problems also include staff turnover. If there is a high staff turnover in the maintenance team, the newly recruited maintenance engineers may not have the adequate knowledge in managing changes in programming frameworks. Thus, additional time must be devoted for the training of the new recruits, consequently expanding maintenance cost.

NEW-AGE ARCHITECTURAL CHALLENGES

Software technology is becoming increasingly indispensable in the current scenario. It is influencing lives, businesses, manufacturing ventures, agriculture, health and many other different fields in a way that could never have been anticipated a few decades ago.

Software does not require complex machinery to be created, it may very well be developed on personal computers today which are accessible to all the individuals in the general public. This gives an impression that it can be created by anybody with specialized abilities and those who are willing to gain required proficiency with some easy to utilize programming language. At the same time, its intangibility makes it more invisible creating an illusion that it is only a minor part of the devices it is controlling hiding the fact that it is a core part of any other software or hardware that it controls (Koussouris & Nitto, 2016). Therefore, generally, there has been an inclination to direct investments and focus toward the development and enhancement of the devices as opposed to the software itself and falsely claim that the improvement in devices is more important than the improvement of the underlying software which operates it. As science and technology advances, the demand to build software to support the scientific researches increases phenomenally. This can be challenging as the software developer can face a huge difficulty in understanding the domain for which the software application is developed. Defining a scope for these can also be difficult (Koussouris & Nitto, 2016). Both application domain specialists and software engineers are required coordinate with each other in order to complete such a project. This is particularly mandatory for scientific software development.

Researches in software engineering domain are constantly highlighting that high-quality software requires explicit aptitudes and the reception of good and controlled development and operation practices. Software development requires correct instruments and techniques throughout the lifecycle of software, through the usage of new technology and new ideal models, yet guaranteeing efficiency of procedures and quality of software. The most recent progressions have triggered an expansion of perspectives in testing, deployment, management of new software releases and have simultaneously permitted specialists and professionals to recognize new and efficient methodologies for making and operating software and services (Koussouris & Nitto, 2016). The configuration, assembly, management and maintenance of more infrastructural software can be challenging due to the way the software interfaces with other parts of the software. The reliability on a particular software is also a very important factor in building software for current applications and needs.

Software development process is challenging due to the varying procedures and innovative viewpoints of the stakeholders and software developers (Koussouris & Nitto, 2016). Stakeholders are unable to provide a more definite and concrete portrayal

of the application for which the software is expected to be designed and developed. In consideration about process, methodologies and productivity, existing ideas should be restructured and rebuilt for meeting the present needs of the industry. Another idea of profitability ought to be characterized, where “lines of code” should not be used as the accurate measure of productivity any longer and software must be estimated only on other important characteristics such as ease of use, quality and versatility. Lack of additional opportunities to easily acquire client feedback and data can possibly be detrimental to software improvement and software evolution widening the development and improvement cycles (Koussouris & Nitto, 2016). Software is also the main driving force behind the CPS (Cyber Physical Systems) and IoT (Internet Of Things) standards, and their further development is intensely connected to the capacity of software to be both trustworthy and versatile to continuous changes and also aid the empowerment of diverse application contexts. The principle challenges caused by IoT incorporate the improvement of models, strategies and configuration apparatuses for IoT or CPS empowered applications going past formal techniques and research to make reflections and formalisms for reasoning and building about frameworks with diverse and increasingly complex components. CPS additionally need novel techniques for programming flexibility, scalability and maintainability. All things considered, frameworks should be consistently altered and kept up to meet changing prerequisites during runtime. In this context, the new requirements are likely to be run time adjustment of software Quality Assurance in CPS conditions capable to manage vulnerability and inconstancy simultaneously, software awareness of hardware to guarantee web scale execution and adaptability.

There is a great need to examine into design patterns development. New patterns at the architectural level portraying the commitments or requirements to be satisfied by the framework in which the software is running, and to approve and institutionalize them are required. Strategies and the most proficient method to apply them into a dynamic context environment are also required (Koussouris & Nitto, 2016). Accordingly, issues, for example, bringing together perceptions, structure design, interoperability, devices incorporation, stimulation and investigation ought to be carried out which can be challenging. Analysing such patterns will allow the software being built to reach a better level of quality and eradicate customer dissatisfaction. At present, the issue of offering appropriate quality guarantees must be re-examined to adapt to the developing patterns in software designing and quicken the selection paces of novel techniques for software development.

At present, although Big Data offers the capacity to attain a lot of information on the behaviour of an application, limited advancement has been accomplished in creating feedback analysis tools (Koussouris & Nitto, 2016). Thus, along these lines further research is required in the design level, and in the capacity to pinpoint explicit underlying root causes of performance degradation in the application code and in the

Challenges in Developing Software in Today's Scenario

utilization of Artificial Intelligence strategies for quality engineering. Additionally, there is a lack of reference quality instances of code and extra-functional properties in numerous classes of applications and domains. One other central part of research directly connected to any product designing action is that of requirements engineering. Moving towards stand-alone applications from monolithic applications and adopting a Computerized Single Market and Connected-world mentality builds multifaceted nature of information capturing and representation. New gadgets, services and even people become part of a software powered environment along with adaptability, constant evolution and interconnection contradicts current prerequisite building as existing methodologies don't represent dynamicity of utilization and unknown requirements. There is a strong requirement for a profoundly unique way to deal with emerging behaviour from systems and clients. Technological advancements and patterns are revealing insight into potential research points including multichannel big data examination for necessities elicitation from enormous scope locales like smart city foundations which interconnect people, machines and mostly software qualities and conduct, novel strategies towards client for removing low priority necessities appropriately.

Protection and security at configuration time as well as during runtime of the product is another significant aspect that ought to be handled to conform the advancement of software improvement techniques in the scenarios where the vulnerabilities is consistently extending (Koussouris & Nitto, 2016). Unique consideration with respect to protection and security must be given in complex circulated frameworks which in numerous cases needs to deal with huge information volumes. Difficulties include identification of contextual systems patterns related to privacy leaking code snippets, secure computation of data structures, approaches for establishing optimality of encryption levels, continuous source code assessment at design time as well as vulnerability assessment of the developed applications, secure packaging and placement mechanisms of the developed applications over programmable infrastructure, mechanisms supporting efficient and secure management of applications and services, real time risk identification and assessment techniques along with the triggering of the appropriate mitigation actions, security and privacy mechanisms focused on distributed and big data application.

As datasets managed by software are continually expanding, aside from providing novel calculations, new framework structures and programming foundations should be capable of readily operating with large datasets without demanding drastic changes to be applied to the software to make it handle big data. Research difficulties for software development in this aspect include novel devices utilizing systems of Artificial Intelligence and data mining (Koussouris & Nitto, 2016) to reveal hidden knowledge aspects and extract information from sensor-based architectures, excavating

knowledge which is impossible for humans to do manually, but is necessary to be brought into human attention and supervision.

Finally, there is a constant need towards hastening open source software innovations (Koussouris & Nitto, 2016). Numerous ventures need legitimate network commitment and management structures, quality confirmation and a vision on the most proficient method to add to the open advanced market. Open source software administration includes various challenges related to software engineering and production processes identified with software development, including approach and apparatus support for the recognition of logical inconsistencies, ambiguities, and gaps in requirements specification and decoupled designs. Moreover, open source software creation incorporates authoritative difficulties that may be met by an interdisciplinary approach focusing on the creation and the board of networks of code patrons, commentators, analysers, first level clients, and so forth and a complete improvement and communication approach consolidating existing devices under a normal, formalized arrangement of procedures.

MANAGEMENT CHALLENGES

Apart from these challenges at each stage, there may also be other challenges which need to be addressed as well. These include globalization which cause a high competition amongst software companies. Older legacy systems and infrastructure issues span almost across every software development stage. SaaS (Software As A Service) offerings are taking over which pose a huge challenge for the software development companies. Amongst various users of software, some may be basic users, some may be power users, administrators and some may be strict IT users. This great diversity in users leads to multiple complex user level requirements which can be challenging to meet. The companies face huge difficulty in attracting and retaining applicable talent in their companies in current highly competitive scenario. The concern about the Return On Investment (ROI) can build huge pressure on the companies. A limited budget can threaten the quality of the product being developed with increased effort and difficulty to choose among the functionalities which should be retained and the ones to be dropped and the pressure due to compromises on the quality. Poor project management and project development also leads to software project failure. Frequently stakeholders and management are unwilling to allocate budget for activities of a project which they are not a part of but which might be very crucial for the project.

SOLUTIONS AND RECOMMENDATIONS

Overarching

Challenges in software developed are inevitable. Few solutions are more effective in order to overcome frequently encountered challenges. Software requirements should be clear to understand by everyone, complete in its formulation, feasible to implement, easy to test and should only include the requirements that are consented to by clients and stakeholders. In agile development, close coordination with stakeholders and clients are very important to guarantee that changing or rising necessities are accurately comprehended and implemented. Timeline chart should be properly framed which permits adequate time for planning, analysis, design, implementation, testing and integration. Also, too much work load on developers should be avoided to maintain optimum productivity. Satisfactory testing is mandatory to assess the functionality of the built software. It is highly advisable to begin testing at an early stage, re-test after fixes or changes, plan for allocating sufficient time for testing and debugging. Start implementing the basic necessities which are indispensable and be prepared to face situations in which the clients or stakeholders demand unnecessary changes and increments once software development process has started, and be set up to clarify any concerns regarding the work product and its results. In the event that changes are important, they ought to be reflected properly in software development process and the related timeline chart should be modified accordingly after considering the changes which need to be applied. Coordination with clients and stakeholders to realize their requirement is the secret of success for software development. In case of agile software development, initial requirements are volatile and might change fundamentally, necessitating that efficient communication procedures be set up and followed. Provide proper documentation of the developed software and extend maintenance facilities in future if the client requires any support.

Approach-Focused

To overcome the inherent challenges in traditional software development methodologies, new approaches such as Agile, Scrum and DevOps are opted nowadays.

AGILE METHODOLOGY

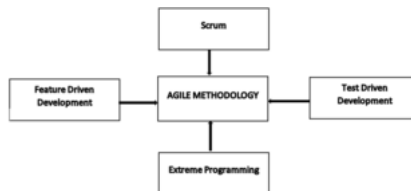
Agile is a very powerful software development tool. In agile methodology, iterative development and prototyping are opted to accommodate the volatile requirements.

This methodology is more efficient than the traditional software development processes as it enables product delivery in increments (Kumar & Bhatia, 2000).

Agile methodology includes other methodologies like Scrum, Crystal Clear, Extreme Programming (XP), Adaptive Software Development (ASD), Feature Driven Development (FDD), and Dynamic Systems Development Method (DSDM) Crystal, Lean Software Development, etc (Wang et al., 2009).

Extreme programming improves a product by making few changes in the software development stages. In planning stage, the whole project is divided into iterations and release plan is also devised. The design is refactored wherever possible. Test driven development is adopted in the coding and implementation phase. In scrum, product is developed through a series of iterations called sprints. Each sprint is approximately 2 to 4 weeks long. The Scrum Master is responsible to supervise the project as there are no traditional software engineering roles (Kumar & Bhatia, 2000). Feature driven development is a client-centric and architecture-centric software process (Livermore, 2007). It emphasises on the creation of a features list which will form the basis of planning, designing and building. In crystal method, more importance is given to product development rather than the tools being used or processes (Livermore, 2007).

Figure 1. Agile software development methodologies



There are some limitations in agile methodology. This method may not be suitable for large projects as numerous iterations are required which also increases the budget. The main focus is on product delivery rather than design quality (Kumar & Bhatia, 2000).

SCRUM

After completing the requirement elicitation, the Scrum team organizes a sprint planning session where the important tasks to meet the requirements are separated into small, more easily manageable tasks. The team prepares a sprint backlog and

Challenges in Developing Software in Today's Scenario

planning is done. The group chooses a period for each run. The group gets together regularly for a brief Scrum meeting. This is the cycle followed by a Scrum group throughout the product development (Ma'arif et al., 2018).

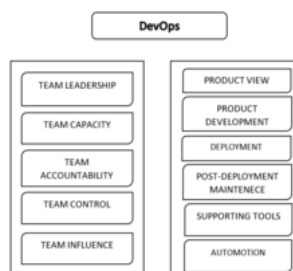
Scrum helps in keeping check on the progress of the product due to sprint planning that allows product release with features added incrementally (Ma'arif et al., 2018). The team gets clear picture of the work product through scrum meetings. Customer and stakeholder feedbacks are useful in improving the quality of the work product in the next incremental release. Scrum enables effective use of time and money (Chandana, 2019).

Sprint planning can be very challenging for the scrum teams and place a lot of pressure on them. The entire project is likely to collapse with improper implementation (Ma'arif et al., 2018). Lack of cooperation and involvement of scrum team can have detrimental effects on the project. Daily meetings can build up frustration and depression among team members. This framework is more likely to fail if there are more inexperienced team members. Staff turnover can have huge negative impact (Chandana, 2019).

DevOps

DevOps is a set of practices to strengthen the collaboration between development and IT operations. The major focus of DevOps is continuous delivery and deployment of software product (Senapathi, 2018). It emerged to bridge the gap between software development and software deployment (Debois, 2011).

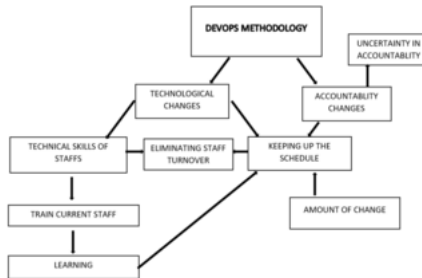
Figure 2. DevOps



DevOps are more suitable for quick development and deployment of products. The detrimental effects of market changes can be managed better using this methodology. Clarity on product development and deployment is a huge advantage in this approach. Customer feedback can be used to improve the quality of the product.

Challenges in implementing DevOps include requirement of highly skilled workforce, changing technology, uncertainty in responsibilities, etc (Senapathi, 2018). DevOps developers need to be highly skilled. New DevOps techniques can be hard to implement into the industries within short duration. This approach is relatively expensive as more skilled labour is required.

Figure 3. Challenges in DevOps implementation



FUTURE RESEARCH DIRECTIONS

Organizations are increasingly facing the challenges of software development as a result of emerging technologies, and to keeping up with their move towards digital transformation. Implementing digital solutions require organizations to enable radical changes at Business Model, Operating Model and Technology Model layers. One of the Operating Model layer level changes require paradigm shift to newer development methodologies like Agile, Scrum and DevOps. This research has taken a overarching view of the challenges in the traditional software development methodologies, and how newer methodologies like Agile, Scrum and DevOps help overcome such challenges, shedding light on their own challenges too. Future research can pick-up each methodology and delve in greater detail, their approach, features and execution to creating humongous impact to delivering Digital projects. A case study based approach to comparing and contrasting the newer methodologies aligning to the objectives of various projects, will add further value to the theme of this chapter.

CONCLUSION

Many organizations are losing competitiveness due to their lack of adoption to newer software development methodologies. This chapter has perused the research tradition and found that in order to develop a high-quality deliverable, all afore-

Challenges in Developing Software in Today's Scenario

mentioned challenges need to be considered and resolved in view of the solutions and recommendations provided. The representation of software development challenges in regard to the stages in which they are encountered serve to be more useful to devise specific and efficient solutions. This study has lent numerous perspectives in that direction, showing the important software development challenges and overcoming them. Organizations must understand and adopt newer development methodologies such as Agile, Scrum and DevOps in order to have competitive edge.

Table 1. Overview of challenges

Waterfall model	Agile Methodology	Scrum	DevOps
<ul style="list-style-type: none"> · Clarity in requirements is crucial as this model cannot accommodate changing requirements · Rigid sequential model · Relatively expensive bug fixes · All the product constraints must be satisfied within single development cycle · Improper prioritization of requirements or features can create instability in framework design · Relatively more technical and resource constraints · User feedback cannot be used to drastically improve the product · Relatively more interoperation with old legacy frameworks may be demanded · Testing and debugging the entire product in one go can be difficult and few bugs may get through undetected · Large risk factor · Time and cost overruns 	<ul style="list-style-type: none"> · Relatively expensive · Coordination and synchronisation among team members is indispensable · Not suitable for very large projects · Design quality may be compromised 	<ul style="list-style-type: none"> · Sprint planning can be very challenging and may exert a lot of pressure on scrum team · Entire project may collapse with improper implementation · Requires experienced, cooperative and dedicated team members · Daily meetings can build up frustration and depression 	<ul style="list-style-type: none"> · Demands highly skilled workforce · Inability to implement new DevOps techniques instantly in industries · Relatively expensive · DevOps developers should be well aware of all their responsibilities · Shortage of tool knowledge

REFERENCES

- Abran, A., & Moore, J. W. (2014). *Guide to the software body of knowledge (SWEBOK). Ironman version*. IEEE Computer Society Press.
- Ahmed, Ahmad, Ehsan, Mirza, & Sarwar. (2010). *Agile Software Development: Impact on Productivity and Quality*. IEEE.

- Bass, L., Clements, P., & Kazman, R. (2003). *Software Architecture in Practice* (2nd ed.). Addison-Wesley.
- Bhatt. (2017). *A Survey of Effective and Efficient Software Testing Technique and Analysis*. Academic Press.
- Bohl, M., & Rynn, M. (2000). *Tools for Structured Design: An Introduction to Programming Logic* (5th ed.). Prentice Hall.
- Chandana. (2019). *Scrum Project Management: Pros and Cons*. Retrieved from <https://www.simplilearn.com/scrum-project-management-article>
- Debois, P. (2011). Devops: A software revolution in the making? *Cutter IT Journal*, 24, 8.
- Gupta & Sharma. (2015). *Software Maintenance: Challenges and Issues*. Academic Press.
- Imam, A. (2018). *Software Development Life Cycle: The phases of SDLC*. Retrieved from <https://blog.testlodge.com/software-development-life-cycle/>
- Koussouris, S., & Di Nitto, E. (2016). *Current and Future Challenges of Software Engineering for Services and Applications*. Academic Press.
- Kumar & Bhatia. (2012). Impact of Agile Methodology on Software Development Process. *International Journal of Computer Technology and Electronics Engineering*, 2(4).
- Livermore, J. A. (2007). *Factors that impact implementing an Agile Software Development Methodology*. IEEE. doi:10.1109/SECON.2007.342860
- Ma'arif, Shahar, Yusof & Satar. (2018). *The Challenges of Implementing Agile Scrum in Information Systems Project*. Academic Press.
- McConnell, S. (2004). *Code Complete* (2nd ed.). Microsoft Press.
- Otero. (2012). *Software Design Challenges*. Retrieved from <http://www.ittoday.info/ITPerformanceImprovement/Articles/2012-06Otero.html>
- Pressman, R. S. (2010). *Software Engineering: A practitioner's approach* (International Edition). McGraw Hill.
- Senapathi, Buchan, & Osman. (2018). *DevOps Capabilities, Practices, and Challenges: Insights from a Case Study*. Academic Press.
- Seyed, Danesh, & Ahmad. (2011). *Software release planning challenges in software development: An empirical study*. Academic Press.

Challenges in Developing Software in Today's Scenario

Sokappadu, Mattapullut Gopaul, Paavan, & Devi. (2016). *Review of Software Maintenance Problems and Proposed Solutions in IT consulting firms in Mauritius*. Academic Press.

Wang, S., & Xie. (2009). Analysis on Agile Software Development Methods from the View of Informationalization Supply Chain Management. *3rd International Symposium on Intelligent Information Technology Application Workshops*.

Zafar, A. (2011). *Investigating Integration Challenges and Solutions in Global Software Development*. Academic Press.

ADDITIONAL READING

Whittaker, J. A. (2000). What is Software Testing? And Why Is It So Hard? *IEEE Software*, 17(1), 70–79. doi:10.1109/52.819971

KEY TERMS AND DEFINITIONS

Cyber Physical System: A framework where a component is controlled or observed by computer-based calculations. In these systems, the physical and programming segments are profoundly interlaced, ready to work on various spatial and transient scales, display numerous and unmistakable behavioural modalities, and interface with one another in manners that change with setting.

Data Integrity: The support and the affirmation of the precision and consistency of information over its whole life cycle, and is a basic viewpoint to the plan, execution and use of any framework which stores, processes, or recovers information.

Internet of Things: An arrangement of interrelated processing gadgets which may be mechanical and computerized machines and the capacity to move information over a network without expecting human-to-human or human-to-computer cooperation.

Open-Source Software: A program in which source code is delivered under a permit where the copyright holder awards clients the rights to study, change, and distribute the product to anybody and for any reason. Open-source programming might be done in a cooperative public way. Open-source programming is a case of open collaboration.

Prioritizing Requirements: The method of distinguishing and ordering a given set of requirements with the objective of getting a common reasoning for apportioning them into subsequent product releases.

Regression Testing: A type of software testing to confirm that new modifications done to the product has induced great changes before the change. In regression testing, not all possible paths in the program are tested. Rather a part of the test cases is selected and re-run to find the error in the program.

Requirements Volatility: The requirements for a product is not fixed but it is constantly changing throughout the software development life cycle.

Test Specification: A report which specifies what functionalities and capabilities of the software are to be tested during the testing phase, the method of testing and the frequency of the testing process.

Compilation of References

- Abba, E., Aibinu, A. M., & Alhassan, J. K. (2019). Development of multiple mobile networks call detailed records and its forensic analysis. *Digital Communications and Networks*, 5(4), 256–265. doi:10.1016/j.dcan.2019.10.005
- Abran, A., & Moore, J. W. (2014). *Guide to the software body of knowledge (SWEBOK). Ironman version*. IEEE Computer Society Press.
- Adkinson Orellana, L., Dago Casas, P., Sestelo, M., & Pintos Castro, B. (2021). A New Approach for Dynamic and Risk-Based Data Anonymization. In *13th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2020)*. Springer. 10.1007/978-3-030-57805-3_31
- Ahmad, T. (2019). Technology Convergence and Cybersecurity: A Critical Analysis of Cybercrime Trends in India. *27th Convergence India Pragati Maidan*, 29-31. Available at SSRN: <https://ssrn.com/abstract=3326232>
- Ahmadi, M., Ulyanov, D., Semenov, S., Trofimov, M., & Giacinto, G. (2016, March). Novel feature extraction, selection and fusion for effective malware family classification. In *Proceedings of the sixth ACM conference on data and application security and privacy* (pp. 183-194). 10.1145/2857705.2857713
- Ahmed, Ahmad, Ehsan, Mirza, & Sarwar. (2010). Agile Software Development: Impact on Productivity and Quality. IEEE.
- Ahmed, A. M., & Adnan, F. (2019, August). A Machine Learning based Approach for Mapping Personality Traits and Perceived Stress Scale of Undergraduate Students. *Modern Education and Computer Science*, 8, 42–47.
- Al Hosani, H., Yousef, M., Al Shouq, S., & Iqbal, F. (2020). State of the art in digital forensics for small scale digital devices. In *Proceedings of 11th International Conference on Information and Communication Systems (ICICS)* (pp. 72-78). Academic Press.
- Al Mutawa, N., Baggili, I., & Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. *Digital Investigation*, 9, S24–S33. doi:10.1016/j.diin.2012.05.007

- Al-Dhaqm, A., Razak, S., Othman, S. H., Ngadi, A., Ahmed, M. N., & Mohammed, A. A. (2017). Development and validation of a database forensic metamodel "DBFM". *PLoS One*, *12*(2), e0170793. doi:10.1371/journal.pone.0170793 PMID:28146585
- Al-Hadadi, M., & AlShidhani, A. (2013). Smartphone forensics analysis: A case study. *International Journal of Computer and Electrical Engineering*, *5*(6), 576–580. doi:10.7763/IJCEE.2013.V5.776
- Alhanahnah, M., Lin, Q., Yan, Q., Zhang, N., & Chen, Z. (2018). Efficient signature generation for classifying cross-architecture IoT malware. *Proceedings of the 6th IEEE Conference on Communications and Network Security*. 10.1109/CNS.2018.8433203
- Ali, M. (2019, July). *The 25 Best Datasets for Natural Language Processing*. <https://lionbridge.ai/datasets/the-best-25-datasets-for-natural-language-processing/>
- Ali, A., Abd Razak, S., Othman, S. H., Mohammed, A., & Saeed, F. (2017). A metamodel for mobile forensics investigation domain. *PLoS One*, *12*(4), e0176223. doi:10.1371/journal.pone.0176223 PMID:28445486
- Ali, K. M. (2012). Digital Forensics Best Practices and Managerial Implications. *Fourth International Conference on Computational Intelligence, Communication Systems and Networks*, 196-199. 10.1109/CICSyN.2012.44
- Alisa, B., & Grzegorz, B. (2018). Improving Self-Esteem with Motivational Quotes: Opportunities for Digital Health Technologies for People With Chronic Disorders. *Frontiers in Psychology*, *9*, 2126. doi:10.3389/fpsyg.2018.02126 PMID:30450071
- Allan, B., Gareth, O. R., Jeffrey, S. R., & Panayiotis, T. (2001, April). Finding Authorities and Hubs From Link Structures on the World Wide Web. *Proceedings of the 10th international conference on WWW*, 415-429.
- Allcott, H., & Gentzkow, M. (2017, May). Social media and fake news in the 2016 election. *The Journal of Economic Perspectives*, *31*(2), 211–236. doi:10.1257/jep.31.2.211
- Alyahya, T., & Kausar, F. (2017). Snapchat analysis to discover digital forensic artifacts on android smartphone. *Procedia Computer Science*, *109*, 1035–1040. doi:10.1016/j.procs.2017.05.421
- Ammar, Abdelmoez & Hamdi. (2014). *Software Engineering using Artificial Intelligence Techniques: Current State and Open Problems*. Academic Press.
- Antivirus software. (n.d.). https://en.wikipedia.org/wiki/Antivirus_software
- Appavu, S., Rajaram, R., Muthupandian, M., Athiappan, G., & Kashmcera, K. S. (2009, July). Data mining based intelligent analysis of threatening email. *Knowledge-Based Systems*, *22*(5), 392–393. doi:10.1016/j.knosys.2009.02.002
- Artificial Intelligence for a smarter kind of cybersecurity. (n.d.). Retrieved from <https://www.ibm.com/in-en/security/artificial-intelligence>

Compilation of References

- Atilla O., Hamit, E. (2012). *An Application of Decision Trees in Intrusion Detection*. Academic Press.
- Atlam, H. F., Alenezi, A., Walters, R. J., Wills, G. B., & Daniel, J. (2017). Developing an adaptive risk-based access control model for the Internet of things. In *Proceedings of IEEE International Conference on Internet of Things (iThings), IEEE Green Computing and Communications (GreenCom), IEEE Cyber, Physical, and Social Computing (CPSCom), and IEEE Smart Data (SmartData)* (pp. 655-661). 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.103
- Atlam, H. F., & Wills, G. B. (2020). IoT security, privacy, safety, and ethics. In M. Farsi, A. Daneshkhah, A. Hosseinian-Far, & H. Jahankhani (Eds.), *Digital Twin Technologies and Smart Cities. Internet of Things (Technology, Communications and Computing)* (pp. 123–149). Springer. doi:10.1007/978-3-030-18732-3_8
- Atlam, H., Walters, R., & Wills, G. (2018). Internet of things: State-of-the-art, challenges, applications, and open issues. *International Journal of Intelligent Computing Research*, 9(3), 928–938. doi:10.20533/ijicr.2042.4655.2018.0112
- AV-test, Malware, The Independent IT-Security Institute. (2014), Retrieved from <http://www.av-test.org/en/statistics/malware>
- Bachrach, Y., Kosinski, M., Graepel, T., Kohli, P., & Stillwell, D. (2012). Personality and patterns of facebook usage. *Proceedings of the 4th Annual ACM Web Science Conference*, 24–32. 10.1145/2380718.2380722
- Backer, C. (2009). *Digital forensics on small scale digital devices. Seminar Topic: Covert channels and Embedded Forensics, Ruhr-University Bochum*. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.392.8017&rep=rep1&type=pdf>
- Baggili, I., & Behzadan, V. (2019). Founding the domain of AI forensics. In *Proceedings of the Workshop on Artificial Intelligence Safety (SafeAI 2020)* (pp. 31-35). Academic Press.
- Baggili, I. M., Mislán, R., & Rogers, M. (2007). Mobile phone forensics tool testing: A database driven approach. *International Journal of Digital Evidence*, 6(2), 168–178.
- Bailey, M., Oberheide, J., Andersen, J., Mao, Z. M., Jahanian, F., & Nazario, J. (2007, September). Automated classification and analysis of internet malware. In *International Workshop on Recent Advances in Intrusion Detection* (pp. 178-197). Springer. 10.1007/978-3-540-74320-0_10
- Barmatsalou, K., Cruz, T., Monteiro, E., & Simoes, P. (2018). Current and future trends in mobile device forensics: A survey. *ACM Computing Surveys*, 51(3), 1–31. doi:10.1145/3177847
- Barnett, V. (1978). The study of outliers: Purpose and model. *Applied Statistics*, 27(3), 242–250.
- Baror, S. O., Ikuesan, R. A., & Venter, H. S. (2020). A defined digital forensic criteria for cybercrime reporting. In *Proceedings of International Conference on Cyber Warfare and Security* (pp. 617-XVIII). Academic Conferences International Limited.

- Barss, P. (2019). *Eliminating Bias in AI*. Retrieved from: <https://techxplore.com/news/2019-07-bias-ai.html>
- Bass, L., Clements, P., & Kazman, R. (2003). *Software Architecture in Practice* (2nd ed.). Addison-Wesley.
- Belani, Vukovic & Car. (2019). Requirement Engineering Challenges in building AI-based. *Complex Systems*.
- Bharathidason & Venkataeswaran. (2014). Improving Classification Accuracy based on Random Forest Model with Uncorrelated High Performing Trees. *International Journal of Computers and Applications*, 101(13).
- Bhatt. (2017). *A Survey of Effective and Efficient Software Testing Technique and Analysis*. Academic Press.
- Bohl, M., & Rynn, M. (2000). *Tools for Structured Design: An Introduction to Programming Logic* (5th ed.). Prentice Hall.
- Botafogo, R., Rivlin, E., & Shneiderman, B. (1992). Structural analysis of hypertext: Identifying hierarchies and useful metrics. *ACM Transactions on Information Systems*, 10, 142–180. doi:10.1145/146802.146826
- Broadhurst, R., & Chang, Y. (2012). *Cybercrime in Asia: Trends and Challenges*. SSRN Electronic Journal. doi:10.2139/ssrn.2118322
- Bryson, J. J. (n.d.). *The past decade and future of AI's impact on society*. Retrieved from <https://www.bbvaopenmind.com/en/articles/the-past-decade-and-future-of-ais-impact-on-society/>
- Burnaev, E., & Smolyakov, D. (2016, December). One-class SVM with privileged information and its application to malware detection. In *2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)* (pp. 273-280). IEEE. 10.1109/ICDMW.2016.0046
- Chandana. (2019). *Scrum Project Management: Pros and Cons*. Retrieved from <https://www.simplilearn.com/scrum-project-management-article>
- Chandler, S. (2020). *How explainable AI is helping Algorithms avoid bias*. Retrieved from <https://www.forbes.com/sites/simonchandler/2020/02/18/how-explainable-ai-is-helping-algorithms-avoid-bias/#333c7b8f5ed3>
- Chattopadhyay, A., & Mitra, U. (2018). Attack detection and secure estimation under false data injection attack in cyber-physical systems. *2018 52nd Annual Conference on Information Sciences and Systems (CISS)*, 1–6. doi:10.1109/ciss.2018.8362307
- Chattopadhyay, A., & Mitra, U. (2020). Security Against False Data-Injection Attack in Cyber-Physical Systems. *IEEE Transactions on Control of Network Systems*, 7(2), 1015–1027. doi:10.1109/TCNS.2019.2927594

Compilation of References

Chelliah, J. B., Ajith, P. A., Samtani, G. C., Paul, D., & Bachhav, C. (2019). Security Implications in Cyber Physical Systems. *International Journal of Innovative Technology and Exploring Engineering*, 8(6S), 85–88.

Chernyshev, M., Zeadally, S., Baig, Z., & Woodward, A. (2017). Mobile Forensics: Advances, Challenges, and Research Opportunities. *IEEE Security and Privacy*, 15(6), 42–51. doi:10.1109/MSP.2017.4251107

Chhabra, G. S., Singh, V. P., & Singh, M. (2020). Cyber forensics framework for big data analytics in IoT environment using machine learning. *Multimedia Tools and Applications*, 79(23), 15881–15900. doi:10.1007/11042-018-6338-1

Comiter, M. (2019). *Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About it*. In Belfer Center for Science and International Affairs, Harvard Kennedy School.

Computer crime costs \$67 billion, FBI says – CNET. (n.d.). https://www.insight.com/content/dam/insight/en_US/pdfs/symantec/symantec-corp-internet-security-threat-report-volume-18.pdf

Cristina, S., Fabio, C., Luca, P., Michal, K., David, S., Nicu, S., Marco, C., & Bruno, L. (2017). What your Facebook Profile Picture Reveals about your Personality. *Proceedings of the 25th ACM international conference on Multimedia*, 460-468.

Dataflair. (2020). *Advanced Python Project – Detecting Fake News with Python*. <https://data-flair.training/blogs/advanced-python-project-detecting-fake-news>

de Montjoye, Farzanehar, Hendrickx, & Rocher. (2017). Solving Artificial Intelligence's Privacy Problem. *Artificial Intelligence and Robotics in the City*.

Debois, P. (2011). Devops: A software revolution in the making? *Cutter IT Journal*, 24, 8.

Degang, S., Yulan, H., Zhixin, S., Guokun, X., & Wei, Z. (2019). An Efficient Anomaly Detection Framework for Electromagnetic Streaming Data. *ACM ICBDC*, 151-155.

Dimitar, N. K., Christopher, M., & Ruslan, V. (2017). Cyber Threat Hunting Through the use of an isolation Forest. *International Conference on Computer Systems and Technologies, ACM CompSys*, 163-170.

Dixon & Eagan. (2019). 3 ways AI will change the nature of cyber attacks. Retrieved from: <https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/>

Dubey, V. (2017). *Admissibility of electronic evidence: an Indian perspective*. *Forensic Research & Criminology International Journal*.

Elhadad, Li, & Gebali. (2019). Fake News Detection on Social Media: A Systematic Survey. *Communications Computers and Signal Processing (PACRIM) IEEE Pacific Rim Conference on*, 1-8.

- Fabrizio, A., Fabio, F. (2016). Toward Generalizing the Unification with Statistical Outliers: The Gradient Outlier Factor Measure. *ACM Transactions on Knowledge Discovery from Data*, 10(3), 1–26.
- Faheem, M., Le-Khac, N. A., & Kechadi, T. (2014). Smartphone forensic analysis: A case study for obtaining root access of an android samsung s3 device and analyse the image without an expensive commercial tool. *Journal of Information Security*, 5(03), 83–90. doi:10.4236/jis.2014.53009
- Farnaaz & Jabbar. (2016). Random Forest Modeling for Network Intrusion Detection System. *Procedia Computer Science*, 89(213-217).
- Farnadi, G., Zoghbi, S., Moens, M. F., & Cock, M. D. (2013). Recognizing personality traits using facebook status updates. *Proceedings of the workshop on computational personality recognition (WCPR13) at the 7th international AAAI conference on weblogs and social media (ICWSM13)*.
- Fei, T. L., Kai, M. T., & Zhi-Hua, Z. (2008). Isolation Forest. *Eighth IEEE International Conference on Data Mining*, 413–422.
- Fei, T. L., Kai, M. T., & Zhi-Hua, Z. (2012). Isolation-based Anomaly Detection. *ACM Transactions on Knowledge Discovery from Data*, 3, 1–39.
- Feldt, .de Oliveria Neto, & Torkar. (2018). Ways of applying Artificial Intelligence in Software Engineering. Academic Press.
- Filipe, F., Tommaso, Z., Caio, B. V. S., & Anderson, S. (2019). Quantitative comparison of unsupervised anomaly detection algorithms for intrusion detection. *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, 318–327.
- Freund, Schapire, & Abe. (1999). A short introduction to Boosting. *Jinkō Chinō Gakkaishi*, 14, 771–780.
- Fukami, A., & Nishimura, K. (2019). Forensic Analysis of Water Damaged Mobile Devices. *Digital Investigation*, 29, S71–S79. doi:10.1016/j.diin.2019.04.009
- Gaikwad, D. P., & Ravindra, C. (2015). Intrusion Detection System using Bagging Ensemble method of Machine Learning. *Proceedings of the International Conference on Computing Communication Control and Automation*, 291-295. 10.1109/ICCUBEA.2015.61
- Gallo. (2015, Jan). Artificial Neural Networks: tutorial. In *Encyclopedia of Information Science and Technology* (3rd ed.). IGI Global.
- Gavriliuț, D., Cimpoșu, M., Anton, D., & Ciortuz, L. (2009, October). Malware detection using machine learning. In *2009 International Multiconference on Computer Science and Information Technology* (pp. 735-741). IEEE. 10.1109/IMCSIT.2009.5352759
- Gentry, E., & Soltys, M. (2019). SEAKER: A mobile digital forensics triage device. *Procedia Computer Science*, 159, 1652–1661. doi:10.1016/j.procs.2019.09.335

Compilation of References

- German, B. (2017). *Glass classification: Can you correctly identify glass type?* <https://www.kaggle.com/uciml/glass/data>
- Global Digital Forensics. (2020). *Case study: Banking industry executive level financial fraud.* <https://evestigat.com/case-study/banking-industry-executive-level-financial-fraud/>
- Goel, M., & Kumar, V. (2019, March). Layered Framework for Mobile Forensics Analysis. *Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE)*.
- González-López, J., Ventura, S., & Cano, A. (n.d.). Distributed selection of continuous features in multilabel classification using mutual information. *IEEE Trans. Neural Netw. Learn. Syst.* Available: <https://ieeexplore.ieee.org/document/8877992>
- Gopalan, H. S., Suba, A. S., Ashmithashree, C., Gayathri, A., & Andrews, J. V. (2019). Digital Forensics using Blockchain. *International Journal of Recent Technology and Engineering (IJRTE)*, 8(2S11), 182–184. doi:10.35940/ijrte.b1030.0982s1119
- Graham, L. A., Cohen, S. J., & Shmavonlan, B. M. (1967). Some methodological approaches to the psychophysiological correlates of behavior. In *Emotional stress. Psychological and physiological reactions* (pp. 178–191). Medical, Industrial and Military Implications.
- Graham, S. R., & Smith, K. S. (2020). *Cybercrime and Digital Deviance*. Published by Routledge., doi:10.4324/9781351238090
- Grégoire, M., Wojciech, S., & Klaus-Robert, M. (2018, February). Methods for interpreting and understanding deep neural networks. *Digital Signal Processing*, 73, 1–15. doi:10.1016/j.dsp.2017.10.011
- Gupta & Sharma. (2015). *Software Maintenance: Challenges and Issues*. Academic Press.
- Gupta, S., Thirukovalluru, R., Sinha, M., & Mannarswamy, S. (2018). CIMTDetect: A Community Infused Matrix-Tensor Coupled Factorization Based Method for Fake News Detection. *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*. 10.1109/ASONAM.2018.8508408
- Hadjidj, R., Debbabi, M., Lounis, H., Iqbal, F., Szporer, A., & Benredjem, D. (2009, March). Towards an integrated e-mail forensic analysis framework. *Digital Investigation*, 5(3-4), 124–137. doi:10.1016/j.diin.2009.01.004
- Halpern, D., Piña, M., & Vásquez, J. (2017). Loneliness, personal and social well-being: towards a conceptualization of the effects of cyberbullying/Soledad, bienestar social e individual: hacia una conceptualización de los efectos del cyberbullying. *Cult. y Educ.*, 29(4), 703–727. doi:10.1080/11356405.2017.1370818
- Han, Y. H., Yuan, X., Li, C., & Li, X. (2017). DeepDefense: Identifying DDoS Attack via Deep Learning. *IEEE International Conference on Smart Computing (SMARTCOMP) IEEE*, 1-8.

- Harichandran, V. (2015). A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. *Computers & Security*.
- Hassen, M., Carvalho, M. M., & Chan, P. K. (2017, November). Malware classification using static analysis based features. In *2017 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1-7). IEEE. 10.1109/SSCI.2017.8285426
- Hauger, W. K., & Olivier, M. S. (2015). The state of database forensic research. *2015 Information Security for South Africa ISSA 2015 Conf.* 10.1109/ISSA.2015.7335071
- Hawkins, D. (1980). *Identification of Outliers*. Chapman and Hall.
- He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 770-778). 10.1109/CVPR.2016.90
- Herrera, L. A. (2020). Challenges of acquiring mobile devices while minimizing the loss of usable forensics data. *Proceedings of 2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 1-5.
- Hieu, M., Dung, T., Lam, N., Hoa, H. N., Hai, A. T., & Duc, T. (2018). Detecting Attacks on Web Applications using Autoencoder. *Proceedings of the Ninth International Symposium on Information and Communication Technology*, 416–421.
- Hoelz, B. W., Ralha, C. G., & Geeverghese, R. (2009). Artificial intelligence applied to computer forensics. In *Proceedings of the 2009 ACM symposium on Applied Computing (SAC '09)* (pp. 883-888). Association for Computing Machinery. 10.1145/1529282.1529471
- Hur, J. B., & Shamsi, J. A. (2017, December). A survey on security issues, vulnerabilities and attacks in Android based smartphone. In *Proceedings of 2017 International Conference on Information and Communication Technologies (ICICT)* (pp. 40-46). IEEE.
- Hyvärinen, H., Risius, M., & Friis, G. (2017). A Blockchain-Based Approach Towards Overcoming Financial Fraud in Public Sector Services. *Business & Information Systems Engineering*, 59(6), 441–456. doi:10.1007/12599-017-0502-4
- Imam, A. (2018). *Software Development Life Cycle: The phases of SDLC*. Retrieved from <https://blog.testlodge.com/software-development-life-cycle/>
- Internet Security Threats Report. Symantec. (n.d.). <http://www.symantec.com/threatreport/>
- Irons, A. D., Stephens, P., & Ferguson, R. I. (2009). Digital Investigation as a distinct discipline: A pedagogic perspective. *Digital Investigation*, 6(1-2), 82–90. doi:10.1016/j.diin.2009.05.002
- Jakub, N., Ahmet, T., & Rafal, S. (2017, May). LSTM Recurrent Neural Networks for Short Text and Sentiment Classification. *International Conference on Artificial Intelligence and Soft Computing CAISC 2017*, 553-562.
- James, J. I. (2013). *G. P. Challenges with Automation in Digital Forensic Investigations*.

Compilation of References

- Jason, B. (2017). *Datasets in NLP*. <https://machinelearningmastery.com/datasets-natural-language-processing/>
- Jeeva, S. C., & Rajasingh, E. B. (2017). Phishing URL detection-based feature selection to classifiers. *Int. J. Electron. Secur. Digit. Forensics.*, 9(2), 116–131. doi:10.1504/IJESDF.2017.083979
- Jeffrey P., Richard S., Christopher D. M. (2014). GloVe: Global Vectors for Word Representation. *Empirical Methods in Natural Language Processing (EMNLP)*, 1532-1543.
- Jiahao, W. (2019). *NLP Text Preprocessing: A Practical Guide and Template*. <https://towardsdatascience.com/nlp-text-preprocessing-a-practical-guide-and-template-d80874676e79>
- John, O. P., & Srivastava, S. (1999). The big five trait taxonomy: History, measurement, and theoretical perspectives. *Handbook of personality: Theory and research*, 2(1999), 102–138.
- John, W. (2014). *Encyclopedia of Business Analytics and Optimization*. IGI Global Publication.
- Kantardzic, M. (2011). *Data Mining: Concepts, Models, Methods, and Algorithms*. Wiley publishers, IEEE press. doi:10.1002/9781118029145
- Karie, N. M., Kebande, V. R., & Venter, H. S. (2019). Diverging deep learning cognitive computing techniques into cyber forensics. *Forensic Science International: Synergy*, 1, 61–67. PMID:32411955
- Karie, N. M., Kebande, V. R., Venter, H., & Choo, K. R. (2019). On the importance of standardising the process of generating digital forensic reports. *Forensic Science International: Reports*, 1, 100008. doi:10.1016/j.fsir.2019.100008
- Karthika, V., & Jaganathan, S. (2019). A quick synopsis of blockchain technology. *International Journal of Blockchains and Cryptocurrencies*, 1(1), 54–66. doi:10.1504/IJBC.2019.101852
- Kataria, A., Anjali, T., & Venkat, R. (2014, February). Quantifying smartphone vulnerabilities. In *Proceedings of 2014 International Conference on Signal Processing and Integrated Networks (SPIN)* (pp. 645-649). IEEE.
- Khan, S., Shiraz, M., Abdul Wahab, A. W., Gani, A., Han, Q., & Bin Abdul Rahman, Z. (2014). A comprehensive review on adaptability of network forensics frameworks for mobile cloud computing. *The Scientific World Journal*.
- Kim, A., & Dennis, A. R. (2018). Says who? The effects of presentation format and source rating on fake news in social media. *Proceedings of the 51st Hawaii International Conference on System Sciences*. 10.24251/HICSS.2018.497
- Kim, Kim, & Lee. (2016). Performance analysis of the malware classification method in accordance with the changes in assembly code. *Journal of the Korean Institute of Communication Sciences*, 885-886.

- Kim, S., & Kim, H. (2016). A new metric of absolute percentage error for intermittent demand forecasts. *Int. J. Forecasting*, 32(3), 669-679. Available: <https://linkinghub.elsevier.com/retrieve/pii/S0169207016000121>
- Kinable, J., & Kostakis, O. (2011). Malware classification based on call graph clustering. *Journal in Computer Virology*, 7(4), 233-245.
- Kobielus, J. (2020). *Advancing AI with Neuromorphic Computing platform*. Retrieved from: <https://informationweek.com/big-data/ai-machine-learning/advancing-ai-with-neuromorphic-computing-platforms/a/d-id/1337587>
- Koganti & G. (2019). Forensic Acquisition of IOS Devices. *International Journal of Recent Technology and Engineering*, 8(4), 10847–10855. doi:10.35940/ijrte.D4374.118419
- Kolosnjaji, B., Zarras, A., Webster, G., & Eckert, C. (2016, December). Deep learning for classification of malware system call sequences. In *Australasian Joint Conference on Artificial Intelligence* (pp. 137-149). Springer. 10.1007/978-3-319-50127-7_11
- Kolter, J. Z., & Maloof, M. A. (2006). Learning to detect and classify malicious executables in the wild. *Journal of Machine Learning Research*, 7(Dec), 2721–2744.
- Kömmerling, O., & Kuhn, M. G. (1999). Design Principles for Tamper-Resistant Smartcard Processors. *Smartcard*, 99, 9–20.
- Kotteti, C. M. M., Dong, X., Li, N., & Qian, L. (2018). Fake news detection enhancement with data imputation. *IEEE 16th Int. Conf. on Dependable Autonomic and Secure Comp.*, 187-192.
- Koussouris, S., & Di Nitto, E. (2016). *Current and Future Challenges of Software Engineering for Services and Applications*. Academic Press.
- Krishnan, S. C. L. (2014). Legal Concerns and Challenges in Cloud Computing. *2nd International Symposium on Digital Forensics and Security (ISDFS 2014)*.
- Kumar & Bhatia. (2012). Impact of Agile Methodology on Software Development Process. *International Journal of Computer Technology and Electronics Engineering*, 2(4).
- Kwon, D., Natarajan, K., Suh, S. C., Kim, H., & Kim, J. (2018, July). An empirical study on network anomaly detection using convolutional neural networks. In *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)* (pp. 1595-1598). IEEE. 10.1109/ICDCS.2018.00178
- Labiche, Y., Kolbah, B., & Mehrfard, H. (2013). Combining Static and Dynamic Analyses to Reverse- Engineer Scenario Diagrams. *IEEE Int. Conf. Softw. Maintenance*, 10.
- Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., Metzger, M. J., Nyhan, B., Pennycook, G., Rothschild, D., Schudson, M., Sloman, S. A., Sunstein, C. R., Thorson, E. A., Watts, D. J., & Zittrain, J. L. (2018, March). The science of fake news. *Science*, 359(6380), 1094–1096. doi:10.1126/science.aao2998 PMID:29590025

Compilation of References

- Leskovec, J., Rajaraman, A., & Ullman, J.D. (2016). *Mining of Massive Datasets* (2nd ed.). Cambridge University Press.
- Lin, X., Chen, T., Zhu, T., Yang, K., & Wei, F. (2018). Automated forensic analysis of mobile applications on Android devices. *Digital Investigation*, 26, S59–S66. doi:10.1016/j.diin.2018.04.012
- Liu, W., Ren, P., Liu, K., & Duan, H. X. (2011, September). Behavior-based malware analysis and detection. In *2011 first international workshop on complexity and data mining* (pp. 39-42). IEEE. 10.1109/IWCDM.2011.17
- Liu, L., Wang, B. S., Yu, B., & Zhong, Q. X. (2017). Automatic malware classification and new malware detection using machine learning. *Frontiers of Information Technology & Electronic Engineering*, 18(9), 1336–1347. doi:10.1631/FITEE.1601325
- Liu, Y., Jourabloo, A., Ren, W., & Liu, X. (2017). *Dense face alignment*. ICCVW. doi:10.1109/ICCVW.2017.190
- Livermore, J. A. (2007). *Factors that impact implementing an Agile Software Development Methodology*. IEEE. doi:10.1109/SECON.2007.342860
- Li, X., & Ye, N. (2001). Decision tree classifiers for computer intrusion detection. *Parallel and Distributed Computing Practices*, 4(2), 179–190.
- Lohiya, R., John, P., & Shah, P. (2015). Survey on mobile forensics. *International Journal of Computers and Applications*, 118(16).
- Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. *Digital Investigation*, 28, 44–55. doi:10.1016/j.diin.2019.01.002
- Ma'arif, Shahar, Yusof & Satar. (2018). *The Challenges of Implementing Agile Scrum in Information Systems Project*. Academic Press.
- MacCarthy. (2019). *How to address new privacy issues raised by artificial intelligence and machine learning*. Retrieved from <https://www.brookings.edu/blog/techtank/2019/04/01/how-to-address-new-privacy-issues-raised-by-artificial-intelligence-and-machine-learning/>
- Malhotra, P., Vig, L., Shroff, G., & Agarwal, P. (2015, April). Long short term memory networks for anomaly detection in time series. In *Proceedings* (Vol. 89). Presses universitaires de Louvain.
- Marco, C., Alessandro, V., Cristina, S., & Alessandro, P. (2013). Unveiling the Multimedia Unconscious: Implicit Cognitive Processes and Multimedia Content Analysis. *Proceedings of ACM-MM*, 213–222.
- Marín, G., Casas, P., & Capdehourat, G. (2019, May). Deep in the Dark-Deep Learning-Based Malware Traffic Detection Without Expert Knowledge. In *2019 IEEE Security and Privacy Workshops (SPW)* (pp. 36-42). IEEE. doi:10.1109/SPW.2019.00019

- Mathew, A. (2019). Cyber Security through Blockchain Technology. *International Journal of Engineering and Advanced Technology*, 9(1), 3821–3824. doi:10.35940/ijeat.A9836.109119
- McConnell, S. (2004). *Code Complete* (2nd ed.). Microsoft Press.
- Meffert, C., Clark, D., Baggili, I., & Breitinger, F. (2017). Forensic state acquisition from Internet of things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition. In *Proceedings of the 12th International Conference on Availability, Reliability, and Security (ARES '17)* (pp. 1-11). Association for Computing Machinery. 10.1145/3098954.3104053
- Mellars, B. (2004). Forensic Examination of Mobile Phones. Digital Investigation. *The International Journal of Digital Forensics & Incident Response*, 1(4), 266–272.
- Mena, J. (2003). *Investigative data mining for security and criminal detection*. Butterworth-Heinemann.
- Michael, J. G. (2018). *How to Create a Simple Neural Network in Python*. <https://www.kdnuggets.com/2018/10/simple-neural-network-python.html>
- Michal, M., Tadesse, H., Bo, X., & Liang, Y. (2018). Personality Predictions Based on User Behaviour on the Facebook Social Media Platform. *IEEE Access*.
- Michal, K., David, S., & Thore, G. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States of America*, 110(15), 5802–5805. doi:10.1073/pnas.1218772110 PMID:23479631
- Miltiadis, K., Alexios, M., Nikos, V., Marianthi, T., & Dimitris, G. (2010). An Insider Threat Prediction Model. *LNCS*, 6264, 26–37.
- Mirjalili, V., & Ross, A. (2017). *Soft biometric privacy: Retaining biometric utility of face images while perturbing gender*. ICB.
- Mirza, A. H., & Cosan, S. (2018, May). Computer network intrusion detection using sequential LSTM neural networks autoencoders. In *2018 26th Signal Processing and Communications Applications Conference (SIU)* (pp. 1-4). IEEE. 10.1109/SIU.2018.8404689
- Mohaisen, A., Alrawi, O., & Mohaisen, M. (2015). Amal: High-fidelity, behavior-based automated malware analysis and classification. *Computers & Security*, 52, 251-266.
- Mohanty, R. (2018). *Will AI change the game for Cyber Security in 2018?* Retrieved from: <https://www.paladion.net/hubfs/Paladion--2018/resources-18/collaterals-18/will-AI-change-the-game-for-cyber-security-in-2018/Will%20AI%20Change%20the%20Game%20for%20Cyber%20Security%20in%202018%20-%20Whitepaper.pdf?hsLang=en-us>
- Montanez, A. (2014). Investigation of cryptocurrency wallets on iOS and Android mobile devices for potential forensic artifacts. Dept. Forensic Sci., Marshall Univ.

Compilation of References

- Mullan, P., Riess, C., & Freiling, F. (2019). Forensic source identification using JPEG image headers: The case of smartphones. *Digital Investigation*, 28, S68–S76. doi:10.1016/j.diin.2019.01.016
- Murphy, C. A. (2009). *Developing process for mobile device forensics*. Madison. Retrieved, October 03, 2020 from <https://digital-forensics.sans.org/media/mobile-device-forensic-process-v3.pdf>
- Murphy, M. (2017). Study: Fake news hits the workplace. *Leadership IQ*. <https://www.leadershipiq.com/blogs/leadershipiq/study-fake-news-hits-the-workplace>
- Nemetz, S., Schmitt, S., & Freiling, F. (2018). A standardized corpus for SQLite database forensics. *Digital Investigation*, 24(Supplement), S121–S130. doi:10.1016/j.diin.2018.01.015
- Ninawe, P. N., & Ardhapurkar, S. B. (2014). Forensic-as-a-service for mobile devices (literature survey). *Int. J. Comput. Sci. Inform. Technol*, 5(6), 7776–7778.
- Oshikawa, R., Qian, J., & Wang, W. Y. (2020). A survey on natural language processing for fake news detection. *Proceedings of the 12th Conference on Language Resources and Evaluation (LREC 2020)*, 6086–6093.
- Otero. (2012). *Software Design Challenges*. Retrieved from <http://www.ittoday.info/ITPerformanceImprovement/Articles/2012-06Otero.html>
- PandaLabs Annual Report. (2017). *Panda Security*. https://www.pandasecurity.com/mediacenter/src/uploads/2017/11/PandaLabs_Annual_Report_2017.pdf
- Park, W., Youngin, Y., & Kyungho, L. (2018). Detecting Potential Insider Threat: Analyzing Insiders' Sentiment Exposed in Social Media. *Security and Communication Networks*, 2018, 1–8. doi:10.1155/2018/7243296
- Patridge, D. (Ed.). (1991). *Artificial Intelligence and Software Engineering*. Ablex.
- Peyre, G. (2019). *Mathematical Foundations of Data Sciences*. CNRS and DMA, Ecole Normale Supérieure. Available: <https://mathematical-tours.github.io>
- Piscini, E., Dalton, D., & Kehoe, L. (2019). *Blockchain & Cyber Security - An assessment of the security of blockchain technology*. Retrieved September 13, 2020 from <https://www2.deloitte.com/tr/en/pages/technology-media-and-telecommunications/articles/blockchain-and-cyber.html>
- Polachowska, K. (2019). *The 12 challenges of AI adoption*. Retrieved from <https://neoteric.eu/blog/12-challenges-of-ai-adoption/>
- President's Council of Advisors on Science and Technology (U.S.). (2016). *Report to the president, forensic science in criminal courts: Ensuring scientific validity of feature-comparison methods*. Executive Office of the President of the United States, President's Council of Advisors on Science and Technology.
- Pressman, R. S. (2010). *Software Engineering: A practitioner's approach* (International Edition). McGraw Hill.

- Qadir, A. M., & Varol, A. (2020). The role of machine learning in digital forensics. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-5). IEEE. 10.1109/ISDFS49300.2020.9116298
- Qing, W., Weifeng, L., & Bowen, D. (2018). Spatio-temporal Anomaly Detection in Traffic Data. *Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control*, 46, 1–5.
- Rad, B. B., Nejad, M. K. H., & Shahpasand, M. A. R. Y. A. M. (2018). Malware classification and detection using artificial neural network. *Journal of Engineering Science and Technology*, 13, 14–23.
- Rai, K., Devi, M. S., & Guleria, A. (2016). Decision tree based Algorithm for Intrusion Detection. *International Journal of Advanced Networking and Applications*, 7(4), 2828–2834.
- Raikwar, M., Mazumdar, S., Ruj, S., Gupta, S. S., Chattopadhyay, A., & Lam, K. (2018). A Blockchain Framework for Insurance Processes. *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. doi:10.1109/ntms.2018.8328731
- Raluca, T., & Remus, R. (n.d.). *HITS Algorithm - Hubs and Authorities on the internet*. <http://pi.math.cornell.edu/~mec/Winter2009/RalucaRemus/Lecture4/lecture4.html>
- Rayan, N. (2017). *Digital forensics report*. http://www.rnyte-cyber.com/uploads/9/8/5/9/98595764/exampledigiforensicsrprt_by_ryan_nye.pdf
- Rieck, K., Holz, T., Willems, C., Düssel, P., & Laskov, P. (2008, July). Learning and classification of malware behavior. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 108-125). Springer. 10.1007/978-3-540-70542-0_6
- Rizwan Ahmed, R. V. (2005). *Mobile Forensics: an Overview, Tools, Future trends and Challenges from Law Enforcement perspective*. Emerging Technologies in E-Government.
- Rohmeyer, P. (2010). Technology malpractice. In J. Bayuk (Ed.), *CyberForensics. Springer's Forensic Laboratory Science Series* (pp. 141–148). Humana Press.
- Ronen, R., Radu, M., Feuerstein, C., Yom-Tov, E., & Ahmadi, M. (2018). *Microsoft malware classification challenge*. arXiv preprint arXiv:1802.10135
- Rughani, P. H., & Bhatt, P. (2017). Machine learning forensics: A new branch of digital forensics. *International Journal of Advanced Research in Computer Science*, 8(8), 217–222. doi:10.26483/ijarcs.v8i8.4613
- Sachdev, H., Wimmer, H., Chen, L., Abdul-Al, C. F., & Powell, L. M. (2018). *A Digital Forensic Tool for Mobile Devices: Paraben*. ToKnowPress.
- Safety Detectives. (n.d.). <https://www.safetydetectives.com/blog/most-dangerous-new-malware-and-security-threats/>

Compilation of References

- Safjański, T., & James, A. (2020). Europol's crime analysis system—Practical determinants of its success. *Policing. Journal of Policy Practice*, 14(2), 469–478.
- Sai, D. M., Prasad, N. R. G. K., & Dekka, S. (2015). The Forensic Process Analysis of Mobile Device. *Int. J. Comput. Sci. Inf. Technol*, 6(5), 4847–4850.
- Sanchez, L., Grajeda, C., Baggili, I., & Hall, C. (2019). A practitioner survey exploring the value of forensic tools, AI, filtering, and safer presentation for investigating child sexual abuse material (CSAM). *Digital Investigation*, 29, S124–S142. doi:10.1016/j.diin.2019.04.005
- Saxe, J., & Berlin, K. (2015, October). Deep neural network based malware detection using two dimensional binary program features. In *2015 10th International Conference on Malicious and Unwanted Software (MALWARE)* (pp. 11–20). IEEE. 10.1109/MALWARE.2015.7413680
- Schetinger, V., & Manuel, M. O. (2017). Humans Are Easily Fooled by Digital Images. *Computers & Graphics*, 70, 142–151. doi:10.1016/j.cag.2017.08.010
- Senapathi, Buchan, & Osman. (2018). *DevOps Capabilities, Practices, and Challenges: Insights from a Case Study*. Academic Press.
- Seyed, Danesh, & Ahmad. (2011). *Software release planning challenges in software development: An empirical study*. Academic Press.
- Shaheen, J. A., Asghar, M. A., & Hussain, A. (2017). Android OS with its Architecture and Android Application with Dalvik Virtual Machine Review. *International Journal of Multimedia and Ubiquitous Engineering*, 12(7), 19–30. doi:10.14257/ijmue.2017.12.7.03
- Sharmeen, S., Huda, S., Abawajy, J. H., Ismail, W. N., & Hassan, M. M. (2018). Malware threats and detection for industrial mobile IoT networks. *IEEE Access: Practical Innovations, Open Solutions*, 6, 15941–15957. doi:10.1109/ACCESS.2018.2815660
- Shu, K., Cui, L., & Wang, S. (2019). defend: Explainable fake news detection. *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, KDD*, 395–405.
- Shu, Zhou, Wang, Zafarani, & Liu. (2019). *The role of user profile for fake news detection*. CoRR, abs/1904.13355
- Shu, K., Sliva, A., Wang, S., Tang, J., & Liu, H. (2017, September). Fake News Detection on Social Media: A Data Mining Perspective. *SIGKDD Explorations*, 19(1), 22–36. doi:10.1145/3137597.3137600
- Sikorski, M., & Honig, A. (2012). *Practical malware analysis: the hands-on guide to dissecting malicious software*. No Starch Press.
- Simon, D. D. A., Anna, P. L., Christoph, G., & Hans, D. S. (2019). Security in Process: Detecting Attacks in Industrial Process Data. *Proceedings of the Third Central European Cybersecurity Conference*, 5, 1–6.

- Simonyan, K., & Zisserman, A. (2014). *Very deep convolutional networks for large-scale image recognition*. arXiv preprint arXiv:1409.1556
- Singh, A. J., & Bhardwaj, A. (2014). Android vs. IOS: An Architectural Perspective. *International Journal of Innovative Research and Development*, 3(1), 82–90.
- Singh, J., Millard, C., Reed, C., Cobbe, J., & Crowcroft, J. (2018). Accountability in the IoT: Systems, law, and ways forward. *Computer*, 51(7), 54–65. doi:10.1109/MC.2018.3011052
- Sokappadu, Mattapullut Gopaul, Paavan, & Devi. (2016). *Review of Software Maintenance Problems and Proposed Solutions in IT consulting firms in Mauritius*. Academic Press.
- Soni, S. (2017). *Caught in the talent crunch?* Retrieved from: <https://www.magzter.com/article/Business/Entrepreneur-magazine/Caught-In-The-Talent-Crunch>
- Sophie, Wade, & Watson. (2017, July). Can people identify original and manipulated photos of real-world scenes? *Cognitive Research: Principles and Implications*, 30.
- Sowmiya, B., & Poovammal, E. (2019). Blockchain Technology Is a Boost to Cyber Security. In *Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems*. IGI-Global. doi: . doi:10.4018/978-1-5225-8241-0.ch013
- Srivastava, A., & Vatsal, P. (2016). Forensic importance of SIM cards as a digital evidence. *Journal of Forensics Research*, 7(322), 2. doi:10.4172/2157-7145.1000322
- Staerman, G., & Forest, F. I. (2019). Article. *Proceedings of Machine Learning Research*, 101, 332–347.
- Statista Research Department. (2016). *Internet of things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)*. Retrieved August 10, 2020, from <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>
- Sundar Krishnan, B. Z. (2019). Smartphone Forensic Challenges. *International Journal of Computer Science and Security*, 13(5).
- Sun, H., Wang, X., Buyya, R., & Su, J. (2017). CloudEyes: Cloud based malware detection with reversible sketch for resource constrained internet of things (IoT) devices. *Software, Practice & Experience*, 47(3), 421–441. doi:10.1002pe.2420
- Sunita, D. (2018). Constructing an Ethical Hacking Knowledge Base for Threat Awareness and Prevention. IGI Global.
- Sunita, D. (2019). C-ASFT: Convolutional Neural Networks based Anti-Spam Filtering Technique. *International Conference on Computational Science and Applications (ICCSA) 2019*.
- Sunita, D. (2018). *Insiders Attack Analysis in Building an Effective Cyber Security for an Organization*. In *Psychological and Behavioral Examinations in Cyber Security*. IGI Global.

Compilation of References

- Svenmarck, D. P., & Luotsinen, D. L. (2018). *Possibilities and challenges for Artificial Intelligence in Military Applications*. Paper presented in NATO Big data and Artificial intelligence for Military Decision Making Specialists Meeting, Bordeaux, France. Retrieved from <https://blog.eccouncil.org/the-role-of-ai-in-cybersecurity/>
- Tadesse, Z., & Thomas, G. D. (2019). Anomaly detection in the presence of missing values for weather data quality control. *Proceedings of the 2nd ACM SIGCAS Conference on Computing and Sustainable Societies*, 65–73.
- Tan, X., & Yu, H. (2017). Effective small interfering RNA design based on convolutional neural network. *IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, 16-21.
- Taylor, J. P., Dargahi, T., Dehghantanha, A., Parizi, M. R., & Choo, R. K. (2019). A Systematic Literature Review of Blockchain Cybersecurity. *Digital Communications and Networks.*, 6(2), 147–156. doi:10.1016/j.dcan.2019.01.005
- Tejas Karia, A. A. (2015). The Supreme Court of India re-defines admissibility of electronic evidence in India. *Digital Evidence and Electronic Signature Law Review*, (12), 37.
- Thing, V. L., Ng, K. Y., & Chang, E. C. (2010). Live memory forensics of mobile phones. *Digital Investigation*, 7, S74–S82. doi:10.1016/j.diin.2010.05.010
- Tian, Z., Li, M., Qiu, M., Sun, Y., & Su, S. (2019). Block-DEF: A secure digital evidence framework using blockchain. *Information Sciences*, 491, 151–165. doi:10.1016/j.ins.2019.04.011
- Timofey, B., Victor, P., Kirill, S., Nikita, P. (2018). Detecting anomalies in Kotlin code. *Companion Proceedings for the ISSTA/ECOOP 2018 Workshops*, 10–12.
- Train_data.csv. (n.d.). <https://www.kaggle.com/what0919/intrusion-detection/>
- Taylor, T., Straub, J., & Snell, N. (2019). Classifying fake news articles using natural language processing to identify in-article attribution as a supervised learning estimator. *IEEE 13th Int. Conf. on Semantic Comp.*, 445-449.
- Tyugu, E. (2011). *Artificial Intelligence in Cyber Defense*. Paper presented at 3rd International conference on Cyber Conflict, Tallinn, Estonia.
- Umar, R., Riadi, I., & Zamroni, G. M. (2018). Mobile forensic tools evaluation for digital crime investigation. *Int. J. Adv. Sci. Eng. Inf. Technol.*, 8(3), 949. doi:10.18517/ijaseit.8.3.3591
- UN Global Pulse. (2012). *Big Data for Development: Challenges and Opportunities*. Retrieved from <https://beta.unglobalpulse.org/wp-content/uploads/2012/05/BigDataforDevelopment-UNGlobalPulseMay2012.pdf>
- University of Southern California. (2020). *How do we remove biases in AI systems? Start by teaching them selective amnesia*. Retrieved from: <https://techxplore.com/news/2020-02-biases-ai-amnesia.html>

- Van Zandwijk, J. P., & Boztas, A. (2019). The iPhone Health App from a forensic perspective: Can steps and distances registered during walking and running be used as digital evidence? *Digital Investigation*, 28, S126–S133. doi:10.1016/j.diin.2019.01.021
- Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017, September). Long short-term memory based operation log anomaly detection. In *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 236-242). IEEE. 10.1109/ICACCI.2017.8125846
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146–1151.
- Wachter, S. (2018). Normative challenges of identification in the Internet of things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review*, 34(3), 436–449. doi:10.1016/j.clsr.2018.02.002
- Wallace, S. (2013). Impartiality in the news. In *Journalism: New Challenges*. CJCR: Centre for Journalism & Communication Research, Bournemouth University.
- Wang, L., Zhang, R., & Zhang, S. (1892). A Model of Computer Live Forensics based on Physical Memory Analysis. *Proceedings of 1st International Conference on Information Science J. Clerk Maxwell, A Treatise on Electricity and Magnetism*, 68–73.
- Wang, G., Li, W., Aertsen, M., Deprest, J., Ourselin, S., & Vercauteren, T. (2019). Aleatoric uncertainty estimation with test-time augmentation for medical image segmentation with convolutional neural networks. *Neurocomputing*, 338, 34–45. doi:10.1016/j.neucom.2019.01.103 PMID:31595105
- Wang, J., & Pei, D. (2017). Kernel-based deep learning for intelligent data analysis. In *Proceedings of 2017 First International Conference on Electronics Instrumentation & Information Systems (EIIS)* (pp. 1-5). IEEE. 10.1109/EIIS.2017.8298716
- Wang, S., & Xie. (2009). Analysis on Agile Software Development Methods from the View of Informationalization Supply Chain Management. *3rd International Symposium on Intelligent Information Technology Application Workshops*.
- WeBank. (2019). Federated Learning, white paper V1.0. Author.
- Wilson, R., & Chi, H. (2017, April). A case study for mobile device forensics tools. In *Proceedings of the SouthEast Conference* (pp. 154-157). 10.1145/3077286.3077564
- Wondflow. (2019). *Natural Language processing examples*. <https://www.wonderflow.co/blog/natural-language-processing-examples>
- Xiangyang, L., Nong, Y. (2003). Decision tree classifiers for computer intrusion detection. *Real-Time System Security*, 77–93.

Compilation of References

- Xing, Y., Wenli, Z., Nanfei, S., & Hao, Z. (2019). A Fast and Efficient Local Outlier Detection in Data Streams. *Proceedings of the 2019 International Conference on Image, Video and Signal Processing*, 111–116.
- Ya-Lin, Z., Longfei, L., Jun, Z., Xiaolong, L., & Zhi-Hua, Z. (2018). Anomaly Detection with Partially Observed Anomalies. *Companion Proceedings of the The Web Conference*, 639–646.
- Yampolskiy, R. V. (2019). Unexplainability and incomprehensibility of artificial intelligence. *Journal of Artificial Intelligence and Consciousness*, 07(02), 277–291. doi:10.1142/S2705078520500150
- Yu-Hsuan, K., Zhenhui, L., & Daniel, K. (2018). Detecting Outliers in Data with Correlated Measures. *Proceedings of the 27th ACM International Conference on Information and Knowledge Management*, 287–296.
- Yulianto, Sukarno, & Suwastika. (2019). Improving AdaBoost-based Intrusion Detection System (IDS) Performance on CIC IDS 2017 Dataset. *Proceedings of the 2nd International Conference on Data and Information Science, Journal of Physics*, 1192.
- Yuxin, D., & Siyi, Z. (2019). Malware detection based on deep learning algorithm. *Neural Computing & Applications*, 31(2), 461–472. doi:10.100700521-017-3077-6
- Zafar, A. (2011). Investigating Integration Challenges and Solutions in Global Software Development. Academic Press.
- Zeng, X.-D., Chao, S., & Wong, F. (2010). Optimization of Bagging Classifiers based on SBCB Algorithm, *Proceedings of the Ninth International Conference on Machine Learning and Cybernetics*.
- Zhang, Y., Rong, C., Huang, Q., Wu, Y., Yang, Z., & Jiang, J. (2017, August). *Based on multi-features and clustering ensemble method for automatic malware categorization*. In *2017 IEEE Trustcom/BigDataSE/ICSS*. IEEE.
- Zhangyu, C., Chengming, Z., & Jianwei, D. (2019). Outlier detection using isolation forest and local outlier factor. *Proceedings of the Conference on Research in Adaptive and Convergent Systems*, 161–168.
- Zouhair, C., Noredine, A., Khalid, M., Amina, E. O., & Mohamed, R. (2019). Newest collaborative and hybrid network intrusion detection framework based on suricata and isolation forest algorithm. *Proceedings of the 4th International Conference on Smart City Applications*, 77, 1–11.
- Zoya, K. (2020). *Digital forensics: Applications and challenges*. Retrieved June 13, 2020, from <https://legaldesire.com/digital-forensics-applications-and-challenges/4>

About the Contributors

Sanjay Misra is full Professor of Computer Engineering at Covenant University (400-500 ranked by THE(2019)) Nigeria. He is PhD. in Inf. & Know. Engg (Software Engg) from the Uni of Alcalá, Spain & M. Tech.(Software Engg) from MLN National Institute of Tech, India. He is the most productive researcher(no.1) in Nigeria during 2012-17,13-18,14-19 & 15-20 (in all disciplines),in comp science no 1 in the country & no 4 in the whole continent. Total around 400 articles (SCOPUS/WoS) with 300 coauthors from around the world (-90 JCR/SCIE) in the core & appl. area of Soft Engg, Web Engg, Health Informatics, Cybersecurity, Intelligent systems, AI etc. He got several awards for outstanding publications (2014 IET Software Premium Award (UK)), and from TUBITAK-Turkish Higher Education, and Atilim University). He has delivered more than 100 keynote/invited talks/public lectures in reputed conferences and institutes (traveled around 60 countries). He got several awards for outstanding publications (2014 IET Soft. Premium Award(UK)), &from TUBITAK-Turkish Higher Education,& Atilim Uni).He edited 42 LNCS & 6 IEEE proc, 3books, EIC of 'IT Personnel and Project Management, Int J of Human Capital & Inf Technology Professionals -IGI Global & editor in various SCIE journals.

Chamundeswari Arumugam is a Professor at the Department of Computer Science and Engineering, Sri Sivasubramaniya college of Engineering, Kalavakkam, Tamil Nadu, India. She received her Ph.D. (Engineering) on Software Estimation from Anna University, India, in 2013 and has supervised many M.E and B.E. thesis in the areas of Machine Learning, Software Engineering, Cyber Security, etc. Has published over 25 research papers in International Journal and Conference proceedings. Reviewer for the International Journal of Systems and Software Security and Protection, IGI Global publishers.

Suresh Jaganathan, Associate Professor in the Department of Computer Science and Engineering, Sri Sivasubramaniya Nadar College of Engineering, has more than 22 years of teaching experience. He received his PhD in Computer Science from Jawaharlal Nehru Technological University, Hyderabad, M.E Software

About the Contributors

Engineering from Anna University and B.E Computer Science & Engineering, from Madurai Kamarajar University, Madurai. He has more than 30 publications in refereed International Journals and Conferences. Apart from this, to his credit, he has filed two patents and written a book on “Cloud Computing: A Practical Approach for Learning and Implementation”, published by Pearson Publications. He is an active reviewer in reputed journals (Elsevier - Journal of Networks and Computer Applications, Computer in Biology and Medicine). His areas of interest are Distributed Computing, Deep Learning, Data Analytics, Machine learning & Blockchain Technology.

Saraswathi S., Associate Professor in the Department of Computer Science and Engineering has around 16 years of teaching experience. She received her Ph.D. from Anna University in 2015, Masters in Computer Science & Engineering (M.E.) from Manonmaniam Sundaranar University in 2005 and Bachelor in Computer Science & Engineering (B.E.) from National Engineering College, Manonmaniam Sundaranar University in 1999. She is a member of ACM and IEEE. She has two faculty internal funded projects funded by SSN trust. Her area of research includes Network Security, Cryptography, Cyber Forensic and IOT.

* * *

Sunita Vikrant Dhavale, BE, ME, PhD (CSE), CIEH, is currently working as Assistant Professor in Department of Computer Engineering, Defense Institute of Advanced Technology (DIAT), Pune. Her research area includes cyber security, artificial intelligence, image/audio/video security, bio metric, deep learning. She is EC-Council’s Certified Ethical Hacker (CEH-v9). She has authored two books and more than 30 papers in reputed international journals and conference proceedings. She is member of various professional bodies including IEEE, ACM, ISACA, IETE, IAENG. She is recipient of 1) NVIDIA Hardware Research Grant - TITAN V GPU for Jan 2019, 2) IETE-M N Saha Memorial Award -2016, 3) Outstanding Women Achiever Award for Engineering Category by VENUS International Women Awards (VIWA-2016), 4) Top performer in Four Week online FDP titled “FDP301x: Mentoring Educators in Educational Technology”, organized by Pandit Madan Mohan Malaviya National Mission for Teachers and Teaching (PMMMNTT), MHRD, GoI, IIT Bombay, May 2018 5) Top performer in Four Week AICTE approved online FDP by IIT Bombay on - Use of ICT in Education for Online and Blended Learning, May 2016.

Uma Maheswari Sadasivam has a combination of academics and Industry research experience. Passionate about Data Science and AI, Machine learning and an experienced in Data Warehouse, BI as well. Currently heading AI research and commercial projects at Tecple Innoventions based Mysuru, India. A Strong education professional with a Master's degree focused in Computer Science and Engineering from BITS Pilani. I teach computer science and engineering subjects for undergraduate and post graduate degree courses. Currently teaching postgraduate courses for employees of Verizon data. Though worked in IT as Program manager, now Principal research consultant I prefer teaching as it lets to carry my research related works. I continue to work as an Adjunct faculty and Principal AI and ML consultant at Tecple Innoventions Solutions Pvt Ltd, <https://tecpleglobal.com/>.

Srinivasan Vaidyanathan is a former “Director – Projects” in Cognizant, India. He has been an accomplished and results-driven delivery director in IT services industry and has 24.5 years of progressive, managerial and leadership experience in high visibility and multifaceted roles in IT majors, Cognizant and Capgemini. He had led large-scale software deliveries for several flagship customers that cut across industrial sectors. He has demonstrated success of delivery management, business development, Resource Planning, Financials, HR and Quality Management in his professional domain. He has hands-on experience in leading Knowledge Management initiatives at various capacities of his corporate tenure. He has proven abilities to implement standards, procedures, and processes that improve software delivery quality. He has a PhD in Knowledge Management from VIT, and MS in Software Engineering from BITS. His PhD thesis is in the areas of Knowledge Sharing through Social Media, Knowledge Creation and Individual Performance in IT Organizations. To his credit, he has published key research papers and book chapters in the areas of Knowledge Management and Software Engineering, in reputed International Journals and Publications.

Senthil Velan is a personable, motivated and dynamic faculty of Computer Science and Engineering with more than 20 years of teaching and research experience achieving laurels in both industria and academia. Dr Senthil completed his Master's in Computer Science at Wichita State University, USA and Doctorate in Computer Science and Engineering at Anna University, India. He has published more than 40 papers in International Conference and International Journals and posses Dale Carnegie High Impact teaching skills bagging several Best Teacher Awards. Dr Senthil is currently working as Assistant Professor of Computer Science and Engineering at Amity University Dubai.

About the Contributors

Yongbin Yu received the Ph.D. degree, M.S. degree in circuits and systems from the University of Electronic Science and Technology of China (UESTC) in 2008 and 2004 respectively. During 2013-2014, he has joined the department of Electrical Engineering and Computer Science, University of Michigan in Ann Arbor, USA, as a visiting scholar. Currently, he is an associate professor with the School of Information and Software Engineering, UESTC. He has served as the advanced evaluator of information classified security at the MPS Information Classified Security Protection Evaluation Center, and worked for three years in industrial R&D companies including the Dongfang Steam Turbine Ltd. and Chengdu Ruida Technology Co.. He has published over 30 technical papers and 2 books. His research interests include big data and memristor.

Index

A

Adversarial AI 179, 185, 190, 197
 Adversarial attack 185-186
 Adversarial Forgetting 177, 180-181, 190, 197
 AI 30-31, 34-36, 40, 43, 45, 86, 132, 152, 177-197
 android 2, 5-6, 9-11, 13-15, 24-28, 63-64
 Artificial Neural network 82, 98, 115, 125
 Auto encoders 84-86, 89-91

B

bagging classifier 67-69, 71, 74-75, 77
 bias 108, 177, 179-180, 183-184, 190-191, 194-195, 197
 Blackbox 55, 177, 180, 185, 197
 Blockchain 33, 45, 145, 147-148, 151-152, 154-163, 191
 Boltzmann machine 84, 89, 91

C

challenges 1, 4, 6, 22-23, 25-26, 31, 33-35, 42-43, 45, 48, 64, 81, 133-135, 143-144, 156, 162, 165, 174, 177-178, 180-182, 187-188, 193-196, 199-203, 205, 207-208, 211-212, 214-215, 218-221
 Convolutional Neural Networks 81-83, 86-87, 92-93, 95, 97, 99, 101-102, 105, 107, 109, 112, 114, 175
 correlation 30, 37-38, 42, 45, 51, 173-174
 Cyber Crime 2, 51, 146
 Cyber Physical System 221

Cyberattack 145

Cybersecurity 2, 30, 33, 47-48, 67-68, 70, 79, 85, 93-94, 101, 112, 116, 145-146, 148-151, 161-163, 174, 178, 187, 191, 195-196

D

data analysis 45, 47, 63, 68, 86, 174
 data breach 179, 182, 188, 197
 data extraction 2, 4, 20, 28, 122
 data integrity 5, 205, 221
 data privacy 165, 171, 177, 179-180, 182, 189-190, 194, 197
 Data Scarcity 177, 180, 184, 191, 197
 data sets 69, 118, 128, 185, 194
 data transparency 185, 198
 datasets 22, 69, 86, 101, 131-132, 148, 171, 184, 188-189, 193, 197-198, 213
 decision tree 67-68, 71-73, 77-80, 165
 deep learning 31-32, 36, 39, 41-42, 44-46, 81-82, 84-91, 95, 97, 99, 102, 104-105, 112, 114-119, 123-124, 128, 131, 148, 164, 166, 170-171, 173-174, 181, 185, 187
 deep neural network 32, 87, 93, 95, 101, 105, 107, 115, 124, 130
 DevOps 201, 215, 217-220
 digital evidence 2-3, 8, 25, 27-30, 32, 45, 58, 61, 85-86, 134-135, 144, 151, 163
 digital forensics investigation 22-23
 Digital Resource 45

Index

E

evidence 2-5, 7-8, 18-19, 23, 25, 27-34, 37-42, 45, 51-52, 58-61, 63, 81, 85-86, 134-135, 140-144, 151, 163
extraction 2, 4-5, 7, 18-20, 28, 30, 32-33, 63-64, 91, 101, 113, 122-123, 144, 181
Extreme programming 216

F

Faraday Bag 137, 144
Feasibility study 202
feature extraction 91, 101, 113, 122-123
federated learning 177, 180, 189-190, 192, 196, 198
Financial Frauds 30, 152
forensics 1-8, 18-19, 22-45, 47, 49-54, 56-58, 60-66, 81, 85-86, 91, 134-144, 151-152, 162-163, 178, 191, 194
framework design 202
fully connected 97, 106-107, 110, 172

G

Generative Adversarial Networks 85, 88

H

HexDump 136, 144

I

Impact analysis 208
insider threats 149, 174
insurance 145, 156-161, 163
Internet of things (IoT) 30, 45, 92
investigations 5, 24, 30, 32, 35, 61, 143, 187
iOS 1-2, 5-6, 9, 11-12, 15, 24, 26-28
isolation forest 67-71, 73-74, 77-80

K

Keras API 41, 46

M

machine learning 29-30, 35-37, 39, 43-44, 47-48, 50, 64-65, 67, 69, 71, 78-80, 82, 86, 89-90, 98-101, 112-114, 116, 118, 123-124, 142, 148-149, 165, 168, 170-171, 176, 181-186, 188-189, 191-192, 194, 196-198
MalNet 93, 101-102, 105-106, 109
malware 15, 23-24, 30, 33-35, 42, 51, 53-54, 90-116, 147-150, 186
malware analysis 93-94, 96-98, 114-115
ML 29-30, 32-33, 35-36, 38-40, 47-48, 50, 149, 170, 182, 191-192
mobile devices 3-4, 7-9, 11, 19-20, 22, 24-28, 39, 51, 134-136, 138-141
mobile forensics 1-3, 6-8, 18, 22-23, 25-26, 28, 32, 64, 134-144
mobile phones 2-5, 22, 27, 51, 62, 134, 189
model fit 119, 126-127, 130
motivational quotes 164, 166, 168-169, 173, 175

N

neural networks 36, 81-84, 86, 92, 95, 97, 114, 116, 124-127, 131, 175, 179, 181, 184, 190, 192
NLP 117-118, 121-124, 130, 132, 164, 170-171, 174

O

Open-Source Software 221

P

pooling layer 93, 97, 109
prediction 30-31, 38, 40-42, 46, 70, 73, 77, 83, 97, 122, 124, 130, 164-166, 169-171, 173-174, 179, 181, 183-184, 190, 192, 194, 197
Prioritizing Requirements 221
psychological analysis 169, 171, 173

R

random forest 68-69, 71, 73, 77-79, 185, 192
regression testing 209, 222
Requirement analysis 199, 202-203
Requirements Volatility 203, 222
ResNet 109-112
risks 138, 145, 149-150, 160, 182, 208

S

Scrum 201, 215-220
security 2, 6-7, 9, 14, 16, 22-26, 28, 30-31,
33-35, 40, 43-45, 47-48, 51, 61, 65,
67-68, 70, 79-80, 85, 91, 93-94, 96,
101, 112-114, 116, 139-141, 143-145,
147-150, 156-157, 161-163, 165, 171,
173-175, 178, 182, 186-188, 191, 194-
196, 198, 205, 213

Simple Neural Network 117, 124-125,
130, 132
smart phones 3-4, 28, 188-189
social networks 48, 133, 164
Software Defects 199

T

Test Specification 206, 222

V

VGGNet 109-112
vulnerabilities 1-2, 6, 9, 13, 15, 24, 26, 61,
90, 178, 185, 213