ADVANCES IN CYBER SECURITY

CYBER SECURITY AND DIGITAL FORENSICS

Challenges and Future Trends

Edited By
Mangesh M. Ghonge
Sabyasachi Pramanik
Ramchandra Mangrulkar
Dac-Nhuong Le

Scrivener Publishing

WILEY

Cyber Security and Digital Forensics

Scrivener Publishing
100 Cummings Center, Suite 541J
Beverly, MA 01915-6106

Advances in Cyber Security

Series Editors: Rashmi Agrawal and D. Ganesh Gopal

Scope: The purpose of this book series is to present books that are specifically designed to address the critical security challenges in today's computing world including cloud and mobile environments and to discuss mechanisms for defending against those attacks by using classical and modern approaches of cryptography, blockchain and other defense mechanisms. The book series presents some of the state-of-the-art research work in the field of blockchain, cryptography and security in computing and communications. It is a valuable source of knowledge for researchers, engineers, practitioners, graduates, and doctoral students who are working in the field of blockchain, cryptography, network security, and security and privacy issues in the Internet of Things (IoT). It will also be useful for faculty members of graduate schools and universities. The book series provides a comprehensive look at the various facets of cloud security: infrastructure, network, services, compliance and users. It will provide real-world case studies to articulate the real and perceived risks and challenges in deploying and managing services in a cloud infrastructure from a security perspective. The book series will serve as a platform for books dealing with security concerns of decentralized applications (DApps) and smart contracts that operate on an open blockchain. The book series will be a comprehensive and up-to-date reference on information security and assurance. Bringing together the knowledge, skills, techniques, and tools required of IT security professionals, it facilitates the up-to-date understanding required to stay one step ahead of evolving threats, standards, and regulations.

Publishers at Scrivener
Martin Scrivener (martin@scrivenerpublishing.com)
Phillip Carmical (pcarmical@scrivenerpublishing.com)

Cyber Security and Digital Forensics

Edited by
Mangesh M. Ghonge
Sabyasachi Pramanik
Ramchandra Mangrulkar
and
Dac-Nhuong Le

WILEY

This edition first published 2022 by John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA and Scrivener Publishing LLC, 100 Cummings Center, Suite 541J, Beverly, MA 01915, USA

For more information about Scrivener publications please visit www.scrivenerpublishing.com.

Wiley Global Headquarters
111 River Street, Hoboken, NJ 07030, USA

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Library of Congress Cataloging-in-Publication Data

ISBN 978-1-119-79563-6

Cover image: Pixabay.com
Cover design by Russell Richardson

Set in size of 11pt and Minion Pro by Manila Typesetting Company, Makati, Philippines

Printed in the USA

10 9 8 7 6 5 4 3 2 1

Contents

Preface

Cyber security and digital forensics are an important topic nowadays, which provides many challenging issues in relation to security, identity, intrusion detection, advanced threat detection, privacy preservation etc.

The goal of this edited book is to outline the cyber security and digital forensic challenges and future trends. The book focuses on how to secure computers from hackers and how to deal with obtaining, storing, evaluating, analysing and presenting electronic evidences. Current threats are getting more complicated and advanced with the rapid evolution of adversarial techniques. Networked computing, and portable electronic devices have broadened the role of digital forensics beyond traditional investigations into computer crime.

The main focus of this book is to provide the reader with a broad coverage of the topics that includes different concepts, models, and terminology along with examples and illustrations to show substantial technical field details. It motivates readers to practice tougher security and defense processes to cope with attackers and mitigate the situation. Practically every crime now requires some aspect of digital evidence; digital forensics provides the techniques and instruments for articulating these evidences. Digital forensics also has a number of uses for information. In addition, it has a crucial role to play in information security, security breach investigations yield useful knowledge which can be used to develop more secure systems.

Increasing overall use of computers as a way to store and retrieve high-security information requires appropriate security measures to safeguard the entire computing and communication scenario. The facets of information security are becoming a primary concern with the introduction of social media and its technology to protect the networks and the cyber environment from various threats.

This book aims at young professionals of technology, privacy, and confidence to use and improve industry reliability in a distributed manner, as well as computer scientists and software developers seeking to conduct

research and develop cyber security and digital forensic tools. This book also benefits researchers and students of advanced computer science and information technology levels.

The book focuses on cutting-edge work from both academia and industry, and seeks to solicit original research chapters with specific emphasis on cyber security and digital forensic challenges and future trends. This book also outlines some of the exciting areas of future research in cyber security and digital forensics which will lead to additional innovations in this area of research.

Organization of the Book

The book is organized into 16 chapters. A brief description of each of the chapters follows:

Chapter 1
Service-Oriented Architecture (SOA) has proven its applicability on technologies like the Internet of Things (IoT). The major benefits of SOA architecture are flexibility, better information flow, re-usability and scalability, which make it worthy to use in IoT. This concept, when adopted with generic IoT architecture, creates layers that ask and deliver service to each other. Communication protocols play an important part here, but security always remains a major concern while dealing with a huge number of heterogeneous components of IoT. This chapter provides a survey of enabling protocols, the taxonomy of layer-wise attacks and security issues of the service-oriented IoT architecture. The chapter also describes major vulnerabilities related to the adaption of SOA into IoT. We feel that this chapter can give directions to researchers for enhancing security and privacy in IoT.

Chapter 2
Broadly, Cryptography refers to the passing of secret information from one place to another securely so that only intended receivers can decrypt it. Security of the modern public key cryptographic algorithms and protocols is mainly dependent on the complexity of the factorization of the product of large prime numbers. But due to technological developments in the field of computation and evolution of new mathematical techniques, the problem of the factorization of the product of integers is not complex anymore nowadays. The growing research interests in Quantum computing technology is also making the modern public cryptographic algorithms unsafe. Researchers have proved that modern cryptographic algorithms such as

RSA are breakable using quantum computers in polynomial time complexity. Therefore, attempts are being made to design new cryptographic algorithms using Quantum Computing techniques. Quantum cryptography is an emerging field which works on principles of quantum physics. In this paper, an attempt has been made to introduce quantum cryptography, analysis on supremacy of quantum cryptography over modern cryptography, discussion on key distribution using quantum physics, and implementation challenges in quantum key distribution. We have proposed two key verification mechanisms for BB84 protocol, analysis on quantum attacks on modern cryptographic digital signatures, post-quantum digital signatures and finally discussion on future directions of this technology.

Chapter 3
Constant growth in crime rates instigates computational resources for examination at a robust rate. Whatever data being examined with the help of forensic tools needs to be stored in the digital memory. Hence artificial intelligence is the upcoming machine learning technology which is comprehensive for human minds and provides capacity of digital storage media which can be accessed when in need. The purpose of our current research is to have broader understanding about the applicability of Artificial Intelligence (AI) along with computational logic tools analysis. The present artificial neural network helps in detection of criminals through comparison of faces by employing deep learning which offers neural networks. Thus, our paper focus on the computational forensic approaches built with AI applications to detect and predict possible future crimes. Several in-built algorithms control and create a model image in a camera which can be utilized in forensic casework to solve cases robustly.

Chapter 4
The adoption of cloud platforms is gradually increasing due to the several benefits of cloud computing. Despite the numerous benefits of cloud computing, data security and privacy is a major concern, due to lack of trust on cloud service provider (CSP). Data security can be achieved through the cryptographic techniques, but processing on encrypted data requires the sharing of a secret key with the CSP to perform operations on cloud data. This leads to the breach of data privacy. The power of cloud computing is fully utilized if one is able to perform computations on encrypted data outsourced to the cloud. Homomorphic Encryption (HE) enables to store data in encrypted form and perform computations on it without revealing the secret key to CSP. This chapter highlights existing HE techniques, their

implementations in various libraries, and existing work in the field of computations on homomorphic encryption used in various applications like healthcare, financial.

Chapter 5
This chapter is an attempt to theoretically analyze human behavior and the constructions of intelligent artifacts through robotics. It highlights how the process of human development and comprehension of human behavior can be marked as a flagpole in understanding the construction of robotic systems in the repertoire of motor, perceptual, and cognitive capabilities. Technologies such as artificial intelligence and Neuro Linguistic Programming (NLP) are helping in behavioral mapping. The various functions of talent on-boarding, talent development and the off-boarding process can help in effective management which can be utilized in people through synthetic psychology. This helps in rationally understanding human behavior through robotics. Further this gives an overview of human-robot interaction (HRI) and how they are helpful in mental health care, social skill development and improving the psychosocial outcome through robotics. Synthetic psychology's impact on neuroscience and its medical diagnostics are also discussed in the chapter. Implications, suggestions, and limitations along with the ethical issues are discussed for exploring the potential of this emerging technology.

Chapter 6
The world is increasingly interconnected with the internet, which acts as a nervous system for every organisation. We can easily find interconnected devices in every home in the form of Smart devices, computer networks, and so on. The data generated by mobile devices increases rapidly because of the increase in the huge number of mobile devices, which takes more time in analysing the digital evidence. The objective of this chapter is to contribute to the history of digital forensics, the Evolutionary cycle, various investigation phases of digital forensics and give a detailed explanation about the types involved in digital forensics. This chapter demonstrates a brief study about how digital evidence plays an important role in investigation. In addition to this, we also explained the forensics tools as commercial bases as well as open-source software. During the investigation phase, determining the appropriate forensics tools depends upon the digital devices and Operating System. In some cases, multiple tools can be used to extract the full digital data.

Chapter 7
Any machine exposed to the Internet today is at the risk of being attacked and compromised. The popularity of the internet is not only changing our life view, but also changing the view of crime in our society and all over the world. The reason for Forensic Investigation is increased computer crime. Digital technology is experiencing an explosion in growth and applications. This explosion has created the new concept of the cyber-criminal, and the need for security and forensics experts in the digital environment. The purpose of digital forensics is to answer investigative or legal questions to prove or disprove a court case. To ensure that innocent parties are not convicted and that guilty parties are convicted, it is mandatory to have a complete forensic process carried out by a qualified investigator who implements quality control measures and follows standards. In this paper, types of Digital Forensics with their tools and techniques of investigation are discussed. This chapter also involves the challenges in carrying out Digital forensics.

Chapter 8
A Cyber Physical System (CPS) is an amalgamation of multicomponent, networked intelligent digital systems with an ability to interact with humans in realtime and in usually uncertain physical environment. CPS finds its uses in multiple sectors including health care. The term 'Medical Cyber Physical System' (MCPS) describes a prominent branch of CPS pivoting its health care sector use cases. The use of MCPS increases the need to collect more data, process it, and to put it into action. With large amounts of data being collected, modelled, and trained to produce appropriate actions also sheds light towards CPS Security (CPSSEC) mechanisms. There exist multiple proposed security mechanisms for CPSs. However, there is a lack of consolidated framework to assess and benchmark its security aspects. In this chapter, authors have explained the need for such a framework for assessing the security of MCPSs and have proposed one, named 4S (Step-by-Step, Systematic, Score Based, Security Pivotal) Assessment and Benchmarking Framework. An assessment on a hypothetical MCPS has also been done to illustrate the use of the 4S framework. Such a framework can render useful for system designers and can also be improved by other researchers to strengthen the security aspect of MCPSs.

Chapter 9
Data in IoT domains is significantly analysed and the information is mined as required. The results from the devices are then shared among the interested devices for better experience and efficiency. Sharing of data

is rudimentary in any IoT platform which increases the probability of an adversary gaining access of the data. Blockchain, which consists of blocks that are connected together by means of cryptographic hashes, SHA256 being the most popularly used hash function in the blockchain network, is a newly adapted technology for secure sharing of data in IoT domains. A lot of challenges involving the integration for blockchain in IoT has to be addressed that would ultimately provide a secure mechanism for data sharing among IoT devices.

Chapter 10
Security systems have been one of the most challenging systems to secure assets and protect privacy over the past few years. Because of the increase in. electronic transactions, the demand for rapid and precise identification and authentication is high. Face can be used as an identification and authentication tool. Face recognition possess many challenges like pose variation, blurriness, low resolution, illumination, facial expression, viewing angle and lighting conditions. Most of the work has been carried out to address the challenges in face recognition. Forensic face recognition is more challenging than normal face recognition because forensic images are of poor quality due to facial images captured under unfavorable circumstances. The forensic world is also becoming difficult and challenging because numerous crimes occur frequently and criminal investigators use face as a valuable and forensic tool. Forensic experts use domain-specific methods and perform a manual comparison to identify the suspects. The manual comparison takes more time and effort. As a result, it is possible to develop novel approaches to automate the process of domain-specific methods. The main objective of this chapter is to describe how face recognition is an important and most significant topic in forensics and the challenges which exist in forensic face recognition. From this chapter, researchers will be motivated to pursue research in the area of forensic face recognition since research in this field is at an infant stage.

Chapter 11
Traditional Computer Forensics seems to be no longer as trivial as decades ago, with a very restricted set of available electronic components, entering the age of digital formation of hardware and software too. It has recently been shown how cyber criminals are using a sophisticated and progressive approach to target digital and physical infrastructures, people and systems. Therefore, the analysis approach faces many problems due to the fact that billions of interconnected devices produce relatively at least small bits of evidence that comprehend the Data Analysis paradigm effortlessly. As a

consequence, the basic methodology of computer forensics requires to adapt major attention to develop smart and fast digital investigation techniques. Digital forensics investigation frameworks are occupied with lots of toolkits and applications according to the need of any criminal incident. Using the Digital Forensics Process's microscope, specific objects are discussed and analysed with respect to which tools are needful. Also, where the scope of attention is required to enhance the feature in it. This research leads to increased awareness, challenges and opportunities for Digital Forensics process with respect to different fields such as networks, IoT, Cloud computing, Database system, Big data, Mobile and handheld devices, Disk and different storage media, and Operating system.

Chapter 12
Machine learning (ML) and deep learning (DL) have both produced overwhelming interest and drawn unparalleled community interest recently. With a growing convergence of online activities and digital life, the way people have learned and function is evolving, but this also leads them towards significant security concerns. Protecting sensitive information, documents, networks and machine-connected devices from unwanted cyber threats is a difficult task. Robust cybersecurity protection is necessary for this reason. For a problem solution, current innovations like machine learning and deep learning is incorporated to cyber threats. This paper also highlights the problems and benefits with using ML/DL and presents recommendations for research directions for machine learning and deep learning in cybersecurity.

Chapter 13
Machine learning (ML) is the latest buzzword growing rapidly across the world, and ML possesses massive potential in numerous domains. ML technology is a subset of Artificial Intelligence (AI) and empowers digital machines with the ability to learn without being explicitly programmed, i.e., the capability to learn from past experiences. Since the last decade, ML technology has been used in various domains because it possesses numerous interesting characteristics such as adaptability, robustness, learnability, and its ability to take instant actions against unexpected challenges. The traditional cybersecurity systems are built on rules, attack signatures, and fixed algorithms. Thus, the systems can act only upon the *'knowledge'* fed to them and human intervention is continually required for the proper functioning of traditional cybersecurity systems. On the other hand, ML technology can recognize various patterns from past experiences and is capable of predicting or detecting future attacks based on seen or unseen

data. The ML technology is capable of handling massive real-time network data which allows various issues present in conventional cybersecurity systems to be overcome. In the present chapter, various issues related to the applications of ML in cybersecurity have been discussed. The effectiveness of applying ML technology in cybersecurity affairs has been thoroughly investigated. The contemporary challenges being faced by researchers in the realm have been identified and discussed. The current chapter presents available datasets and algorithms for the successful implementation of ML technology in the domain of cybersecurity. The datasets are also compared across various parameters. Finally, applications of ML practices by three renowned businesses, Facebook, Microsoft, and Google are explored.

Chapter 14
Blockchain will become the world's most basic technology—to go ahead. The revolution has actually already begun. The advent of distributed control system (DCS) and supervisory control and data acquisition (SCADA) has led to the necessity for automation, connection, and stable IoT Security systems from the dark web. There are no autonomous decision-making and real-time connectivity capabilities in existing innovative structures, a requirement for flexible, complex development systems. This research introduces to these tests an independent, stable, and interactive Blockchain-based framework. To connect computers, consumers, tools, dark web supplier, and other peers, it is possible to build with the Internet of Things (IoT) and cloud services in support of the proposed software. The recommendation would check the argument with a small, real-life IoT network blockchain using the Smart Contract functionality and reliable pair to open ledger functionality. A private Blockchain would operate on one board unit and bridge this case study to a micro-controller with IoT sensors. Distributed control system (DCS) and supervisory control and data acquisition (SCADA) in the dark web platform have been introduced to implement this device to study and analyze the existing approach with IoT-Towards Automated IoT Industry to improve the security system using blockchain technology.

Chapter 15
A developer must have an understanding ability of secure coding to create secure applications. A secure coding knowledge is focused on the combination of multiple mechanisms for exploiting and protecting typical malicious inputs to vulnerabilities of an application. The aim of this chapter is to review the recent techniques about exploitation and protection of common malicious inputs to online applications implemented by PHP script

for a developer to enhance the security of web pages. This chapter provides essential knowledge and mechanisms to vulnerabilities management for secure online applications.

Chapter 16
Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment. Ransomware is a way of stealing money in which a user's files are encrypted and the decryption key is held by the attacker until a ransom amount is paid by the victim. Organizations need to have a full inventory of all the devices that are connected to the network and protect with an updated security solution. It is mandatory to study ransomware and its strategies to protect your computer system from being infected. Various types of ransomware attacks along with their features are studied by highlighting the major methodology used in the launching of ransomware attacks. Also, the comparative analysis of various ransomwares, detection mechanisms as well as prevention policies against ransomware attacks are summarized.

Editors
Dr. Mangesh M. Ghonge
Department of Computer Engineering, Sandip Institute of Technology and Research Centre, Nashik, Maharashtra, India
Dr. Sabyasachi Pramanik
Department of Computer Science and Engineering, Haldia Institute of Technology, Haldia, West Bengal, India
Dr. Ramchandra Mangrulkar
Department of Computer Engineering, D.J. Sanghvi College of Engineering, Mumbai, Maharashtra, India
Dr. Dac-Nhuong Le
Associate Dean of Faculty of Information Technology, Haiphong University, Vietnam

Acknowledgment

We wish to acknowledge the help of all the people involved in this project and, more specifically, the authors and reviewers that took part in the review process. Without their support, this book would not have become a reality. We thank God for the opportunity to pursue this highly relevant subject at this time, and each of the authors for their collective contributions. Our sincere gratitude goes to all the chapter authors around the world who contributed their time and expertise to this book. We wish to acknowledge the valuable contributions of all the peer reviewers regarding their suggestions for improvement of quality, coherence, and content for chapters. Some authors served as referees; we highly appreciate their time and commitment. A successful book publication is the integrated result of more people than those persons granted credit as editor and author.

Editors
Dr. Mangesh M. Ghonge
Department of Computer Engineering, Sandip Institute of Technology and Research Centre, Nashik, Maharashtra, India
Dr. Sabyasachi Pramanik
Department of Computer Science and Engineering, Haldia Institute of Technology, Haldia, India
Dr. Ramchandra Mangrulkar
Department of Computer Engineering, D.J. Sanghvi College of Engineering, Mumbai, Maharashtra, India
Dr. Dac-Nhuong Le
Associate Dean of Faculty of Information Technology, Haiphong University, Vietnam