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

Table of Contents

Cover

Title Page

Copyright

Preface

Acknowledgment

1 A Comprehensive Study of Security Issues and Research Challenges in Different Layers of Service-Oriented IoT Architecture

- 1.1 Introduction and Related Work
- 1.2 IoT: Evolution, Applications and Security Requirements
- 1.3 Service-Oriented IoT Architecture and IoT Protocol Stack
- 1.4 Anatomy of Attacks on Service-Oriented IoT Architecture
- 1.5 Major Security Issues in Service-Oriented IoT Architecture
- 1.6 Conclusion
- References

2 Quantum and Post-Quantum Cryptography

- 2.1 Introduction
- 2.2 Security of Modern Cryptographic Systems
- 2.3 Quantum Key Distribution
- 2.4 Post-Quantum Digital Signature
- 2.5 Conclusion and Future Directions
- References

3 Artificial Neural Network Applications in Analysis of Forensic Science

- 3.1 Introduction
- 3.2 Digital Forensic Analysis Knowledge
- 3.3 Answer Set Programming in Digital Investigations
- 3.4 Data Science Processing with Artificial Intelligence Models
- 3.5 Pattern Recognition Techniques
- 3.6 ANN Applications
- 3.7 Knowledge on Stages of Digital Forensic Analysis
- 3.8 Deep Learning and Modelling
- 3.9 Conclusion
- References

4 A Comprehensive Survey of Fully Homomorphic Encryption from Its Theory to Applications

- 4.1 Introduction
- 4.2 Homomorphic Encryption Techniques
- 4.3 Homomorphic Encryption Libraries
- 4.4 Computations on Encrypted Data
- 4.5 Applications of Homomorphic Encryption
- 4.6 Conclusion
- References

5 Understanding Robotics through Synthetic Psychology

- 5.1 Introduction
- 5.2 Physical Capabilities of Robots
- 5.3 Traditional Psychology, Neuroscience and Future Robotics

5.4 Synthetic Psychology and Robotics: A Vision of the Future

5.5 Synthetic Psychology: The Foresight

5.6 Synthetic Psychology and Mathematical Optimization

5.7 Synthetic Psychology and Medical Diagnosis

5.8 Conclusion

References

6 An Insight into Digital Forensics: History, Frameworks, Types and Tools

6.1 Overview

6.2 Digital Forensics

6.3 Digital Forensics History

6.4 Evolutionary Cycle of Digital Forensics

6.5 Stages of Digital Forensics Process

6.6 Types of Digital Forensics

6.7 Evidence Collection and Analysis

6.8 Digital Forensics Tools

6.9 Summary

References

7 Digital Forensics as a Service: Analysis for Forensic Knowledge

7.1 Introduction

7.2 Objective

7.3 Types of Digital Forensics

7.4 Conclusion

References

8 4S Framework: A Practical CPS Design Security Assessment & Benchmarking Framework

8.1 Introduction

8.2 Literature Review

8.3 Medical Cyber Physical System (MCPS)

8.4 CPSSEC vs. Cyber Security

8.5 Proposed Framework

8.6 Assessment of Hypothetical MCPS Using 4S Framework

8.7 Conclusion

8.8 Future Scope

References

9 Ensuring Secure Data Sharing in IoT Domains Using Blockchain

9.1 IoT and Blockchain

9.2 IoT Application Domains and Challenges in Data Sharing

9.3 Why Blockchain?

9.4 IoT Data Sharing Security Mechanism On Blockchain

9.5 Conclusion

References

10 A Review of Face Analysis Techniques for Conventional and Forensic Applications

10.1 Introduction

10.2 Face Recognition

10.3 Forensic Face Recognition

10.4 Conclusion

References

11 Roadmap of Digital Forensics Investigation Process with Discovery of Tools

11.1 Introduction

11.2 Phases of Digital Forensics Process

11.3 Analysis of Challenges and Need of Digital Forensics

11.4 Appropriateness of Forensics Tool

11.5 Phase-Wise Digital Forensics Techniques

11.6 Pros and Cons of Digital Forensics Investigation Process

11.7 Conclusion

References

12 Utilizing Machine Learning and Deep Learning in Cybesecurity: An Innovative Approach

12.1 Introduction

12.2 Proposed Method

12.3 Experimental Studies and Outcomes Analysis

12.4 Conclusions and Future Scope

References

13 Applications of Machine Learning Techniques in the Realm of Cybersecurity

13.1 Introduction

13.2 A Brief Literature Review

13.3 Machine Learning and Cybersecurity: Various Issues

13.4 ML Datasets and Algorithms Used in Cybersecurity

13.5 Applications of Machine Learning in the Realm of Cybersecurity

13.6 Conclusions

References

14 Security Improvement Technique for Distributed Control System (DCS) and Supervisory Control-Data

Acquisition (SCADA) Using Blockchain at Dark Web Platform

14.1 Introduction

14.2 Significance of Security Improvement in DCS and SCADA

14.3 Related Work

14.4 Proposed Methodology

14.5 Result Analysis

14.6 Conclusion

References

15 Recent Techniques for Exploitation and Protection of Common Malicious Inputs to Online Applications

15.1 Introduction

15.2 SQL Injection

15.3 Cross Site Scripting

15.4 Cross Site Request Forgery

15.5 Command Injection

15.6 File Inclusion

15.7 Conclusion

References

16 Ransomware: Threats, Identification and Prevention

16.1 Introduction

16.2 Types of Ransomwares

16.3 Ransomware Life Cycle

16.4 Detection Strategies

16.5 Analysis of Ransomware

16.6 Prevention Strategies

16.7 Ransomware Traits Analysis

16.8 Research Directions

16.9 Conclusion

References

Index

End User License Agreement

List of Illustrations

Chapter 1

Figure 1.1 IoT devices and platforms.

Figure 1.2 Security requirements and attacks in IoT.

Figure 1.3 General service-oriented architecture.

Figure 1.4 Service-oriented IoT architecture [49].

Figure 1.5 IoT protocol stack [52].

Figure 1.6 Attacks on software services.

Figure 1.7 Attacks on application layer and transport layer protocols.

Figure 1.8 Attacks on network layer protocols.

Figure 1.9 Attacks on link and physical layer protocols.

Chapter 2

Figure 2.1 BB84 key exchange protocol.

Figure 2.2 E91 key exchange protocol.

Chapter 3

Figure 3.1 Artificial neural network works as patterns in predicting information...

Figure 3.2 Deep learning enabled cyber forensic investigation analysis.

Figure 3.3 Hidato puzzle (Hidoku) matrix list (Kjellerstrand, 2015).

Figure 3.4 Role of artificial intelligence in data science.

Figure 3.5 Model for pattern recognition in forensic analysis.

Figure 3.6 Phases of digital investigation provides knowledge in forensic scienc...

Figure 3.7 Pattern recognition in deep learning algorithm.

Chapter 4

Figure 4.1 Working of homomorphic encryption.

Figure 4.2 Timeline of homomorphic encryption schemes from PHE to FHE.

Chapter 6

Figure 6.1 Flow process of digital forensics.

Figure 6.2 Cloud forensics flow process.

Figure 6.3 Flow process of mobile forensics.

Figure 6.4 Process of network forensics.

Figure 6.5 Evidence collection of storage devices.

Chapter 7

Figure 7.1 Digital forensics steps.

Figure 7.2 Branches of digital forensics.

Figure 7.3 Security threats of database system.

Figure 7.4 Forensic process of database systems.

Figure 7.5 Mobile device evidence proof extraction process.

Figure 7.6 Workflow of cloud forensic process.

Chapter 8

Figure 8.1 Flowchart with main sections and blocks inside each section.

Figure 8.2 Flowchart of MVM/quick assessment.

Figure 8.3 Flowchart of DCPS assessment.

Figure 8.4 Flowchart of HMSB assessment.

Figure 8.5 Flowchart of score calculation.

Figure 8.6 Flowchart of self benchmarking.

Figure 8.7 Hypothetical CPS’s block diagram.

Figure 8.8 Use case diagram of CIPMA system.

Chapter 9

Figure 9.1 Architecture of IoT.

Figure 9.2 Blockchain architecture.

Figure 9.3 IoT application domains.

Figure 9.4 Data shared IoT domains.

Chapter 10

Figure 10.1 Possible outcomes in the verification task [2].

Figure 10.2 Possible outcomes in the identification task [2].

Figure 10.3 Illumination variations [14].

Figure 10.4 Pose variations [14].

Figure 10.5 Facial expressions [14].

Figure 10.6 Architecture of forensic face recognition for manual and automated a...

Figure 10.7 Facial aging [26].

Figure 10.8 Facial marks [26].

Figure 10.9 Forensic sketch recognition [26].

Figure 10.10 Face recognition in video [26].

Figure 10.11 Partial occlusion features [26].

Figure 10.12 Glimpse of images captured from different datasets [27, 28].

Figure 10.13 Facial components [13].

Chapter 11

Figure 11.1 Entities affected by criminal activity.

Figure 11.2 Domain-wise hierarchy of digital forensics.

Figure 11.3 Phases of digital forensics process.

Figure 11.4 Elaboration of digital forensics phases.

Figure 11.5 Cyber-attack incidents with more than $1 million losses [13].

Figure 11.6 Growth of malware and phishing websites which are used to commit cri...

Figure 11.7 Evidence bag and faraday bags [15].

Figure 11.8 Procedure of data acquisition.

Figure 11.9 Disk partitioning for recovery of tampered and deleted file/document...

Figure 11.10 Sample of recovery of deleted data from USB using autopsy tool.

Figure 11.11 Collection of memory dump using Dumpit software.

Figure 11.12 Collection of information about the USB devices connected to a syst...

Figure 11.13 Recovery of JPEG image file with detailed information about startin...

Figure 11.14 Recovery of JPEG image file with detailed information about startin...

Figure 11.15 Analyzing the memory dump collected Dumpit in WinHex tool.

Figure 11.16 Image duplication of a USB using FTK toolkit.

Chapter 12

Figure 12.1 Set of experiments amidst many organizations.

Chapter 13

Figure 13.1 Modules of Microsoft’s security solutions.

Chapter 14

Figure 14.1 Industrial IoT: threats and countermeasures.

Figure 14.2 Hierarchal structure of IoT functionality layers.

Figure 14.3 An event-based approach for the protection of IoT networks.

Figure 14.4 Percentage of users targeted in different sectors.

Figure 14.5 Individual distribution of different types of crime rates.

Figure 14.6 Comparison of online transactions for last 10 years.

Chapter 16

Figure 16.1 Working of ransomware.

Figure 16.2 Types of ransomwares.

Figure 16.3 Ransomware life cycle.

Figure 16.4 Ransomware analysis.

List of Tables

Chapter 1

Table 1.1 Summary of application layer protocols.

Table 1.2 Summary of transport layer protocols and features.

Table 1.3 Summary of link layer and physical layer protocols (short range).

Table 1.4 Summary link layer and physical layer protocols (long range).

Table 1.5 Security issues in each layer of service oriented IoT architecture.

Table 1.6 Major threats in application - interface layer.

Table 1.7 Major threats in network layer.

Table 1.8 Major threats in sensing layer.

Chapter 2

Table 2.1 Security level of cryptographic systems.

Table 2.2 Round two candidates.

Table 2.3 Round three candidates.

Chapter 3

Table 3.1 Application of artificial neural networking in predicting diseases.

Chapter 4

Table 4.1 Libraries for various FHE implementation.

Table 4.2 Comparison of HE libraries based on various features.

Chapter 6

Table 6.1 Various forensics tools.

Chapter 8

Table 8.1 Points division for main sections.

Table 8.2 Points division for DCPS sections.

Table 8.3 Levels of system’s preparedness for handling attacks for cyber attacks...

Table 8.4 Cyber attacks & threats corpus of assessments.

Table 8.5 Levels of system’s preparedness for handling attacks for physical thre...

Table 8.6 Physical threats corpus of assessments.

Table 8.7 Levels of system’s preparedness for handling attacks for medical threa...

Table 8.8 Medical threats corpus of assessments.

Table 8.9 Levels of system’s preparedness for handling attacks exceptional situa...

Table 8.10 Exceptional situation caused attacks & threats - corpus of assessment...

Table 8.11 Points division for HMSB section.

Table 8.12 Results of cyber attacks & threats from its corpus of assessments.

Table 8.13 Results of physical threats from its corpus of assessments.

Table 8.14 Results of exceptional threats from its corpus of assessments.

Table 8.15 Results of medical threats from its corpus of assessments.

Table 8.16 Results of cyber attacks & threats from its corpus of assessments.

Table 8.17 Results of physical threats from its corpus of assessments.

Table 8.18 Results of exceptional threats from its corpus of assessments.

Table 8.19 Results of medical threats from its corpus of assessments

Chapter 9

Table 9.1 IoT devices (source gartner).

Table 9.2 Types of trust.

Chapter 10

Table 10.1 Comparison of various face recognition approaches.

Table 10.2 Comparison of various forensic face recognition approaches.

Chapter 11

Table 11.1 Criminals and attackers usually perform malicious activity by using t...

Table 11.2 Different file system uses to analyze and recover the file [21].

Table 11.3 Details of different carving techniques [23, 24].

Table 11.4 Description of volatile data forensic toolkit [25].

Table 11.5 Description of non-volatile data forensic toolkit [26].

Chapter 12

Table 12.1 Distributing info.

Table 12.2 Classifiers’ success in recognizing various categories of feedback re...

Table 12.3 Classifiers’ success in pinpointing various categories of malwarerela...

Table 12.4 Classifier’s success for distinguishing various forms of malware rela...

Table 12.5 Classifiers’ success by defining various forms of malware related to ...

Table 12.6 Categories of dispersal of responses for five businesses indicates t...

Table 12.7 The delivery category related to malware in five businesses reveals ...

Chapter 13

Table 13.1 Comparison of key characteristics of various datasets.

Chapter 14

Table 14.1 Comparison of various studies carried out for detection of separate a...

Table 14.2 The use of smart contracts in various domains.

Table 14.3 The user-targeted in various industrial sectors.

Chapter 16

Table 16.1 Ransomware traits.

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

Scrivener Publishing

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.

Limit of Liability/Disclaimer of Warranty

While the publisher and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives, written sales materials, or promotional statements for this work. The fact that an organization, website, or product is referred to in this work as a citation and/or potential source of further information does not mean that the publisher and authors endorse the information or services the organization, website, or product may provide or recommendations it may make. This work is sold with the understanding that the publisher is not engaged in rendering professional services. The advice and strategies contained herein may not be suitable for your situation. You should consult with a specialist where appropriate. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read.

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

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