ADVANCES IN CYBER SECURITY

CYBER SECURITY AND NETWORK SECURITY

Edited By
Sabyasachi Pramanik
Debabrata Samanta
M. Vinay
Abhijit Guha

Scrivener Publishing

WILEY

Table of Contents

List of Tables

Chapter 1

Chapter 2

Chapter 5

Chapter 11

List of Illustrations

Chapter 1

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Chapter 9

Chapter 10

Chapter 11

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 Network Security

Edited by

Sabyasachi Pramanik

Debabrata Samanta

M. Vinay

and

Abhijit Guha

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 © 2022 Scrivener Publishing LLC
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 9781119812494

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

Dedication

This book is dedicated to my parents, my spouse, my elder sister and my son Arnab Pramanik.

Dr. Sabyasachi Pramanik

To my parents Mr. Dulal Chandra Samanta, Mrs. Ambujini Samanta, my elder sister Mrs. Tanusree Samanta and daughter Ms. Aditri Samanta.

Dr. Debabrata Samanta

To my parents Mr. Madhava Rao R, Mrs. Padma M Rao from whom I learnt the Intonation.

Dr. M. Vinay

To my parents Mr. Nilay Guha, Mrs. Shila Guha; my uncles Mr. Malay Guha and Mr. Pralay Guha; My wife Mrs. Gargee Chakraborty and daughter Ms. Arohi Guha.

Abhijit Guha

Preface

This book focuses on the “interdisciplinarity” of cyber security and network security which contributes to the emerging dialogue on the direction, content and techniques involved in the growth and development of cyber security and network security education and training. The book “Cyber Security and Network Security: Advances, Applications and Emerging Trends” presents the latest methodologies and trends in detecting and preventing cyber and network threats. Investigating the potential of current and emerging security technologies, this publication is an all-inclusive reference source for academicians, researchers, students, professionals, practitioners, network analysts, and technology specialists interested in the simulation and application of cyber and computer network protection. It presents theoretical frameworks and the latest research findings in cyber security and network security technologies while analyzing malicious threats which can compromise cyber and network integrity. It discusses the security and optimization of cyber and computer networks for use in a variety of disciplines and fields. Touching on such matters as mobile and VPN security, IP spoofing, and intrusion detection, this edited collection emboldens the efforts of researchers, academics, and network administrators working in both the public and private sectors. This edited compilation includes chapters covering topics such as attacks and countermeasures, mobile wireless networking, intrusion detection systems, next-generation firewalls, and more. Information and communication systems are an essential component of our society, forcing us to become dependent on these infrastructures. At the same time, these systems are undergoing a convergence and interconnection process that, besides its benefits, raises specific threats to user interests. Citizens and organizations must feel safe when using cyberspace facilities in order to benefit from its advantages.

The current trends and future directions of diverse Cyber security and Network Security Research with applications in various domains are covered in this book. Assaults on computers are gradually becoming one of the most common problems on the planet. As the scope of digital misbehavior grows, it is critical to look into fresh techniques and advancements that can aid ensure the internet network’s security. Continuous technological advancements have necessitated a deliberate approach to security challenges.

Chapter 1 explores that data security, both inside and outside client devices, is a very important problem in today’s society, which is primarily operated through programs interacting over the internet. The MSME sector and new businesses are primarily moving to the cloud to take advantage of the emerging virtual market prospects and to change their work culture to the online arena. As a result, workplace communication that previously took place behind closed doors and in locked storage rooms with data has transitioned to a more public setting, with files being sent through the public internet to public facing servers. As many of the servers for Public/Hybrid Cloud models are owned jointly by two or more parties/stakeholders, this creates a whole new set of security and compliance issues. As a result, data in transit, i.e. data moving in and out of the cloud, as well as data at rest, i.e. data stored in the cloud, must be encrypted so that no third party can access it without the owner’s permission. Data from a client application, such as an Enterprise Communication Application, would be encrypted using updated algorithms and accessible securely through a set of Access Control capabilities with Least Privilege Access Policies in this suggested study model. The data is then packaged and sent over SSL Layers to a server-side application instance running in a public cloud (here)/private cloud, which decrypts the data and sorts it accordingly before saving it to object-based storages, NoSQL databases, and ledger databases with high availability and security at rest. The data at rest is further encrypted, and when requested, it can be packaged and given back to the client application with the essential encryption in transit conditions met. The transactions are carried out using role-based assigning systems and least access privilege access mode, thus obliterating the ideas of data eavesdropping, personal security risks, and so on.

Chapter 2 discusses the use of cloud technology which has grown in recent years. Cloud computing has become an essential component of modern life. Many businesses have been attracted to relay because of the on-demand service providing flexibility enabled by cloud technology. It is not necessary to purchase servers, databases, or other advanced technologies in order to start a new business. Simultaneously, data security in the cloud is extremely concerning and necessitates some attention. With the use of the user's cloud records, switches, and routers, cybercriminals can gain access to the user's systems in a variety of methods. Cloud computing is distributed computing, and it is impossible to imagine cloud computing without these techniques. The security procedures are still in their infancy. Identifying the cyber criminal's cybernetic proof is critical. Cloud service providers rarely give cloud security analysts access to cloud logs or virtual machine instances. For cyber criminals to abuse cloud computations at any time, they only need cybernetic evidence. To prevent cyber criminals from intruding, security procedures must be strengthened. Cloud forensics is one approach to carry out such tasks. There is a lot of research going on in this subject, but there are still a lot of problems to tackle. HPCBC is a high-performance cluster-based computing (HPCBC) technology that can be employed in IoT and AI applications instead of supercomputers. HPCBC uses a parallel processing system. Cloud forensics could be given a new direction with the support of high-performance cluster-based computing, according to this article. Simultaneous imaging and upload, as well as encryption, are available for the files. With the Remote desktop connection, the files should be processed in real-time stream processing. This survey article offers a variety of perspectives on cloud forensic methods and methodologies.

Chapter 3 includes that in the last few decades, cyber-attacks have become far more common. According to statistics, 12.4 million attacks were documented in 2009, and this number has since climbed to 812.67 million known occurrences in 2018. To be fair, these are merely the documented cases; there are many more. Small cyber attacks to massive Ransom ware attacks or a mix of several complex cyber attacks that include advanced exploitation techniques and persistence capacity for long-term infiltration campaigns. However, the deployment of malware was a common thread in all of the cyber attacks that have occurred thus far. To counter these attacks, we must first comprehend malware’s basic structure, functionality, and impacts on the target. This paper gives an in-depth look at malware architectures by studying the malware using a technique known as malware analysis, as well as other related methods that vary based on the type of malware and a closer look at several types of malware, as well as certain well-known malware methods.

Chapter 4 discusses that fraud is one of the most common sources of substantial financial consequences in today’s society, not just for businesses but also for individual customers. The extraction of user profiles based on previous transaction data and then deciding whether or not an incoming transaction is a fraud based on those profiles is an important approach of detecting fraud. The suggested block-chain technology enables certified users to securely store, review, and exchange digital data, facilitating the development of trust, integrity, and transparency in online commercial connections. Block-chain systematically examines the resilience of block-chain-based reputation systems, with a focus on the secure and reliable extraction and transfer of data to customers. Block-chain uses cryptographic hashes generated from summarized shopping blocks that are signed and sent to enable a safe and secure online buying experience without the need for third-party intervention.

In Chapter 5, it is shown that the demand for blockchain-based identity management systems is especially evident in the internet age; we've been dealing with identity management issues since the internet's inception. Privacy, security, and usability have all been cited as major concerns. User identities are organized using identity management systems (IDMSs), which also manage authentication, authorization, and data interchange over the internet. In addition to a lack of interoperability, single points of vulnerability, and privacy concerns, such as allowing bulk data collection and device tracking, traditional identity management systems suffer from a lack of interoperability, single points of vulnerability, and privacy concerns. Blockchain technology has the potential to alleviate these problems by allowing users to track who owns their own IDs and authentication credentials, as well as enabling novel information ownership and administration frameworks with built-in control and consensus methods. As a result, the number of blockchain-based identity management solutions, which can benefit both enterprises and clients, has been fast expanding. We'll classify these frameworks using scientific criteria based on differences in blockchain architecture, administration methods, and other important features. Context is provided by scientific classification, which includes the depiction of significant concepts, evolving principles, and use cases, as well as highlighting important security and privacy concerns.

In Chapter 6, the concept of feed forward networks is introduced which serve as the foundation for recurrent neural networks. Simple writing analysis is the best analogy for RNN, because the prediction of the next word is always dependent on prior knowledge of the sentence's contents. RNN is a form of artificial neural network that is used to recognize a sequence of data and then analyze the results in order to predict the outcome. The LSTM is a type of RNN that consists of a stack of layers with neurons in each layer. This article also goes into the issues that each technology has as well as possible remedies. Optimization algorithms alter the features of neural networks, such as weights and learning rates, to reduce losses. Optimization Algorithms in Neural Networks is one of the sections. A section dedicated to some of the most current in-depth studies on Steganography and neural network combinations. Finally, for the prior five years, we give an analysis of existing research on the current study (2017 to 2021).

In Chapter 7, it has been found that cyber physical systems (CPS) will be used in the majority of real-time scenarios in the future. The use of such technologies is unavoidable in order to make the world smarter. However, as the use of such technologies grows, so does the need for improved privacy. Users will not be easily used to such systems if the privacy component is compromised. Because Cyber Physical Systems use a variety of heterogeneous sensor data sources, incorporating a high level of privacy is becoming increasingly difficult for system designers. The applicability of the precise penalty function and its benefits in increasing the privacy level of cyber physical systems will be presented in this chapter. We'll compare this to existing privacy-preserving strategies in cyber-physical systems and discuss how our suggested privacy framework could be improved in the future.

In Chapter 8, the increasing demands for the preservation and transit of multi-media data have been a part of everyday life over the last many decades. Images and videos, as well as multimedia data, play an important role in creating an immersive experience. In today's technologically evolved society, data and information must be sent rapidly and securely; nevertheless, valuable data must be protected from unauthorized people. A deep neural network is used to develop a covert communication and textual data extraction strategy based on steganography and picture compression in such work. The original input textual image and cover image are both pre-processed using spatial steganography, and then the covert text-based pictures are separated and implanted into the least significant bit of the cover image picture element. Following that, stego-images are compressed to provide a higher-quality image while also saving storage space at the sender's end. After that, the stego-image will be transmitted to the receiver over a communication link. At the receiver's end, steganography and compression are then reversed. This work contains a plethora of issues, making it an intriguing subject to pursue. The most crucial component of this task is choosing the right steganography and image compression method. The proposed technology, which combines image steganography and compression, achieves higher peak signal-to-noise efficiency.

Chapter 9 shows the number of mobile network-connected devices is steadily increasing. The 5G network will theoretically provide a speed of 20 gigabits per second, allowing customers to access data at a rate of 100 megabits per second. Around the world, there are estimated to be 5 billion gadgets. With the advancement of wearable technology, a typical client can now carry up to two network-connected devices or engage in D2D communication. Clients are attracted to the 5G network because it advertises reduced inertness information correspondence, faster access and data transfer rates, and a more secure nature. As the number of supporters grows, concerns about information and computerized assurance will grow in order to keep up with the integrity of data security. Similarly, with any type of data security, there are always concerns about the safety of clients and their sensitive information. This chapter will discuss how to secure the diverse structures that are associated with networks, where these networks are vulnerable to compromise, well-known attack tactics, and how to avoid technical discrepancies.

Chapter 10 has explored the modern Information Technology environment necessitates increasing the value for money while ignoring the potency of the gathered components. The rising demand for storage, networking, and accounting has fueled the growth of massive, complex data centers, as well as the big server businesses that manage several current internet operations, as well as economic, trading, and corporate operations. A data centre can hold thousands of servers and consume the same amount of electricity as a small city. The massive amount of calculating power required to run such server systems controls a variety of conflicts, including energy consumption, greenhouse gas emissions, substitutes, and restarting affairs, among others. This is virtualization, which refers to a group of technologies that cover a wide range of applications and hobbies. This can be applied to the sectors of hardware and software, as well as innovations on the outskirts of virtualization's emergence. This study demonstrates how we proposed using virtualization technologies to gradually transform a traditional data centre structure into a green data centre. This study looks into the reasons for the price profits of supporting virtualization technology, which is recommended by practically every major company in the market. This is a technology that can drastically reduce capital costs in our environment while also almost committing to low operating costs for the next three years while pursuing the finance. We'll talk about value in terms of cost and space, with space equating to future cost.

The security of big data is being studied, as well as how to keep the performance of the data while it is being transmitted over the network. There have been various studies that have looked into the topic of big data. Furthermore, many of those studies claimed to provide data security but failed to maintain performance. Several encryption techniques, including RSA and AES, have been utilized in past studies. However, if these encryption technologies are used, the network system's performance suffers. To address these concerns, the proposed approach employs compression mechanisms to minimize the file size before performing encryption. Furthermore, data is spit to increase the reliability of transmission. Data has been transferred from multiple routes after the data was separated.

If any hackers choose to collect that data in an unauthentic method, they will not be able to obtain complete and meaningful data. By combining compression and splitting mechanisms with big data encryption, the suggested model has improved the security of big data in a network environment. Furthermore, using a user-defined port and various pathways during the split transmission of large data improves the dependability and security of big data over the network projects in Chapter 11.

Acknowledgments

We express our great pleasure, sincere thanks, and gratitude to the people who significantly helped, contributed and supported to the completion of this book. Our sincere thanks to Fr. Benny Thomas, Professor, Department of Computer Science and Engineering, CHRIST (Deemed to be University), Bengaluru, Karnataka India, and Dr. Arup Kumar Pal, Assistant Professor, Department of Computer Science and Engineering, Indian Institute of Technology (Indian School of Mines) Dhanbad, Jharkhand India for their continuous support, advice and cordial guidance from the beginning to the completion of this book.

We would also like to express our honest appreciation to our colleagues at the Haldia Institute of Technology Haldia, West Bengal, India, and CHRIST (Deemed to be University), Bengaluru, Karnataka India, for their guidance and support.

We also thank all the authors who have contributed some chapters to this book. This book would not have been possible without their contribution.

We are also very thankful to the reviewers for reviewing the book chapters. This book would not have been possible without their continuous support and commitment towards completing the chapters' review on time.

To all of the team members at Scrivener Publishing, who extended their kind cooperation, timely response, expert comments, and guidance, we are very thankful to them.

Finally, we sincerely express our special and heartfelt respect, gratitude, and gratefulness to our family members and parents for their endless support and blessings.

Sabyasachi Pramanik
Department of Computer Science and Engineering, Haldia Institute of Technology, Haldia, West Bengal, India
sabyalnt@gmail.com
Debabrata Samanta
Department of Computer Science, CHRIST (Deemed to be University) Bengaluru, Karnataka
debabrata.samanta369@gmail.com
M. Vinay
Department of Computer Science, CHRIST (Deemed to be University), Bangalore, India
vinay.m@christuniversity.in
Abhijit Guha
First American India Private Limited, Bangalore, India
aguha@firstam.com