CYBER PHYSICAL SYSTEMS

SECURITY CONCERNS AND PRACTICES

Editors:
Ashish Kumar
Rohit Kumar Sachan

Bentham Books

Cyber Physical Systems: Security Concerns and Practices

Edited by

Ashish Kumar
School of Engineering and Technology
BML Munjal University
Gurugram, Haryana
India

&

Rohit Kumar Sachan
Department of Computer Science and Engineering (CSE)
Sharda School of Computing Science
and Engineering (SSCSE), Sharda University
Greater Noida, India

Cyber Physical Systems: Security Concerns and Practices

Editors: Ashish Kumar and Rohit Kumar Sachan

ISBN (Online): 979-8-89881-705-3

ISBN (Print): 979-8-89881-706-0

ISBN (Paperback): 979-8-89881-707-7

Published by Bentham Science Publishers Pte. Ltd. Singapore,

in collaboration with Eureka Conferences, USA.

First published in 2026.

need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.

3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Pte. Ltd.
No. 9 Raffles Place
Office No. 26-01
Singapore 048619
Singapore
Email: subscriptions@benthamscience.net

CONTENTS

PREFACE

The rapidly converging nature of computing and networking systems has led to significant advancements in terms of efficiency within cyberspace by improving human-machine interactions and transforming physical processes in order to increase the efficiency and performance of physical systems. The development of cyber-physical systems (CPS) has enabled the real-time evolution of physical systems by integrating diverse modern domains into a single intelligent CPS, with a primary focus on security architecture.

This book consolidates many emerging technologies (including blockchain, steganography, and cryptography) as they relate to the incorporation of security principles into CPS. Based on this analysis, the book provides readers with a solid grounding in the design of CPS security architecture and provides various examples of how to apply this understanding across industries, including healthcare, financial services, smart grid, and many other intelligent systems. The main goal of this book is to describe some of the problems, solutions, and advancements needed to improve the security of CPS at both the data and hardware levels. Additionally, the book addresses the need to design and deploy strong CPS designs to support trust and fairness among end consumers.

The book has been designed to provide the reader with an overview of both the theoretical and practical aspects of cybersecurity architecture in CPS. The book describes the theoretical foundation of CPS and provides examples of the techniques, trends, challenges, innovations, and advancements used to understand the background and innovations in CPS. The practical implementation of CPS in real-world case studies, which illustrate the continuing growth of CPSs in different application areas, is also elaborated. The development of the book is divided into major categories, each discussing a different aspect of CPS. Chapter 1, titled "*Cyber-Physical Systems: Intrusion Prevention Techniques and Trends,*" discusses techniques used to reduce the number of breaches within CPS by investigating intrusion detection and prevention mechanisms and their respective challenges (*i.e*., processing in real time and bridging the gap between physical and digital), as well as practical strategies for enhancing the resilience of CPS by implementing current technologies, such as blockchain and artificial intelligence. Chapter 2, titled "*Advances in Intrusion Detection for Cyber Physical Systems: Techniques and Innovations*," identifies and explains fundamental cybersecurity principles such as confidentiality, integrity, authorized access and the concept of identity, as well as provides in-depth discussion and research on the various types of intrusion detection systems available today, with examples of how they are the most advanced intrusion-detection systems developed to date to combat the threat of increased cyberattacks. Chapter 3, titled "*The Evolving Cyber Threat Landscape: Risks, Challenges, and Defense Strategies,*" provides a more in-depth examination of cybersecurity, particularly in the context of threats to the CPS. It explores new cyber-investigation techniques (forensics) to investigate crimes. Chapter 4, titled "*Data Security Challenges in Cyber-Physical Systems: An Analytical Approach*," emphasizes the need for adaptive, scalable security frameworks and compliance with privacy regulations like GDPR and HIPAA. The data security challenges in CPS highlight the integration of blockchain, machine learning, and quantum computing to prevent cyberattacks on these systems.

Chapter 5, titled "*Role of Cryptography in Cyber-Physical Systems,*" highlights the various tools available to secure information in CPS, such as symmetric and asymmetric encryption, different types of signing algorithms, hashing algorithms, lightweight cryptographic schemes, and homomorphic encryption. Chapter 6, titled "*A steganography model using the Randomized Salt LSB technique for cyber physical system*," compares various methods of

steganography and highlights issues regarding each method, including robustness, visibility, security, integrity, and capacity, while introducing a new way of using the LSB method combined with cryptographic techniques for efficient storage of data in cover images. Randomised salts are introduced to increase invisibility, error correction codes are used to ensure secure embedding, and cryptographic techniques, such as AES, are implemented to provide strong protection. Chapter 7, titled "*The Importance of Quantum Computing in Cyber-Physical Systems,*" describes future applications for quantum computing to transform CPS design, improve CPS, and provide a range of security challenges due to quantum mechanics. Chapter 8, titled "*A Systematic Analysis of Traditional vs*. Blockchain-based Integrity Verification for Cloud Data in Cyber Physical System," describes current methods of auditing outsourced cloud data, classifying the current operational methods, and developing the next generation of auditing systems. Chapter 9, titled "*Enhancing the Security Architecture of Cyber Physical Systems Using Blockchain*," reviews various blockchain-enabled cyber-physical systems, focusing on their real-time applicability and addressing limitations and challenges for future reliability and trust enhancement in these systems.

Advanced hybrid systems, such as smart grid CPS for home automation, should be reviewed for cybersecurity. Chapter 10 titled "*Cybersecurity Architecture for Home Area Network in Smart Grid Cyber-Physical System,*" discusses cyber threats like phishing attacks, ransomware, data breaches, and distributed denial-of-service for smart grid systems in home automation. This chapter proposes a cybersecurity architecture to secure home-area networks in the smart-grid CPS. Chapter 11, titled "*AI-Driven Solutions for Mitigating Security Hazards in Smart Grid CPS*," discusses the AI-powered smart grids for their efficient and reliable functioning by handling cyber-attack management to improve communication and IT infrastructure. Chapter 12, titled "*Cyber Physical System: Case Studies in Cyber Security,*" explores CPS's cybersecurity problems through real-world case studies and an analysis of cyberattacks. The need for cybersecurity, safety, and resilience is elaborated in essential industries to review the consequences of cyberattacks on CPS, addressing the complex and critical real-world problems.

This book inspires readers to understand the fundamentals, challenges, and opportunities of deploying cybersecurity in CPS. This work provides the foundation for CPS not only to improve quality but also to shape the future of CPS and essential industries.

Ashish Kumar
School of Engineering and Technology
BML Munjal University
Gurugram, Haryana
India

&

Rohit Kumar Sachan
Department of Computer Science and Engineering (CSE)
Sharda School of Computing Science and Engineering (SSCSE)
Sharda University, Greater Noida
India

List of Contributors

Abhay Shukla	Department of Computer Science and Engineering, Rama University, Kanpur, India
Anindya Ghatak	Department of Mathematics, SCSET, Bennett University, Greater Noida - 201310, India
Akshay Dheeraj	Indian Agricultural Statistics Research Institute, New Delhi, India
Amit Kumar Dwivedi	Department of CSE, Madan Mohan Malviya University of Technology, Gorakhpur, India
Ashish Kumar	School of Engineering and Technology, BML Munjal University, Gurugram, Haryana, India
Arush Sachdeva	Department of Computer Science, IIIT Hyderabad, Hyderabad, India
Anu Saini	Department of Computer Science and Engineering, GB Pant DSEU Campus, Delhi, India
Akash Mishra	Department of Cyber Security and Digital Forensics, Rashtriya Raksha University, Gujarat, India
Brijendra Pratap Singh	Department of Computer Science & Engineering, School of Computer Science Engineering & Technology, Bennett University, Greater Noida, India
Chetankumar Chudasama	Computer Engineering Department, Marwadi University, Rajkot, Gujarat, India
Chirag Bhalodia	Computer Engineering Department, Marwadi University, Rajkot, Gujarat, India
Deepak Kumar Verma	Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, India
Devansh Mehrotra	Department of Mathematics, SCSET, Bennett University, Greater Noida - 201310, India
Gaurav Pandey	Department of Applied Science, Rama University, Kanpur, India
Gopal Singh Rawat	SCSET, Bennett University, Greater Noida, India
Hansa Vaghela	Computer Engineering Department, Marwadi University, Rajkot, Gujarat, India
Himanshu Nandanwar	Department of Computer Science and Engineering, Delhi Technological University, Delhi, India
Ila Kaushik	Department of Computer Science and Engineering, Delhi Technological University, Delhi, India
Krupali Gosai	Computer Engineering Department, Marwadi University, Rajkot, Gujarat, India
Modassir Alam	Department of Electronics and Communication Engineering, Galgotias University, Greater Noida, India
Nikhil Sharma	Sharda School of Computing Science & Engineering, Sharda University, Greater Noida, Uttar Pradesh, India

Namita Tiwari	Department of Mathematics, CSJM University, Kanpur - 208001, India
Naveen Kumar	Department of Computer Science and Engineering, Sardar Vallabhbhai National Institute of Technology, Surat, India
Nandini Bansod	Department of Forensic Science, Shri Vaishnav Institute of Forensic Science, Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore, India
Rajnish Kumar Chaturvedi	Department of Computer Science & Engineering, School of Computer Science Engineering & Technology, Bennett University, Greater Noida, India
Rajesh Kumar Shrivastava	School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India
Rohit Kumar Sachan	Department of Computer Science & Engineering (CSE), Sharda School of Computing Science & Engineering (SSCSE), Sharda University, Greater Noida, India
Sukriti Goyal	Department of Computer Science and Engineering, Guru Gobind Singh Indraprastha University, Delhi, India
Santosh Kumar Srivastava	Department of Computer Science and Engineering, GL BAJAJ Institute of Technology and Management, Greater Noida, Uttar Pradesh, India
Satyam Omar	Centre for Artificial Intelligence, Madhav Institute of Technology & Science, Deemed University, Gwalior-474005, India
Sugata Adhya	Department of Mathematics, The Bhawanipur Education Society College, Kolkata, West Bengal, India
Sandeep Mishra	Digital.ai Software, Benguluru, India
Sunita Kumari	Department of Computer Science and Engineering, GB Pant DSEU Campus, Delhi, India
Usha Chauhan	Department of Electronics and Communication Engineering, Galgotias University, Greater Noida, India
Vishal Singh	School of Computer Science and Engineering, Bennett University, Greater Noida, India
Vandit Akhilesh Barola	SCSET, Bennett University, Greater Noida, India
Vikas Kumar Jain	School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India
Vimal Kumar	Department of Computer Science & Engineering, School of Computer Science Engineering & Technology, Bennett University, Greater Noida, India
Vijay Dwivedi	Department of Computer Science and Engineering, United College of Engineering & Research, Prayagraj, India

CHAPTER 1

Cyber-Physical Systems: Intrusion Prevention Techniques and Trends

Chetankumar Chudasama[1], Krupali Gosai[1], Hansa Vaghela[1], Chirag Bhalodia[1] and **Deepak Kumar Verma[1,*]**

[1] *Computer Engineering Department, Marwadi University, Rajkot, Gujarat, India*

Abstract: Cyber-physical systems (CPS) play an important role in critical infrastructures such as energy grids, healthcare, transportation, and industrial automation. They, however, cannot withstand advanced attacks because they operate on interconnected networks. In this chapter, a detailed analysis of CPS-specific intrusion detection and prevention methods is provided. It examines challenges such as real-time processing, the diversity of the system, and the integration of physical and digital spaces. The chapter presents realistic means of enhancing the resistance of CPS to malicious attacks by demonstrating the latest techniques, resources, and case studies. It also discusses the latest trends and technologies to be used in next-generation CPS as strong defense mechanisms against intrusion, including blockchain, to ensure secure communication and AI application in detection systems.

Keywords: AI-based intrusion detection, Cyber-Physical Systems (CPS), Intrusion prevention, Industrial automation cybersecurity, Intrusion detection, Next-generation CPS security.

INTRODUCTION

Because of rapid progress in constructive technologies, a notable increase is observed in the requirements placed on the physical environment. This also calls for the study of cyber-physical systems (CPS), which are advanced systems that combine computing, communication, and control. They are crucial components of the Industrial Internet of Things and Industry 4.0 [1].

They can perceive their surroundings and subsequently control the mechanical systems around them [2]. Activities are usually executed by a network of tiny devices with one or more sensing, computing, or communication capabilities.

[*] **Corresponding author Deepak Kumar Verma:** Computer Engineering Department, Marwadi University, Rajkot, Gujarat, India; E-mail: deepakkumar.verma@marwadieducation.edu.in

Ashish Kumar & Rohit Kumar Sachan (Eds.)

Such aspects have unique physical characteristics or information-sensing features and are interfaced with a cyber-system that transmits data to a computing unit [3].

CPS integrates computational algorithms with the physical world because the latter has actuators and sensors, which enable any physical task to be controlled by the feedback system of its co-existing counterpart. Using actuators and devices that can modify the system's state, this control system creates self-feedback, enabling the integration of efficiency and reliability. The idiom “smart things” is broad and can therefore include adjusting one's household temperature or controlling the movement of a self-driving car.

DEFINITION OF CPS

CPSs were initially recommended as a brand-new technology for bridging the cloud and the natural world in a computing application [4]. This description did not correctly represent the concept. Gill [5] from the National Science Foundation explains that cyber-physical systems are grammatically defined as “physical, biological, and engineering systems whose operations are integrated, monitored, and controlled by the computing core.” Materially, everything within a cyber-physical system is connected through the computing core. This consequently points to the obvious that the core is a distributed system that provides real-time responses. Modern CPSs can be understood as a combination of control, communication, and computing resources that are integrated to impact real-world ecosystems.

Importance of Cyber-physical Systems

CPS plays a significant role in explaining emergent systems and services using innovation as an independent system and subsystem and converting old systems into new systems that are more efficient in their operations. This merger has established the groundwork for knowledgeable and autonomous systems that do not require extensive human control. Perhaps, a paradigm shift, prompted by the introduction of CPS, which provides an excellent contribution in other spheres, includes:

Operational Excellence: It enhances energy efficiency, reduces costs, and improves resource management, among other benefits, by optimizing CPS processes through regular real-time adjustments. An example of this is consumption forecasts, which help forecast the quantity of electricity supplied by automated power distribution systems.

Improved Security: CPS can enhance security in health and the automotive industries by surveying environmental conditions and responding to emergencies much more quickly than a human can.

Availability: CPS is more extensively monitored in the system, and more predictive maintenance increases the reliability of an asset. This helps maintain assets rationally, preventing possible failures and their development.

Scalability: Small, compact, and customizable, the scalability of CPS is one of its strongest suits, making it suitable for many large and small, robust industrial infrastructures.

Examples of Cyber Physical Systems

Smart Grids: The smart grid is a classic example of a cyber-physical system in operation. It can be witnessed in power systems worldwide. However, the functioning of traditional power grids differs significantly, as they operate through an integrated generation and distribution system. Without smart grids, traditional systems were prone to sophisticated failures. Smart grids seem to have limitations as they adopt cyber-physical systems.

Autonomous Vehicles: An equally important area of interest in CPS is autonomous vehicles. When an autonomous vehicle travels, it uses a collection of devices, including LIDAR, radar, sensors, cameras, and GPS. Some algorithms help process data collected from these sensors to perform driving calculations at specific moments during navigation. Several actuators employ these calculations and steer the vehicle by accelerating or braking as needed.

Industrial Internet of Things (IIoT): The Integrated Industrial Internet is the most relevant example of a domain where cyber-physical systems rapidly evolve. The IIoT is the integration of computing devices, sensors, communication devices, and data analysis with different components of an industry. This integration helps increase productivity, maintenance measures, and performance in the industrial and manufacturing sectors.

Rising Cybersecurity Challenges in CPS

Why CPS is Vulnerable to Cyber Intrusions

CPS increasingly combines computational algorithms with physical systems in the modern world. Furthermore, these systems extend from intelligent grids to autonomous vehicles or industrial control systems. As a result, they tend to increase efficiency, safety, and reliability. Nevertheless, their interconnected

CHAPTER 2

Advances in Intrusion Detection for Cyber Physical Systems: Techniques and Innovations

Abhay Shukla[1,*] and **Gaurav Pandey**[2]

[1] *Department of Computer Science and Engineering, Rama University, Kanpur, India*

[2] *Department of Applied Science, Rama University, Kanpur, India*

Abstract: Cyberattacks have evolved into the latest form of weapon in Cyber Physical Systems. With artificial intelligence (AI) assisting malicious attackers, cybercrime is being made more sophisticated, and that is, for sure, very dangerous. This is a big challenge for our society, whether it is fraud in banks or AI-generated deepfake videos. As most individuals are now able to access their cyberworld through mobile devices, the need for the confidentiality, integrity, and authorized availability of their data sits at the top rung of the cybersecurity ladder. A cybersecurity failure casts doubt on its trustworthiness. This chapter presents the types of intrusion detection, which are generally divided into Signature-based Intrusion Detection Systems (SIDS) and Anomaly-based Intrusion Detection Systems (AIDS). In addition, it offers a taxonomy of modern IDS, an in-depth review of key new papers, and a selection of well-known datasets for analysis purposes. In this chapter, we present a comprehensive survey of IDS methods, types, and techniques, along with their pros and cons. This work compares different machine-learning-based approaches available in the literature for the detection of zero-day attacks, along with their drawbacks and benefits, such as the generation and update of information for new attacks, false alarms, and accuracy. This chapter consolidates the recent developments in the field and presents a detailed analysis of the contemporary landscape of IDS research. The synthesis thus provided sheds light on important ideas that can lead to more advanced intrusion-detection systems capable of responding to the ballooning variety of hazards that threaten cyberspace.

Keywords: Artificial intelligence, Anomaly-based intrusion detection systems (AIDS), Adaptive security scalable solutions, Cybersecurity machine learning zero-day attack detection, Cloud computing, Deep learning, Intrusion detection system (IDS), Internet of things, 5G networks.

[*] **Corresponding author Abhay Shukla:** Department of Computer Science and Engineering, Rama University, Kanpur, India; E-mail: abhayshukl@gmail.com

Ashish Kumar & Rohit Kumar Sachan (Eds.)

INTRODUCTION

With the evolution of cyberattacks, particularly with the recent creation of zero-day attacks that target previously unknown vulnerabilities, Intrusion Detection Systems [1] are becoming increasing important and necessary. The emergence of such threats, however, is too fast for traditional signature-based IDS, which leads researchers to consider more adaptive approaches like machine learning and anomaly-based detection techniques. Exploiting the power of these techniques can help discover new forms of attacks for previous campaigns and improve the general efficiency and situational awareness of detection systems. Given the growing complexity and sophistication of cyber threats, the need for resilient and agile Intrusion Detection Systems (IDSs) has emerged as a pressing priority. The latest advances in firefighting methods (FM) and real-time analytics of this kind represent a significant enhancement in performance for IDS. Data were collected during the study's exploration of basic concepts of Intrusion Detection Systems (IDS) and their categorization into network-based, host-based, and hybrid systems. Then, the investigation shifted to exploring various detection methodologies, such as signature-based, anomaly-based, and machine learning-based solutions. It focuses on novel advancements in machine learning and AI for the improvement of IDS skills and knowledge, especially from the perspective of zero-day attack [1] detection. In addition, the study highlighted various limitations of existing IDSs, such as problems with increased false positive rates and scalability, as well as issues with adapting to new and emerging threats. In addition, the paper addresses the suggested solutions and future research efforts to address these challenges, such as more advanced anomaly detection algorithms and the fusion of different types of data for more accurate results. This extensive research aims to provide a clear picture of the status of IDS research and to shed light on areas with future research potential. Based on synthesizing that data, this research seeks to offer an important knowledge base for scholars, cybersecurity specialists, and IT managers working to strengthen digital defense systems in increasingly complex threat landscapes. However, the progress made in machine learning and AI holds great potential to support and improve the functioning of IDSs, but they also pose new threats and exploit vulnerabilities. Over-reliance on complex algorithms and massive datasets may introduce new risks and privacy issues. Even more sophisticated attackers may be able to compromise or deceive such systems, making AI-based detection and prevention even more technologically backward. One of the major challenges indeveloping an effective intrusion detection system is the constant evolution of malicious software, also known as malware. Malware developers are using ever-more-complicated techniques to evade detection, like obfuscation and data-hiding tactics. The fundamental problem is with the detection of unknown and hidden malware. At the same time, the list of complex security threats, such as cyber-attacks that aim

at internet users *via* zero-day vulnerabilities, is endless. Computer security is increasingly important due to the dependence of organizations on information systems. By employing sophisticated attacks and advanced malware, the cybersecurity landscape faces a monumental challenge in the hands of malicious actors. The fast pace of this threat landscape necessitates continuous advancement in cyber defense strategies and intrusion detection systems to protect against emerging threats and ensure the seamless operation and credibility of businesses reliant on technology.

Countries have been significantly affected by zero-day attacks. The Symantec Internet-Security Threat Report for the year 2017 discusses in detail how the number of zero-day attacks surpassed three billion in 2016, with a significant increase in volume and severity compared to previous years [2]. Data Breach-According to 2017 reports, since 2013, hackers have been able to breach around nine billion data records. Diving into the cybercrime ecosystem, there is a significant evolution of malicious actors pivoting some of their attack surface insights away from banking customers and instead aiming for financial institutions themselves, seeking to distrupt various operations [3]. As a result, this realignment has increased the need to detect zero-day attacks in the cybersecurity space. Fig. (**1**) shows the zero-attack process, which is a well-defined series of steps.

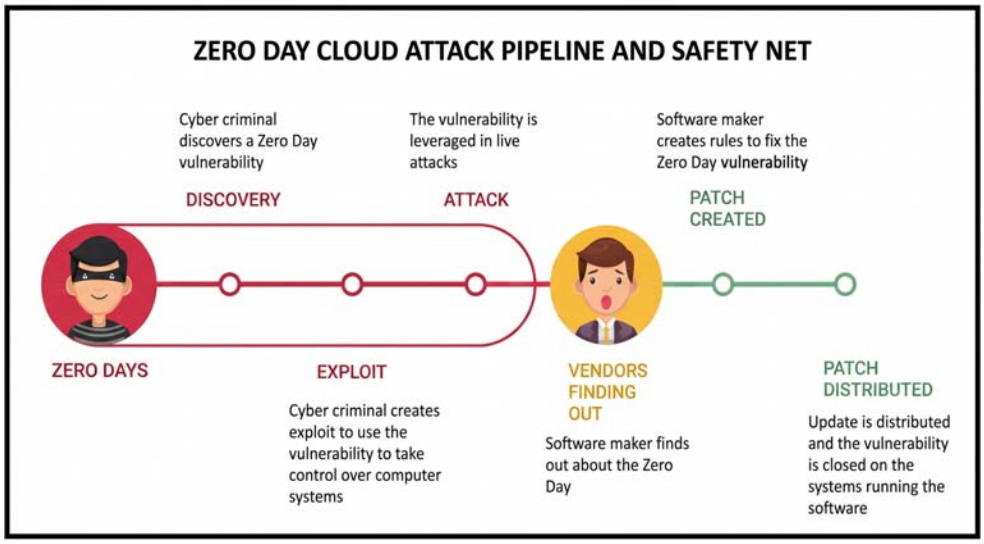

Fig. (1). Zero-day Attack process.

Major cyber compromises have shown the global reach and destructive power of digital malware, illustrating the need for strong defensive measures. Malicious

CHAPTER 3

The Evolving Cyber Threat Landscape: Risks, Challenges, and Defense Strategies

Nikhil Sharma[1], Sukriti Goyal[2], Ila Kaushik[3], Deepak Kumar Verma[4,*], Santosh Kumar Srivastava[5] and **Himanshu Nandanwar[6]**

[1] Sharda School of Computing Science & Engineering, Sharda University, Greater Noida, Uttar Pradesh, India

[2] Department of Computer Science and Engineering, Guru Gobind Singh Indraprastha University, Delhi, India

[3] Department of Computer Science and Engineering, Delhi Technological University, Delhi, India

[4] Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, India

[5] Department of Computer Science and Engineering, GL BAJAJ Institute of Technology and Management, Greater Noida, Uttar Pradesh, India

[6] Department of Computer Science and Engineering, Delhi Technological University, Delhi, India

Abstract: Today, all humans stay and work in a participatory cyber-world. The Internet connects computer systems to share data. As the cyber world permeates almost all fields of everyday work, it is becoming increasingly necessary that people understand its technological and political underpinnings, activities, capabilities, risks, and problems. Over the past few years, society has become hostile to system-related perpetrations that either directly or insidiously cause damage to people or industries, termed "cybercrime." Cybercrime can be committed from any location, and the consequences are indefinite. It is not bound to any particular area. It can occur across any field, including government, education, finance, and healthcare. This chapter focuses on cybercriminals' activities, *i.e.*, how they execute cybercrimes, how investigators investigate cybercrimes, and how to prevent cybercrimes worldwide. It is observed that conventional approaches to crime investigation do not work as well in cybercrimes. Thus, to avoid such perpetrations, some modern methods are required, such as cyber forensics and biometrics. However, we also need a solution to secure the cyberworld from cybercrime, which requires understanding the plausible cyber risks and challenges, as dealing with cybercrime is very tough. In this chapter, cybersecurity is presented in detail, including the risks and challenges in modern society, to avoid the occurrence of cyberattacks.

Keywords: Biometrics, Cyber crime, Cyber forensics, Cyberattacks, Security.

[*] **Corresponding author Deepak Kumar Verma:** Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, India; E-mail: deepak.verma1980@gmail.com

INTRODUCTION

Cybercrime is a criminal act committed through computer systems and the Internet. Anything from downloading illegitimate files to stealing billions of dollars from online bank accounts is included in cybercrime [1]. It also comprises non-monetary delinquencies, like designing and disseminating viruses on other systems or illegally sharing private business data online. The most significant form of cybercrime is identity theft, in which criminals use Internet services to steal confidential data from other consumers [2]. "Pharming" and "Phishing" are the two most common ways to do this. Both of these processes attract users towards the illegitimate websites that seem to be legitimate, where they are asked to provide confidential details, which include login information such as username, password, e-mail ID, contact number(s), address, credit card details, bank details and many other details and then, using all of this information, the criminal steals that user's identity [3]. That is why checking a site's web address (URL) is essential to ensure it is legitimate before providing personal details. Cybercrime is divided into three classes by the United States Department of Justice. Crimes in which the computer system is used as an auxiliary to a crime fall under the first class of cybercrime. Using a computer to save illegitimately obtained information is an example of this class. Crimes in which the computing gadget is the goal fall under the second-class category. For example, the goal is to gain network access. Crimes in which the computer system is used as a tool to establish a DoS, *i.e.*, Denial-of-Service Attack, fall under the third-class category of cybercrime [4]. The growth and development of the cyberworld have led to a series of phenomena that have structured the society in which people live. All humans have seen the growth of information technology firms, which have generated millions or billions of jobs worldwide, directly or indirectly [5]. With the evolution of computer systems, society has also been hostile to the emergence of cyber perpetrations. Examinations require professional services with expertise in computer systems and law enforcement protocols [6].

CLASSIFICATION OF CYBER CRIMES

Cybercrimes are broadly categorized into four classes. A crime against an individual falls under category one: cybercriminals committing a crime against a person. Cybercrimes against individuals [7] result in cyber disputation, which occurs when notoriety is achieved through the use of computer systems and the Internet. Another example is email spoofing, which refers to an email whose header is crafted to appear to be generated by one source, but is actually transmitted from another [8]. Cyber stalking and persecution also fall under this category of cybercrimes, where cyber stalking means following the actions or activities of an individual over the Internet. It can be implemented using many

protocols, such as user net groups, email, and chat rooms. Spamming is the transmission of unwanted or mass emails for commercial or non-commercial advertising purposes [9]. Crimes against property fall under the second category, which includes intellectual property crimes (*e.g.*, trademark, copyright, and patent), online threats, and computer system hacking [10]. For example, it includes Internet Time Theft, which means using Internet hours by an unknown or unauthorized person by stealing the password. In reality, it is the person who paid for the services.

Another example is credit card fraud, which implies using a credit card to gain money or commit fraud. Perpetrators may steal a credit card, replicate that card number, or take over a victim's account and mail the credit card to their location. Sometimes, they may open a new credit card in the victim's name or attempt other strategies to steal money or buy goods. The third example includes intellectual property crimes, which include stealing computer source code, copyright infringement, software piracy, and trademark infringement. The third category falls under crimes against the organization, where the crimes are committed to intimidate national or international governments or any organization using Internet services [11]. Cybercrimes are committed to instill fear among humans, and cyber-terrorism is defined as crimes against a government, including cyberattacks on government websites or military data, *etc.* [12].

One of the crimes is a virus attack: a computer virus program that can contaminate other programs on the computer, too, by changing them so that a replica of itself is created. Viruses can also affect the files and the boot sector of a computer. Trojan Horse is an authorized program that works from within and appears to be an authorized program, thereby hiding what it is actually doing. Data misguiding is a type of crime that includes modifying raw information just before a system implements it, and then modifying it after implementation. Unauthorized access to a computer is the unauthorized use of a network or computer system that can be accessed without the owner's permission in two ways: modification or deletion of data, or the criminal reading or replicating private and valuable data that is neither removed nor changed. The fourth category is crimes against society, where cybercrimes that influence the interests of society to a considerable extent are considered crimes against society [13], which comprises different types of attacks such as Web Jacking; in this case, hackers obtain access and command over the website of another person or an organization and can modify the concernments of the website either for achieving a political aim or for obtaining cash [14]. Forgery involves revenue stamps, mark sheets, currency notes, *etc.*, which can be produced using computer systems, high-quality scanners, and printers. Cyberterrorism is when criminals use computer resources to spread terror among people.

CHAPTER 4

Data Security Challenges in Cyber-Physical Systems: An Analytical Approach

Usha Chauhan[1,*], Modassir Alam[1], Vishal Singh[2] and **S.P.S. Chauhan[3]**

[1] *Department of Electronics and Communication Engineering, Galgotias University, Greater Noida, India*

[2] *School of Computer Science and Engineering, Bennett University, Greater Noida, India*

[3] *School of Computer Science and Engineering, GNIOT Group of Institution, Greater Noida, India*

Abstract: Cyber Physical Systems have linked processes in physical systems to various computing processes that have reached numerous sectors, including healthcare, energy, transportation, and manufacturing. It can be described as a highly connected system in which physical processes can be monitored and controlled through real-time data. Considering that such processes are in a very critical state given that operations have been entrusted to Cyber Physical Systems, the heavy reliance that organizations have shown on these systems exposes CPS to numerous security flaws. These flaws may lead to various data breaches, which may also result in loss of life or economic disaster. With that, this paper will discuss some of the major data security challenges that have been associated with Cyber Physical Systems. The paper will discuss some of these challenges, such as data integrity and confidentiality, the real-time accessible nature of data, and reliability. The paper will also discuss examples of how various technologies like blockchain technology, machine learning, and quantum computing have been linked to tackling security challenges. Technologies like machine learning and quantum computing that have shown great potential to transform the field like this or even in a completely different way may be linked to fields like encryptive communication. This research work is mainly focused on providing insight into developing adaptive and scalable security frameworks that could counter changing cyber attacks by examining current and potential security concerns while emphasizing a critical need to ensure a CPS system remains compliant with privacy-related legislations, namely GDPR and HIPAA, referred to as data protection laws related to individuals' personal data. The paper, in general, puts forward a need to adopt the "whole and multi-disciplinary approach" to security in a CPS system through innovative and evolving technologies and governance techniques.

Keywords: Attacks, Blockchain, Cyber physical systems, Cybersecurity, Security.

[*] **Corresponding author Usha Chauhan:** Department of Electronics and Communication Engineering, Galgotias University, Greater Noida, India; E-mail: usha.chauhan@galgotiasuniversity.edu.in

Ashish Kumar & Rohit Kumar Sachan (Eds.)

INTRODUCTION

The 'Cyber-Physical Systems' or 'CPS' has been included as part of critical infrastructure operation due to its connection to a computational system. The 'CPS' system has, in fact, introduced significant change to healthcare, transportation, and manufacturing in a fashion that ensures complete efficiency in these arenas [1, 2]. Considering this, it is essential to realize that 'CPS' presents security threats to critical infrastructure, as it operates in conjunction with physical devices to respond to physical conditions, hence introducing security threats to critical infrastructure once it is incorporated into a digital system. The security risks posed by 'CPS' can disrupt the system in various ways, ranging from data breaches to physical device destruction, as well as the destruction of living organisms [3, 4]. The need to understand various 'CPS' security challenges, like those from numerous security threats, necessitates knowledge of various 'CPS' threats to critical infrastructure.The various CPS security challenges to critical infrastructure, along with potential solutions and recent discoveries, include approaches such as machine learning and blockchain technology [5, 6].

Key Contributions

- Analysis of the security challenges facing CPS, including issues related to real-time data processing, data integrity, and confidentiality.
- Identifying vulnerabilities within different areas of application of CPS, such as self-driving cars, smart grid technology, or the field of healthcare.
- Recommendations for the development of a layered, adaptive, and scalable architecture of CPS.

Organization of the Chapter

The structure of this chapter:

- **Introduction**: Introduction to the topic of CPS, security challenges, and the need for securing critical infrastructures.
- **Cyber-Physical Systems Overview**: CPS definition, their significance, and an in-depth discussion on their security needs.
- **Key Security Issues**: Explanation of key security issues particular to CPSs involving hard real-time requirements, data integrity, and physical layer security.
- **Current Security Technologies**: An overview of existing security technologies, including intrusion detection and prevention systems, secure communications technologies, and authentication technologies.
- **Innovations in CPS Security**: Information on the innovations present within

the field of CPS security development. This can include innovations like blockchain technology.

- **Standards and Regulatory Frameworks**: Overview of some standards and frameworks that play a vital role in establishing security requirements for CPS, such as GDPR, HIPAA, and the NIST Cybersecurity Framework.
- **Case Studies**: Real-world examples of vulnerabilities in CPS systems include recent exploits such as Stuxnet and the BlackEnergy attacks in Ukraine.
- **Ethical Aspects**: Discussion on the ethical aspects associated with the security of CPS in terms of privacy, accountability, and AI.
- **Future Trends**: Research on trends in the security of Computer Programs Systems in the future, including zero trust architecture and autonomous security.
- **Conclusion**: Findings of the research, recommendations on future directions of CPS security research.

CYBER-PHYSICAL SYSTEMS OVERVIEW

What are Cyber-Physical Systems?

As mentioned earlier, CPSs are very tightly integrated systems. They integrate computational elements with physical processes. They use sensors, actuators, and data available in real time to monitor or control physical systems. CPS includes autonomous vehicles, smart grids, industrial systems, and healthcare systems like pacemakers [7 - 9]. As shown in Fig. (**1**), in the case of CPS, integration occurs between its cyber and physical parts *via* a cloud interface.

The most dominant feature of CPS is its interaction with physical systems using data in its decision-making process. For driverless cars, sensors and actuators (like cameras and radars) collect data and identify risks using that data. Similarly, using real-world conditions of demand and supply in a grid, a smart grid optimizes using CPs optimistically for electricity generation and supply [10, 11].

The systems are used in environments where there is a need for timely decision-making for safety and efficiency reasons. As CPSs move further into the general environment, the importance of protecting them from cyberattacks supersedes all other concerns exponentially [12].

CPS integrates various cyber, physical, and cyber-physical elements within an architecture with a central gateway. This shows the complexity of CPS. The architecture is represented in Fig. (**2**).

CHAPTER 5

Role of Cryptography in Cyber-Physical Systems

Satyam Omar[1,*], Anindya Ghatak[2], Namita Tiwari[3] and **Devansh Mehrotra[2]**

[1] *Centre for Artificial Intelligence, Madhav Institute of Technology & Science, Deemed University, Gwalior - 474005, India*

[2] *Department of Mathematics, SCSET, Bennett University, Greater Noida - 201310, India*

[3] *Department of Mathematics, CSJM University, Kanpur - 208001, India*

Abstract: Cyber-physical systems (CPS) are becoming significant for industrial activities and progressive infrastructure. The information security of these systems heavily depends on cryptographic techniques. These systems are susceptible to cyberattacks because of various communication and physical components. Cryptography minimizes these attacks by safeguarding data transfer through authentication, integrity, and confidentiality. Symmetric and asymmetric encryption, signing algorithms, hashing, lightweight cryptographic schemes, and homomorphic encryption are some important tools that provide a secure and efficient infrastructure for a variety of CPSs like energy, healthcare, industrial, and transportation systems. Creating strong, effective, and scalable cryptographic frameworks will be essential as CPS utilization grows in order to safeguard these systems from changing dangers and guarantee their security, dependability, and credibility.

Keywords: Authentication, Cyber-physical systems, Cryptography, Data confidentiality, Data integrity.

INTRODUCTION

In the period of technological advancement, Cyber-Physical Systems (CPS) have become an important component of modern infrastructure across sectors, like transportation, healthcare, energy, and manufacturing. By synthesizing the computing capacity and connectedness of real-world physical processes, CPSs enable previously considered science-fiction advancements. CPS security is not merely a technical problem; it must ensure the resilience, safety, and dependability of key processes.

Cryptography is a fundamental component of CPS security, enabling the safeguarding of private data, verifying devices, and providing secure communi-

* **Corresponding author Satyam Omar:** Centre for Artificial Intelligence, Madhav Institute of Technology & Science, Deemed University, Gwalior - 474005, India; E-mail: satyamomar840@gmail.com

Ashish Kumar & Rohit Kumar Sachan (Eds.)

cation [1]. Cryptography essentially turns information into an unintelligible format that cannot be converted back to the original form without

the right keys, protecting data from unwanted access. This competence is essential for CPS because of the high stakes involved in their work. For example, a security breach that controls electric grids in the CPS may cause calamitous outages; on the other hand, an attack on autonomous cars could imperil lives.

Cryptographic functions address the security goals required for the secure functioning of CPS [2]. Control commands and sensor readings that contain important information are protected by preserving confidentiality. Data integrity ensures that any changes to data transferred between two components are not introduced. Due to authentication, only legitimate devices and people can access the data. Lastly, non-repudiation is also a security service provided by digital signatures, ensuring the signer's accountability.

Although cryptography is an important tool for the security of CPS, its implementation is not quite simple. Due to CPS's storage and computational limitations, we have to face many significant difficulties. Despite their secure foundation, conventional cryptographic algorithms like RSA and ECDSA [3] often have long processing times and require significant resources, which are incompatible with CPS's operating features. For instance, limited-resource devices like sensors and actuators might not be able to handle the computational expenses of public-key cryptography (PKC). This is why lightweight cryptographic algorithms are drawing the attention of researchers due to the optimized security and efficiency of the system.

Cryptography in CPS [4] plays an important role in the security of communication networks. Interconnected components are responsible for frequently transmitting data *via* wired or wireless channels using CPS. So, these channels need interception and alteration resistance. Along with this, CPS also uses modern cryptographic tools like homomorphic encryption, which allows the computation of encrypted data without decrypting it. For zero-knowledge-based identification and authentication, a zero-knowledge proof helps the prover identify himself to the verifier. These state-of-the-art techniques are still developing and must be further optimized before they can be used in CPS.

For providing security to CPS, cryptography alone is not sufficient. For the best outcomes, the integration of cryptography with the correct hardware implementation can do the job for us. Furthermore, due to advances in cryptanalysis of the existing schemes and the increasing power of computer architecture, it is important to update the security infrastructure of CPS continuously. Ethical considerations and government regulations are also essential

to embed in the CPSs deployed in defence and healthcare systems, where privacy plays a more important role than other technical advancements. The functionality and advantages of CPS must be enabled while maintaining user privacy by implementing cryptographic solutions.

The preliminaries and basic cryptographic tools that are deployed in securing the CPS's infrastructure are discussed in the following section. Then, we discuss various CPSs and the significance of cryptographic techniques in them. Finally, we conclude the article in the last section.

CRYPTOGRAPHIC TECHNIQUES

There are several cryptographic techniques that are practical for protecting CPS. These methods are CPS-friendly, such as storage-constrained, distributed architecture, and real-time data transmission. The cryptographic tools used in CPS are as follows [3]:

- **Symmetric Key Cryptography:** This cryptographic technique involves only one key in the infrastructure. This single key is used for encrypting raw messages and decrypting intelligible messages. Similarly, this key is used to sign a message to construct the signature and verify it. The security of these types of systems depends on the secrecy of the key. If the key is compromised, the system's security is also compromised. These systems are much faster than the public-key systems described below.

Standard symmetric encryption algorithms include:

- **AES (Advanced Encryption Standard):** Sensitive information is frequently encrypted using this highly effective and safe technique, which has key lengths of 128, 192, or 256 bits. It was established as a security standard by NIST in 2001. There are four phases in AES functioning that make it secure: SubBytes, ShiftRows, MixColumns, and AddRoundKey. SubBytes phase uses a substitution operation, which is a non-linear step. ShiftRows shifts the rows of the state matrix cyclically while keeping the first row fixed. Due to this step, each ciphertext bit depends on various plaintext bits. MixColumn is a transformation that transforms each column of a state matrix using some operation over a finite field. AddRoundKey is the last step of each round, where a key is XORed with the state.
- **DES (Data Encryption Standard):** Due to its susceptibility to brute-force assaults, this outdated standard with a 56-bit key is now considered insecure. It was established by NIST in 1977 as a security standard. It has four steps: initial permutation, round key generation, Feistel rounds, and inverse initial permutation. There are 16 Feistel rounds, consisting of expansion, key mixing,

CHAPTER 6

A Steganography Model Using the Randomized Salt LSB Technique for Cyber Physical Systems

Rajnish Kumar Chaturvedi[1,*], Brijendra Pratap Singh[1], Gopal Singh Rawat[1], Vandit Akhilesh Barola[1] and **Akshay Dheeraj[2]**

[1] *Department of Computer Science & Engineering, School of Computer Science Engineering & Technology, Bennett University, Greater Noida, India*

[2] *Indian Agricultural Statistics Research Institute, New Delhi, India*

Abstract: In today's world, with the advancement of technology, there is always a possibility of sensitive information being exposed during communication. Privacy is the most essential property of any communication, specifically where computation, network, and physical processes are tied together. To address this issue, one of the most popular security methods, steganography, has been used for many years. This chapter discusses and compares various methods of steganography. The study analyzes various existing steganography methods and identifies issues like robustness, visibility of information, security, integrity, and capacity. The state-of-the-art steganography tries to overcome these issues, but still, there is scope to improve them. To address these issues, this chapter proposes a security model to increase the robustness of the steganography methods with high capacity and low detectability. Here, we propose a novel steganography method based on the LSB method. The proposed work integrates existing cryptographic techniques to efficiently store data in the cover image. It includes randomized salts to increase invisibility and error-correction code (ECC) blocks with proper padding to prevent the loss of data during transmission. Embedding information is made secure by introducing ECC and strong cryptographic techniques like AES. The employed data-embedding procedures are efficient and do not distort images because optimal pattern sizes are determined and appropriate pixels are chosen for modification. We also consider the LSB modification and padding processes in such a way that data capacity is maximized while relatively keeping the quality and the fidelity of the image intact. Thus, the proposed steganography model produces a lossless result in cyber physical systems.

Keywords: Cover-image, Cyber-physical system, LSB, Randomization, Steganography, Steganalysis.

[*] **Corresponding author Rajnish Kumar Chaturvedi:** Department of Computer Science & Engineering, School of Computer Science Engineering & Technology, Bennett University, Greater Noida, India;
E-mail: chaturvedi040@gmail.com

INTRODUCTION

In the evolving era of advanced technology, where communications over the internet are becoming too obvious, there is an exponential growth in cyberattacks, specifically around network sniffing. With the technology moving towards integrating physical and computational processes, leading towards controlled physical systems in real-time, Cyber-Physical Systems (CPS) have drawn a lot of attention from industry and academia. CPS has major applications such as transmitting information securely between medical devices and sharing highly sensitive information between government bodies and business parties, where the problem of data sniffing over the internet poses significant issues [1]. Some of the major areas where the necessity of securing data is a must are mainly the healthcare sector, military-based agencies, and the overall internet servers where the whole world is connected [2]. According to the IBM 2023 report [3], the average cost of data breach in the year 2023 was around 4.45 million USD, with an increase rate of 2.3% from the previous year. Besides all these, there has been an enormous rise in data security breaches in the healthcare sector, up 53.3% since 2020, which has cost around 10.93 million USD.

These cases are drawn from some of the most common data security issues, such as data masking, unauthorized access, and advanced persistent threat attacks, most specifically in the healthcare sector [4]. Out of all the challenges, ransomware attacks and the escalating potential to crack encryption techniques are the most problematic. To enhance security, various techniques have been used, such as encryption, authentication, and access control. Steganography is one such technique that aids in enhancing security. Steganography is the practice of concealing a secret message behind a normal message, image, or other medium. The word “steganography” comes from the Greek words “steganos,” meaning “covered” or “hidden,” and “graphia,” meaning “writing.” Put these words together, and you have got something close to “hidden writing” or “secret writing.” This ancient practice has been used for thousands of years to keep communications private [5]. Steganography is the process used to hide text, audio, video, images, *etc*. By this, we can represent information within another cover file, in such a manner that the presence of the information is not noticeable to the human eye.

The purpose of steganography is to keep secrets and deceive. Steganography is a form of data hiding and can be executed in different ways. The techniques use a cover image, a secret message, a stego image, and a stego key. Image steganography embedding can be categorized into spatial and transform-domain embedding. Techniques such as discrete wavelet transform (DWT), continuous wavelet transform (CWT), and discrete cosine transform (DCT) are classified as

transform-domain embedding. Whereas, multiple-based national systems (MBNS), pixel value differencing (PVD), exploiting modification directions (EMD), and least significant bits (LSB) are classified under spatial transform embedding.

The Least Significant Bit (LSB) technique, which is easy to understand, simple to implement, and has the largest embedding capacity, is a popular data-hiding algorithm. LSB requires minimal modification of the carrier file, making it computationally efficient for embedding and extracting the hidden message. When implemented carefully, altering only the least significant bits often results in minimal changes to the carrier file, especially for media with a high number of bits per pixel. LSB can be applied to various digital media formats, including images, audio, and video. This versatility makes it a suitable choice for the proposed model. It provides an additional layer of security by hiding information within digital media [6]. It is often used in conjunction with encryption, providing a double-layered security approach for data protection.

With the advancement of quantum computing, it has high potential to crack the most advanced encryption techniques, on which 90% of the world's data is encrypted and protected [7]. Steganography makes it tough to locate hidden facts, particularly when techniques are well implemented. This helps in stopping unauthorized access to sensitive records. Employing steganography helps in enhancing security, mainly when covert conversation and high-security measures are required [8 - 10]. Researchers have proposed various steganography-based solutions. However, existing state-of-the-art schemes have issues such as invisibility, capacity, complexity, robustness, detectability, and size alteration. There are many methods within the domain of LSB techniques, but as the technology advances, the reverse algorithm for decoding them becomes easier.

In this context, to develop a more robust steganography technique for the CPS, we propose a new steganography model with complex decoding, which makes it difficult to detect the existence of hidden data in the cover file. Ensuring data security is crucial for CPS-based applications as they rely on sensor data for real-time decision-making. This work reviews and analyses existing methods and integrates them to form a robust algorithm, which makes it harder to decode. The proposed algorithm alters the LSB bit of the pixels; thus, negligible changes to the cover file are observed. Here, the secret data is stored by changing the corresponding LSB bit of the RGB pixels in a distorted way. Our proposed model can hide large amounts of data within digital media of CPS, enabling secure storage and transmission of confidential information without altering the size of the cover image.

CHAPTER 7

The Importance of Quantum Computing in Cyber-Physical Systems

Anindya Ghatak[1,*], **Satyam Omar**[2] and **Sugata Adhya**[3]

[1] *Department of Mathematics, SCSET, Bennett University, Greater Noida - 201310, India*

[2] *Centre for Artificial Intelligence, Madhav Institute of Technology & Science, Deemed University, Gwalior-474005, India*

[3] *Department of Mathematics, The Bhawanipur Education Society College, Kolkata, West Bengal, India*

Abstract: Using the ideas of quantum mechanics, Quantum computing transfers information in completely new ways. It sets out to develop many fields of science and technology, including Cyber-Physical Systems (CPS). Using computer algorithms, CPS helps to solve real-world physical systems. Hence, it plays a prominent role in areas like self-driving cars, automated factories, healthcare, smart energy networks, and robotics. While traditional computing has been used to design CPS, the rise of quantum computing is poised to enable new capabilities. In particular, it solves difficult problems more quickly and, hence, offers better security. In this survey, we discuss how quantum computing can be utilized in CPS, focusing on its possible applications, future impacts on system design, improvements, security, and challenges.

Keywords: Cyber-physical systems, Quantum cryptography, Superposition.

INTRODUCTION

Cyber-Physical Systems, also known as CPS, are embedded in computing and communication systems to create intelligent, autonomous systems. These integrated systems can interact through sensors and actuators. On the other hand, computational components make decisions, process data, and organize actions based on real-time inputs. Based on quantum mechanics, Quantum computing has the ability to enhance the capabilities of CPS by solving problems that are extremely difficult in classical systems. Moreover, quantum computers can execute multiple solutions in parallel. Therefore, quantum computation significantly speeds up the computation for certain problems. In addition to that,

[*] **Corresponding author Anindya Ghatak:** Department of Mathematics, SCSET, Bennett University, Greater Noida - 201310, India; E-mail: anindya.ghatak@bennett.edu.in

Ashish Kumar & Rohit Kumar Sachan (Eds.)

quantum entanglement enables qubits to share correlations that classical bits cannot achieve. This unique property provides a foundation for tackling complex tasks in areas such as cryptography, optimization, and simulation.

In the following, we explore the potential role of quantum computing in CPS, focusing on its applications, particularly in optimization, real-time data processing, machine learning, and cybersecurity. We also examine how quantum algorithms can increase system efficiency and security.

Overview of Quantum Computing

Quantum computing is different from classical computing. It processes data through quantum bits (qubits). Qubits may be present in superpositions or entanglement of states [1].

Basic Concepts of Quantum Computing

a) ***Qubits:*** Qubits are expressed in terms of classical bits $|0\rangle$ and $|1\rangle$ as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

Where a complex number α and β satisfy $|\alpha|^2 + |\beta|^2 = 1$.

Here α and β are amplitudes of the corresponding states. The above single equation provides the probabilities of $|\psi\rangle$ in one of the states $|0\rangle$ or $|1\rangle$. After measurement, we obtain the probabilities $|\alpha|^2$ and $|\beta|^2$ of the states, $|0\rangle$ or $|1\rangle$, respectively.

b) ***Superposition and Measurement:*** In quantum mechanics, superposition is a key concept. For example, the qubit.

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Exists in a superposition of $|0\rangle$ and $|1\rangle$.

This feature enables quantum computers to examine different possibilities. As a result, superposition dramatically increases computational efficiency.

c) ***Entanglement:*** Directly related qubits are said to be entangled. For example, consider the following entangled state:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

For entangled qubits, the state of one cannot be described in isolation and without the help of others. This correlation between entangled qubits is a key feature of quantum computing.

Gates and Operations in Quantum Computing

In quantum computing, qubits are manipulated using quantum gates. Quantum gates are unitary operations. Hence, under the action of quantum gates, preserve the norm of the quantum state. These quantum gate operations are represented by matrices.

a) ***Pauli Gates:*** The simplest and basic quantum gates are Pauli gates, namely Pauli-X, Y, and Z gates. The Pauli-X gate is also called a quantum NOT gate. It flips the state of a qubit:

$$X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle.$$

The Pauli-Z gate flips a phase of the qubit:

$$Z|0\rangle = |0\rangle, \quad Z|1\rangle = -|1\rangle.$$

The Pauli-Y gate is a combination of the Pauli-X and Pauli-Z gates and introduces both bit and phase flips.

b) ***Hadamard Gate:*** Hadamard gate, a widely used quantum gate, is often used to create superpositions of the $|0\rangle$ and $|1\rangle$ states. It transforms $|0\rangle$ and $|1\rangle$ as follows:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

c) ***CNOT Gate:*** The Controlled-NOT (CNOT) is defined by:

$$\text{CNOT}|a, b\rangle = |a, a \oplus b\rangle.$$

The CNOT gate is essential in creating entangled states.

Quantum Algorithms

Below, we discuss the most famous quantum algorithm [1,2,3,4].

a) ***Shor's Algorithm:*** It provides an algorithm that factors large integers exponentially faster classical computer. It uses widely used cryptographic protocols, such as RSA [2].

CHAPTER 8

A Systematic Analysis of Traditional *vs.* Blockchain-based Integrity Verification for Cloud Data in Cyber-Physical Systems

Amit Kumar Dwivedi[1,*], **Rajesh Kumar Shrivastava**[2] and **Vikas Kumar Jain**[2]

[1] *Department of CSE, Madan Mohan Malviya University of Technology, Gorakhpur, India*

[2] *School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India*

Abstract: In a digital era, Cyber-Physical Systems (CPSs) integrate real-world objects with digital devices and data storage. Processing this ubiquitous data requires data outsourcing to third-party utilities such as the cloud. Data outsourcing is an efficient and viable approach for data owners to successfully manage their data online. It improves the system's capacity to manage larger workloads and boosts data accessibility. The data owner will continue to have concerns about the privacy and security of cloud data due to the involvement of an untrusted third party. Therefore, the data owner must accord utmost importance to the auditing of outsourced data integrity as an essential requirement. This chapter provides a thorough analysis of the current auditing techniques used for outsourced data, delving into them in detail. It provides a general classification of currently operational auditing systems to facilitate comprehension of the literature and encourage scholars in this field to refine their concepts for greater precision. Moreover, it provides a prospective future direction in the domain.

Keywords: Cyber physical systems, Data flow, Deterministic system, Probabilistic system, Storage auditor.

INTRODUCTION

Cyber-physical systems (CPS) are a design approach that offers numerous advantages to the economy and society because they combine ubiquitous data and modern technology. Stated differently, in CPS, the cyber components, including communication networks and computer devices, are connected to the physical process or system [1]. Because of how closely these components are connected, one component's functionality depends on the other. In domains like Industrial

* **Corresponding author Amit Kumar Dwivedi:** Department of CSE, Madan Mohan Malviya University of Technology, Gorakhpur, India; E-mail: akd1981@gmail.com

Ashish Kumar & Rohit Kumar Sachan (Eds.)

Internet of Things (IIoT), health, IoT, and agriculture, CPS has grown rapidly in recent years. Stability, reliability, robustness, security, and privacy are important research areas when creating intelligent, effective, and adaptable systems.

Business needs force companies to outsource data and other IT resources to the cloud. Cloud reduces costs, supports maintenance, provides computational resources, and increases the availability of IT resources. But security and privacy are still areas for work with third-party cloud vendors. Data outsourcing is profitable in many contexts. We can define some quality measures of data outsourcing.

- **Improved Outcome:** Better reachability and availability help to grow the business. Availability and power of computation improve the quality of the outcome. In digital processing, better resources improve turnaround time, which in turn improves outcomes.
- **Availability:** Cloud services remove client communication barriers and ensure 24X7 data availability. It establishes trust in business.
- **Transparency:** Since data is available in the cloud and all the participants and stakeholders can access data, it will provide transparency among all. It also increases trust [2].

Fig. (**1**) shows the working model of CPS. In this model, users store business data in cloud storage, which helps an organization process input and ensure the availability of input data for end users. But a major question arises here about data integrity and privacy.

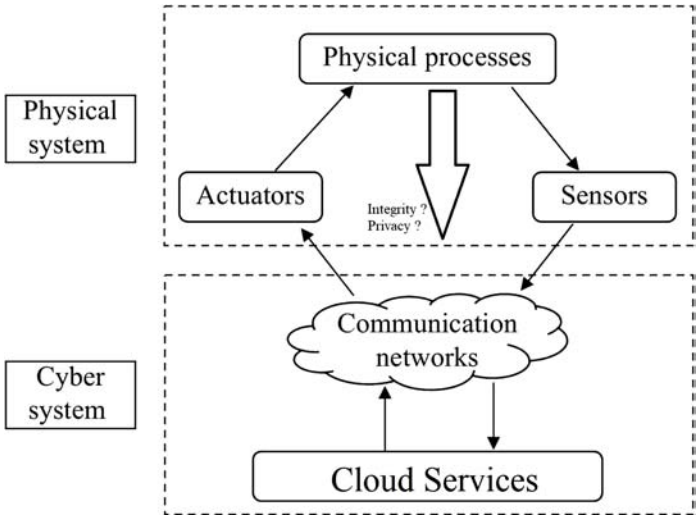

Fig. (1). Cyber-physical system.

ICT firms typically handle substantial volumes of data. They generate, analyze, and execute various actions (such as insertion, deletion, and updating) on the data. These organizations have ownership of the data they possess.

The ICT organization's data consumers may access data remotely from the cloud. The users also require timely access to data. Hence, the company must ensure the provision of sufficient data storage and data accessibility to its users. Costly infrastructure for storage and personnel to administer the infrastructure are prerequisites for the local storage and management of data.

Outsourcing with data is a cost-effective method for data owners to maintain their data. A Cloud Service Provider (CSP) is a business that offers storage-as-a-service to the data owner. When outsourcing, the data owner is expected to only pay for the resources used, following a" Pay as you go" model, to the CSP. As the CSP offers storage-as-a-service to different ICT enterprises, it has the potential to grant unauthorized users access to the outsourced data. The CSP has the potential to collude with a rival organization and manipulate or delete an organization's data for financial gain. Additionally, it can remove infrequently viewed data from certain organizations to optimize storage efficiency.

Given that outsourced data is a valuable resource, prioritizing its security is of utmost importance. Furthermore, a CSP that is not trusted cannot guarantee the security of the data that has been outsourced. Hence, the data proprietor must securely retain their data to ensure that only approved users designated by the data proprietor can access the data (*i.e*., data secrecy), and that only authorized people can make changes to the data that has been outsourced (*i.e*., data integrity).

Confidentiality of data can be attained by employing symmetric key encryption. Before delegating the responsibility of data encryption to the CSP, the data owner employs symmetric key encryption. The encryption/decryption key is stored in local storage. The CSP is unable to decipher and comprehend the contents without the decryption key. However, the CSP may permit illegal alterations to the encrypted data that has been outsourced. Hence, the data owner requires a way to identify any illegal alterations made to the encrypted outsourced data, thereby ensuring data integrity is maintained.

Auditing [3 - 7] is a post hoc method for verifying the integrity of outsourced data. It happens periodically. The frequency of the audit may depend on the importance of the outsourced data; *i.e*., more important data means a more frequent audit cycle. Only the data owner or any trusted third-party (TPA) under the supervision of the data owner can audit the outsourced data. Who will be the auditor of the outsourced data? It depends on the data outsourcing scenario. For example, if only the data owner and CSP are in the scenario, then outsourced data

CHAPTER 9

Enhancing the Security Architecture of Cyber-Physical Systems Using Blockchain

Ashish Kumar[1,*] and **Rohit Kumar Sachan**[2]

[1] *School of Engineering and Technology, BML Munjal University, Gurugram, Haryana, India*

[2] *Department of Computer Science & Engineering (CSE), Sharda School of Computing Science & Engineering (SSCSE), Sharda University, Greater Noida, India*

Abstract: Blockchain is an emerging technology that ensures the development of highly secure and reliable systems for industrial development. To build trust and fairness in recent advancements, cyber-physical systems have adopted blockchain technology to monitor and control the involved physical devices and equipment. Blockchain technology is based on a decentralized framework that integrates distributed ledger technology and consensus mechanisms for validating and securing user data and the sharing of information. Blockchain can enable diverse applications to secure data sharing and management for authenticating and improving the user experience. In this chapter, we have reviewed and elaborated on the various blockchain-enabled cyber-physical systems to improve their applicability in real-time. In addition, the limitations and challenges of deploying blockchain technology in cyber-physical systems are reviewed to determine future directions for improving reliability and trust in these systems.

Keywords: Blockchain, Cyber-physical systems, Distributed ledger, Healthcare, Intelligent transportation, Reliability, Smart contract, Security.

INTRODUCTION

With the development and growth of the industrial revolution, the security of cyber-physical systems (CPSs) has become really important [1, 2]. CPSs require continuous and frequent data exchange, storage, and access to serve the various requests. CPSs have a wide range of applications, such as augmented reality, automated data transmission, and reliable hardware systems that generate large amounts of processing data with the aid of security, accuracy, and low latency [3, 4]. To ensure seamless, faster, and secure communication, distributed systems are more efficient and popular in comparison to centralized ones. Distributed systems are generally based on service-based interactions in which there are a few service

[*] **Corresponding author Ashish Kumar:** School of Engineering and Technology, BML Munjal University, Gurugram, Haryana, India; E-mail: ashish.gupta14d@gmail.com

nodes that provide facilities to other nodes in the network [5, 6]. Blockchain technology (BT) has a range of applications to serve such kinds of applications with enhanced security [7, 8].

Earlier, BT emerged as a cryptocurrency bitcoin but now has a lot of applications to transform society by overcoming the limitations of the existing systems [9]. BT stores and processes data in a chain of blocks to ensure secure, distributed, efficient, and flexible transmission. BT has addressed the limitations of the centralized system and provides support for fault tolerance, checking balances, and maintaining records [10]. It supports distributed decision-making and can provide a highly secure environment for processing secure transactions. BT uses a distributed ledger to record, verify, and confirm transactions [3]. This mechanism adopts a consensus protocol or smart contract (SC) that acts as an agreement between the various users in blockchain applications for validating the blocks in the chain.

SC is a self-executing script or algorithm stored in a block that validates, confirms, and executes a transaction between various users [5]. SC is written in a specific programming language that every member of the blockchain network must agree upon before communication begins. All the necessary conditions are recorded in the SC, eliminating the requirement for executing any separate contracts or agreements. Once the conditions are accepted, the SC can automatically conclude the various activities without needing to request permission each time [11]. This not only introduces transparency in the network but also ensures faster communication.

Initially, BT technology was designed for securing financial transactions only. However, its importance is also realized for securing several applications such as healthcare [12, 13], industrial development [1, 10, 14], and academia [15, 16]. Apart from this, BT has potential applications in various domains that involve human activity to effectively use its benefits. CPS can exploit the advantages of BT for designing specific systems for a certain application, along with the optimal selection of hardware and software [17]. CPS is a combination of various computations containing physical processes that gather data from the environment, process it, and generate output back to the physical environment. CPS involves systems that require high reliability, accuracy, and security to manage critical data [18, 19]. CPS has a wide range of applications in the medical domain: life support systems; academia: record management; industry: grids, communication systems, water resources, and many more. Hence, BT technology can be both helpful and innovative in ensuring the reliable transmission of information across the cited applications of CPS. The major contribution of the work is as follows:

- To summarize the details and benefits of various types of blockchain to understand the potential of the BT.
- To analyze various CPS applications and review their security and accuracy using blockchain for highly reliable development
- To identify the salient features, challenges, and limitations of deploying BT in designing CPS systems.

The rest of the chapter is organized as follows. The details of BT, its types, and the benefits for managing various decentralized CPS systems are elaborated. The applications of various CPSs are reviewed and discussed. The limitations and challenges for BT in developing secure and reliable CPS are also discussed. Lastly, the chapter's concluding remarks and future directions are discussed.

BLOCKCHAIN TECHNOLOGY

The blockchain revolution started in 2008 when an anonymous article was published and discussed Bitcoin as a Peer-to-Peer electronic cash system [20]. It was the first article that discussed the cryptocurrency Bitcoin. BT was adopted as a technology for managing and issuing Bitcoin currency. After this, BT has emerged as one of the key techniques for securing a wide range of applications by providing suitable solutions. Blockchain consists of a chain of information blocks connected with each other, containing various transaction records. The first block in the row is known as the genesis block, whereas the rest of the blocks are known as the parent block [21]. Each block of the blockchain is composed of a block header and a block body. Block headers consist of block version, Merkle tree root hash (MTRH), timestamp, nBits, nonce, and parent block hash [22]. The block version represents block validation rules. MTRH consists of the hash value of all transactions, the timestamp represents the current time, and nBits sets a target threshold. Nonce is a 4-byte field increase with every hash, and the parent block hash contains the hash value of the previous block.

Types of Blockchain

BT ensures end-to-end secure transmission and sharing of information. BT authorizes the members of the blockchain to exchange information among themselves. Based on the permission model, BT can be categorized as permissionless, permissioned, and both [23]. Fig. (**1**) depicts the various types of BT. Permissionless BT is a public type of blockchain in which all users can participate. Any user can join or leave the network without any permission at any time. All users can read or write to the ledger without any authorization from any centralized controller. The task is distributed, reducing the risks of a single authority. These BT hold a multiparty consensus mechanism to publish, record, and monitor resources for maintaining the blocks of the blockchain. Generally,

CHAPTER 10

Cybersecurity Architecture for Home Area Network in Smart Grid Cyber-Physical System

Brijendra Pratap Singh[1,*], Vimal Kumar[1], Rajnish Kumar Chaturvedi[1], Sandeep Mishra[2], Vijay Dwivedi[3] and **Naveen Kumar[4]**

[1] *Department of Computer Science & Engineering, School of Computer Science Engineering & Technology, Bennett University, Greater Noida, India*

[2] *Digital.ai Software, Benguluru, India*

[3] *Department of Computer Science and Engineering, United College of Engineering & Research, Prayagraj, India*

[4] *Department of Computer Science and Engineering, Sardar Vallabhbhai National Institute of Technology, Surat, India*

Abstract: Smart grid is a critical energy infrastructure that includes advanced power electronics devices, Internet of Things devices, communication infrastructure (advanced metering infrastructure), software application program, and demand response program (enables an active consumer who takes active decisions on consumption based on dynamic pricing and incentives). Cyber-physical energy systems provide active participation in load and power supply management. End consumers use devices controlled *via* the internet. These devices are enabled with artificial intelligence. Advances in the smart grid also open the door to cyberattacks. Cyber threats are a major concern for the smart grid. Cyber threats are actions intended to jeopardize the availability, confidentiality, or integrity of systems. They can come from a variety of sources, including nation-state actors, hacktivists, insider threats, and cybercriminals. Phishing attacks, ransomware, data breaches, and distributed denial-of-service (DDoS) attacks are common cyber threats that exploit flaws in systems or human behavior. It also employs advanced strategies such as social engineering and artificial intelligence. This book chapter describes past cyberattacks on the smart grid. This book chapter proposes a cybersecurity architecture to secure a home area network in a smart grid cyber-physical system.

Keywords: Cyber security, Cyber-physical system, Home area network, Malware attack, Neighborhood area network, Smart meter, Smart grid.

[*] **Corresponding author Brijendra Pratap Singh:** Department of Computer Science & Engineering, School of Computer Science Engineering & Technology, Bennett University, Greater Noida, India;
E-mail: brijendra.singh@bennett.edu.in

Ashish Kumar & Rohit Kumar Sachan (Eds.)

INTRODUCTION

A smart grid is a critical infrastructure. A hacker infiltrated the U.S. power grid [1]. A cyberattack incident was reported on the Ukrainian grid in 2015 and 2016 [1]. Cyber threats can be from rival countries, terrorists, and criminal gangs.

Physical threat can be from a geomagnetic solar flare, which generates an electromagnetic pulse, or a short-range missile explosion in the atmosphere by a terrorist [2]. Smart grid is a critical cyber-physical infrastructure that provides a backbone energy infrastructure to industries, railways, hospitals, universities, schools, commercial hubs, and households. Smart grid has components namely, (i) energy generation units (such as coal power plants, nuclear power plants, hydro power plant, wind power plant, solar power plant, *etc*.), (ii) transmission system, (iii) distribution system, (iv) active consumers (through demand response program, dynamic pricing), (v) communication system (such as, home area network, neighborhood area network, wide area network, advanced metering infrastructure), (vi) distributed energy storage, (vii) microgrid. Real-time data transfer provides utilities with benefits such as real-time pricing, outage monitoring, power theft detection, data integrity protection, and improved service. Utility companies will have a better chance of operating more steadily and effectively if the data is received on time [3]. Advanced metering infrastructure eliminates the task of manual meter reading. At the electricity utility center, a data management system stores, processes, and analyzes data collected from smart meters [4 - 5].

Energy Generation

Energy is one of the major requirements of 21st-century human society. Electric energy is used in transportation (*e.g.*, railways, electric vehicles), industry, and households. Electrical energy generation is done by various means such as nuclear power plant (electrical energy is produced by using nuclear fission), coal power plant (electrical energy is produced by fired coal), hydro power plant (electrical energy is produced by building dam and water reservoir), wind power plant (by using wind turbine), and solar power plant (by solar radiation).

Transmission System

Usually, electrical energy is generated far from its point of use. There are reasons such as the availability of raw materials (coal, water, land) and safety. Therefore, the electrical energy is generated in bulk and transmitted to places where it is used. Electrical energy is transmitted at a very high voltage using a step-up transformer. At the point of distribution, electrical energy is converted at low voltage by the step-down transformer.

Distribution System

A distribution system consists of the electrical station from which electrical energy is distributed to the point of use, such as households, industries, and commercial activity points.

Demand Response Program

Demand response program is a policy/software program that provides a way to involve consumers as active consumers. Active consumers can respond to dynamic pricing [6]. According to the price, a consumer can reduce or increase their electricity consumption. Dynamic pricing is a tool to control the peak demand. To meet the demand at peak load time, an electrical infrastructure requires huge investments. The problem is that most of the time the demand is not too high for which the electrical infrastructure is built.

Communication System

Modernization of electrical infrastructure includes advanced devices such as Phasor Measurement Unit (PMU), smart meter, and smart appliances (controlled through a smartphone *via* the Internet). Home area network, neighboring area network, and wide area network are components of the smart grid.

Distributed Energy Storage

Advances in storage technology paved the way for the storage of energy. Energy is stored in periods of low consumption, and the saved energy is used in the period of peak load. In the era of solar power, the energy is stored and used at night. An electric vehicle uses storage.

Microgrid

A microgrid is a small-sized grid (of capacity 100 kilowatt to some megawatts). It consists of loads and distributed energy resources (solar, wind, gas turbine, small-scale hydropower, *etc*.). A microgrid operates either in isolated mode or grid-connected mode. The microgrid acts as an independent entity [7]. An instance of a microgrid is depicted in Fig. (**1**).

A smart grid is made up of communication technology, adjustable loads, and distributed energy supplies that are all connected. Microcontrollers, network protocols, and intelligent power electronic devices connect the distributed energy resources and controllable loads. Fig. (**2**) shows an example of a smart grid system, complete with renewable energy sources, network routers, energy manag-

CHAPTER 11

AI-Driven Solutions for Mitigating Security Hazards in Smart Grid Cyber Physical System

Arush Sachdeva[1], **Sunita Kumari**[2] and **Anu Saini**[2,*]

[1] *Department of Computer Science, IIIT Hyderabad, Hyderabad, India*

[2] *Department of Computer Science and Engineering, GB Pant DSEU Campus, Delhi, India*

Abstract: AI-enabled smart grids combine the existing power grid infrastructure of electric utilities with artificial intelligence technologies to provide higher levels of energy delivery, efficiency, dependability, and sustainability, enhancing power management and mobility in grids and microgrids with artificial intelligence and data. AI-based smart grids enable efficient energy distribution, enhanced grid reliability, easier energy consumption, and greater cost-effectiveness. Energy demand prediction using algorithms is improving the existing power distribution network. ML algorithms handle large datasets from installed sensors, smart meters, and weather data. It helps electricity providers balance the supply and demand. At one level, the smart grid can identify and act on cyberattacks, equipment failures, and power quality issues, increasing reliability and reducing outages. With the ability to process vast amounts of data and analyze it in real time, artificial intelligence makes this feasible. AI helps us use renewable energy more efficiently. It observes how electricity flows between the generation and the grid and *vice versa*. Therefore, the grid's carbon footprint gets reduced. Energy management systems enable customers to participate in demand-side programs by shifting their consumption in response to real-time prices and grid conditions. An artificial intelligence system combines weather forecasts and power flow data to predict grid failures and improve the reliability of the smart grid.

Keywords: Artificial intelligence (AI), AI-based security solutions, Cyber-physical systems (CPS), Cybersecurity, Distributed energy resources (DER), Data integrity, Risk mitigation, Security hazards, Smart grid, Threat detection.

INTRODUCTION

A smart grid refers to an electrical grid that uses information and communication technology, along with other advanced technologies, to monitor and manage the transport of electricity from all generation sources to meet the varying electricity demands of end-users. It makes power generation and distribution more efficient,

* **Corresponding author Anu Saini:** Department of Computer Science and Engineering, GB Pant DSEU Campus, Delhi, India; E-mail: anuanu16@gmail.com

Ashish Kumar & Rohit Kumar Sachan (Eds.)

dependable, reliable, and sustainable [1]. The use of smart grids is crucial for tackling greenhouse gas (GHG) emissions, reducing CO_2, and integrating renewable energy sources. Smart grids are an enhancement of traditional grids to more dynamic and reliable systems. They are more dependable and flexible. It will be difficult to meet the growing demand for energy and the increasing use of distributed energy resources, particularly renewable energy sources such as solar and wind. Innovation in technology, both present and future, is necessary to overcome these obstacles [2, 3].

In the field of Smart Grid Cyber-Physical Systems (CPS), artificial intelligence (AI) has completely changed how electrical power networks function. Sustainability, dependability, and efficiency have all increased. To improve distributed energy resource management and more efficiently use electricity, smart grids rely on real-time communication and metering systems. On the other hand, the grid's physical infrastructure, which connects to digital systems, is prone to multiple glitches. Because of the fragile security configuration, the electrical grid is susceptible to both physical and cyberattacks that could cause disruptions and information leaks. As a result, ensuring the security and resilience of smart grid CPS has proven to be a significant challenge.

As they are solely reliant on communication protocols and IT systems, they are becoming susceptible to cyberattacks. Attackers can exploit such flaws to alter data, disrupt power transfers, or access control systems. As these infrastructures increasingly rely on AI/ML, there is a new threat of adversarial attacks and data poisoning that can further make the electricity sector vulnerable. AI-based solutions can effectively tackle security threats. AI can identify mistakes, anticipate threats, and automatically make decisions to stop security incidents using algorithms, machine learning, and real-time analytics [6]. AI can also power a smart grid infrastructure, improving its systems to identify intrusive responses and develop new tactics [7]. This makes it possible to identify weaknesses and strengthen defenses against cyber-physical attacks.

The security risks related to smart grid Cyber-Physical Systems (CPS) are examined in this chapter in relation to AI. It takes into account a number of techniques, such as Multi-Agent Systems (MAS), Machine Learning (ML), and Deep Learning (DL). The chapter examines ways to strengthen smart grids' security framework. Additionally, it examines current research and relevant case studies to support the idea that AI can enhance the security and resilience of critical infrastructure (CI) [8].

Background

Cities getting smarter is one thing, but making them more sustainable is another thing altogether. Surely, it has an innovative appearance and vibe, and it is a sustainable city of tomorrow. Nonetheless, this is quite a complex system. A new governance model must unite all the key players, including individuals, enterprises, and local communities. We must further investigate to clarify its perimeter better. Most global cities are leveraging digital apps to increase intelligence. ICTs should be used to enhance the lives of city dwellers. But these technologies are simply tools that help make living in a city easier, cheaper, and cleaner. The primary challenge is to make the city more sustainable and liveable while also highlighting the need for community participation.

Energy Management in Sustainable Cities

As per the report, 4.6 million people or 58% of the world's population will make urban areas their homes by 2025. The percentage is likely to reach 80% in the rich countries. It is also predicted that by 2050, 75% of the world's population will live in cities. Moreover, they will also be densely populated. Over the last few years development of cities has become very fast. Consequently, they face issues such as energy access, overpopulation, climate change, and environmental degradation. Cities consume around 65% of the energy in the world.

A true frenzy of energy consumption has begun, especially in lighting, tempering, and transportation [7, 6]. It is necessary to fight these issues to fight climate change and air pollution. Future cities must be properly organized and structured to address these issues.

Evolution of Power Distribution Grids

The growing need to meet our power consumption is changing consumption and manufacturing methods. Intelligent appliances, the rise of electric cars, and the great integration of distributed energy resources into the medium-voltage power networks help to explain this change. Because of their challenging power profile and weather instability, which create power balancing problems, renewable energy generation, including solar and wind, has another motivating rationale behind these developments. The dependability and stability of the electrical system are strongly influenced by all these challenges [9].

According to Fig. (**1**), the power grid topology is compared to a smart grid. The usual grid uses a centralized generation (coal/nuclear plants) and one-way generation, while the smart grid integrates renewable energy sources, smart meters, demand response systems, and two way communication network with the

CHAPTER 12

Cyber-Physical Systems: Case Studies in Cybersecurity

Akash Mishra[1,*] and **Nandini Bansod**[2]

[1] *Department of Cyber Security and Digital Forensics, Rashtriya Raksha University, Gujarat, India*

[2] *Department of Forensic Science, Shri Vaishnav Institute of Forensic Science, Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore, India*

Abstract: The relationship between both the computing system(s) and the physical system(s) is defined through Cyber-Physical Systems (CPS); CPS establishes an interface between what computers can do digitally and what they can do based on physical laws. CPS are crucial components of every business, regardless of whether it is in the commercial, defense, or any other market sector; CPS include healthcare, military, transportation, manufacturing, and other sectors. The number and complexity of connections between CPS continue to grow, thereby increasing the number of cyber-threats that can impact the digital aspect(s) of CPS as well as their physical components (*e.g.*, facilities, factories). This chapter will examine numerous examples of actual CPS cyberattacks and analyze how these attacks created cyber risk, thereby compromising or disrupting the security of both digital and physical systems that comprise CPS.

Keywords: Attack vectors, Cyber-physical systems, Cybersecurity, Protection mechanisms, Resilience, Security standards, Vulnerabilities.

INTRODUCTION

Cyber-Physical Systems (CPS) integrate physical and computational processes through sensors, actuators, embedded devices, and communication networks. Actuators use real-time sensor data to control devices, other equipment, and embedded systems that process it [1]. An autonomous car is a good example of a CPS, in which sensors collect information about the surrounding environment (such as traffic conditions or obstacles) that onboard computers can process to inform navigation and control decisions. Likewise, CPS is used to monitor and control electricity flow using real-time data from smart grid systems that manage distribution. Such use cases include industrial control systems in manufacturing,

[*] **Corresponding author Akash Mishra:** Department of Cyber Security and Digital Forensics, Rashtriya Raksha University, Gujarat, India; E-mail: akash.dfis@gmail.com

Ashish Kumar & Rohit Kumar Sachan (Eds.)

medical devices for patient monitoring, and robots on automated manufacturing lines [2, 3].

Real-time interaction with the physical world greatly increases automation and efficiency and is enabled by cyber-physical systems. Still, their widespread use in sectors such as manufacturing, transportation, energy, and cybersecurity is increasingly critical to the health of critical infrastructure. With the rise of connected devices, CPS relies heavily on a network that, when connected, increases the risk of cyber-attacks by creating opportunities for the theft of sensitive data and causing disruption to the physical components of that industry (CPS). In other words, maintaining the integrity of CPS is only possible if a robust cybersecurity strategy supports CPS. Due to CPS's vulnerability to cyber threats that could disrupt service delivery, cause financial damage to the organization, and/or harm the public, protecting critical infrastructure has become an increasingly urgent priority. Throughout history, there have been countless incidents across critical infrastructure sectors, including energy, water treatment, healthcare, and transportation. The following are examples of some of the largest cyber incidents that affected critical infrastructure industries Table **1** [7].

Table 1. Important cybersecurity incidents impacting critical infrastructure between 2003 and 2024.

Year	Incident Type	Threat Nature	Targeted Entity	Affected Region
2003	Malware	Slammer Worm	Ohio Nuclear Power Plant Network	United States of America
2005	Accident	Sensor Failure	Taum Sauk Hydroelectric Power Station	United States of America
2007	Worm	Stuxnet	Iranian Nuclear Facilities	Iran
2008	Software	Installed Software Update	Georgia Nuclear Power Plant Shutdown	United States of America
2011	Unauthorized Access	Backdoor	Springfield Pumping Station	United States of America
2012	Disruptive	DDoS	Iranian Infrastructure (Nuclear and Oil)	Iran
2015	DDoS	BlackEnergy Malware	Ukrainian Power Grid	Ukraine
2016	Malware	Shamoon-2	Saudi Government Computers	Saudi Arabia
2017	Ransomware	Petya	Ukrainian Electricity Firm	Ukraine
2020	Malware	Triton/Trisis	Saudi Aramco's Oil Facilities	Saudi Arabia
2021	Ransomware	DarkSide Ransomware	Colonial Pipeline	United States of America
2021	Malware	SolarWinds (SUNBURST)	US Federal Agencies and Private Sector	United States of America (global)

(Table 1) cont.....

Year	Incident Type	Threat Nature	Targeted Entity	Affected Region
2022	Ransomware	Conti Ransomware	Costa Rican Government and National Institutions	Costa Rica
2023	DDoS & Ransomware	Akira Ransomware & DDoS attacks	European Energy Sector	European Union (Germany, Italy, France)
2024	Malware	Various APT Attacks	Critical Infrastructure in the US, EU, and Asia	Global

The Evolution of Cybersecurity in Cyber-Physical Systems

Cybersecurity is an ever-increasing challenge as the number of risks grows with the increased complexity and connectivity of Cyber-Physical Systems (CPS). Cybersecurity will continue to evolve with these CPS, as concerns shift from protecting standalone products from malware or deleting user credentials to protecting entire product networks that are vulnerable to attack. Furthermore, threats will originate not only from within the cyber realm but also from physical threats outside it. Integrating the physical components of a CPS with its associated digital control functions presents a unique set of issues for cybersecurity practitioners, as CPS may pose threats related to the provision of electric power, safety, bodily harm, and physical damage to components or systems, thereby harming end-users. Cybersecurity professionals will find themselves confronted with increasing difficulties caused by Eva, which powerful attackers may exploit to cause physical damage by disrupting Cybersecurity's ability to keep a CPS effective. Cybersecurity must protect not only the digital aspects of your CPS but also its physical aspects. Cybersecurity must employ effective methods to detect, analyze, and mitigate cyber threats while simultaneously providing security against physical-world threats [6]. Fig. (**1**) provides a graphical representation of the size and scope of the cybersecurity market for CPS in terms of cybersecurity services [7].

CYBERSECURITY CHALLENGES IN CYBER-PHYSICAL SYSTEMS (CPS)

Cyber-physical systems (CPS) pose a distinct set of cybersecurity challenges due to the integration of physical systems with digital devices. These challenges exist across several areas, including prototype design, security issues, cyber-physical system evolution, and the Internet of Things [8], as well as in all aspects where Cyber-Physical Systems interface with each other. Some examples of serious problems that could impact cyber-physical systems are shown in the following image.

SUBJECT INDEX

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

Ashish Kumar

Dr. Ashish Kumar, Ph.D., is currently working as an Associate Professor at BML Munjal University, Gurugram, Haryana, India. He worked at Bennett University, Uttar Pradesh, and Bharati Vidyapeeth's College of Engineering (affiliated with GGS Indraprastha University), New Delhi, from August 2009 to March 2026. He completed his Ph.D. in Computer Science and Engineering from Delhi Technological University (formerly DCE), New Delhi, India, in 2020. He received the Best Researcher Award from Delhi Technological University for his contribution to the computer vision domain. He completed his M.Tech. with distinction in Computer Science and Engineering from GGS Indraprastha University, New Delhi. He has published more than 45 research papers in various reputed national and international journals and conferences. He has published 15+ book chapters in various Scopus-indexed books. He has authored/edited several books in the AI, computer vision, and healthcare domains. He is an active member of various international societies and clubs. He is a reviewer for many reputed journals and serves on the technical program committees of various national and international conferences. Dr. Kumar has also served as a session chair at many international and national conferences. His current research interests include object tracking, image processing, artificial intelligence, and medical imaging analysis. He is actively associated with professional organizations as a Senior Member of IEEE and a lifetime member of ISTE.

Rohit Kumar Sachan

Dr. Rohit Kumar Sachan is currently serving as an Associate Professor at the Sharda School of Computing Science & Engineering, Sharda University, Greater Noida, where he is actively engaged in both teaching and research. Prior to joining Sharda University, he worked as an Assistant Professor at Bennett University, Greater Noida. Before that, he held research positions at the Indian Institute of Technology (IIT) Kanpur, where he served as a Senior Project Engineer and later as a Post-Doctoral Fellow at the C3i Hub, IIT Kanpur. He earned his Ph.D. from the Motilal Nehru National Institute of Technology (MNNIT), Allahabad, which further strengthened his foundation in advanced areas of computer science and engineering. With approximately ten years of combined academic and research experience, Dr. Sachan has developed strong expertise in several cutting-edge domains. His primary research interests include Cyber Security, Blockchain Forensics, Machine Learning Applications, and Nature-Inspired Algorithms. Dr. Sachan is an active member of several leading professional organizations, including the Institute of Electrical and Electronics Engineers (IEEE) and the Association for Computing Machinery (ACM).