10

Emerging Security and Privacy Schemes for Cyber-physical Systems

Abidemi Emmanuel Adeniyi[1], Rasheed Gbenga Jimoh[2], Joseph Bamidele Awotunde[2], Peace Busola Falola[3], Oluwatobi Blessing Olorunfemi[4] and Agbotiname Lucky Imoize[5]

[1]Department of Computer Science, Bowen University, Nigeria
[2]Department of Computer Science, University of Ilorin, Nigeria
[3]Computer Science Unit, Distance Learning Center, University of Ibadan, Nigeria
[4]Department of Computer Science, Redeemer's University, Nigeria
[5]Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Nigeria

Email: abidemi.adeniyi@bowen.edu.ng; jimoh_rasheed@unilorin.edu.ng; awotunde.jb@bowen.edu.ng; peacefalola@gmail.com; olorunfemib@run.edu.ng; aimoize@unilag.edu.ng

Abstract

The challenges and possibilities in security and privacy are unique due to the rapidly evolving cyber-physical systems (CPS) landscape. Their increasing integration into essential infrastructures like healthcare, transportation, and energy has made it imperative for them to be secure and their data to remain private. This chapter discusses how both CPS digital and physical elements relate, considering sophisticated cyberattacks with physical consequences. Specifically, this chapter analyzes the vulnerabilities resulting from the merger of evermore complex systems with extensive connectivity and cyber-attack sophistication and its impact on privacy in a data-centric world. The chapter underlines the importance of improving security solutions in cyber-space to protect against both present and future attacks. This also touches on advanced technological alternatives, including encryption algorithms for

secure data transformation, machine learning models for threat forecasting and unusual activity detection, and strong user authentication systems that allow only genuine people to get into important machines. Moreover, it highlights how vital privacy-preserving technologies like differential privacy and federated learning are because they enable one to harness all advantages associated with enormous datasets without compromising anybody's confidentiality. This chapter proposes a research agenda that would focus on developing adaptable, integrated security frameworks that are reactive and proactive in identifying and neutralizing threats before they strike. It consists of an ongoing cycle of research, implementation, and refinement of security measures complemented by continuous monitoring of an improving threat landscape so that CPS can remain safe and dependable as the backbone of modern civilization.

10.1 Introduction

Cyber-physical systems (CPS) blend physical and computational operations, integrating them to create a complicated interplay between the digital and physical realms. This has made it vital for industries like healthcare, transportation, or industrial automation to employ strong security measures as these systems grow significantly across various fields. In the last 10 years, linking embedded systems, communications, and controls has formed the centerpiece of research in cyber-physical systems (CPS) to solve problems that arise when merging the cyber and physical worlds [1],[2]. Embedded computers are today common in various sectors such as aerospace, automotive industry, chemical production, civil infrastructure, energy, health care, and others because they have become cheaper and have improved processing power.

Attacks against cyber-physical systems (CPS) can have catastrophic consequences for humans and the environment due to their vital significance in our daily lives. To better comprehend safety-critical cyber-physical systems, attempts have been made to classify assaults and countermeasures. For example, authors in [3] and [4] quantitatively examine the CPS security research trend to identify the distribution of study topics. CPS research is classified based on several application situations, including electricity grids and industrial control systems (ICS) [5]. Some researchers discuss attack detection and secure estimation strategies, whereas others cover automated intrusion detection in CPS [6], [7]. Recent studies have standardized assaults on cyber-physical systems that use physical signals to impact electronic components, particularly sensors [8], [9]. Existing research has not addressed the security and privacy concerns associated with cyber-physical systems' interface

with the physical world, one of their distinguishing features. As the cyber and physical worlds become more interwoven, it's crucial to comprehend the security implications of growing threats and technological advancements.

Cyber-physical systems are increasingly interwoven into key infrastructures, making security breaches potentially disastrous [10]. A hacked vehicle-to-vehicle communication network might lead to accidents by transmitting incorrect distance information. Autonomous automobiles have exacerbated the issue by requiring passengers to trust the vehicle's choices. In addition to security problems, CPS privacy is a big issue. Cyber-physical systems collect vast amounts of data for analysis and decision-making, frequently spreading across large geographic regions. The system uses machine learning algorithms to make informed judgments based on collected information. Data breaches can occur at any system level, from collection to transmission, operation, and storage. Again, most current CPS design techniques do not include data protection, putting the obtained data at risk. The CPS comprises two layers that communicate via networks and the cyber-physical layer, which can be further divided into cyber and physical domains (see Figure 10.1).

Cyber-physical systems (CPS) control the world's essential infrastructure. CPS integrates cyber and physical locations, serving as a bridge between the two. Examples include electricity generation, distribution, water treatment, manufacturing, and mining. These systems are highly integrated and tailored to the relevant area [11]. The dangers inherent in the interconnectedness of the cyber and physical realms demand strong protection. Recent research emphasizes the need to detect suspicious activity within the CPS promptly. Advanced machine learning approaches can aid detection, allowing systems to respond quickly to possible threats [12]. However, the issue remains of scaling these security mechanisms across varied IoT settings while retaining system stability and performance. In addition to technological solutions, academic and industrial collaboration is required to develop comprehensive CPS security procedures. This partnership can result in the creation of best practices and standards that improve the overall security posture of these systems. By harnessing the experience of diverse stakeholders, the field may move more quickly toward tackling the multiple security concerns that CPS confronts.

10.1.1 The key contributions of the chapter

CPS security prospects depend on advances in threat identification techniques and resistance methods for emerging cyber threats. Safety protocols

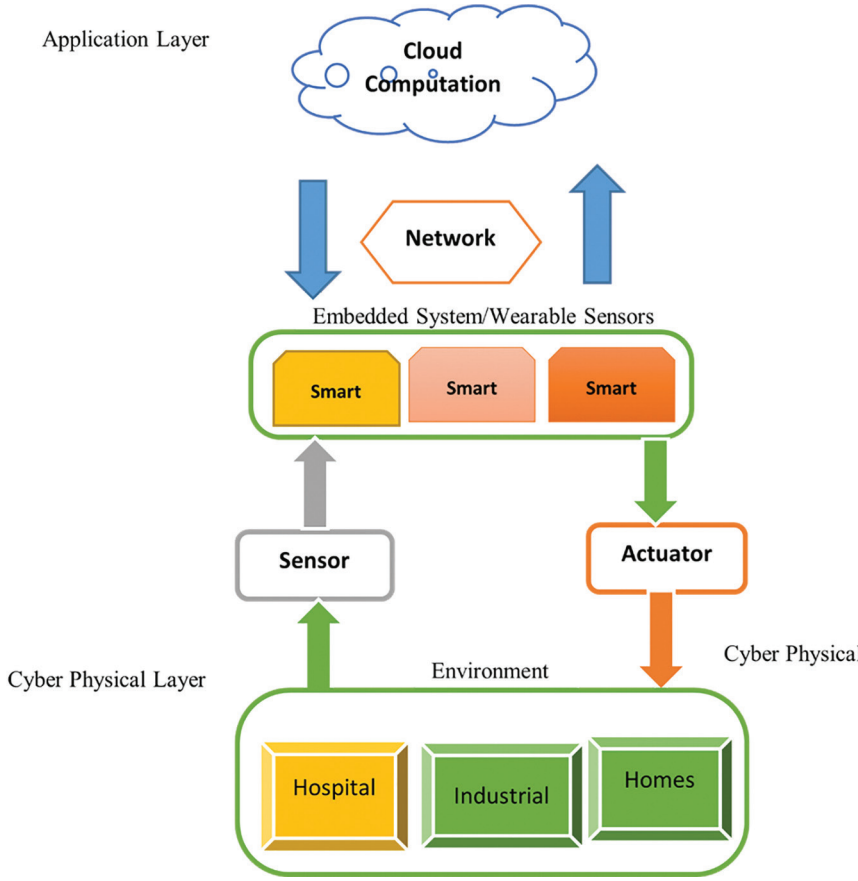

Figure 10.1 CPS architecture.

must adapt as cyber-physical systems change and extend into novel uses. This involves investigating new encryption techniques, such as homomorphic encryption, which allows for the secure computing of encrypted data while maintaining privacy and facilitating data analysis. As CPS becomes more integrated into our everyday lives, the significance of new security and privacy measures cannot be emphasized. The literature discusses various solutions for securing these complex systems, ranging from layered security designs to incorporating machine learning and collaborative frameworks. To address the problems offered by CPS, a multidimensional strategy is required, combining technological innovation with an awareness of human aspects and industry collaboration. As research advances, it is critical to be aware and proactive

in building strong security measures to survive the changing environment of cyber threats.

This chapter covers a range of cyber-physical systems with varying complexity and integration scales. Adopting advanced metering infrastructure (AMI) and household energy management systems has led to a transition toward a more dependable and secure grid, known as the smart grid. The growing infrastructure comprises four parts: electricity generation, transmission, distribution, and end-use. End-users are increasingly integrating intelligent control systems, leading to the development of home automation systems. This chapter provides in-depth coverage of these systems. The other section covers the lowest scale of CPS: healthcare systems, including wearable and implanted medical equipment. Healthcare devices can be worn or implanted to regulate various organ functions [13].

Wireless sensor networks facilitate communication among healthcare equipment. They are susceptible to network assaults and device-level compromises. To prevent cyberattacks on critical infrastructure systems (CPSs), it is important to identify weak components that can be exploited through persistent attacks. CPS utilizes various equipment and structures, including sensors, actuators, PLCs, RTUs, and HMIs [14]. These devices communicate with the Internet to perform tasks like measuring and uploading power meter data for analysis. CPSs have several levels, including operations and communications, physical control, supervisory control, and corporate layers [15]. Each layer is described separately because the physical layer consists of sensors and actuators responsible for directly transmitting data to the control system for processing. Programmable logic controllers (PLCs) and remote terminal units (RTUs) are part of the control layer. These units receive information from physical devices and send orders for execution. The control unit provides instructions about specific tasks using numerical values obtained from physical sensors and actuators. The corporate layer, which connects physical, computer, and network components, is prone to security and privacy vulnerabilities in corporate networks [16]. Attackers might exploit cyber threats by employing sophisticated methods and tools to violate the confidentiality, integrity, and availability (CIA) security principles.

10.1.2 Chapter organization

The remaining parts of this chapter are organized as follows: Section 10.2 presents privacy preservation in cyber-physical system environments and discusses differential privacy for cyber-physical systems. Section 10.3 presents cyber-physicals and cyber threats. Section 10.4 introduces the

modern security and privacy solution for CPS. Section 10.5 concludes the chapter.

10.2 Privacy Preservation in Cyber-physical System Environments

The need to preserve privacy in cyber-physical system (CPS) environments is critical due to the vast amount of personal and sensitive information these systems handle. The combination of physical and cyber components in these systems complicates issues relating to privacy. Privacy preservation protects sensitive information from unauthorized access while allowing for effective network processing [17]. A study introduced privacy preservation in CPS in 2008 to provide data utility while preventing network advertisers from accessing sensitive data [18]. CPS systems generate large amounts of heterogeneous data from multiple sources, necessitating the development of privacy-preserving methods while maintaining network security measures like anomaly detection [19]. Since CPS systems gradually draw in enthusiastic, competent hackers, their principal objective is to gain access to exfiltration control system data that includes energy information, login details for additional system usage, and an awareness of key node locations to cause important kinetic impact.

AQ1

An effective and straightforward way to identify privacy-preserving technologies is based on the aim of data transformation [20]. This categorization includes three categories: data generalization, transformation, and aggregation. Generalization techniques protect data security by transforming sensitive attributes into generic values. Transformation methods add new values to the original data and utilize projection to minimize its dimensions. Aggregation methods divide original data into tiny pieces and adjust private variables based on the average of those parts. Other works focused on data aggregation to ensure system security and privacy [21]. These approaches are excellent in protecting sensitive data from unauthorized access. However, data heterogeneity strategies are still in their infancy in CPS research due to the challenge of properly handling many data types. This is not a minor issue given the wide range of data in CPS ecosystems.

An alternative strategy for categorizing privacy preservation strategies is based on their properties. This type includes four categories: heuristic, reconstruction, cryptography, and blockchain-based [22]. These strategies are seen to be successful in data security. Still, they have limitations such as offering little cryptographic information, incurring high computational costs, failing to describe data standards, whether raw or aggregated, and being unable to scale adequately [23]. Numerous techniques involving data mining

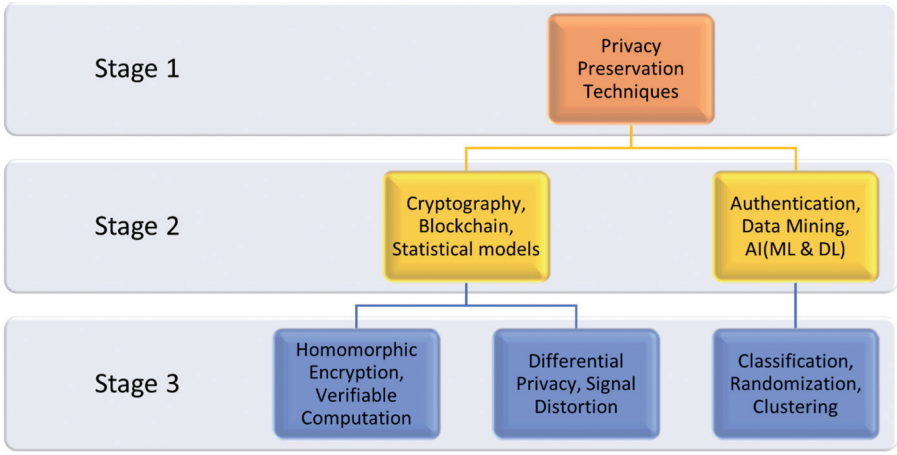

Figure 10.2 Privacy preservation in control systems.

(DM) and machine learning (ML), perturbation (i.e., differentiated privacy (DP)), and encryption were used for transforming, changing, disseminating, and hiding computer data from exposure while analyzing or transferring it through networks. Data in control networks, such as electrical grids, is restricted for safety, confidentiality, and business reasons, making it difficult to access for study purposes [24]. As a result, combating cyber and privacy threats to CPS ecosystems remains an important topic of study, with various studies undertaken specifically to secure CPS physical and network personal data [25-27]. Encryption techniques are typically used to preserve confidential information. However, they still have issues in subsequent evaluation and information management, whereas recently, machine learning, data mining, and statistical methods have been widely utilized [28],[29]. Figure 10.2 illustrates several safeguarding privacy strategies, including their types, methodology, advantages, limitations, and potential improvements.

10.2.1 Differential privacy for cyber-physical systems

Differential confidentiality is an efficient statistical technique that ensures unconditional privacy by making no assumptions about an attacker's knowledge. This assures that perturbed data calculations do not significantly alter when the original data is changed while maintaining data privacy even after access by other parties [30]. The outcomes of any computer are distinct and independent of the initial information in the dataset. Researchers have suggested several privacy-preserving solutions to address specific risks.

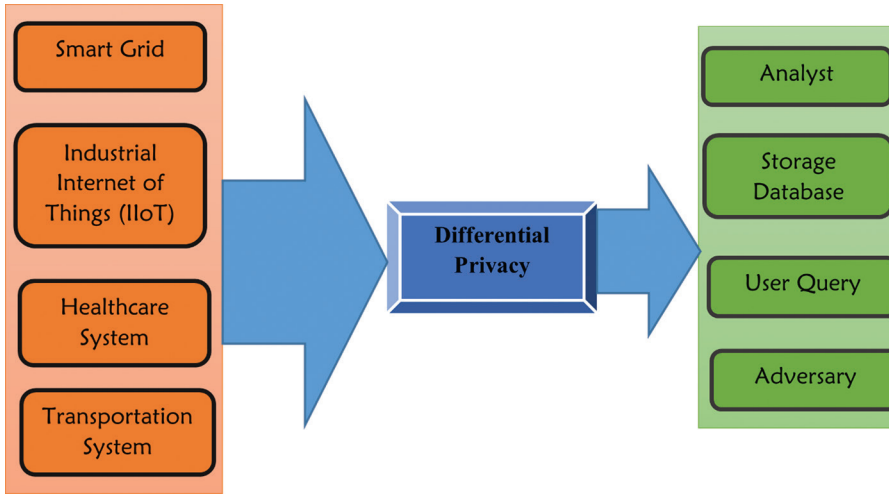

Figure 10.3 Application of differential privacy in the cyber-physical system [36].

Encryption is a fundamental privacy-preserving approach most systems use to secure data from attackers and unknown individuals [31]. It ensures that data is inaccessible to unknown parties. Modern CPSs have limited CPU capability, making encryption difficult to implement [32]. In public key cryptography (also known as asymmetric cryptography), generating and distributing public and private keys is computationally intensive and cannot be effectively carried out on tiny devices with limited resources. Additionally, vulnerabilities in encrypted CPS data can be exploited by brute-force attacks. Encryption techniques in a network of sensors need connections of all nodes to generate and transmit private keys throughout the network. If one node fails in a network of n nodes, it becomes almost hard to decrypt and gather data from CPS nodes due to missing keys.

Differential privacy is a simple privacy preservation approach that doesn't require sophisticated hardware [33]. The design and efficiency criteria for CPSs vary depending on their use. The optimality of differential private mechanisms varies based on application requirements. In certain circumstances, maintaining total privacy is the ideal answer, but in others, offering a certain degree of benefit might be considered optimal [34]. Similarly, there is no definition of an optimum differential privacy solution; instead, researchers working in differential privacy use the phrase "approximate optimal solution" to refer to the most suited solution based on the requirements. Moving on to CPS applications, devices that provide differential privacy often communicate time-series data from one destination to

another in the smart grid context. Smart grid applications often prioritize point-by-point privacy. The most prevalent energy system assault is non-intrusive load monitoring (NILM), which targets smart home users' appliance usage and routines [35]. Differential privacy solutions in smart grids often aim to prevent assaults. Implementing differential privacy solutions in energy systems aims to provide cost-effective medium-level privacy protection while balancing accuracy and privacy. Figure 10.3 shows the use case possibilities for differential privacy in cyber-physical system applications such as analyst data analysis, storage databases, user query assessment, and attacker query requests.

The true explanation is that the computing cost of differential confidentiality consists solely of noise calculation using an established probability distribution. However, encryption nodes must perform specific duties such as key creation and distribution, data encryption, and decryption. Compared to encryption, differential privacy has lower computational complexity. In differential privacy, CPS users may adjust the amount of privacy based on their needs by changing the noise addition value "ε." Unlike anonymization, differential privacy protects original CPS data during query assessment by perturbation methods, preventing data loss. Differential privacy techniques effectively defend against numerical and non-numerical requests [36]. Differential privacy has been widely used in CPSs to protect individual privacy due to its numerous advantages, mathematical and theoretical foundation, and ease of implementation.

10.2.2 Application of authentication-based privacy preservation for CPS

One critical aspect of cyber-physical systems (CPSs) is that they depend on authentication-based privacy to ensure that only authorized users and devices can access sensitive data or systems [37]. Strong authentication protocols are very important to maintain privacy and security in CPS, which are interconnected networks that are often publicly accessible, with device-to-device (D2D) communication occurring frequently. For example, smart grids, autonomous vehicles, and health monitoring systems are typical CPS environments with several layers of communication and data transmission. Consequently, these interactions may expose private or operational information if appropriate measures are not taken for their protection. One way to safeguard such interactions, therefore, is through strict identification processes that verify the identity of users and machines, thus limiting access to confidential information only to persons with legitimate rights to it.

CPS authentication may come in different forms, such as conventional passwords, hardware tokens, or even more developed biometric systems and digital certificates [38],[39]. Each method has advantages and disadvantages concerning privacy, convenience, and security. For example, although biometrics provide high levels of security due to being unique to an individual, it may have big implications for privacy if any of that person's bodily information is exposed. Public key infrastructures (PKIs) enhanced security within CPSs by enabling authentication through digital certificates. Such certificates guarantee the validity of ownership over public keys while preventing tampering; hence, they act as a trust assurance between devices and systems. Finally, digital certificates help encrypt communications, thus safeguarding privacy when transferring data between parties.

In addition to protecting human–computer interactions, authentication in CPS must consider machine-to-machine (M2M) communications [40]. The challenge here is managing and authenticating many device transactions automatically and safely. Techniques like mutual authentication are critical in such cases, where both parties authenticate each other in a communication. This approach is particularly crucial in industrial applications and critical infrastructure since unauthorized access or manipulation of machines' operations can lead to dire consequences [41]. Another level of privacy protection is provided by integrating context-aware authentication mechanisms that consider the circumstances under which access requests are made. These mechanisms make dynamic authentication decisions based on location, time, and type of access request. Doing so enables CPS to make a trade-off between security requirements and user convenience by adjusting their authentication requirements according to the perceived risk level; this way, they ensure continuity of service but always minimize chances for unauthorized entrance into their systems.

Nonetheless, when applying robust authentication strategies in CPS, attention should also be paid to privacy. For instance, storing and processing authentication data, especially biometric data and personal identifiers, should be a ledge to respect users' privacy while complying with applicable data protection laws. This may involve using privacy-enhancing technologies (PETs) such as zero-knowledge proofs that enable authentication without disclosing the real details, protecting the user's privacy. The issue of protecting privacy through authentication-based means in CPS is complicated by various factors that combine to come up with sophisticated technical solutions, system design considerations, and management practices [42]. Importantly, authentication mechanisms must be enhanced to ensure that as CPS continues evolving and becoming more integrated into daily activities, there is enough privacy

protection, hence protecting the complex processes set to run these systems securely.

10.2.3 Application of data mining and machine and deep learning-based privacy preservation in CPS

Data mining, as well as machine learning, is playing a significant role in the advancement of private security techniques within cyber-physical systems [43]. CPS produces immense amounts of information, such as smart grids, health monitoring systems, and urban infrastructure management, which these technologies use to identify patterns, anomalies, and potential hazards – implementing data mining methods with machine learning results in more advanced models aimed at foreseeing privacy violations, thereby protecting personal and business information against unpermitted exposure. The use of machine learning algorithms, especially in pattern recognition and anomaly detection, is important for identifying abnormal behaviors that could indicate intrusions or data leaks in CPS environments [44]. These models are trained on huge amounts of historical data to know what normal means regarding system behavior. They serve as real-time security enhancements and continuously monitor the incoming information for deviations from these norms, making them indispensable for dynamic and complex CPS networks [45]. Furthermore, privacy-preserving data mining techniques are more important than ever in environments where sharing information may put privacy at risk. This is done through differential privacy methods that add some noise or randomness to training datasets for machine learning models, thus preventing others from knowing specific details about any individual entry but leaving just enough accurate detail for meaningful, purposeful analysis. Using such a model allows CPS operators to obtain insights from data while protecting people's personal information they hold on them because otherwise, their lives may be ruined if someone finds out about them.

The creation of federated learning systems is one more significant use for machine learning regarding privacy in CPS [46]. These systems allow the training of machine-learning models on several decentralized devices or servers while keeping their true data intact. For example, utilizing a federated learning approach enables hospitals to enhance their prediction models for patient care without exposing sensitive personal information during that process, hence maintaining confidentiality and compliance with strict medical privacy rules. Moreover, some models could help preserve secrecy by automating data encryption/decryption techniques. Sophisticated models may establish the best possible encryption strategies depending on how much

security the data holds and the environments wherein such information is applied, dynamically adapting accordingly as situations change. This flexibility is essential within CPS, where the system states and outside dangers may advance quickly. Nevertheless, applying data mining and artificial intelligence in data safeguarding is a non-terminating headache.

The utmost importance is on ensuring that no data goes out through the machine learning models themselves. Adversaries can only get to sensitive information if they reverse engineer these models; subsequently, it's crucial always to ensure the safety of the model, especially when it comes to inference data they make, and training processes associated with them. Another challenge facing developers of scalable privacy-preserving machine learning algorithms is their complexity [47]. They should not just succeed in hiding something but should also be capable of processing loads of information quickly to meet the real-time processing required by CPS. Although considering privacy and operational efficiency, CPS can use data mining and machine learning as powerful tools. However, great care must be taken when implementing them. There is the possibility that these technologies will become more complex in CPS as time moves on. They would thus become more powerful in countering any privacy issues, even while allowing these systems to have better data mining capabilities, which is what they are built for.

10.2.4 Artificial intelligence in privacy preserving

AI is the science and engineering of creating intelligent machines that think like humans [48]. John McCarthy, dubbed the "father of AI," was the first to present this notion. AI aims to create expert systems capable of intelligent tasks, learning, situational awareness, and human-like behavior. The first AI application was designed for weather forecasting. AI-based apps (e.g., movie recommendations, early illness detection, Google navigators) rely on large amounts of data to make accurate conclusions and suggestions (Figure 10.4). This might compromise data security and privacy.

As systems are interconnected and complex, AI (artificial intelligence) has an important role in transforming privacy protection in cyber-physical systems (CPSs) through innovative methods that fortify the safety of these environments. The deployment of AI technology plays a critical role in solving different privacy difficulties that CPS are confronted with as they become more important to key infrastructures like power grids, transport systems, and healthcare services [49]. One aspect where AI excels is its ability to rapidly analyze huge amounts of information, pick out possible risks to personal data, and automate enforcement processes for data protection regulations. In

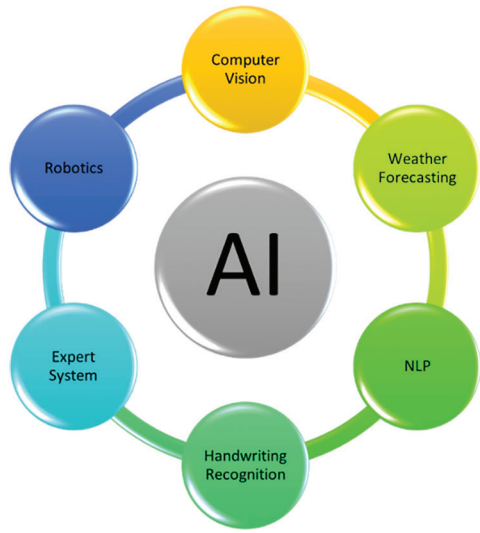

Figure 10.4 Artificial intelligence applications.

CPS, AI may be used to create prediction models that detect privacy breaches before they occur. These models use previous data to understand patterns related to security issues, which allows them to anticipate similar events in the future. This proactive strategy enables system administrators to adopt preventative actions, securing sensitive data. Furthermore, AI-powered systems may automatically alter privacy settings based on real-time data analysis, reacting to new dangers as they emerge without requiring human interaction. This flexibility is critical in contexts where dangerous landscapes are continually shifting. Table 10.1 displays the various AI techniques utilized in the privacy-preserving aspects of CPS.

AI also improves privacy by utilizing powerful anomaly detection techniques. These approaches enable CPS to continually monitor network traffic and user activity, detecting aberrant behaviors that may signal privacy violations. These systems can greatly differentiate near-in-female dissimilarities with negative consequences; they make fewer errors and enhance the speediness of security measures. Further input is that AI supports removing and hiding our data through a process known as privacy-preserving data mining in CPS. Various processes used here include federated learning, which allows the training of an AI model across several separated nodes without having to share any raw information. This approach means important information stays within its locality, lessening the chances of losing such information when using central processing platforms. AI algorithms also assist in executing

Table 10.1 AI in privacy-preserving for CPS.

AI techniques	Application in CPS	Privacy technique	Benefits	Challenges
Federated learning	Distributed learning across multiple CPS devices	Data localization	Enhances privacy by processing data locally	Managing heterogeneous data sources
Differential privacy	Adding noise to data collected from CPS devices	Noise addition	Provides theoretical guarantees of privacy	Balancing privacy with data utility
Homomorphic encryption	Performing computations on encrypted data from CPS	Encryption	Allows data processing while keeping data encrypted	High computational overhead
Secure multi-party computation	Collaborative data analysis without exposing individual inputs	Encryption, secret sharing	Secures data during joint computations	Complexity and scalability issues
Machine learning models	Anomaly detection and predictive maintenance	Model perturbation, data anonymization	Helps in identifying potential threats without revealing sensitive data	Requires continuous model updates

encryption methods such as homomorphic encryption, where the actual data is never revealed. However, it can still be worked on through this type of coding, keeping it safe and ensuring no loss of importance [50]. Using deep learning algorithms, these systems can accurately discern between benign abnormalities and dangerous threats, decreasing false positives and enabling more efficient security responses.

Furthermore, AI helps to maintain privacy in data mining activities inside CPS. Techniques like federated learning, in which AI models are trained across numerous decentralized nodes without exchanging raw data, contribute to data privacy. This technique keeps sensitive information inside its local context, lowering the danger of data leaking during central processing. AI algorithms are also useful in developing encryption techniques such as homomorphic encryption, which allows data to be processed while encrypted, giving security without losing data usefulness. While AI dramatically improves CPS's ability to protect user privacy and security, its deployment must be carefully controlled to balance efficacy, efficiency, and ethical issues. With continued advances in AI research and its application to real-world systems, its role in privacy preservation in CPS is expected to grow more robust and essential, offering a future in which CPS may be both powerful and safe.

10.3 Cyber-physicals and Cyber Threats

A CPS combines physical and communication technologies with cyber, physical, and cyber-physical aspects. A cyber element comprises computing and network components that do not interact directly with the physical world. In contrast, a physical element consists of hardware and industrial components that do not interact directly with the cyber parts. Cyber-physical elements include devices and systems that connect the cyber and physical worlds, such as sensors and actuators [51]. A CPS combines data sources from physical devices and computational and network systems to produce big data. Because of their complexity, big data presents several challenges, particularly regarding system control and data analytics for monitoring and controlling their operations. In a CPS, such as a power system, supervisory control and data acquisition (SCADA) serves as an interface for monitoring and managing activities employing conventional communication and industrial protocols [52]. However, the CPS's interconnectedness of sensors, actuators, and network devices at various power nodes complicates the platform environment (such as a power grid). It generates vast data that must be secured from cyber threats. Table 10.2 shows the variety of cyber threats that can affect CPS.

Table 10.2 Cyber threat and common mitigation strategies.

Cyber threat	Impact on CPS	Common mitigation strategies
Malware	Disruption of operational technology	Regular software updates, anti-malware tools, and network segmentation
Ransomware	Looking for access to critical system	Secure backups, intrusion detection systems, cybersecurity training
Denial of service (DoS)	Overload systems to interrupt services	Distributed denial of service (DDoS) protection, redundancy
Man-in-the-middle attacks	Data interception and manipulation	Encryption, secure communication protocols, VPNs
Data breaches	Unauthorized access to sensitive data	Strong authentication measures, encryption, and access controls
Physical tempering	Direct physical harm to system components	Physical security controls, surveillance systems
Supply chain attacks	Compromise through third-party components	Supplier security assessments and secure software development lifecycle

To detect cyber risks to CPS systems, it's important first to understand their fundamental components. This includes identifying susceptible areas that advanced attackers can exploit. A CPS comprises a variety of sensors, actuators, and components that govern systems and communicate with other networks (including business networks and even Internet connections) to perform CPS tasks [53]. CPSs comprise physical, control, supervisory, and corporate layers. Cyber attackers have produced cyber threats who frequently utilize complex assaulting tactics and tools to violate the confidentiality, integrity, and availability (CIA) security principles. Man-in-the-middle (MITM) attacks and data exfiltration are malicious behaviors that compromise confidentiality [54].

Additional CPS-specific integrity threats include modifying CPS components or registers, exposing system data through fake data injection, data poisoning, and unlawful data or configuration change. This can include data sources such as sensor or device measurements and control commands, which modify the usual occurrences of physical and network devices. Attacks on availability include denial of service (DoS) and distributed DoS. There are other CPS-specific issues in this domain, such as the potential to disrupt the operation of RTUs and PLCs by providing them with incorrect data. This is especially problematic on older systems that lack the processing capability for thorough error checks. Attacks on networks can cause temporary or permanent downtime or physical damage. This can disrupt the regular functioning of

CPSs. Active research is underway to safeguard CPS devices and data against hackers. These measures include preserving privacy, securing original data from unauthorized access, and detecting cyber assaults on CPSs and networks.

10.3.1 Application scenarios of cyber-physical System

Cyber-physical systems (CPSs) combine physical processes, computers, and networking to improve capabilities across various industries, each with its application situations [55]. These systems combine hardware and software with network connectivity to produce responsive environments that vastly increase efficiency, safety, and functionality. The information flow and physical sensing between cyberspace and connected physical devices are described as follows.

A. Industrial sector
   In the industrial sector, CPS is key to Industry 4.0, enabling smart production processes. CPS manages physical manufacturing processes using real-time monitoring, data analytics, and autonomous decision-making capabilities [56]. These systems manage complicated industrial processes, adapt operations in response to demand changes, and forecast equipment maintenance requirements before breakdowns occur, reducing downtime and increasing production efficiency.

B. Transportation sector
   Transportation is another crucial area that benefits from CPS. Intelligent transportation systems (ITS) use CPS to improve traffic management, road safety, and logistical efficiency [57]. Vehicles outfitted with sensors and communication technology communicate with one another and with road infrastructure, allowing for adaptive traffic control, real-time rerouting to reduce congestion, and early warning systems to avert accidents.

C. Healthcare sector
   In the healthcare industry, CPS transforms into complex networks that connect wearable gadgets, implanted sensors, and other medical equipment to continuously monitor patients' health [58]. These systems collect vital data that may be utilized for early diagnosis, individualized treatment regimens, and remote patient monitoring, resulting in considerably improved patient outcomes and healthcare delivery.

D. Energy management
   Energy management also heavily relies on CPS through smart grid technologies. These systems optimize the production, distribution, and

consumption of energy. By integrating renewable energy sources, predicting energy demand, and automatically adjusting supply, smart grids help to efficiently manage resources, reduce costs, and improve the reliability and sustainability of energy systems [59].

E. Environmental monitoring
CPS improves environmental monitoring by tracking environmental variables and changes with sensors and networked technologies [60]. These systems can monitor air and water quality, identify dangerous circumstances such as forest fires or floods, and give data to help protect the environment and guide policy choices.

F. Urban planning management
CPS is important in creating smart cities through urban planning and administration. These systems control everything from traffic and waste management to water delivery and public safety [61]. Smart city CPS employs data from many sensors and sources to optimize city operations, improve government services, and improve citizens' quality of life.

G. Agricultural application
CPS-based agricultural applications include precision agriculture approaches that employ sensors and automated systems to monitor crop conditions, optimize water consumption, and manage fertilizers and pesticides [62]. This careful control contributes to higher agricultural yields, less waste, and a lower environmental effect of farming techniques.

10.4 Modern Security and Privacy Solution for CPS

Modern security and privacy solutions for cyber-physical systems (CPSs) are intended to solve the particular issues given by the combination of physical processes, digital networking, and computing. The demand for better security and privacy safeguards rises as these systems become more widespread and critical – from infrastructure to personal devices.

10.4.1 Advanced cryptographic techniques privacy preservation

Securing calculations in different applications might raise privacy problems by allowing one or several parties to exchange and execute functions

and analyze data inputs [63]. Users share a public key to send encrypted messages, which protects the system's privacy and integrity while allowing access to message content. Cryptographic procedures are often used among academics to provide system security and privacy. Whether symmetric or asymmetric, encryption techniques aim to convert readable data into unreadable text (ciphertext). Symmetric encryption employs a single key for both parties, whereas asymmetric encryption requires a public key for encryption and a private key for decryption. While efficient, the main issue with these techniques is the trustworthiness of the encrypted keys. MITM attacks can compromise keys and render encryption unusable. A public key infrastructure (PKI) approach to secure devices and facilitate message exchange between users on two edges [64]. The registration authority connects public keys to user identities and implements attestation protocols, firewalls, and authentication to restrict the impacts on disclosed devices. Various cryptographic approaches can secure and safeguard vast clouds or control systems data. Secure multiparty computation (SMC), verifiable computation (VC), and homomorphic encryption (HE) are three effective ways to achieve data privacy in scalable and lightweight calculations. These are explained as follows.

SMC-based privacy preservation has become a common encryption mechanism in various forms of encryption but in different data analysis forms like a distributed PPDM; for example, it employs two well-known techniques: MC garbled circuits and secret sharing [65]. Nevertheless, some studies into SMC have limitations because their strategies are vulnerable to multiple attacks and exhibit high communication complexity, which increases exponentially as the number of participants grows. VC-based privacy preservation is a methodology that enables data owners to examine the safety of operations. An intermediate prover is a strong being with the authority to retrieve demands for computation processes, verify these processes, and pass along the outcomes. In contrast with SMC and HE methods, VC can ensure data integrity but not confidentiality during calculations, hence making it necessary whenever there are parties who might not be trusted or enemies could be present.

HE-based privacy preservation: Rivest introduced HE because common encryption techniques can't operate on encrypted data, so the data should be decrypted first, even if cryptography is often employed to keep sensitive information confidential [66]. This implies that users or parties cannot access these services without compromising their privacy. Privacy based on homomorphic encryption (HE) has been widely studied, mainly due to its ability to perform certain arithmetic operations. Several encryption methods support various homomorphic characteristics, such as multiplicatively homomorphic

(RSA), additively homomorphic (Paillier), and the recently proposed fully homomorphic scheme for complex functions. Many HE techniques remain impractical because their computational overheads impede their efficacy; for instance, there is a framework to aggregate data from smart grids while maintaining customer privacy, where an additive HE method is utilized. They leverage attribute-based encryption to enable access control based on the data that is being held.

10.4.2 Blockchain technology privacy preservation

CPS can use blockchain technology for decentralized protection against hacking and privacy violations using a ledger resistant to manipulation or changes [67]. The technology is used to create safe and open transactions that possess the completeness of information without being subject to control by any one party, making it important in supply chains, smart electrical grids, or even in other kinds of Internet of Things (IoT) [68]. Within a blockchain, something like a message input can be associated with another message that is not more than n bytes long. The key aspects that define a blockchain are addressed below.

Decentralization: all participating parties (i.e., nodes/participants) have the authority to control/add, edit, or validate the appended transactions rather than having them centrally coordinated (peer-to-peer). In a decentralized blockchain network, each user is called a miner, participating in the consensus process and confirming each freshly delivered transaction to grow the chain. This feature lowers the likelihood of a single-point failure or data compromise. Validated transactions on the blockchain are immutable, meaning any changes require verification by other nodes. The consensus protocol ensures the integrity and authenticity of blockchain data by requiring each node to create the same output based on its rules (degree of confidence).

The blockchain network relies on anonymity to ensure integrity among users (miners), with just their addresses necessary. To maintain anonymity and privacy, distinct public keys can be used for each miner. This study topic promises to ensure system security and privacy for users and data transactions. Transparency is the habit of regularly evaluating data in the same miner for self-auditing and preventing corruption. Trustworthiness: data transactions (i.e., records) are continually verified and validated, with their integrity achieved using a cryptographic mechanism (hash) created for each one, which is kept in a block over the blockchain, which guarantees that it cannot be altered or updated (persistence).

10.4.3 Artificial intelligence and machine learning techniques

The new techniques that artificial intelligence (AI) and machine learning (ML) advance are changing privacy and security issues in cyber-physical systems (CPSs) [69]. As cyber-physical systems (CPSs) are critical infrastructures such as smart grids or healthcare systems, using AI and ML for security and privacy is no longer just an option but mandatory. These technologies excel at managing the intricacies of large and interlinked systems and can tackle problems that traditional security systems do not address. Anomaly detection is one of the main application situations for AI and ML in CPS security. With the help of ML algorithms trained on huge datasets, it would be possible to understand what normal system behavior looks like for a specific task; once this knowledge is acquired, live operations can be monitored to find any difference from expected outcomes [70]. These abnormalities may stand for security breaches, for example, an intrusion by a stranger or virus attacks. For example, in the case of a smart grid, ML models can identify atypical power patterns that imply potential cybercrimes or even physical interference with such infrastructures.

Artificial intelligence (AI) and machine learning (ML) are making a revolutionary impact on privacy and security in cyber-physical systems (CPSs) by offering a variety of creative application scenarios. Since CPSs increasingly form the backbone of critical infrastructure, including smart grids and healthcare systems, utilizing AI and ML for security and privacy is no longer just an option but a necessity. These technologies can tackle intricate issues in huge interconnected systems that conventional security measures cannot handle. Anomaly detection is one of the main application scenarios for AI and ML in CPS security. Machine learning algorithms can be trained on large datasets to recognize normal system behavior and then watch for deviations during real-time operations. Such deviations may signal potential threats such as unauthorized access or malware infiltration. For example, within a smart grid, machine learning models may detect abnormal patterns of electricity use which could point to a breach in cybersecurity or physical interference with the infrastructure.

Privacy preservation is another area in which AI and ML have made significant strides. Techniques such as federated learning enable the creation of ML models on decentralized data, allowing learning from sensitive data without any need to centralize it. This tactic is quite beneficial to CPS environments like hospitals, where the privacy of patient information comes first but still undeniably benefits from predictive analytics. Moreover, differential privacy that utilizes machine learning allows adding random noise into datasets or queries, thereby safeguarding individual data points within larger

datasets. In this manner, CPS can use data for optimization and performance enhancement without infringing on personal privacy. CPS, AI, and ML also improve security through enhanced cryptographic processes like homomorphic encryption, which permits direct manipulation of encrypted information. **AQ2** To optimize these procedures, ML models can make them more applicable in real-time or almost real-time settings such as banking services where protection against fraud and latency time is a vital consideration. In CPS network security, ML algorithms fine-tune and adapt firewall tactics to changing flow dynamics and risk environments. Moreover, intricate security arrangements may be handled by AI across different CPS elements, thus safeguarding uniformity while minimizing the chances for mistakes in a set-up that would result in a lack of protection.

However massive that potential seems, AI and ML face challenges when transforming CPS privacy and security. To use all these technologies effectively, we should tackle issues related to a lack of transparency in ML models and a tendency to exhibit some form of prejudice or biases over time, thereby compromising its security properties. Consequently, as long as we expect development to be never-ending in terms of more extensive involvement with every aspect of our lives today, AI and ML are going to assume certain important roles when it comes to protecting such systems from new types of threats intended at them while making sure they strictly obey words concerning confidentiality standards set by any people's society these days The multiple range of ways that AI and ML could change the CPS for it to be kept secure and private are vast; however, they come with their problems. To fully utilize the strengths of these technologies, lack of transparency in ML models, possible biases, and even safety issues must be considered seriously. With more advancements to make attachments of CPS at various activities of our societies, they will be strangled up by strict privacy practices together with AI and ML, which are vital in safeguarding them against new threats developed every time.

10.4.4 Challenges and research opportunities

In the sphere of cyber-physical systems (CPSs), there have been a lot of challenges and research opportunities about privacy and security issues owing to the increasing complexity and criticality of these systems. Many believe the most important thing is ensuring that systems have strong security and strict confidentiality, as CPS integrates physical processes with digital networking and control systems. CPSs connect to the Internet with Modus TCP/IP, creating concerns about cybersecurity and data privacy [71]. Cybersecurity needs to find new cyber- and zero-day attacks and secure the cyber and physical

components of CPSs. These attacks may change lawfully operational actions and violate availability and confidentiality. Integrity attacks on CPS devices and networks can sniff, steal, or tamper with information, including network traffic and telemetry [72]. The security and privacy challenges are still unresolved in CPSs and their networks.

One of the primary challenges facing CPS security is bringing together devices and systems that are not only heterogeneous but whose security capabilities and standards widely differ [73]. This heterogeneity complicates the deployment of uniform security measures across all components, leading to vulnerabilities that malicious persons can easily exploit. In addition, many CPSs have strict real-time operational requirements, such as driving critical infrastructures or autonomous cars, which impose stringent latencies on security solutions, making it difficult to deploy comprehensive computationally intensive security mechanisms. The scalability of security solutions is also a major challenge. The security mechanisms should grow together with CPS networks, which must become more complex and larger without sacrificing speed or usability. It includes secure and efficient data handling in large quantities, particularly in light of the upcoming Internet of Things (IoT) era, when billions of devices will be communicating nonstop.

The scalability of security solutions is another major challenge. As CPS networks become more complicated, security mechanisms need to be enlarged without hampering efficiency or practicality. This includes the ability to securely and efficiently manage increasing resources, particularly due to the emergence of the Internet of Things (IoT) era in which billions of devices constantly produce and transmit information. It's imperative to consider the complicated nature of CPSs, comprised of physical and communication entities, network protocols, and limited computing power/storage contraptions when considering methods for preserving privacy and detecting intrusions. Thus, every suggested approach should demand significant computing abilities to manage complex protocols/devices, identify new types of invasions, and safeguard sensitive information from unlawful disclosure. In addition, they should adapt themselves and ensure reliability to manage the dynamic conditions within a CPS, such as power networks, by utilizing feature projection and dimensionality reduction schemes on the original dataset. Creating a detailed and complete profile for the unique normal events is not simply feasible, especially if one is collecting data from measurements taken from sensors and network packets since there are always some discrepancies in their distinction between normal and deviant behaviors. There are mistakes on false positive and false negative rates when an ideal case lies within an area of hacking, and the opposite holds for a criminal act violated as lawful. Consequently, this chapter seems significant because it would argue against

models that diseased privacy could cause errors of this kind to ascend, thereby making it necessary to maintain high detection levels for effective protection of CPS, which is a deep defense strategy.

Research opportunities in privacy and security within the cyber-physical systems field (CPS) are available. The development of advanced encryption techniques, such as homomorphic encryption and secure multi-party computation, is one area that shows some promise; these enable the processing of encrypted data, thus enhancing their security and user privacy levels. However, more work is needed to optimize these technologies to be computationally efficient for real-time cyber-physical systems (CPSs) applications. An additional major theme of inquiry is the utilization of artificial intelligence (AI) and machine learning (ML) in improving CPS security [74]. Security risks can be forecasted and spotted faster with AI and ML, enabling automated security operations. However, these innovations provide fresh weak points together with their implementation; therefore, they need to undergo careful consideration so as not to violate these systems' integrity. Moreover, a new approach must be in place to construct effective anomaly detection mechanisms that precisely identify and react to unprecedented dangers instantly. Such a system must be able to differentiate between harmless deviations from the normality line and authentic attempts at breaking system security laws. The process requires constant learned behavior pattern adjustments capable of going along with emerging malicious techniques.

Privacy by design is a concept that can be studied further, as it requires that CPS developers consider privacy issues during the design stage [75]. This way, they will not only obey the law but also earn the trust of clients and customers through showing dedication to confidentiality. Finally, given that most CPSs operate in different countries with various legal regimes, research on privacy and security standardization is a priority. It entails examining the impact of regulations such as GDPR on CPS functioning and identifying models that cater to multiple legislative demands while still maintaining strong privacy and safety measures. Tackling these challenges and utilizing these research opportunities requires a multi-disciplinary approach combining cybersecurity, data science, law, and ethics skills. Therefore, CPS privacy and security not only have difficult problems but are also changing places for innovations and improvements.

10.4.5 Lesson learned

Security and privacy issues concerning CPS are properly dealt with in this chapter. In addition, it shows how to combat them through different methods.

It is clear from the chapter that there are many issues in maintaining the security and privacy of CPS. Still, research development can also provide better adapted and stronger solutions than the existing ones. The major takeaways from the chapter are:

i. When CPS integrates various physical and digital components, it can be tricky to achieve uniform security across different systems with different security capabilities. This complexity necessitates adaptable and scalable security solutions.

ii. Many CPSs run under strict real-time constraints, meaning their security must not impede system performance. Thus, we need Africa-focused solutions to balance strong protection against little attack latency.

iii. These companies, such as CPS, usually handle large amounts of sensitive data. Ensuring privacy while allowing such data to be used in operations or decision-making processes becomes a major problem for every organization dealing with such information. Privacy-preserving data mining and federated learning are identified as potential solutions.

iv. This chapter comprehensively examines the evolution of threats facing cyber-physical systems (CPSs), including complex cyberattacks that may have physical implications. Because the threat landscape continues to be dynamic, it also emphasizes continuous improvement of technologies and practices related to security.

v. Machine learning algorithms and artificial intelligence have great potential for enhancing CPS security through better anomaly detection, predictive modeling, and automated response systems. However, this technology integration comes with various challenges, such as ensuring the security of machine learning models themselves.

vi. Addressing security and privacy challenges in cyber-physical systems (CPSs) calls for collaboration among academia, industry, and government to develop new standards, best practices, and fit-for-purpose solutions in developing such systems. This is important since no discipline can advance men's lives within such present-day contexts regarding computer science advancements alone.

10.4.6 Key future research direction

The security and privacy of CPS are dynamic and complex areas with multiple challenges and great opportunities for research and innovation. Tackling

these issues calls for a collaborative approach from different fields to improve technologies that protect these vital systems without infringing on users' privacy. CPS security will probably be characterized by fast-paced technological advancements, meaning that flexible and foresighted research strategies are essential. The following are the key areas of research direction to shape the landscape of CPS security and privacy.

i. Investigating cryptographic advancements like homomorphic encryption or algorithms that can resist quantum revolution. This type of technology can potentially protect information traveling and stored safely without being affected by new developments in computer science (like quantum computing).

ii. Predicting and avoiding violations before they occur through improved machine learning algorithms' efficiency also forms a big research area. These systems should focus on decreasing the number of false alarms while increasing immediate reaction capacity.

iii. While AI plays an important role in managing and securing CPS, its integration with privacy-preservation technologies, such as differential privacy and federated learning, will become indispensable. The purpose of this is to guarantee that AI enhances security without compromising on privacy.

iv. Another crucial research area is creating CPS security mechanisms resistant to sophisticated, state-sponsorship attacks. These include technological solutions and regulatory and policy measures that further strengthen these vital systems' security positions.

v. Furthermore, near-future studies must emphasize building interdisciplinary partnerships consisting of specialists from the cybersecurity domain, engineering experts, ethicists, and legal practitioners. All these experts working together would help tackle the multifaceted problems facing CPS and bring forth effective methods that are also lawful or moral.

10.5 Conclusion

The emerging security and privacy challenges threatening these systems are explored in detail in this chapter. These complexities are inherent within these integral systems and are vulnerable to unique and advanced threats. This is because they are the ones that form an interface between cyber technologies and physical processes and, therefore, face new kinds of attacks. The

progressive importance of developing robust security and privacy measures cannot be overstated, as they underlie critical infrastructure and profoundly influence daily living. It can be concluded from the chapter that future CPS security will depend on the development of highly advanced collective adaptive security frameworks that can keep pace with fast-changing technology and threats. With the increasing complexity and connectivity of CPS environments, there is a need for flexible security to meet changing conditions while including all possible cyberattack scenarios. Considering that so much data is generated from these systems, attention must be paid to privacy issues, requiring solutions that ensure personal privacy but do not compromise their overall functionalities or efficacy levels.

References

[1] MacCarthy, B. L., & Ivanov, D. (2022). The Digital Supply Chain—emergence, concepts, definitions, and technologies. In The digital supply chain (pp. 3–24). Elsevier.

[2] Vermesan, O., Bröring, A., Tragos, E., Serrano, M., Bacciu, D., Chessa, S., ... & Bahr, R. (2022). Internet of robotic things–converging sensing/actuating, hyperconnectivity, artificial intelligence, and IoT platforms. In Cognitive hyperconnected digital transformation (pp. 97–155). River Publishers.

[3] Giraldo, J., Sarkar, E., Cardenas, A. A., Maniatakos, M., & Kantarcioglu, M. (2017). Security and privacy in cyber-physical systems: A survey of surveys. IEEE Design & Test, 34(4), 7–17.

[4] Lun, Y. Z., D'Innocenzo, A., Malavolta, I., & Di Benedetto, M. D. (2016). Cyber-physical systems security: a systematic mapping study. arXiv preprint arXiv:1605.09641.

[5] He, H., & Yan, J. (2016). Cyber-physical attacks and defenses in the smart grid: a survey. IET Cyber-Physical Systems: Theory & Applications, 1(1), 13–27.

[6] Meshram, C., Imoize, A. L., Jamal, S. S., Alharbi, A. R., Meshram, S. G., & Hussain, I. (2022). CGST: Provably Secure Lightweight Certificateless Group Signcryption Technique Based on Fractional Chaotic Maps. IEEE Access, 10, 39853–39863.

[7] Giechaskiel, I., & Rasmussen, K. (2019). Taxonomy and challenges of out-of-band signal injection attacks and defenses. IEEE Communications Surveys & Tutorials, 22(1), 645–670.

[8] Giechaskiel, I., Zhang, Y., & Rasmussen, K. B. (2019). A framework for evaluating security in the presence of signal injection attacks. In

Computer Security–ESORICS 2019: 24th European Symposium on Research in Computer Security, Luxembourg, September 23–27, 2019, Proceedings, Part I 24 (pp. 512–532). Springer International Publishing.

[9] Yan, C., Shin, H., Bolton, C., Xu, W., Kim, Y., & Fu, K. (2020, May). Sok: A minimalist approach to formalizing analog sensor security. In 2020 IEEE Symposium on Security and Privacy (SP) (pp. 233–248). IEEE.

[10] Rass, S., Schauer, S., König, S., & Zhu, Q. (2020). Cyber-security in critical infrastructures (Vol. 297). Springer International Publishing.

[11] Cortés, J., Dullerud, G. E., Han, S., Le Ny, J., Mitra, S., & Pappas, G. J. (2016, December). Differential privacy in control and network systems. In 2016 IEEE 55th Conference on Decision and Control (CDC) (pp. 4252–4272). IEEE.

[12] Awotunde, J. B., Adeniyi, A. E., Babatunde, A. O., Olagunju, M., Imoize, A. L., & Olanloye, O. D. (2024). 12 An Cryptographic Enhanced Lightweight Algorithm Towards Securing Wireless Networks and Big Data. Computational Modeling and Simulation of Advanced Wireless Communication Systems, 297.

[13] Abdulraheem, M., Adeniyi, E. A., Awotunde, J. B., Imoize, A. L., Jimoh, R. G., Oladipo, I. D., & Falola, P. B. (2024). Artificial Intelligence of Medical Things for Medical Information Systems Privacy and Security. In Handbook of Security and Privacy of AI-Enabled Healthcare Systems and Internet of Medical Things (pp. 63–96). CRC Press.

[14] Paridari, K., O'Mahony, N., Mady, A. E. D., Chabukswar, R., Boubekeur, M., & Sandberg, H. (2017). A framework for attack-resilient industrial control systems: Attack detection and controller reconfiguration. Proceedings of the IEEE, 106(1), 113–128.

[15] Feng, C., Palleti, V. R., Mathur, A., & Chana, D. (2019, February). A Systematic Framework to Generate Invariants for Anomaly Detection in Industrial Control Systems. In NDSS (pp. 1–15).

[16] Moustafa, N., Creech, G., & Slay, J. (2017). Big data analytics for intrusion detection system: Statistical decision-making using finite Dirichlet mixture models. Data Analytics and Decision Support for Cybersecurity: Trends, Methodologies and Applications, 127–156.

[17] Rajesh, N., Sujatha, K., & Lawrence, A. A. (2016). Survey on privacy preserving data mining techniques using recent algorithms. International Journal of Computer Applications, 133(7), 30–33.

[18] Aggarwal, C. C., & Yu, P. S. (2008). A general survey of privacy-preserving data mining models and algorithms (pp. 11–52). Springer US.

[19] Abiodun, M. K., Imoize, A. L., Awotunde, J. B., Lee, C. C., Adeniyi, A. E., Chioma, U., & Li, C. T. (2023). Analysis of a Double-stage Encryption Scheme Using Hybrid Cryptography to Enhance Data Security in Cloud Computing Systems. Journal of Library & Information Studies, 21(2).

[20] Adeniyi, A. E., Jimoh, R. G., & Awotunde, J. B. (2024). A systematic review on elliptic curve cryptography algorithm for the internet of things: Categorization, application areas, and security. Computers and Electrical Engineering, 118, 109330.

[21] Ferrag, M. A., Maglaras, L. A., Janicke, H., & Jiang, J. (2016). A survey on privacy-preserving schemes for smart grid communications. arXiv preprint arXiv:1611.07722.

[22] Awotunde, J. B., Adeniyi, A. E., Babatunde, A. O., Olagunju, M., Imoize, A. L., & Olanloye, O. D. (2024). 12 An Cryptographic Enhanced Lightweight Algorithm Towards Securing Wireless Networks and Big Data. Computational Modeling and Simulation of Advanced Wireless Communication Systems, 297.

[23] Awotunde, J. B., Farhaoui, Y., Imoize, A. L., Folorunso, S. O., & Adeniyi, A. E. (2023, November). An Enhanced Internet of Medical Things Data Communication Based on Blockchain and Cryptography for Smart Healthcare Applications. In The International Conference on Artificial Intelligence and Smart Environment (pp. 305–313). Cham: Springer Nature Switzerland.

[24] Zhu, T., Xiong, P., Li, G., Zhou, W., & Philip, S. Y. (2020). Differentially private model publishing in cyber-physical systems. Future generation computer systems, 108, 1297–1306.

[25] Zhu, T., Li, G., Zhou, W., & Philip, S. Y. (2017). Differential privacy and applications. Cham, Switzerland: Springer International Publishing.

[26] Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustainable Cities and Society, 50, 101660.

[27] Imoize, A. L., Balas, V. E., Solanki, V. K., Lee, C. C., & Obaidat, M. S. (Eds.). (2023). Handbook of Security and Privacy of AI-Enabled Healthcare Systems and Internet of Medical Things. CRC Press.

[28] Adeniyi, A. E., Abiodun, K. M., Awotunde, J. B., Olagunju, M., Ojo, O. S., & Edet, N. P. (2023). Implementation of a block cipher algorithm for medical information security on cloud environment: using modified advanced encryption standard approach. Multimedia Tools and Applications, 82(13), 20537–20551.

[29] AbdulRaheem, M., Awotunde, J. B., Chakraborty, C., Adeniyi, E. A., Oladipo, I. D., & Bhoi, A. K. (2023). Security and privacy concerns in the smart healthcare system. In Implementation of Smart Healthcare Systems using AI, IoT, and Blockchain (pp. 243–273). Academic Press.

[30] Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Differential privacy techniques for cyber-physical systems: A survey. IEEE Communications Surveys & Tutorials, 22(1), 746–789.

[31] Boulemtafes, A., Derhab, A., & Challal, Y. (2020). A review of privacy-preserving techniques for deep learning. Neurocomputing, 384, 21–45.

[32] Li, C. T., Weng, C. Y., Chen, C. L., Lee, C. C., Deng, Y. Y., & Imoize, A. L. (2022). An efficient authenticated key agreement scheme supporting privacy-preservation for internet of drones communications. Sensors, 22(23), 9534.

[33] Raisaro, J. L., Choi, G., Pradervand, S., Colsenet, R., Jacquemont, N., Rosat, N., ... & Hubaux, J. P. (2018). Protecting privacy and security of genomic data in i2b2 with homomorphic encryption and differential privacy. IEEE/ACM transactions on computational biology and bioinformatics, 15(5), 1413–1426.

[34] Abi Sen, A. A., Eassa, F. A., Jambi, K., & Yamin, M. (2018). Preserving privacy in the internet of things: a survey. International Journal of Information Technology, 10, 189–200.

[35] Ramadan, R., Huang, Q., Zalhaf, A. S., Bamisile, O., Li, J., Mansour, D. E. A., ... & Yehia, D. M. (2024). Energy Management in Residential Microgrid Based on Non-Intrusive Load Monitoring and Internet of Things. Smart Cities, 7(4), 1907–1935.

[36] Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Differential privacy techniques for cyber-physical systems: A survey. IEEE Communications Surveys & Tutorials, 22(1), 746–789.

[37] Sain, M., Normurodov, O., Hong, C., & Hui, K. L. (2021, February). A survey on the security in cyber-physical systems with multi-factor authentication. In 2021 23rd International Conference on Advanced Communication Technology (ICACT) (pp. 1–8). IEEE.

[38] Sudarsan, S. V., Schelén, O., & Bodin, U. (2021). Survey on delegated and self-contained authorization techniques in CPS and IoT. IEEE Access, 9, 98169–98184.

[39] Adeniyi, J. K., Ajagbe, S. A., Adeniyi, E. A., Mudali, P., Adigun, M. O., Adeniyi, T. T., & Ajibola, O. (2024). A biometrics-generated private/public key cryptography for a blockchain-based e-voting system. Egyptian Informatics Journal, 25, 100447.

[40] Mishra, A., Jha, A. V., Appasani, B., Ray, A. K., Gupta, D. K., & Ghazali, A. N. (2023). Emerging technologies and design aspects of a next-generation cyber-physical system with a smart city application perspective. International Journal of System Assurance Engineering and Management, 14(Suppl 3), 699–721.

[41] Dafflon, B., Moalla, N., & Ouzrout, Y. (2021). The challenges, approaches, and used techniques of CPS for manufacturing in Industry 4.0: a literature review. The International Journal of Advanced Manufacturing Technology, 113, 2395–2412.

[42] Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustainable Cities and Society, 50, 101660.

[43] Mohammed, A. S., Reinecke, P., Burnap, P., Rana, O., & Anthi, E. (2022). Cybersecurity challenges in the offshore oil and gas industry: an industrial cyber-physical systems (ICPS) perspective. ACM Transactions on Cyber-Physical Systems (TCPS), 6(3), 1–27.

[44] Jeffrey, N., Tan, Q., & Villar, J. R. (2023). A review of anomaly detection strategies to detect threats to cyber-physical systems. Electronics, 12(15), 3283.

[45] Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues, and future trends. Microprocessors and Microsystems, 77, 103201.

[46] Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Alazab, M., ... & Gadekallu, T. R. (2022). Federated learning for intrusion detection system: Concepts, challenges, and future directions. Computer Communications, 195, 346–361.

[47] So, J., Guler, B., & Avestimehr, S. (2020). A scalable approach for privacy-preserving collaborative machine learning. Advances in Neural Information Processing Systems, 33, 8054–8066.

[48] Cao, L. (2022). AI science and engineering: a new field. IEEE Intelligent Systems, 37(1), 3–13.

[49] Rani, S., Kataria, A., Chauhan, M., Rattan, P., Kumar, R., & Sivaraman, A. K. (2022). Security and privacy challenges in the deployment of cyber-physical systems in smart city applications: State-of-art work. Materials Today: Proceedings, 62, 4671–4676.

[50] Su, G., Wang, J., Xu, X., Wang, Y., & Wang, C. (2024). The Utilization of Homomorphic Encryption Technology Grounded on Artificial Intelligence for Privacy Preservation. International Journal of Computer Science and Information Technology, 2(1), 52–58.

[51] Greer, C., Burns, M., Wollman, D., & Griffor, E. (2019). Cyber-physical systems and Internet of things.

[52] Balla, A., Habaebi, M. H., Islam, M. R., & Mubarak, S. (2022). Applications of deep learning algorithms for Supervisory Control and Data Acquisition intrusion detection system. Cleaner Engineering and Technology, 9, 100532.

[53] Pivoto, D. G., De Almeida, L. F., da Rosa Righi, R., Rodrigues, J. J., Lugli, A. B., & Alberti, A. M. (2021). Cyber-physical systems architectures for industrial Internet of things applications in Industry 4.0: A literature review. Journal of manufacturing systems, 58, 176–192.

[54] Alkofahi, H., Alawneh, H., & Skjellum, A. (2024). MitM attacks on intellectual property and integrity of additive manufacturing systems: A security analysis. Computers & Security, 140, 103810.

[55] Wang, L., & Haghighi, A. (2016). The combined strength of holons, agents, and function blocks in cyber-physical systems. Journal of Manufacturing Systems, 40, 25–34.

[56] Antons, O., & Arlinghaus, J. C. (2022). Data-driven and autonomous manufacturing control in cyber-physical production systems. Computers in Industry, 141, 103711.

[57] Liu, Y., Tao, X., Li, X., Colombo, A. W., & Hu, S. (2023). Artificial intelligence in smart logistics cyber-physical systems: State-of-the-art and potential applications. IEEE Transactions on industrial cyber-physical systems, 1, 1–20.

[58] Shaikh, T. A., Rasool, T., & Verma, P. (2023). Machine intelligence and medical cyber-physical system architectures for smart healthcare: Taxonomy, challenges, opportunities, and possible solutions. Artificial Intelligence in Medicine, 102692.

[59] Alotaibi, I., Abido, M. A., Khalid, M., & Savkin, A. V. (2020). A comprehensive review of recent advances in smart grids: A sustainable future with renewable energy resources. Energies, 13(23), 6269.

[60] Adedeji, K. B., & Hamam, Y. (2020). Cyber-physical systems for water supply network management: Basics, challenges, and roadmap. Sustainability, 12(22), 9555.

[61] Juma, M., & Shaalan, K. (2020). Cyber-physical systems in the smart city: Challenges and future trends for strategic research. In Swarm Intelligence for Resource Management in the Internet of Things (pp. 65–85). Academic Press.

[62] Peladarinos, N., Piromalis, D., Cheimaras, V., Tserepas, E., Munteanu, R. A., & Papageorgas, P. (2023). Enhancing smart agriculture by implementing digital twins: A comprehensive review. Sensors, 23(16), 7128.

[63] Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in the blockchain system. Journal of network and computer applications, 126, 45–58.

[64] Marino, F., Moiso, C., & Petracca, M. (2019). PKIoT: A public key infrastructure for the Internet of Things. Transactions on Emerging Telecommunications Technologies, 30(10), e3681.

[65] Gunawan, D. (2020). Classification of privacy preserving data mining algorithms: a review. Jurnal Elektronika dan Telekomunikasi, 20(2), 36–46.

[66] Matta, P., Arora, M., & Sharma, D. (2021). A comparative survey on data encryption Techniques: Big data perspective. Materials today: proceedings, 46, 11035–11039.

[67] Maleh, Y., Lakkineni, S., Tawalbeh, L. A., & AbdEl-Latif, A. A. (2022). Blockchain for cyber-physical systems: Challenges and applications. Advances in blockchain technology for cyber-physical systems, 11–59.

[68] Azizi, N., Malekzadeh, H., Akhavan, P., Haass, O., Saremi, S., & Mirjalili, S. (2021). IoT–blockchain: Harnessing the power of the Internet of Things and blockchain for the smart supply chain. Sensors, 21(18), 6048.

[69] Salau, B. A., Rawal, A., & Rawat, D. B. (2022). Recent advances in artificial intelligence for wireless internet of things and cyber-physical systems: A comprehensive survey. IEEE Internet of Things Journal, 9(15), 12916–12930.

[70] Jamal, A. A., Majid, A. A. M., Konev, A., Kosachenko, T., & Shelupanov, A. (2023). A review on security analysis of cyber-physical systems using Machine learning. Materials today: proceedings, 80, 2302–2306.

[71] Luo, L., Morales-Gonzalez, C., Wang, S., Ling, Z., & Fu, X. (2024, February). Unified View of IoT and CPS Security and Privacy. In 2024 International Conference on Computing, Networking, and Communications (ICNC) (pp. 495–499). IEEE.

[72] Omolara, A. E., Alawida, M., & Abiodun, O. I. (2023). Drone cybersecurity issues, solutions, trend insights, and future perspectives: a survey. Neural computing and applications, 35(31), 23063–23101.

[73] Wang, Z., Xie, W., Wang, B., Tao, J., & Wang, E. (2021). A survey on recent advanced research of CPS security. Applied Sciences, 11(9), 3751.

[74] Abdulhussein, M. (2024). The Impact of Artificial Intelligence and Machine Learning on Organizations Cybersecurity. Liberty University.

[75] Horváth, I. (2022). Designing next-generation cyber-physical systems: Why is it an issue? Journal of Integrated Design and Process Science, 26(3–4), 317–349.

Author Queries

		Pageno.
AQ1	The sentence beginning 'Since CPS systems gradually draw in enthusiastic, competent hackers…' has been altered for clarity, please check that the meaning is correct.	294
AQ2	The sentence beginning 'To optimize these procedures, ML models can make …' has been altered for clarity, please check that the meaning is correct.	310