Journal of Autonomous Intelligence (2024) Volume 7 Issue 4
doi: 10.32629/jai.v7i4.1336

REVIEW ARTICLE

Security in cyber physical systems: Transformation and challenges

Sandeep Singh Bindra[*], Alankrita Aggarwal

Department of Computer Science & Engineering, Chandigarh University, Mohali 140413, India

*** Corresponding author:** Sandeep Singh Bindra, sandeep.bindra@gmail.com

ABSTRACT

Network technology has significantly improved due to the growing use of Cyber-Physical Systems (CPS) in various industries, including healthcare, transportation, and communication. The efficiency of these domains has increased overall due to the transmission of sensor data to the cloud and its use by various apps. However, increased data transfer increases the risk of unauthorized modification and data breaches. The degree of risk varies per domain, and security is a crucial area of concentration to mitigate these concerns. Significant developments in network technology have resulted from the growing use of Cyber-Physical Systems (CPS) in various industries, including healthcare, transportation, and communication. The efficiency of these fields has increased overall due to sensor data being sent to the cloud and used by various applications. However, data breaches and unauthorized alteration are risks that come with increased data flow. Depending on the domain, the risk level varies, and security is a key concern in addressing these concerns.

Keywords: CPS; security; attacks

ARTICLE INFO

Received: 10 October 2023
Accepted: 27 October 2023
Available online: 2 February 2024

1. Introduction

The evolution of networks from local area networks to large-scale systems like the Internet has enabled the creation of Cyber-Physical Systems (CPS), which combine physical and cyber components to monitor and control physical processes in real-time[1]. Industry sectors where CPS has gained importance include manufacturing, healthcare, transport, and smart cities[2]. Automation has even ushered in a new age marked by the integration of autonomous vehicles at the nexus of agriculture and CPS[3,4]. The network infrastructure makes CPS's flawless and effective operation possible, which permits communication between physical and cyber components. Because it must offer high reliability, low latency, and high bandwidth to meet the real-time needs of physical processes, network architecture is essential to the success of CPS. Furthermore, to guarantee system availability and performance, CPS networks are frequently constructed with redundancy, failover methods, and load balancing[5].

Numerous factors, including interoperability, scalability, safety, and dependability, must be considered by CPS. The system must safeguard the privacy of users and stakeholders while being scalable, reliable, and safe to use. The system also has to be able to interface with other systems and withstand increased workload without degrading[6]. A thorough methodology that considers these problems must be used in their design and implementation to enable the proper operation of CPS. However, security is a top priority for CPS networks since these networks are vulnerable to cyberattacks that might have disastrous consequences[7]. Malicious actors can infiltrate CPS networks to seize control of physical processes, posing risks to safety and security. Building CPS networks with security is essential to prevent illegal access and attacks. It involves adding functions like intrusion detection systems, encryption, and access control.

1.1. Motivation

In order to ensure the secure and efficient operation of these systems, secure communication protocols have been developed in response to the growing requirement for communication between physical and cyber components in CPS. Its communication's security level may be examined to find flaws and raise the system's overall security. It can deliver the finest service while strengthening security by maintaining users' and stakeholders' dependability, safety, and privacy. In order to reduce any possible dangers or threats, there is an increasing focus on analyzing and enhancing the security level of CPS communication protocols.

1.2. Related surveys

Several recent studies have investigated various aspects of Cyber-Physical Systems (CPS), including their security systems, integration with cloud computing and big data for healthcare, game theory, resilience assessment, intrusion response systems, and artificial intelligence approaches. Hasan et al.[8] examined the protocols for and present difficulties with smart grid cyber-physical and cyber security systems. They also established relationships among various things, such as technology, applications, and communication protocols and standards, and provided suggestions in light of those findings. A survey on combining cyber-physical systems, cloud computing, and big data for healthcare systems was given by Gupta and Singh[9]. They emphasized the healthcare sector's fundamental difficulties and unresolved problems while highlighting CPS's technical advancements. In particular, Tushar et al.[10] discuss the CPS and offer information on the applicability of game theory. Additionally, various game theoretic approaches and CPS types were discussed, and it was discovered that game theory applies to the same. This survey aided in the game-theoretic identification of the CPS. A CPS resilience assessment approach was created by Cassottana et al.[11] based on an analysis of the literature on disruption incidence. They used a case study to analyze the effects of interruption.

In a survey on cyber threats in CPS, Duo et al.[12] published their findings. They looked at the event- and time-driven systems and especially paid attention to confidentiality, availability, and integrity. They covered the attacks on availability and integrity in great depth. Additionally, unresolved problems and difficulties offer researchers a direction for future investigations. In their review of intrusion response systems from 2023, Bashendy et al.[13] examined strategies for keeping the CPS secure from threats, including cyberattacks. They discovered that techniques based on reinforcement learning (RL) were better suitable from the perspective of CPS security. Focusing on artificial intelligence methods, Salau et al.[14] propose a survey for CPS. They reviewed several machines learning techniques, including distributed, federated, and transfer learning — All of which the researchers have previously used to learn enormous amounts of data — And predictions in the CPS with IoT. They also emphasized the difficulties associated with these techniques. Additionally, concentrating on CPS security, Kim et al.[15] review various attack detection techniques. They provided numerical examples and focused on anomaly identification in physics, networks, and machine learning. Additionally, they offer the researchers a route for further development.

Further, a study of security topics like attacks and vulnerabilities was done by Agrawal and Kumar[16], emphasizing Industrial CPS. They also covered a decade survey, numerous security difficulties, and research challenges. For further information on applying deep reinforcement learning algorithms in CPS, see Rupprecht and Wang[17]. They concentrated on activities requiring motor control and resource allocation.

1.3. Contribution of paper

This paper's contribution is that it presents an approach-wise and attack-wise analysis to provide a distinct viewpoint on security issues in CPS. The article outlines the security vulnerabilities in CPS and offers solutions and advice to deal with them. This work adopts a broader perspective to analyze the security risks of CPS, in contrast to other publications that concentrate on a specific area or architecture and attacks. In light of this, this paper presents an improved understanding of CPS's security issues and offers insightful advice on making CPS more secure.

1.4. Survey architecture

This survey article discusses several CPS-related concepts, such as architecture, security issues, security measures against technology and assaults, difficulties, and suggestions, as shown in **Figure 1**. A screening procedure to weed out pertinent articles was used during the survey, and the findings were also included. An in-depth discussion of the CPS architecture is followed by a presentation of security issues and possible security measures from both a technological and an attack standpoint. The conclusion summarises the results of the survey and includes recommendations and challenges.

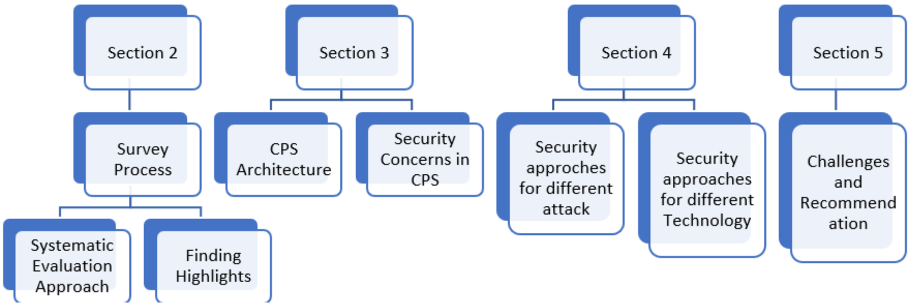

Section 2
Section 3
Section 4
Section 5
Survey Process
CPS Architecture
Security Concerns in CPS
Security approches for different attack
Security approaches for different Technology
Challenges and Recommend ation
Systematic Evaluation Approach
Finding Highlights

Figure 1. Survey architecture of the security issues of the CPS architecture.

2. Survey process

Researchers frequently employ various strategies to create an all-encompassing evaluation, and it takes careful preparation and execution to write a systematic survey[18,19]. This survey article's distinctive design offers a detailed review of the available literature on the selected topic by drawing influence from diverse writing styles. The technique used, which covers the search procedure, inclusion and exclusion criteria, data collecting, and data analysis, is thoroughly described in this section. In addition, the survey attempts to reduce the possibility of bias and ensure that all pertinent studies are included in the analysis using a systematic method. So, Survey results are also highlighted in this section.

2.1. Systematic evaluation approach

In order to achieve a complete and comprehensive analysis of the literature, many crucial stages were taken in the writing process for this survey paper. Defining the survey's scope, including the particular domains and architectures that would be covered, and the research question came first. The next step was preliminary searching for pertinent articles using different databases and search engines. After that, publications that matched the study topic and scope were chosen from the search results using inclusion and exclusion criteria that had been predetermined. After the first screening, the papers underwent a more thorough examination, which included a critical assessment of the methodologies, findings, and conclusions made in each piece. The unique CPS designs, security issues, and methods covered in each paper were then the subject of data extraction. In order to find recurring themes and patterns in the literature, the data obtained were analyzed and synthesized. The results were then organized and presented, with an emphasis on offering suggestions and insights for further study and improvement in the area of CPS security. Overall, the strategy employed in this survey article was created to guarantee a rigorous and thorough examination of the literature and to offer insightful information about the state of CPS security research at the time of writing.

Research questions: This paper focuses on the following research questions to analyze and provide future directions. Moreover, the scope of each research question is also deliberated in the **Table 1**:

Table 1. Research questions and scope.

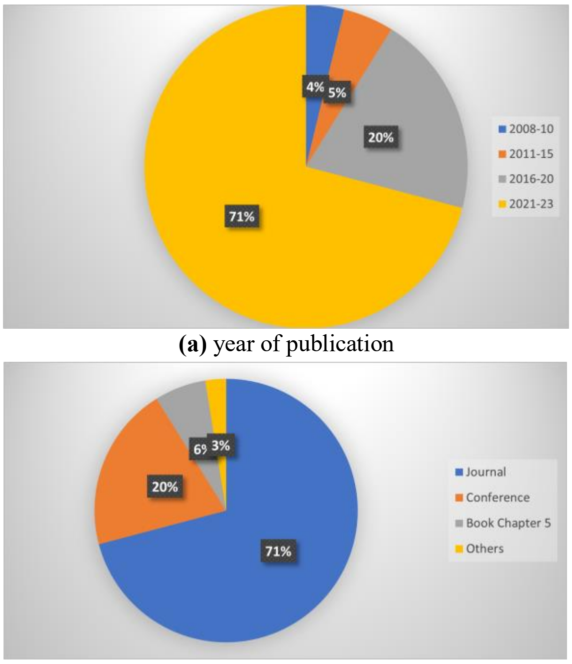
Sr. No.	Research questions	Scope
RQ1	What are the security concerns and challenges in cyber-physical systems (CPS) architecture design?	This question focuses on the security concerns and challenges in CPS architecture design.
RQ2	How practical are different security approaches and techniques in mitigating cyber threats?	This question looks at the effectiveness of various security approaches and techniques.
RQ3	What are the most common types of attacks in the CPS, and what strategies are most effective in preventing and responding to them?	This question examines common cyber-attacks and strategies to prevent and respond to them.
RQ4	How can machine learning or deep learning techniques enhance network security?	This question looks at the use of machine learning in network security.
RQ5	What are the current challenges of security in CPS?	This question focuses on security limitations based on future directions that will be provided

Search process: This comprehensive search seeks to locate pertinent research works from reputable electronic sources and premier CPS security conferences. The study looks at several security measures for CPS, including attack and other risks and security approaches based on [learning| optimization| trust| cryptography]. Many well-known electronic databases are used to gather a wealth of data for the study, including Springer, IEEE, Elsevier, Google Scholar, Wiley, MDPI, and others. The abundance of research papers and publications on CPS security in these databases makes them the ideal resource for this investigation.

Inclusion and exclusion criteria: This comprehensive examination of the literature focuses on the security of CPS and includes quantitative and qualitative research studies published between 2008 and 2023. Keywords like "Security Risks in CPS", "Attacks in CPS" and "Security Approaches in CPS" were used, as well as the search terms "Security Approach [in, for] [name of attack] [in, for] CPS" and "Security [threats, vulnerabilities, attacks] [in, for] CPS" to find pertinent literature. Many research studies in this field were considered based on the provided search phrases. The search used various electronic sources, including books, journals, and conference proceedings. Based on the suitability of their methodology, databases, journals, and conferences as selection criteria for this study, pertinent papers were chosen.

Data collection and analysis: The research papers are chosen according to predetermined inclusion and exclusion criteria to cover the majority of security measures for significant CPS attacks. Therefore, all of the information is gathered from the specified electronic databases and taken into account for this research study. Additionally, the analysis of the gathered data is based on different years, journals, conferences, and book chapters. As a result, the following **Figure 2** computes and displays the distribution of all the obtained data year-wise, journal-wise, and conference-wise.

After carefully evaluating the systematic survey, the screening procedure's findings have been presented clearly and aesthetically attractive. The total number of articles found during the first search process is shown in **Figure 3** below, along with the number of pertinent articles that made it past the second phase filter procedure and were finally chosen for inclusion in the survey. This concise and helpful summary of the screening findings offers essential information about the breadth and depth of the survey.



(a) year of publication

(b) type of source

Figure 2. Analysis of the literature: **(a)** year of publication; **(b)** type of source.

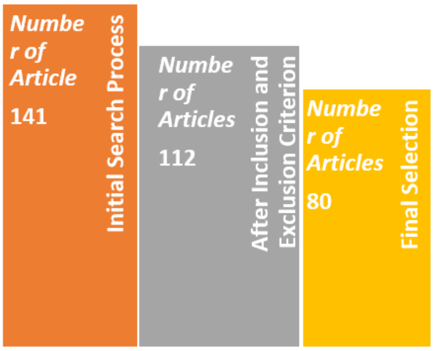


Figure 3. Screening results.

2.2. Findings highlight

According to a comprehensive review of CPS architecture and security, this area has several security-related challenges. Network security, data security, system security, and physical security are the security issues discovered. The poll also revealed that CPS is subject to a variety of assaults. Different strategies to counteract these attacks were put forth in the research papers evaluated for the survey, including intrusion detection systems, machine learning-based strategies, and cryptographic techniques. The poll also highlights several difficulties in putting these security measures into practice. Future directions for field researchers and practitioners are suggested by the survey's conclusion, including creating standardized CPS security procedures and more effective security solutions. **Figure 4** highlights the finding of the survey.

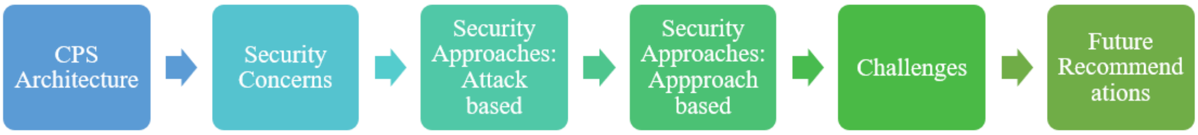

CPS Architecture
Security Concerns
Security Approaches: Attack based
Security Approaches: Appproach based
Challenges
Future Recommend ations

Figure 4. Findings of the survey.

3. CPS architecture and security

Cyber-physical systems (CPS) are a new technology that combines computation and communication with physical processes. Transportation, industry, healthcare, and vital infrastructure are just a few sectors that employ these systems. CPS can lower expenses while increasing automation and system efficiency. However, to ensure their safe and secure operation, they also present new security issues that must be resolved. Physical processes, computational systems, and communication networks make up the CPS, which is a complex system[20]. Machines, sensors, and other physical objects may be used in CPS as physical processes. Physical processes are controlled by computer systems made up of hardware and software, and data and commands may be sent back and forth between the computing systems and physical processes thanks to communication networks[21].

A few advantages of CPS are better system effectiveness, increased automation, and cost savings[22]. These advantages do, however, come with considerable security dangers. CPS is susceptible to cyberattacks, which may have dire repercussions. An assault on a healthcare system, on the other hand, may result in fatalities. As an illustration, an attack on a transport system might cause accidents. Therefore, protecting the physical components from cyber-attacks is one of the primary security considerations for CPS. Attackers may utilize weaknesses in the CPS's physical components to destroy the system or access private information[23]. For instance, a hacker may access the sensors in a manufacturing facility and change how things are made or steal private data.

3.1. CPS architecture

For physical and digital components to interact and communicate, a system's architecture is referred to as a "cyber-physical system" (CPS). Control systems, communication networks, computing systems, and physical processes are just a few of the many disciplines that must be integrated for contemporary systems to be developed, implemented, and managed[24]. The four main parts of a CPS architecture are generally sensors, controllers, communication networks, and actuators, as shown in **Figure 5**. Physical phenomena like temperature, pressure, or motion must be detected, measured, and converted by sensors into digital data that controllers can process. In order to carry out the necessary activities, controllers must analyze the sensor data, make judgments, and operate the actuators[25]. Actuators oversee the carrying out of physical actions based on the decisions made by the controllers, while communication networks permit information interchange between the different CPS components.

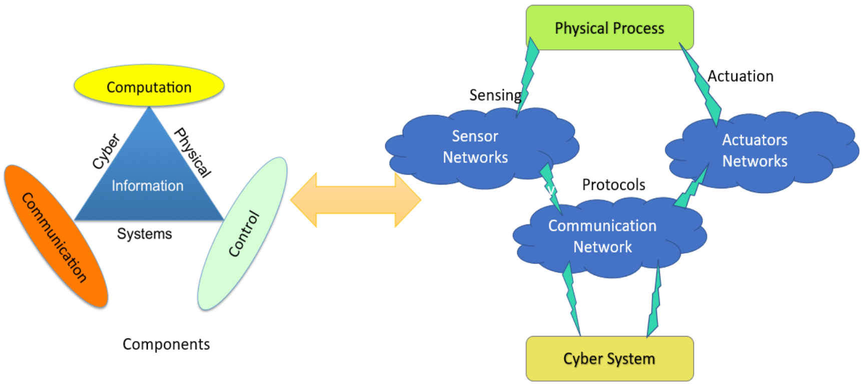


Figure 5. Components of the CPS architecture.

Based on its functionality, which may be divided into three basic categories: control, sensing, and actuation, the CPS architecture can be further categorised[26]. In a control-based CPS architecture, each physical component of the system is monitored and controlled by a single central controller. In a sensing-based CPS architecture, the emphasis is on using sensors to measure physical variables in real-time and with high accuracy.

On the other hand, actuator-based CPS design emphasizes the execution of physical activities via actuators according to decisions made by the controller. Integration of cyber and physical systems is a critical component of CPS architecture. The creation of a virtual model of the physical system that is used to design and test the cyber system, as well as co-simulation, which involves simulating the physical and cyber systems simultaneously, are two techniques that can be used to achieve this integration. The CPS design must also take security and safety concerns into account. These challenges may be resolved using various strategies, including access control, data encryption, and failure detection and recovery.

3.2. Security concerns in CPS

This section deliberates in detail on different security concerns of CPS, including threats, vulnerabilities, and attacks, also highlighted in **Table 2**.

3.2.1. CPS security threats

The combination of physical and cyber dangers to CPS security results in cyber-physical hazards, a severe worry that must be addressed immediately. Alguliyev et al.[27] state that the primary emphasis of their study is on cyber risks since they provide a severe risk to Industrial IoT security because of the weaknesses caused by advanced metering infrastructure and SCADA problems. Electronic assaults are becoming simpler to launch from any machine, unlike physical attacks that need a physical presence and precise tools, and their impacts are compounded by the smart meter's sensitivity to far-off threats. As a result, without adequate defenses and preventative measures, minimizing and resisting electronic attacks is difficult, as further corroborated by Cleveland[28], Metke and Ekl[29], and other sources.

CPS systems are additionally susceptible to several dangers, such as wireless exploitation, wireless jamming or de-authentication waves, surveillance, remote access, information disclosure, unauthorized access, interception, GPS exploitation, and information gathering, all of which have the potential to have detrimental effects like industrial espionage, financial losses, and blackouts. In addition, these dangers breach ethical standards and undermine privacy and data confidentiality, integrity, and availability.

Physical threats, including physical loss, damage, and maintenance concerns, represent a severe risk to CPS security[30]. The sub-stations are less secure and more vulnerable to disruption and sabotage, even if the power-generating stations are heavily guarded. The most concerning scenario is when a hostile attacker malfunctions many substations since it might result in a total blackout of large urban areas for several hours. Self-healing systems that detect defects or disruptions contain the problem and alert the appropriate management system can help reduce the dangers brought on by physical threats to CPS. However, to avoid aggressive theft or physical tampering, it is still necessary to increase backup capacity for crucial components and strengthen access controls, authentication, and authorization systems, including password-based, biometric, and access cards.

Table 2. Security concerns in CPS (literature analysis).

Authors	Risks	Application	Remarks	Security Requirement
Alguliyev et al.[27]	Cyber Security Risks	CPS	Difficult to Control or Handle	Yes
Cleveland[28]	Cyber Security Risks	Automated Meter Reading (AMR) technologies	Encryption is not the only solution	Yes
Metke and Ekl[29]	Cyber Security Threats	Smart Grid Systems	access and communication capabilities for wide-area networks	Yes
Yaacoub et al.[30]	Cyber Security Threats	Internet of Cyber-Physical Things	cryptographic and non-cryptographic solutions for security threats	Yes

Table 2. (*Continued*).

Authors	Risks	Application	Remarks	Security Requirement
Kitchin and Dodge[31]	CPS Vulnerabilities	Smart City	Both remedial and preventive approaches can help to mitigate the attackers	Yes
Basan et al.[32]	CPS vulnerabilities	Smart Factory	Different security protocols can be used	Yes
Duo et al.[12]	Security Attacks	CPS	Availability, integrity, and confidentiality are the potential attackers	Yes
Ju et al.[33]	Security Attacks	Adhoc CPS	Reliability directly breaches security	Yes

3.2.2. CPS vulnerabilities

The primary objective of industrial espionage, sometimes referred to as active assaults or reconnaissance, is the vulnerability in a security defect. As a result, vulnerability assessment, which seeks to determine remedial and preventative methods to remove, mitigate, or decrease the risk of vulnerabilities, places a high priority on finding weaknesses[31]. Network, platform, and management vulnerabilities are the three main types of vulnerabilities that might develop in CPS. Assumption and isolation, growing connectedness, heterogeneity, USB usage, unethical behavior, espionage, homogeneity, and suspicious personnel are just a few of the elements that contribute to CPS vulnerabilities. One of the main categories of CPS vulnerabilities is cyber vulnerability, which includes dangers from widely used standard protocols like TCP/IP and ICCP that lack basic security measures. Malware like Stuxnet, Duqu, RED October, Gauss, Shamoon, Mahdi, and Slammer Worm can also lead to cyber vulnerabilities[32].

Short-range wireless communications and open/wireless protocols like Ethernet are susceptible to attacks, including meet-in-the-middle, sniffing, eavesdropping, wiretapping, wardialing, botnets, Trojan attacks, rootkit attacks, and replay attacks. Wireless communications over a long distance are vulnerable to intrusion and eavesdropping. SQL injection is still the most prevalent online vulnerability because it enables attackers to get unauthorized access to any server database[34]. Medical equipment that depends on wireless communications is also vulnerable to several wireless attacks, such as jamming, replay, and modification attacks. Similar protocols like ICS, DNP3, and Modbus can be used in the architecture of intelligent grid power systems, making them susceptible to the same kinds of flaws. For CPS to be safe and secure, it is essential to recognize and fix its flaws. It is necessary to conduct vulnerability assessments regularly to spot possible dangers and implement corrective and preventative action. To protect against cyber vulnerabilities, it is crucial to implement security measures such as encryption, authentication, and authorization.

3.2.3. Security attacks

This section describes numerous physical and cyber-based assault strategies aimed against various CPS system components. Physical assaults, including various types, have been more common, especially in industrial CPS systems[12]. For example, attackers can deploy stealth malware that distributes harmful software through infected objects, such as contaminated USBs, CDs, drives, and gadgets. Additionally, they can abuse the privilege when unapproved access is granted to server rooms and installation facilities. This enables attackers to insert malicious USBs, steal data, run malicious programs, or infect the device using keystrokes. Other examples of physical assaults include wire cuts, taps, dialing, fake identities, stalkers, CCTV camera interception, key-card hijacking, physical breaches, third-party malicious software providers, and power abuse.

However, there has been an increase in the number of cyberattacks against CPS and IoCPT, and recent research has shown that CPS is particularly susceptible to attacks involving malicious code injection, code reuse, false data injection, Control-Flow Attestation (C-FLAT), and zero-control data. These assaults can potentially shut down CPS industrial systems and equipment entirely. Eavesdropping, cross-site scripting (XSS), SQL injection or SQLi, password cracking, and phishing—which can come in various forms, including spear phishing and vishing—Are all examples of cyberattacks[35]. To secure CPS systems, it is essential to stop these assaults from intensifying, especially in countries like Lebanon, where a lack of cybersecurity reveals severe issues with potentially serious repercussions.

4. Security approaches for CPS: Technology and attack perspectives

The section discusses various security approaches for Cyber-Physical Systems (CPS). With the increasing number of cyber-attacks on CPS, it is crucial to have adequate security measures in place to prevent unauthorized access, data breaches, and other malicious activities. Moreover, this section discusses these approaches in two sub-sections, where the first sub-section highlights the development of security based on attack, and the other section highlights the approaches based on the technology domain.

4.1. Security approaches for different attack

There are several attacks based on which different security techniques were earlier developed by the researchers. In this work, the most commonly existing attacks in CPS are discussed below, along with the security approaches developed. **Table 3** highlights the approaches used for security measures specific to the given attacks:

Table 3. Security approaches w.r.t attacks.

Attack	**Approach**
Eavesdropping Attack	Artificial Noise-based Approach[33]
	Encoding-Decoding[36]
	Key Generation and Digital Signature[37]
	deep learning[38]
	Long-range key generation[39]
	intrusion detection systems (IDS)[40]
	AI and blockchain[41]
Phishing Attack	Routing-based Approach [10.1016/j.psep.2021.03.004]
	Cloud-based Approach [10.1016/j.compind.2022.103715]
	IDS[42]
	Blockchain[43]
	machine learning[44]
	Feature selection[45]
DoS and DDoS Attack	machine learning[46]
	deep learning[47]
	IDS[48]
	Threshold[49]
Malware Attacks	snake optimizer with graph convolutional network[50]
	ensemble learning[51]
	deep learning[52]
	trust-based Approach[53]
	cryptography[54]

Eavesdropping attack: An eavesdropping assault is a sort of cyberattack in which the attacker secretly intercepts and keeps track of the conversation between two parties. Gaining access to sensitive or secret information, such as login credentials, financial information, or personal information, is the aim of an eavesdropping assault. Attacks to eavesdrop can be carried out using various methods, including sniffing, packet capture, or wiretapping. In addition, attackers can intercept and read unencrypted network traffic over unprotected wireless networks, frequently linked to this kind of assault. Different approaches are developed to prevent CPS from this attack for different applications. Like, Ju et al.[33] suggested a way to boost the secrecy performance in ad hoc networks by fusing millimeter-wave and physical layer security approaches. Their strategy uses artificial noise (AN) to produce interference that is impossible for listeners to cancel while considering the reliability-security tradeoff based on user requirements. Further, a decoding schedule that minimises the estimated error while remaining within the energy budget was proposed by Zhou et al.[36]. A recursive reset technique based on probabilistic quantizer features was also devised, enabling listeners to assess the precision of their predictions. They defined a circumstance in which eavesdropping performance increases and included a numerical illustration to illustrate the potency of their techniques. On the other hand, a key generation and digital signature technique based on Ring Learning with Error employing Lattice-based schemes was proposed by Golchha et al.[37]. The suggested Lattice-based Quantum Advanced Encryption Standard, which is used in this technology, provides quicker encryption, decryption, signature validation, and unique keys. Other than that, there are different approaches based on deep learning[38], Long range key generation[39], intrusion detection systems (IDS)[40], AI and blockchain[41], etc.

Phishing attack: Phishing is a sort of cyberattack in which attackers deceive victims into divulging personal data, such as usernames, passwords, and credit card numbers, by employing a variety of social engineering tactics. Phishing attacks may be incredibly destructive in CPS since they might jeopardize the system's security and integrity, potentially endangering users' physical safety. To deal with this attack and provide a level of security, different approaches were developed. Like, an approach to evaluate safety and security threats in CPS was put out by Ji et al.[55]. They provide an overview of attack route models (ARM) and their associated effects, develop a cyber security prevention route (CSPR) based on ARM, propose safety critical variable analysis (SCVA) to measure S&S risk and combine SCVA, CSPR, and physical safety prevention route (PSPR) using the bowtie method. The main addition is that CPS considers safety and security concerns simultaneously, and SCVA offers a quantitative evaluation of risk degree and severity. Further, by utilizing MARISMA, a security management methodology, and eMARISMA, a cloud-based technological environment, Rosado et al.[56] presented a novel technique to analyze risks in CPSs. The other approaches include IDS[42], Blockchain[43], machine learning[44], Feature selection[45], deep learning, etc.

DoS and DDoS attack: CPS are seriously threatened by denial-of-service (DoS) and distributed denial-of-service (DDoS) assaults. DDoS assaults use numerous hacked devices to initiate the attack, making it more challenging to identify and fight against than DoS attacks, which may take down the entire system by overloading it with excessive traffic. Critical infrastructure breakdowns brought on by these attacks, including those in transport and electricity networks, can hurt people physically and destroy technology. The potential of DoS and DDoS assaults grows as CPSs continue to interact with the Internet, underlining the necessity for strong security measures to stop and mitigate these attacks. Like other attacks, distinct approaches were developed based on machine learning[46,57], deep learning[47,58], IDS[48], Threshold[49], etc.

Malware attacks: Malware attacks are a significant concern for CPS, as they can cause severe damage to critical infrastructure. Malware can infiltrate systems through various means, such as phishing, social engineering, and software vulnerabilities. Once inside, it can cause damage by disrupting or manipulating operations, stealing sensitive information, or controlling the system. To prevent and mitigate the damage caused by malware attacks, security measures such as access control, intrusion detection, and anomaly detection must be implemented. In addition, regular updates and patches must be applied to software and systems to address known vulnerabilities. The approaches developed for malware attacks include an approach for malware detection in CPS settings dubbed SOFS-OGCNMD, which uses snake optimizer-based feature selection and an ideal graph convolutional network suggested by Daniel et al.[50]. Other approaches are ensemble learning[51,59], deep learning[52], artificial intelligence, trust-based Approach[53], cryptography[54], etc.

The above-defined attacks are the most common cyber-attacks in CPS. Other than that, there are several approaches for different attacks, but these existing approaches do not deal with the problem of more than one attacker/attack type existence.

Moreover, certain security issues must be addressed in CPS situations where standard operating systems might not be present[60]. Specifically, assaults on CPS that lack a fully functional OS require customised defences. Tampering, vandalism, and component theft are examples of physical assaults that need the use of strong physical security measures like secured enclosures and tamper-evident seals[61]. Redundancy in sensing and cryptographic verification of sensor data are necessary to prevent sensor spoofing or manipulation, which is a serious threat[62]. Hardware-based timekeeping systems and strong protocols are necessary to fend against time synchronisation threats[63]. Physical shielding, leakage minimization methods, and cryptographic safeguards can all be used to lessen side-channel assaults[64]. Furthermore, the weaknesses in wireless communication and the supply chain need the use of strict supply chain security procedures, encryption, authentication, and secure communication protocols. Redundancy and fail-safe systems, ongoing monitoring, timely patching, and thorough training programmes should be used to thwart fail-operational assaults, zero-day exploits, and social engineering techniques, respectively[65]. These customised methods ensure a strong defence against any attacks by acknowledging the special qualities of CPS settings without conventional operating systems.

4.2. Security approaches based on different technologies

This section delineates the approaches based on technology and includes learning-based, trust-based, optimization-based, and cryptography-based approaches in CPS as shown in **Figure 6**. These are the most common technologies developed for secure environments in CPS.

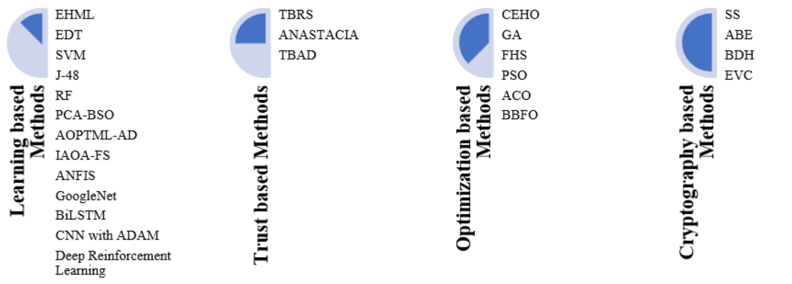


Figure 6. Security approaches based on technologies.

Learning-based methods: Cyberattacks are becoming a significant danger to international security, leading to the emergence of various new types of cybercrime. As a result, it is now more challenging to identify and stop such attacks. Fortunately, using the strength of Machine Learning (ML) techniques, researchers have created sophisticated AI-based models for cybercrime detection and prevention. ML is an essential tool for categorizing and detecting cyber risks, making it a key component of protecting Cyber-Physical Systems (CPS). Further, an effective hybrid machine learning model (EHML) was developed by Lilhore et al.[59] for the identification and categorization of cybercrime. The EHML model builds a more effective cybercrime analysis model using unsupervised learning-based data reduction and supervised learning for crime detection. Furthermore, it chooses pertinent characteristics to find anomalies and outliers utilizing an improved decision tree (EDT) method and an enhanced local outlier factor (ELOF) Technique. On a Kaggle online cybercrime dataset, the study tested the proposed EHML and existing ML methods (SVM, J-48, and Random Forest (RF)). The analysis revealed that the EHML model outperformed conventional ML techniques by 10%, achieving accuracy rates of 95.02%, precision of 95.01%, recall of 94.89%, and an F1-score of 95.89%.

Moreover, for Cyber-Physical Systems (CPS), Kanagala[66] developed a modified deep learning technique to improve data security and efficiently analyze IoT-based data. The method makes use of a deep learning model and a data access algorithm to transform unstructured IoT data into knowledge data while enforcing policy-based access control to safeguard against DoS and DDoS assaults. Performance investigation showed that the method successfully categorizes data, guaranteeing trustworthy data upkeep. Furthermore, it offers continuous security checking of IoT data against DoS and DDoS assaults on CPS applications. ML was used by Abosuliman[67] also to identify network anomalies and DDoS attacks on Industry 4.0 CPSs. The study solves shortcomings of previous approaches by extracting 45 bidirectional network flow parameters from real-world semiconductor manufacturing facility traffic data and creating labeled datasets for ML model training and testing. Based on the eigenvalues of the features, the proposed PCA-BSO method chooses the pertinent features. Through simulations, the study assesses the effectiveness of supervised machine learning algorithms. The Aquila Optimizer with Parameter Tuned ML Based Anomaly Detection (AOPTML-AD) approach was created by Ramachandran et al.[68] to identify aberrant behavior in CPS. The improved Aquila optimization algorithm-based feature selection (IAOA-FS) is used by AOPTML-AD to preprocess network data and choose the best feature subset. The Chimp optimization algorithm (ChOA) with an adaptive neuro-fuzzy inference system (ANFIS) model is used to identify abnormalities. AOPTML-AD beat more modern models, according to performance validation using a benchmark dataset, with an accuracy of 99.37%. Several other versions of learning-based approaches include deep reinforcement learning[69], Machine learning-based IDS[70], GoogleNet-BiLSTM[52], ADAM[71], etc.

Trust-based methods: Security is provided via trust-based security models, which rely on developing trust among system participants. These methods impose security regulations based on the degree of trust between entities. Usually, identification, reputation, and prior behavior are used to develop trust. Each entity in a trust-based security system is given a trust level, which represents the degree of trust that other entities have in that entity. Based on these trust levels, security rules are subsequently implemented. For instance, organizations with higher trust levels could be given more access rights than organizations with lower trust levels. The trust-based approaches are quite effective in providing security for different application-based CPS, including TBRS[72,73], ANASTACIA[74], TBAD[75], etc. These approaches computed a trust factor based on the node's input and output factors.

Optimization-based methods: One of the burgeoning areas is soft computing, also called optimization, which includes fuzzy systems, neural networks, evolutionary computation, rough sets, and probabilistic reasoning. There are a number of optimization techniques that provide different levels of security in CPS. Some of the soft computing algorithms are Improved Chaotic Elephant Herding Optimization (CEHO)[76], genetic algorithm (GA)[77], Fuzzy harmony search (FHS)[78], PSO-Blockchain-Steganography[79], ACO-based[80,81], binary bacterial foraging optimization (BBFO)[82], etc.

Cryptography-based methods: Cyber-Physical Systems (CPS) security depends heavily on cryptography. The interplay between the cyber and physical components of CPS makes it essential to safeguard both components. A number of methods are provided by cryptography to guarantee the confidentiality, availability, and integrity of data in CPS. These methods provide end-to-end security for communication in CPS. Different approaches of cryptography, like, Schmidt Samoa (SS)[83], attribute-based encryption (ABE)[84], Bilinear Diffie-Hellman (BDH)[85], and Event-based Cryptography (EBC)[86], were designed by different researchers. Operating in a resource-constrained context is one of the main obstacles for CPS in cryptography. Traditional cryptographic approaches are challenging to apply on CPS since they frequently have little processing power, memory, and battery life. As a result, researchers are looking at new, lightweight cryptographic methods that may be used in contexts with limited resources.

Other methods: Additionally promising for strengthening the resilience of CPS systems, various active strategies, such as space partitioning and software rejuvenation are also used to improve the security and dependability[87]. As a proactive maintenance strategy, software rejuvenation involves periodically restarting or refreshing software components to prevent problems like memory leaks or degraded states. In the context of CPS, where uninterrupted functionality is crucial, this method is useful in guaranteeing smooth operation[88]. In a similar vein, space partitioning — Which separates various software components across separate memory spaces — appeared as an essential safety feature in CPS. Space partitioning gives an additional layer of redundancy and fault tolerance by limiting any defects or mistakes to specified partitions. This is especially important in contexts where real-time responsiveness and safety are crucial, such in healthcare or transportation[89].

4.3. Security approaches for smaller devices

The use of sophisticated security solutions faces a distinct set of difficulties in the context of CPS, small IoT, and edge devices. These devices frequently work under severe resource limitations, such as restricted access to certain facilities and limited processing power[90]. Therefore, not every strategy discussed above could work in these situations.

It is necessary to move towards preventative security measures in light of these budget constraints. Preemptive methods greatly help CPS, IoT, and edge devices, in contrast to traditional IT systems, which could possess the processing capacity to react to security events in a reactive manner. These actions strengthen their defences against possible attackers without placing an undue strain on their meagre resources.

Effective cryptographic solutions: Ensuring security without overtaxing the device's processing power requires the use of lightweight cryptographic algorithms created for resource-constrained situations[91]. There are clear benefits to using lightweight cryptographic algorithms in situations when resources are limited. They are especially made to minimise the load on device resources through the optimisation of computing operations. This allows for quick execution, even on devices with little processing power. These algorithms are also designed to function in memory-restricted situations, hence reducing the amount of memory needed for cryptographic operations and making them ideal for devices with little RAM. Additionally, by reducing the energy required for cryptographic calculations, lightweight cryptographic systems prioritise energy efficiency — A crucial factor for Internet of Things devices that run on batteries. This results in longer battery life. Furthermore, even in situations when physical attacks might be dangerous, these algorithms show a strong defence against side-channel attacks, preventing unintentional information leaking during cryptographic processes. Because of this extensive collection of features, lightweight cryptographic algorithms are positioned as an essential instrument for guaranteeing operational effectiveness and security in situations with limited resources[92].

Edge-based security policies: Distributing the burden of security while adhering to resource limitations is achieved by enabling edge devices to apply localised security policies, offloading computing demands from the central system. There are a lot of benefits to this strategy, especially in settings with limited resources[93]. Historically, centralised systems or servers have been mostly responsible for managing and enforcing security policies in CPS and IoT systems. The computational burden on the central infrastructure increases with the size and complexity of these systems, though, and this might result in latency problems and performance bottlenecks, particularly in real-time or mission-critical applications. By assigning some security tasks to the devices at the network's edge, edge-based security policies lessen this load. These processing-capable gadgets are placed carefully to keep an eye on and regulate the movements and exchanges in their local area[94]. The system as a whole benefits from shifting security duties to edge devices in a number of ways, including less stress on the central system, better security mechanisms that are more responsive and agile, and better use of computational resources. To avoid possible vulnerabilities, however, good design and implementation are essential. This includes secure communication protocols, authentication, and frequent upgrades to edge devices. Furthermore, to supervise and guarantee the efficacy of the distributed security rules, a strong monitoring and management system needs to be implemented.

Energy-aware encryption techniques: Energy-efficient encryption techniques for battery-powered Internet of Things devices provide a safe and secure compromise, extending device uptime without sacrificing security. This is crucial in situations when it is logistically or financially impractical to replace or recharge batteries often[95]. Furthermore, the implementation of energy-aware encryption plays a crucial role in maintaining the integrity and confidentiality of private data that is transferred or stored by Internet of Things devices, particularly in fields where data security is crucial, such as industrial automation, healthcare, and environmental monitoring. Therefore, the incorporation of these methods into the security architecture of battery-operated Internet of Things devices marks a noteworthy advancement in guaranteeing the durability and efficiency of these essential elements of the Internet of Things network.

5. Challenges and recommendations

Despite the CPS's current security measures, several issues still need to be resolved. First, the dynamic nature of CPS makes it challenging to maintain continuous security, which is one of the main concerns. The heterogeneity of the devices and networks in CPS presents another difficulty since executing a consistent security strategy across all the devices and networks is difficult. Additionally, nowadays, devices generate a large amount of data using IoT and CPS, so securing all the devices and the data they produce is not accessible due to the proliferation. Finally, the security of CPS is constantly challenged by cybercriminals' development of novel and sophisticated attack methodologies. A few of the challenges are described below:

1) Rapidly changing risks: As CPSs develop, security threats do as well. Existing security measures struggle to keep up with attackers' ongoing development of novel and sophisticated techniques to exploit these systems' flaws.
2) The complexity of CPSs makes them susceptible to several attack vectors since they are intricate systems comprising interconnected hardware, software, and networks. As a result, it can be challenging to safeguard every part of the system, even with current security measures.
3) Human mistake: Despite current security measures, human error continues to be one of the most significant obstacles to the safety of CPSs. This can include less complicated errors like using weak passwords or not updating software to more complicated ones like incorrectly configuring security settings.
4) Integration with legacy systems: Many CPSs are layered on top of security-impaired legacy systems already in place. Integrating these systems with modern security techniques can be difficult, especially with compatibility problems.
5) Resources: The processing speed, memory, and bandwidth of many CPSs are constrained. This can make deploying and sustaining current security strategies difficult, particularly ones requiring much computer power.
6) Lack of standardization: CPS security methods are not currently standardized. This may make it challenging for businesses to select the best strategy for their unique requirements, resulting in uncertainty and possible security breaches.

Here are some future recommendations to improve the security level in CPS:

- Communication with optimization for secure path selection: Ensuring data is transferred through a secure channel is a significant difficulty in CPS security. Secure path selection is one method for doing this, which entails selecting optimized data transmission pathways to reduce the risk of attacks. The best path for data transmission may be found using network optimization techniques, such as graph-based algorithms, which consider link quality, traffic load, and security needs.
- The capacity to recognize and respond to assaults in real-time is another crucial component of CPS security. Anomalies in CPS data pointing to a security compromise can be found using deep learning-based detection algorithms. For instance, abnormalities in system behavior that could point to a

cyberattack might be found using unsupervised learning techniques like autoencoders and clustering algorithms. In addition, different types of attacks can be classified, and alerts can be sent to security personnel using supervised learning techniques like neural networks and decision trees.

- Encryption and authentication: Encryption and authentication techniques can be utilized to protect data transfer and guarantee that only authorized users have access to CPS systems.
- Use of multi-factor authentication: By requiring users to submit additional authentication elements in addition to merely a username and password, multi-factor authentication can increase the security of CPS systems. This can involve physical tokens like smart cards or USB keys or biometric authentication methods like fingerprint or facial recognition.

6. Conclusion

In conclusion, using Cyber-Physical Systems (CPS) has transformed network technology and resulted in notable advancements in several industries. Using sensor data by various applications and its transfer to the cloud has enhanced productivity and efficiency. However, the integrity of the network is seriously threatened by the inherent hazards associated with this increasing data traffic, such as data breaches and unauthorized alteration. As a result, organizations and companies using CPS technology now place a high priority on security. To guarantee that the advantages of network technology and CPS are fully realized without jeopardizing the security of the systems, it is imperative to address these issues. Overall, as CPS expands, network technology will progress, and to fully use this technology's potential, it is essential to balance its advantages and disadvantages.

Cyber-Physical Systems (CPS) security is a fast-developing topic as new threats and technologies evolve. Here are a few probable future security areas for CPS:

- Intrusion Detection and Prevention: Creating sophisticated, CPS-specific intrusion detection and prevention systems will be essential. These systems ought to be able to identify and stop assaults that target both the physical and digital parts of CPS.
- Privacy protection: As CPS become increasingly ingrained in our everyday lives, protecting individual privacy and the confidentiality of their data will be crucial. Future research should concentrate on creating privacy-preserving reliable methods that safeguard sensitive data without impairing system performance.
- Resilient Design and Fault Tolerance: Cyberattacks, hardware malfunctions, and communication outages are just a few of the problems that CPS is vulnerable to. Future security efforts should focus on developing CPS with built-in resilience and fault tolerance to guarantee that the system can function securely and effectively even amid such disturbances.
- Threat Intelligence and Analytics: Gathering, analyzing, and sharing threat intelligence data will become increasingly crucial for protecting CPS. In order to recognize and successfully address new risks, sophisticated analytics approaches that can analyze and analyze enormous amounts of data in real time are needed.
- Secure Update and Management: With CPS's growing connection and complexity, securely managing updates and patches for system components is a considerable difficulty. To keep CPS secure against known vulnerabilities, future research should concentrate on creating effective and secure means for firmware, software, and configuration updates.
- Standards and Best Practices: Establishing industry-wide standards and best practises for CPS security will be crucial. Researchers, business professionals, and regulators should work together to create standards and laws that guarantee a uniformly high degree of security within many CPS areas.
- Artificial Intelligence and Machine Learning: Artificial intelligence and machine learning approaches can improve CPS security. Future CPS security will heavily rely on developing intelligent systems capable of seeing abnormalities, foreseeing assaults, and automatically reacting to security issues.

- Secure Interoperability: As CPS grows more linked, it will be essential to provide secure interoperability across various systems and gadgets. The main focus of future work should be the development of standardised protocols and methods that provide secure communication and interaction between diverse CPS components.

Conflict of interest

The authors declare no conflict of interest.

References

1. Rajkumar R (Raj), Lee I, Sha L, et al. Cyber-physical systems. Proceedings of the 47th Design Automation Conference. Published online June 13, 2010. doi: 10.1145/1837274.1837461
2. Kaur A, Chatterjee JM. Applications of Cyber-Physical Systems. Cyber-Physical Systems. Published online July 2022: 289-310. doi: 10.1002/9781119836636.ch13
3. Caviglia R, Gaggero G, Portomauro G, et al. An SDR-Based Cybersecurity Verification Framework for Smart Agricultural Machines. IEEE Access. 2023, 11: 54210-54220. doi: 10.1109/access.2023.3282169
4. Gaggero GB, Fausto A, Patrone F, et al. A Framework for Network Security Verification of Automated Vehicles in the Agricultural Domain. 2022 26th International Conference Electronics. Published online June 13, 2022. doi: 10.1109/ieeeconf55059.2022.9810440
5. Molina E, Jacob E. Software-defined networking in cyber-physical systems: A survey. Computers & Electrical Engineering. 2018, 66: 407-419. doi: 10.1016/j.compeleceng.2017.05.013
6. Calvaresi D, Marinoni M, Sturm A, et al. The challenge of real-time multi-agent systems for enabling IoT and CPS. Proceedings of the International Conference on Web Intelligence. Published online August 23, 2017. doi: 10.1145/3106426.3106518
7. Zografopoulos I, Ospina J, Liu X, et al. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. IEEE Access. 2021, 9: 29775-29818. doi: 10.1109/access.2021.3058403
8. Hasan MK, Habib AA, Shukur Z, et al. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. Journal of Network and Computer Applications. 2023, 209: 103540. doi: 10.1016/j.jnca.2022.103540
9. Gupta A, Singh A. A Comprehensive Survey on Cyber-Physical Systems Towards Healthcare 4.0. SN Computer Science. 2023, 4(2). doi: 10.1007/s42979-023-01669-5
10. Tushar W, Yuen C, Saha TK, et al. A Survey of Cyber-Physical Systems From a Game-Theoretic Perspective. IEEE Access. 2023, 11: 9799-9834. doi: 10.1109/access.2023.3239834
11. Cassottana B, Roomi MM, Mashima D, et al. Resilience analysis of cyber-physical systems: A review of models and methods. Risk Analysis. 2023, 43(11): 2359-2379. doi: 10.1111/risa.14089
12. Duo W, Zhou M, Abusorrah A. A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. IEEE/CAA Journal of Automatica Sinica. 2022, 9(5): 784-800. doi: 10.1109/jas.2022.105548
13. Bashendy M, Tantawy A, Erradi A. Intrusion response systems for cyber-physical systems: A comprehensive survey. Computers & Security. 2023, 124: 102984. doi: 10.1016/j.cose.2022.102984
14. Salau BA, Rawal A, Rawat DB. Recent Advances in Artificial Intelligence for Wireless Internet of Things and Cyber–Physical Systems: A Comprehensive Survey. IEEE Internet of Things Journal. 2022, 9(15): 12916-12930. doi: 10.1109/jiot.2022.3170449
15. Kim S, Park KJ, Lu C. A Survey on Network Security for Cyber–Physical Systems: From Threats to Resilient Design. IEEE Communications Surveys & Tutorials. 2022, 24(3): 1534-1573. doi: 10.1109/comst.2022.3187531
16. Agrawal N, Kumar R. Security Perspective Analysis of Industrial Cyber Physical Systems (I-CPS): A Decade-wide Survey. ISA Transactions. 2022, 130: 10-24. doi: 10.1016/j.isatra.2022.03.018
17. Rupprecht T, Wang Y. A survey for deep reinforcement learning in markovian cyber–physical systems: Common problems and solutions. Neural Networks. 2022, 153: 13-36. doi: 10.1016/j.neunet.2022.05.013
18. Harris JD, Quatman CE, Manring MM, et al. How to Write a Systematic Review. The American Journal of Sports Medicine. 2013, 42(11): 2761-2768. doi: 10.1177/0363546513497567
19. Pati D, Lorusso LN. How to Write a Systematic Review of the Literature. HERD: Health Environments Research & Design Journal. 2017, 11(1): 15-30. doi: 10.1177/1937586717747384
20. Nourian A, Madnick S. A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet. IEEE Transactions on Dependable and Secure Computing. 2018, 15(1): 2-13. doi: 10.1109/tdsc.2015.2509994
21. Liu Y, Peng Y, Wang B, et al. Review on cyber-physical systems. IEEE/CAA Journal of Automatica Sinica. 2017, 4(1): 27-40. doi: 10.1109/jas.2017.7510349
22. Inderwildi O, Zhang C, Wang X, et al. The impact of intelligent cyber-physical systems on the decarbonization of energy. Energy & Environmental Science. 2020, 13(3): 744-771. doi: 10.1039/c9ee01919g

23. Ashibani Y, Mahmoud QH. Cyber physical systems security: Analysis, challenges and solutions. Computers & Security. 2017, 68: 81-97. doi: 10.1016/j.cose.2017.04.005
24. Lee J, Bagheri B, Kao HA. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. Manufacturing Letters. 2015, 3: 18-23. doi: 10.1016/j.mfglet.2014.12.001
25. Sonntag D, Zillner S, van der Smagt P, et al. Overview of the CPS for Smart Factories Project: Deep Learning, Knowledge Acquisition, Anomaly Detection and Intelligent User Interfaces. Springer Series in Wireless Technology. Published online October 13, 2016: 487-504. doi: 10.1007/978-3-319-42559-7_19
26. Zhang J, Pan L, Han QL, et al. Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey. IEEE/CAA Journal of Automatica Sinica. 2022, 9(3): 377-391. doi: 10.1109/jas.2021.1004261
27. Alguliyev R, Imamverdiyev Y, Sukhostat L. Cyber-physical systems and their security issues. Computers in Industry. 2018, 100: 212-223. doi: 10.1016/j.compind.2018.04.017
28. Cleveland FM. Cyber security issues for Advanced Metering Infrasttructure (AMI). 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century. Published online July 2008. doi: 10.1109/pes.2008.4596535
29. Metke AR, Ekl RL. Smart Grid security technology. 2010 Innovative Smart Grid Technologies (ISGT). Published online January 2010. doi: 10.1109/isgt.2010.5434760
30. Yaacoub JPA, Salman O, Noura HN, et al. Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and Microsystems. 2020, 77: 103201. doi: 10.1016/j.micpro.2020.103201
31. Kitchin R, Dodge M. The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. Journal of Urban Technology. 2017, 26(2): 47-65. doi: 10.1080/10630732.2017.1408002
32. Basan E, Mikhailova V, Shulika M. Exploring Security Testing Methods for Cyber-Physical Systems. 2022 International Siberian Conference on Control and Communications (SIBCON). Published online November 17, 2022. doi: 10.1109/sibcon56144.2022.10002880
33. Ju Y, Yang M, Chakraborty C, et al. Reliability-Security Tradeoff Analysis in mmWave Ad Hoc Based CPS. ACM Transactions on Sensor Networks. Published online February 2023. doi: 10.1145/3582556
34. Johari R, Sharma P. A Survey on Web Application Vulnerabilities (SQLIA, XSS) Exploitation and Security Engine for SQL Injection. 2012 International Conference on Communication Systems and Network Technologies. Published online May 2012. doi: 10.1109/csnt.2012.104
35. Kundankumar RS, Malathip. Cyber physical system security by splunk. i-manager's Journal on Communication Engineering and Systems. 2020, 9(2): 41. doi: 10.26634/jcs.9.2.18115
36. Zhou J, Luo Y, Liu Y, et al. Eavesdropping Strategies for Remote State Estimation Under Communication Constraints. IEEE Transactions on Information Forensics and Security. 2023, 18: 2250-2261. doi: 10.1109/tifs.2023.3265343
37. Golchha R, Lachure J, Doriya R. Fog Enabled Cyber Physical System Authentication and Data Security using Lattice and Quantum AES Cryptography. International Journal of Computing and Digital Systems. 2023, 13(1): 267-275. doi: 10.12785/ijcds/130122
38. Wu S, Jiang Y, Luo H, et al. Deep learning-based defense and detection scheme against eavesdropping and typical cyber-physical attacks. 2021 CAA Symposium on Fault Detection, Supervision, and Safety for Technical Processes (SAFEPROCESS). Published online December 17, 2021. doi: 10.1109/safeprocess52771.2021.9693596
39. Gao J, Xu W, Kanhere S, et al. A Novel Model-Based Security Scheme for LoRa Key Generation. Proceedings of the 20th International Conference on Information Processing in Sensor Networks (co-located with CPS-IoT Week 2021). Published online May 18, 2021. doi: 10.1145/3412382.3458256
40. Umer M, Sadiq S, Karamti H, et al. Deep Learning-Based Intrusion Detection Methods in Cyber-Physical Systems: Challenges and Future Trends. Electronics. 2022, 11(20): 3326. doi: 10.3390/electronics11203326
41. Girdhar K, Singh C, Kumar Y. AI and Blockchain for Cybersecurity in Cyber-Physical Systems: Challenges and Future Research Agenda. Blockchain for Cybersecurity in Cyber-Physical Systems. Published online 2023: 185-213. doi: 10.1007/978-3-031-25506-9_10
42. Catillo M, Pecchia A, Villano U. CPS-GUARD: Intrusion detection for cyber-physical systems and IoT devices using outlier-aware deep autoencoders. Computers & Security. 2023, 129: 103210. doi: 10.1016/j.cose.2023.103210
43. Nguyen GN, Viet NHL, Elhoseny M, et al. Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model. Journal of Parallel and Distributed Computing. 2021, 153: 150-160. doi: 10.1016/j.jpdc.2021.03.011
44. Yeboah-Ofori A, Islam S, Lee SW, et al. Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security. IEEE Access. 2021, 9: 94318-94337. doi: 10.1109/access.2021.3087109
45. Quincozes SE, Mosse D, Passos D, et al. On the Performance of GRASP-Based Feature Selection for CPS Intrusion Detection. IEEE Transactions on Network and Service Management. 2022, 19(1): 614-626. doi: 10.1109/tnsm.2021.3088763
46. Raza A, Memon S, Nizamani MA, et al. Machine Learning-Based Security Solutions for Critical Cyber-Physical Systems. 2022 10th International Symposium on Digital Forensics and Security (ISDFS). Published online June 6, 2022. doi: 10.1109/isdfs55398.2022.9800811
47. R M Seyam A, Bou Nassif A, Nasir Q, et al. Deep Learning Techniques to Detect DoS Attacks on Industrial

Control Systems: A Systematic Literature Review. The 7th Annual International Conference on Arab Women in Computing in Conjunction with the 2nd Forum of Women in Research. Published online August 25, 2021. doi: 10.1145/3485557.3485577

48. Hsu YF, Ryusei A, Matsuoka M. Real Network DDoS Pattern Analysis and Detection. 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC). Published online June 2022. doi: 10.1109/compsac54236.2022.00236
49. Mahmood H, Mahmood D, Shaheen Q, et al. S-DPS: An SDN-Based DDoS Protection System for Smart Grids. Chaudhry S, ed. Security and Communication Networks. 2021, 2021: 1-19. doi: 10.1155/2021/6629098
50. Daniel A, Deebalakshmi R, Thilagavathy R, et al. Optimal feature selection for malware detection in cyber physical systems using graph convolutional network. Computers and Electrical Engineering. 2023, 108: 108689. doi: 10.1016/j.compeleceng.2023.108689
51. Liu J, Tang Y, Zhao H, et al. CPS Attack Detection under Limited Local Information in Cyber Security: An Ensemble Multi-Node Multi-class Classification Approach. ACM Transactions on Sensor Networks. Published online March 6, 2023. doi: 10.1145/3585520
52. Achar S, Faruqui N, Whaiduzzaman M, et al. Cyber-Physical System Security Based on Human Activity Recognition through IoT Cloud Computing. Electronics. 2023, 12(8): 1892. doi: 10.3390/electronics12081892
53. Longari S, Pozone A, Leoni J, et al. CyFence: Securing Cyber-physical Controllers Via Trusted Execution Environment. IEEE Transactions on Emerging Topics in Computing. Published online 2023: 1-12. doi: 10.1109/tetc.2023.3268412
54. Chaitanya SMK, Choppakatla N. A novel embedded system for cyber-physical system using crypto mechanism. Multimedia Tools and Applications. 2023, 82(26): 40085-40103. doi: 10.1007/s11042-023-15172-9
55. Ji Z, Yang SH, Cao Y, et al. Harmonizing safety and security risk analysis and prevention in cyber-physical systems. Process Safety and Environmental Protection. 2021, 148: 1279-1291. doi: 10.1016/j.psep.2021.03.004
56. Rosado DG, Santos-Olmo A, Sánchez LE, et al. Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern. Computers in Industry. 2022, 142: 103715. doi: 10.1016/j.compind.2022.103715
57. Machaka P, Ajayi O, Maluleke H, et al. Modelling DDoS Attacks in IoT Networks using Machine Learning. Available online: http://arxiv.org/abs/2112.05477 (accessed on 6 December 2023)
58. Ravi V, Chaganti R, Alazab M. Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system. Computers and Electrical Engineering. 2022, 102: 108156. doi: 10.1016/j.compeleceng.2022.108156
59. Lilhore UK, Simaiya S, Sandhu JK, et al. EHML: An Efficient Hybrid Machine Learning Model for Cyber Threat Forecasting in CPS. 2023 International Conference on Artificial Intelligence and Smart Communication (AISC). Published online January 27, 2023. doi: 10.1109/aisc56616.2023.10084987
60. Wolf M, Serpanos D. Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems. Proceedings of the IEEE. 2018, 106(1): 9-20. doi: 10.1109/jproc.2017.2781198
61. Yang X, Shu L, Liu Y, et al. Physical Security and Safety of IoT Equipment: A Survey of Recent Advances and Opportunities. IEEE Transactions on Industrial Informatics. 2022, 18(7): 4319-4330. doi: 10.1109/tii.2022.3141408
62. Krotofil M, Larsen J, Gollmann D. The Process Matters. Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. Published online April 14, 2015. doi: 10.1145/2714576.2714599
63. Anwar FM, Garcia L, Han X, et al. Securing Time in Untrusted Operating Systems with TimeSeal. 2019 IEEE Real-Time Systems Symposium (RTSS). Published online December 2019. doi: 10.1109/rtss46320.2019.00018
64. Wang H, Sayadi H, Sasan A, et al. Hybrid-shield. Proceedings of the 39th International Conference on Computer-Aided Design. Published online November 2, 2020. doi: 10.1145/3400302.3418783
65. Ratasich D, Khalid F, Geissler F, et al. A Roadmap Toward the Resilient Internet of Things for Cyber-Physical Systems. IEEE Access. 2019, 7: 13260-13283. doi: 10.1109/access.2019.2891969
66. Kanagala P. Effective cyber security system to secure optical data based on deep learning approach for healthcare application. Optik. 2023, 272: 170315. doi: 10.1016/j.ijleo.2022.170315
67. Abosuliman SS. Deep learning techniques for securing cyber-physical systems in supply chain 4.0. Computers and Electrical Engineering. 2023, 107: 108637. doi: 10.1016/j.compeleceng.2023.108637
68. Ramachandran A, Gayathri K, Alkhayyat A, et al. Malik R. Aquila Optimization with Machine Learning-Based Anomaly Detection Technique in Cyber-Physical Systems. Computer Systems Science and Engineering. 2023, 46(2): 2177-2194. doi: 10.32604/csse.2023.034438
69. Wu C, Pan W, Staa R, et al. Deep reinforcement learning control approach to mitigating actuator attacks. Automatica. 2023, 152: 110999. doi: 10.1016/j.automatica.2023.110999
70. Sahani N, Zhu R, Cho JH, et al. Machine Learning-based Intrusion Detection for Smart Grid Computing: A Survey. ACM Transactions on Cyber-Physical Systems. 2023, 7(2): 1-31. doi: 10.1145/3578366
71. Cai T, Jia T, Adepu S, et al. ADAM: An Adaptive DDoS Attack Mitigation Scheme in Software-Defined Cyber-Physical System. IEEE Transactions on Industrial Informatics. 2023, 19(6): 7802-7813. doi: 10.1109/tii.2023.3240586
72. Liang W, Long J, Weng TH, et al. TBRS: A trust based recommendation scheme for vehicular CPS network.

Future Generation Computer Systems. 2019, 92: 383-398. doi: 10.1016/j.future.2018.09.002

73. Gholami N, Torkzaban, Baras JS. On the Importance of Trust in Next-Generation Networked CPS Systems: An AI Perspective. Available online: http://arxiv.org/abs/2104.07853 (accessed on 6 December 2023)
74. Ziegler S, Skarmeta A, Bernal J, et al. ANASTACIA: Advanced networked agents for security and trust assessment in CPS IoT architectures. 2017 Global Internet of Things Summit (GIoTS). Published online June 2017. doi: 10.1109/giots.2017.8016285
75. Liu Y, Liu A, Liu X, et al. A Trust-Based Active Detection for Cyber-Physical Security in Industrial Environments. IEEE Transactions on Industrial Informatics. 2019, 15(12): 6593-6603. doi: 10.1109/tii.2019.2931394
76. Abidi MH, Alkhalefah H, Moiduddin K, et al. Novel improved chaotic elephant herding optimization algorithm-based optimal defense resource allocation in cyber-physical systems. Soft Computing. 2022, 27(6): 2965-2980. doi: 10.1007/s00500-022-07455-4
77. Wu JMT, Srivastava G, Jolfaei A, et al. Security and Privacy in Shared HitLCPS Using a GA-Based Multiple-Threshold Sanitization Model. IEEE Transactions on Emerging Topics in Computational Intelligence. 2022, 6(1): 16-25. doi: 10.1109/tetci.2020.3032701
78. Abidi MH, Alkhalefah H, Umer U. Fuzzy harmony search based optimal control strategy for wireless cyber physical system with industry 4.0. Journal of Intelligent Manufacturing. 2021, 33(6): 1795-1812. doi: 10.1007/s10845-021-01757-4
79. Mohsin AH, Zaidan AA, Zaidan BB, et al. PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture. Multimedia Tools and Applications. 2021, 80(9): 14137-14161. doi: 10.1007/s11042-020-10284-y
80. Sathya Priya J, Saravanan K, Sathyabama AR. Optimized evolutionary algorithm and supervised ACO mechanism to mitigate attacks and improve performance of adhoc network. Computer Communications. 2020, 154: 551-558. doi: 10.1016/j.comcom.2020.02.070
81. Gupta M, Bhatt S, Alshehri AH, et al. Authorization Frameworks for Smart and Connected Ecosystems. Access Control Models and Architectures for IoT and Cyber Physical Systems. Published online 2022: 39-61. doi: 10.1007/978-3-030-81089-4_3
82. Althobaiti MM, Pradeep Mohan Kumar K, Gupta D, et al. An intelligent cognitive computing based intrusion detection for industrial cyber-physical systems. Measurement. 2021, 186: 110145. doi: 10.1016/j.measurement.2021.110145
83. Kannan C, Dakshinamoorthy M, Ramachandran M, et al. Cryptography-based deep artificial structure for secure communication using IoT-enabled cyber-physical system. IET Communications. 2021, 15(6): 771-779. doi: 10.1049/cmu2.12119
84. Junejo AK, Komninos N. A Lightweight Attribute-Based Security Scheme for Fog-Enabled Cyber Physical Systems. Wireless Communications and Mobile Computing. 2020, 2020: 1-18. doi: 10.1155/2020/2145829
85. Xu Z, Liu X, Zhang G, et al. A Certificateless Signature Scheme for Mobile Wireless Cyber-Physical Systems. 2008 The 28th International Conference on Distributed Computing Systems Workshops. Published online June 2008. doi: 10.1109/icdcs.workshops.2008.84
86. Lima PM, Carvalho LK, Moreira MV. Ensuring confidentiality of cyber-physical systems using event-based cryptography. Information Sciences. 2023, 621: 119-135. doi: 10.1016/j.ins.2022.11.100
87. Abdi F, Chen CY, Hasan M, et al. Preserving Physical Safety Under Cyber Attacks. IEEE Internet of Things Journal. 2019, 6(4): 6285-6300. doi: 10.1109/jiot.2018.2889866
88. Romagnoli R, Krogh BH, de Niz D, et al. Software Rejuvenation for Safe Operation of Cyber–Physical Systems in the Presence of Run-Time Cyberattacks. IEEE Transactions on Control Systems Technology. 2023, 31(4): 1565-1580. doi: 10.1109/tcst.2023.3236470
89. Gu X, Easwaran A. Towards safe machine learning for CPS. Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems. Published online April 16, 2019. doi: 10.1145/3302509.3311038
90. Tyagi AK, Sreenath N. Cyber Physical Systems: Analyses, challenges and possible solutions. Internet of Things and Cyber-Physical Systems. 2021, 1: 22-33. doi: 10.1016/j.iotcps.2021.12.002
91. Shah A, Engineer M. A Survey of Lightweight Cryptographic Algorithms for IoT-Based Applications. Advances in Intelligent Systems and Computing. Published online November 20, 2018: 283-293. doi: 10.1007/978-981-13-2414-7_27
92. Jan MA, Khan F, Khan R, et al. Lightweight Mutual Authentication and Privacy-Preservation Scheme for Intelligent Wearable Devices in Industrial-CPS. IEEE Transactions on Industrial Informatics. 2021, 17(8): 5829-5839. doi: 10.1109/tii.2020.3043802
93. Lu Y, Wang D, Obaidat MS, et al. Edge-Assisted Intelligent Device Authentication in Cyber–Physical Systems. IEEE Internet of Things Journal. 2023, 10(4): 3057-3070. doi: 10.1109/jiot.2022.3151828
94. Laroui M, Nour B, Moungla H, et al. Edge and fog computing for IoT: A survey on current research activities & future directions. Computer Communications. 2021, 180: 210-231. doi: 10.1016/j.comcom.2021.09.003
95. Munoz DJ, Montenegro JA, Pinto M, et al. Energy-aware environments for the development of green applications for cyber–physical systems. Future Generation Computer Systems. 2019, 91: 536-554. doi: 10.1016/j.future.2018.09.006