J Inf Process Syst, Vol.14, No.6, pp.1361~1384, December 2018
https://doi.org/10.3745/JIPS.03.0105

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

A Survey on Cyber Physical System Security for IoT: Issues, Challenges, Threats, Solutions

Nam Yong Kim*, Shailendra Rathore*, Jung Hyun Ryu*, Jin Ho Park**, and Jong Hyuk Park*

Abstract

Recently, Cyber Physical System (CPS) is one of the core technologies for realizing Internet of Things (IoT). The CPS is a new paradigm that seeks to converge the physical and cyber worlds in which we live. However, the CPS suffers from certain CPS issues that could directly threaten our lives, while the CPS environment, including its various layers, is related to on-the-spot threats, making it necessary to study CPS security. Therefore, a survey-based in-depth understanding of the vulnerabilities, threats, and attacks is required of CPS security and privacy for IoT. In this paper, we analyze security issues, threats, and solutions for IoT-CPS, and evaluate the existing researches. The CPS raises a number challenges through current security markets and security issues. The study also addresses the CPS vulnerabilities and attacks and derives challenges. Finally, we recommend solutions for each system of CPS security threats, and discuss ways of resolving potential future issues.

Keywords

Cyber Physical System, Internet of Things, Security Analysis, Security Threats

1. Introduction

The Cyber Physical System (CPS) is a new paradigm that pursues the convergence of physical and cyber spaces in which we live. It is a system that is tightly integrated in terms of scale and level with different cyber and physical systems. In the CPS, the cyber environment is a digital environment that is computed, communicated and managed by a world created by computer programs. The physical environment runs various sensors and the Internet of Things (IoT) in the course of time. As such, the CPS includes software, hardware, sensors, actuators, and embedded systems, and is connected to human-machine interfaces and multiple systems. A number of sensors, actuators, and control devices are connected by a network to form a complex system for acquiring, processing, calculating, and analyzing physical environment information and applying the results to the physical environment. The CPS is a technology closely related to the IoT, and a next-generation network-based distributed control system that combines a physical system with sensors and actuators and a computing element that controls it. Therefore, it emphasizes that there are many interactions between the cyber and physical

Manuscript received September 3, 2018; first revision October 19, 2018; accepted October 30, 2018.
Corresponding Author: Jong Hyuk Park (jhpark1@seoultech.ac.kr)
* Dept. of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech), Seoul, Korea ({nykim, rathoreshailendra, jh.ryu, jhpark1}@seoultech.ac.kr)
**Dept. of Computer Science, School of Software, Soongsil University, Seoul, Korea (j.park@ssu.ac.kr)

worlds as a result of the development of information and communication technology (ICT). Dependence on the CPS is gradually increasing in a variety of applications in the energy, transportation, medical and manufacturing sectors.

The development of CPS technology is the key to improving the quality of life more efficiently than ever before, but the risks are becoming more and more acute in terms of security. In addition, the CPS has difficulty assessing threats and vulnerabilities caused by interactions, and new security issues are emerging. This complexity coupled with the heterogeneity of the CPS's components makes it difficult to guarantee the security and privacy of the CPS, and it is also difficult to identify, track, and examine the multiple components of the CPS and targeted attacks on them. Cyber-terrorists can attack real control systems as well as information security in virtual spaces such as computers or Internet servers. In other words, all IoT devices and sensors are connected and controlled on the network, which can result in the spread of security damage from virtual space, i.e., by computer hacking, to real physical systems. This is a serious issue that could shake the foundations of the CPS by directly threatening our lives in the real world. Therefore, we need to gain an in-depth understanding of all these vulnerabilities, threats, and attacks through research on CPS security and privacy controls. This survey presents the differences between IT systems and the CPS with reference to the basic concepts of the CPS.

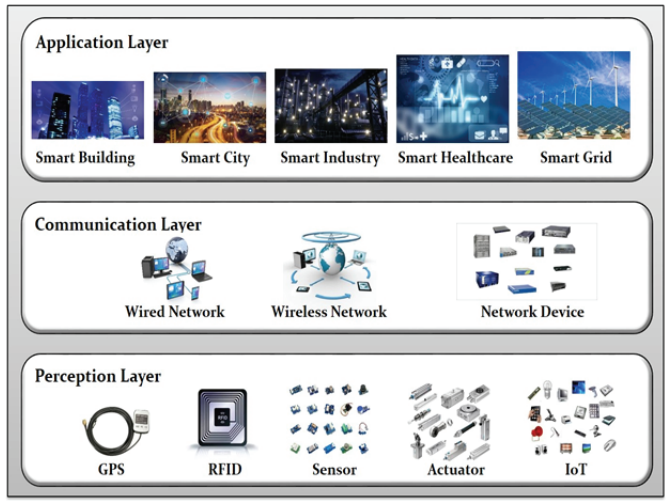


Fig. 1. The fundamental concept of CPS.

As shown in Fig. 1, the CPS is divided into three layers: the perceptual layer, the data transmission layer, and the application layer [1]. The first layer, or perception layer, includes the recognition and the sensor, and consists of the global positioning system (GPS), RFID, sensor, actuator, camera, and IoT. The collected data can be composed of sound, light, mechanical, chemical, thermal, electrical, biology and location data, and the sensor can generate real-time data through node collaboration in wide-area and local network domains [2]. Thus, the perception layer recognizes and collects data, sends it to the communication layer, and collaborates between the IoT nodes in the network [3,4]. The communication layer is responsible for exchanging and processing data between the sensor and the application in communication. This layer communicates using various technologies such as wire (e.g., LAN, WAN), network devices (e.g., Switch, Router), and wireless (e.g., Bluetooth, ZigBee, WiFi, 4G, and 5G). This is one of the key elements of the CPS, which typically has a wide range from local to global [5]. Most

communications are highly available and cost-effective because they can initially process and manage vast amounts of data over the Internet. The communication layer is also responsible for reliability and supports real-time transmission [6]. The application layer can be applied and interacted with various fields, and is sometimes referred to by a different name depending on the application one is using. For example, a typical CPS is the Supervisory Control and Data Acquisition (SCADA) system used in critical infrastructures such as the Smart Grid and the industrial control system (ICS) [7]. This layer processes the information received from the data transport layer and includes the commands to be executed by the physical sensors and actuators, and it controls the commands to be used in each field. In addition, data aggregation of different resources, intelligent processing of large amounts of data, object control and management are performed [5,8].

The range of the CPS includes the smartphones, computers, and automotive devices that we use in everyday life from power plants, water and sewage systems, airports, and industrial infrastructure to railroads. Wang et al. [9] presented the status and development of cyber physical systems and future research directions when applied to manufacturing. This allows future plants to demonstrate their production sites with enhanced security, while the CPS's unique capabilities in networking, communications, and integrated device control support manufacturing intelligence. Griffor et al. [10] investigated the concept of the CPS, and tis domains, aspects, and facets in detail and studied the CPS framework, and presented analysis and output of the CPS framework and use cases using the CPS framework. Wang et al. [11] investigated the security issues and challenges facing the CPS, abstracted the general workflow of the cyber physics system, and identified the vulnerabilities, attack issues, enemy characteristics, and a set of challenges to be solved. They also proposed a context aware security framework for general CPS systems and studied potential research areas and issues. Shi et al. [12] provided a better understanding of the new multi-disciplinary methodology. They provided basic applications to illustrate the capabilities of the CPS, summarized the research process from various perspectives, and demonstrated the involvement of the CPS audience. Maheshwari [13] emphasized the importance of security issues in CPSs that are used extensively in a variety of areas such as critical infrastructure control, vehicle systems, and transportation, social networking, and medical and healthcare systems. Taking into account the existing security issues and security challenges, we have studied the security requirements of the CPS based on attacks on the CPS. Ashibani and Mahmoud [1] analyzed security issues at the various layers of the CPS architecture, studied risk assessment and CPS security technologies, and discussed the challenges, future research areas, and possible solutions. Considering this paper's limitations of the existing survey on CPS security, as shown in Table 1, we also present the contribution of our study in relation to the previous survey in terms of CPS overview and CPS security, issues, and challenges.

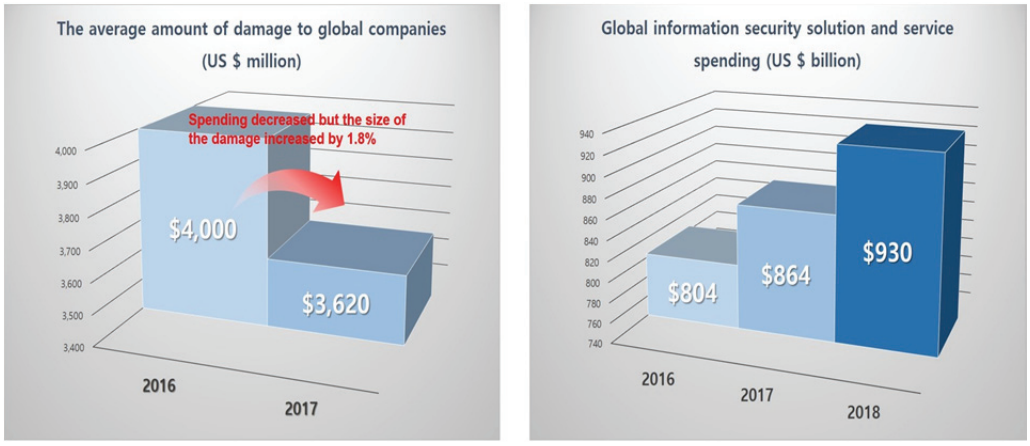
Table 1. Contribution of our study related with existing surveys

	Wang et al. [11]	**Shi et al. [12]**	**Maheshwari [13]**	**Ashibani and Mahmoud [1]**	**This survey**
Year of publication	2010	2011	2016	2017	2018
CPS overview	Limited	Yes	Limited	Yes	Yes
CPS security issues and challenges	Yes	Yes	Yes	Yes	Yes
CPS security threats	Yes	No	Yes	Yes	Yes
Existing CPS security solutions	No	No	No	Yes	Yes
Recent CPS security project and discussion	No	No	Limited	Limited	Yes

The rest of this paper is organized as follows: Section 2 emphasizes the importance of security through current CPS security market research and discusses the unique characteristics of the CPS. It also discusses the issues and challenges of CPS security in detail, and derives various CPS security considerations. Section 3 shows the diversity of CPS attacks by investigating threats, attacks and security solutions on CPS security. Section 4 investigates to lead to projects, and discussions. Section 5 discusses solutions based on threats and provides recommendations for open security issues. Finally, Section 6 presents the conclusion.

2. CPS Security Issues and Challenges

In recent years, cyber-attacks have become more sophisticated in the field of security, making cyber threats increasingly unpredictable. According to a 2017 data breach study by the Ponemon Institute, a security consulting firm specializing in data breaches, the average cost of damages suffered by data breaches worldwide in 2017 was $36.2 million, though less than in the previous year, but the damage increased by 1.8% [14]. It also took an average of 191 days to identify data breach events. In a 2016 survey, a security expert monitored 200,000 security events everyday in order to respond quickly to cyber-attacks [14]. It is analyzed that 60,000 security blogs each month need to acquire information and track false alarms related to cyber threats, requiring around 20,000 hours (about 833 days, 2.3 years) of effort every year. It is also estimated that there will be a shortage of around 1.5 billion security professionals worldwide by 2020. Even now, the issue of cybersecurity shows that the damage is not decreasing even though companies are investing many resources in security. According to Gartner's latest forecast in 2017, worldwide spending on information security solutions and services was $86.4 billion, up 7 percent from 2016, while expenditure on forecasting amounted to $ 93 billion in 2018 [15]. Data on damage to the global market and security solution expenditure are shown in Fig. 2. Therefore, in the CPS, security is becoming more important in terms of behaviorial, analysis, multi-layer, visibility, and governance factors.



(a) (b)

Fig. 2. Global market damage and security solution spending of CPS. (a) Ponemon Institute data breaches and (b) Gartner information security solutions.

It is necessary to pay closer attention to CPS security as the importance of cyber-security grows. In general, the security of the CPS is divided into three areas: physical security, communication security, and control and operational security. Physical security involves protecting information in the network environment, data aggregation in loosely coupled networks, processing, and large-scale sharing; communication security is focused on protecting data and the role of the control system against cyber-attacks [4], and control and operational security is focused on protecting the cyber environment with the aim of mitigating attacks of the control system on the system estimation and control algorithms [16]. Prior to CPS security, the CPS has a variety of goals, design principles, and security requirements. Therefore, we investigated the issues and security objectives pertaining to the CPS and described the requirements and design principles as follows [17].

- Test and analysis complexity: CPS development includes software engineering, mechanical engineering, electrical engineering, systems engineering, and network engineering. In these diverse fields it is difficult to collect, test, and analyze the functional and non-functional software requirements. Overall testing has also become more difficult as there are no effective testing approaches or tools, as well as CPS-related issues. Therefore, development and testing should be capable of recognizing various contexts, working with various types of clients, and communicating smoothly in various fields.
- Design and implementation complexity: Due to the aforementioned issues and constraints, the software design for the target CPS can be very complex. In addition, the CPS must meet many of the requirements imposed by various factors, including the components, application logic, other development environments, programming languages and interface mechanisms, and external constraints.
- Safety: Safety is generally considered an important asset in industrial applications equipped with control systems that are responsible for the technical processes. Computer systems should be designed so that the operation of computer software or hardware does not threaten the environment in such a way that equipment failure will result in death, bodily injury, and large financial losses.
- Security: In the CPS, security can be largely classified into encryption, data information security, and control system security against cyber-attacks. These considerations can be defined as the three main components of security [18]. In cyber physical systems, confidentiality must be considered to protect the user's personal information. The integrity of the CPS should take into account the prevention, detection or blocking of network attacks on the information exchanged between sensors and actuators or controllers. The wide availability of the CPS aims to provide services at all times while avoiding compromises of computing, control, and communications due to hardware failures, system upgrades, or DoS/DDoS attacks [19].

The rest of this section introduces the unique issues for each layer of the CPS, discusses various applications along with the security issues and challenges for the CPS, and presents an analysis of the related research.

2.1 Perception Issues and Challenges

The CPS includes sensors, actuators, and physical environmental issues in a variety of perception environments. The physical environment carries out the instructions received from the control unit and transmits the measurement and monitoring information to the control unit. Konstantinou et al. [16] highlighted the security and privacy issues of the CPS's various components and discussed potential

solutions to improve its robustness. In the power field, most of the real-time digital simulations (RTDS) were used to generate field device input and output signals. In the hydroelectric field, the field devices were constructed with tanks, pumps and sensors. The physical environment has issues protecting access to the devices, and unauthorized objects can access and manipulate the system. To protect the devices from malicious attackers, one must first run the software. However, it does not guarantee any other mechanism implemented by the application unless we trust the underlying binary code [20]. Kumar and Patel [2] raised serious concerns about access to devices and personal information as an aspect of privacy protection at the IoT and discussed IoT security threats and privacy concerns. Here, IoT security issues include front-end sensors and equipment, networks, and back-end IT systems, whereas IoT privacy concerns include device privacy, privacy during communication, and personal information storage issues.

2.2 Communication Issues and Challenges

The communication layer of the CPS sends commands to the devices and system responsible for the network between the control device and the control in order to analyze the various types of information (e.g., measurements, control status, events) received from the control state. The communication requirements affect the physical layer (PHY), the middle layer (MAC), and the network layer (NTW) rather than the application layer. The CPS communication area issues are required for selecting requires the selection of an appropriate communication standard, such as the individual radio link properties of each device to the router or another device, the total capacity and load of the network affecting the individual link, and so on. Regarding the issues of CPS security, it is necessary to strike a balance between the coherent security technologies that are deployed across multiple layers, improved security, and the inherent performance overhead [21]. As a communication challenge, Software Defined Networking (SDN) can reconfigure routing control, Quality of Service, and routing policies as the CPS context changes, thereby ensuring security, reliability, and real-time requirements at the same time. Molina and Jacob [22] discussed recent SDN approaches to mission-critical applications by identifying the trends, challenges, and opportunities for the potential development of software-defined cyber physical networks. This approach also analyzes the possibility of applying the SDN to the CPS, and then briefly summarizes the SDN characteristics and future research that will meet the essential requirements of the CPS. Buczak and Guven [23] addressed the complexity of machine learning (ML) and data mining (DM) algorithms, discussed the issues of applying them to cybersecurity, and provided recommendations on when to use a given approach.

2.3 Application Issues and Challenges

The CPS application monitors, measures, and controls the devices that make up the physical environment. The control part is closely related to the application layer, and research is under way to construct the control using real devices and systems. The diverse environment of applications manifests various security requirements, such as smart buildings, smart cities, smart industries, and smart healthcare and smart grids. Even if the same security service is provided in each environment, it can be applied differently according to the environment or users. A key challenge for application communications is the hierarchical access to sensor data and the privacy of the user authentication process [20]. Sampigethaya and Poovendran [24] have the complex issues with manned and unmanned

aircraft types and large aircraft carrier container management as a future airspace system. It is essential to ensure the superior performance of highly mixed aircraft and airspace systems of a cyber-network, software, storage, and computing. Denker et al. [25] pointed to the need to rely on the CPS of the social scale of future generations, and described how adaptive and reflective observational analysis methodologies, which are essential to building a credible CPS system, can provide the basis for structured adaptation. This method represents a paradigm shift in the monitoring, coordination and control domains of dynamic CPS using an information-centric approach. Al-Jaroodi et al. [17] provided an overview of software engineering issues. While CPS software is related to the nature and type of the CPS with regard to such issues as quality assurance, analysis, design, development and verification, the system is related to the complexity of the software development process used to develop it. Sridhar et al. [26] describe smart grid operations, the related cyber-infrastructure, and power system control which have a direct impact on the quality and quantity of power delivered to the end users. In addition, as it is important to support power application security and infrastructure security, we have reviewed the issues and challenges of CPS security in this Section. CPS security, unlike IT system, can have serious consequences for a variety of industries and sectors if it is compromised. Therefore, CPS security should consider the issues and challenges presented in previous papers.

3. CPS Security Threats and Solutions

CPS security threats can cause serious damage to the physical environment, and each layer of the CPS can be attacked manually or actively. The CPS is also vulnerable to a variety of Internet attacks physical sensors and networks [7]. Thus, threats to the perceptual layer consist of attacks on physical environments such as sensors, actuators, and the IoT; threats to the transport layer include threats to data, data corruption, and system communications; while threats to the application layer consist of user privacy threats from malicious code and counterfeit attacks. As shown in Fig. 3, these diverse threats are classified as CPS security threats. Security against CPS threats comprises a variety of solutions designed to protect physical space, cyberspace, and systems. These solutions indicate that smart environments such as smart buildings, smart cities, smart industries, smart healthcare, and smart grids are essential for real-world applications.

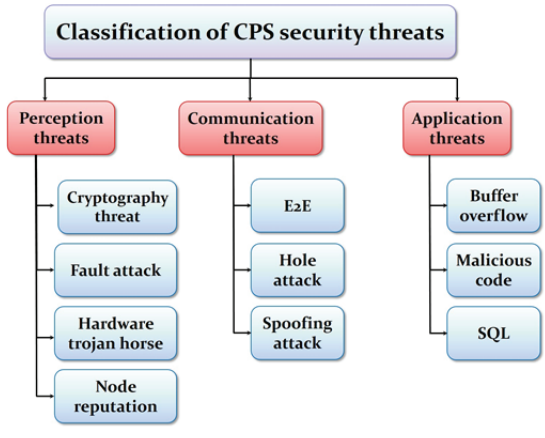


Fig. 3. Classification of CPS security threats.

3.1 Perception Threats

The perceptual layer is a limited computing resource consisting of the physical environment and memory functions such as sensors RFID. Such devices are typically placed in external and outdoor environments, which can cause physical attacks in situations where device components are changed or devices are replaced [27]. In addition, most research on CPS security focuses on cyberspace while ignoring the vulnerability of the hardware layer, thus raising the need for research on the latter. Physical threats include such threats as physical attacks, equipment failures, line failures, electromagnetic leaks, electromagnetic interference, fault attacks, denial of service attacks, perceptual data corruption, data tampering, data password threats, and node reputation.

Cryptography threat: The key elements of CPS security data are the subject of intentional attacks by cyber or hardware layers, and they are collected, transmitted, processed and stored on these distributed hardware devices. The unattended environment also makes the endpoint vulnerable to attack by hardware-based technologies [28]. Lightweight cryptography has been widely used in embedded devices where CPS terminal resources are limited. The use of data-dependent power can also be exposed to attacks when a device handles cryptographic secrets; and differential power analysis (DPA) attacks can target the AES AddRoundKey and SubBytes outputs [29].

Fault attack: A fault attack uses intentionally triggered fault actions on the target device to restore the data password and reverse engineer the internal circuitry. In general, it is known that when a fault attack is triggered, the critical path in all systems encounters a problem with circuit control. A fault attack can also use a variety of solutions which can be broadly categorized as global or local [30].

Hardware Trojan horse: The Troy classification is determined by physical, activation, and behavioral characteristics. Physical properties show the number of added, deleted or corrupted chip components and changes in the chip's physical form. The activation attribute indicates the criteria for performing the activation and destruction functions of Troy. Behavioral characteristics identify the types of destructive behavior introduced by Trojan horses [31].

Node reputation: There are various attacks on node reputation such as node capture, fake nodes, and node outages. Node capture gets or relinquishes information related to the encryption keys on behalf of the nodes, which threatens the security of the entire system [3]. The fake node sends malicious data by adding another node to the network. It also attacks data integrity and launches DoS attacks using the system's node energy [32]. Node abort is an attack that interferes with availability and integrity by making it difficult for the node to read and collect information because it stops the node service [33]. These various node reputation attacks target confidentiality, availability, integrity, and stability.

3.2 Communication Threats

The communication of the CPS needs to be protected to ensure that there are no vulnerabilities in the CPS infrastructure. The CPS should be scalable so as to provide control over a large number of field devices, infrastructure devices, and servers connected to computing and communication resources under a resilient, lightweight, and limited protection scheme. The risks of data transmission include routing attacks, DoS attacks, control attacks, flood attacks, trap doors, Sybil attacks, hole attacks (e.g., sinkhole attacks, wormhole attacks, black hole attacks, gray hole attacks), and routing loop. There are many different threats.

End-to-End (E2E): E2E can lead to end-to-end authentication and threats to core contracts, key management, encryption algorithms, and DoS and DDoS attacks. Also, CPS devices in large-scale environments are geographically dispersed in the field. Distributed devices may be exposed to external parties, and may represent safety and economic risks, thus requiring secure communication. Therefore, the exchanged information should be strongly protected from cyber-attacks on the E2E side through a large-scale CPS. In addition, E2E security support for the protection of personal information between electrical consumers or suppliers in communications for the collection of information from smart meters or energy sources is identified in a non-negotiable manner. Without E2E security support, the reliability of large CPSs can be compromised [34].

Hole attack: Hole attacks include various threats such as wormhole attacks, sinkhole attacks, black hole attacks, and gray hole attacks [35]. A wormhole attack is a serious attack on the wireless sensor network (WSN) routing protocol, and comprises two common attacks. Two malicious nodes look for data packets in one part and send them to the rest of the network through wormhole tunnels, setting up wormhole tunnels for the links in short wait times, creating a very close illusion. This can allow intruders to control numerous paths in the network, thus destroying the correct operation of the routing protocol [36]. The sinkhole attack is the malicious node of the sinkhole that provides the best path to the base station. A sinkhole node has the opportunity to modify data before deleting the message, or delivering it to the base station and creating unnecessary delays [37].

Spoofing attack: A Smurf or spoofing attack is an address attack that continues to send targeted ICMP (internet control message protocol) packets with the same destination address as one of the destination computer addresses to the destination network. If a programmable logic controller (PLC) operates with a modified message in the context of a SCADA system, it can send a crash or dangerous command to the actuator. Also, ARP spoofing is a meson attack that uses an address determination protocol message to trick the other party's data packet into becoming a gateway.

3.3 Application Threats

Application threats are a collection of information from a large number of users at this layer, resulting in attacks that result in data loss, loss of personal information such as user habits and health, and unauthorized access to the device. Attacks at the application layer include user privacy disclosure, unauthorized access, malicious code, database attacks and control command forgery, DoS/DDoS, and vulnerability attacks [38].

Buffer overflow: Buffer overflow is an attack that compromises the program's intended behavior and prevents it from functioning normally. The usual methods are stack smashing and function-pointer manipulation. These attacks result in password reconstruction, content modification, malicious code execution, and software vulnerability exploitation [39].

Malicious code: The malicious code can attack a user's application through various malicious codes of viruses and worms and thereby damage the network. Depending on the injected payload, the compromised process may crash or execute some malicious code. Thus, the ability to hide details without invalidating the intermediate steps is an important element of attack techniques [40].

Structured Query Language (SQL): Most enterprise database applications can be accessed using SQL statements for structural changes and content manipulation. SQL injection occurs when the other party

can manipulate the data entry into the web application, prevent the user from deleting the input, and insert a series of unexpected SQL statements into the query. Thus, we can manipulate the database in a variety of unexpected ways. In recent data and web accessibility, the SCADA system was shown to be one of the best attacks on SQL injection, with a very strong impact on the security of the SCADA system.

3.4 CPS Security Solutions

CPS security is designed to protect the entire environment, ranging from data protection to network security and privacy, from physical to application environments. These diverse security schemes are shown in Fig. 4, with CPS security solutions categorized as device protection, network access detection, malicious code detection and application solutions.

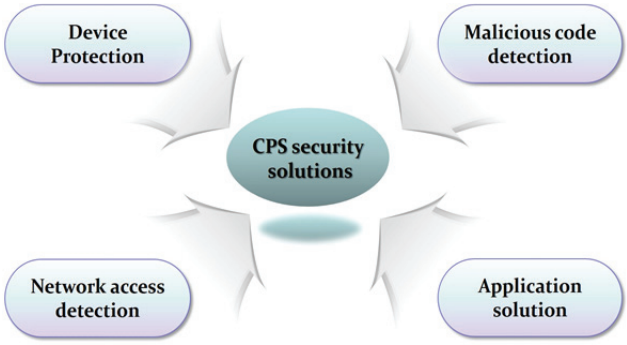


Fig. 4. Security and privacy solutions for CPS.

Device protection: The way to build a secure hardware infrastructure is to design a secure hardware platform with a resilient architecture to defend against cyber-attacks. Jin and Oliveira [41] proposed a SoC architecture with high security based on hardware anchors, which is communication between the OS and the hardware. Hardware anchors are actively monitored and track bus traffic to prevent malicious tampering. Their proposed architecture showed a low performance overhead and was efficient. Oliveira et al. [42] proposed an HW/SW architecture that can safely extend the OS. They developed an emulator-based prototype called *Ianus*. As a result of this experiment, all malicious rootkits were stopped and false positives were not detected for positive modules. Al Ibrahim and Nair [43] proposed a new framework that uses PUF for CPS security. The framework studied synthetic approaches that combine the security attributes of complex PUF elements. A physical unclonable function (PUF) is a digital fingerprint that is used as a unique identifier of a semiconductor device such as a microprocessor. It is based on physical changes that occur naturally in the semiconductor manufacturing process and can be distinguished from other semiconductors. The PUF is commonly used for encryption and is now also used in applications that are implemented as integrated circuits and have high security requirements. Vegh and Miclea [44] proposed an integrated CPS solution modeled as a multi-agent system secured through the WSO2 complex event processor (CEP). The solution analyzes each message and can determine which messages are encrypted and which messages are not encrypted. It also demonstrates the ideal CPS, including secure, efficient, and reliable confidentiality, privacy, and availability. Kocher et al. [29] proposed blocking attacks by adversaries with access to plain

text and cipher text data based on the latest cryptographic primitives such as AES, RSA, ECC, and HMAC. This method of blocking attacks is considered to be a solution that can defend against attacks beyond the normal range, with some improved cryptanalysis results, rather than indiscriminate attacks.

Network access detection: Network and system access defense includes defense and wormhole attack detection algorithms that use the software defined network (SDN) and control system detection. Kathiravelu and Veiga [45] proposed the SD-CPS as an approach an architecture for mitigating the application and design issues faced by the CPS. The SD-CPS uses the SDN switch and controller while synchronizing the SDN, even when there is no SDN switch. Therefore, the SD-CPS is compatible with and applicable to existing CPS deployments without SDN. This provided many research methods for SDN implementation, design, and improvement for alternative evaluation. Gupta [36] proposed a new algorithm for detecting wormhole attacks in the WSN. This algorithm uses a simple search method to find wormhole tunnels and uses bandwidth as a parameter of the WSN to update the frequency table, thus consuming fewer data. Cardenas et al. [46] is possible to detect a computer attack that alters the operation of the target control system by controlling the physical system. In the past, the physical environment and the control domain required interactions between control and security experts that were almost irrelevant, and there were issues with control algorithms and target attacks that surpassed safety and fault. Therefore, whenever a physical device is upgraded, compatibility and new interfaces are introduced to re-test it in order to identify and eliminate all vulnerabilities. In addition, with respect to critical systems, authorized personnel can gain quick and easy access in order to adjust the components of the CPS, but unauthorized access should be immediately blocked and defeated. Sanchez et al. [47] proposed a predictive solution to manage mobility and device lifecycles to meet all the CPS requirements. The solution used the CPS simulators and interpolation algorithms based on infinite loops to compute future system state sequences. It also provided experimental validation to determine the performance of the proposed solution.

Malicious code detection: Various mechanisms for detecting malware have been proposed on the web [48]. However, these mechanisms cannot be applied to prevent malicious code proliferation in the CPS because they represent detection only on the web. Xu et al. [49] proposed an early warning online social network (OSN) worm detection system that utilizes all the characteristics of an OSN. The system adds a "bait friend" with a legitimate OSN user group and uses the maximum range algorithm to detect communication between users. The detection system also distinguishes malicious propagation from legitimate user communications by implementing network and local correlation mechanisms when evidence obtained from the "bait friends" indicates that a suspicious malicious code has been propagated to the communication. Rathore et al. [50] proposed a machine learning-based approach to XSS attack detection for the Social Networking Service (SNS). In this approach, XSS attack detection is based on three functions, namely, URL, Web page, and SNS, and is compared with other approaches to verify the effectiveness of the proposed approach. The results of our evaluation show that our approach in the SNS environment achieved the best performance with the highest accuracy, and the lowest false positives in the SNS environment.

Application solution: Application solutions handle applications in a variety of smart environments, including smart buildings, smart cities, smart industries, smart healthcare, smart grids, and related solutions. Khalid et al. [51] proposed a collaborative robotic CPS (CRCPS) structure for human-robot collaboration (HRC) that allows human operators to integrate and use various interactive technologies.

We also studied design methodologies for HRC environments for various industrial scenarios that enable the implementation of solutions. Kim et al. [52] proposed CF-CloudOrch, a cloud orchestration using a lightweight container technology that makes up a simple network management infrastructure. We then used the Container Docker and Docker Swarm to configure the fog nodes and implement the full managed services cloud orchestration. IoT network management is essential, as the IoT network can be used for future IT based on efficient and simple management. Sharma et al. [53] proposed a scalable distributed smart-city architecture to meet the design principles required for the sustainable smart city. However, there are a variety of issues related to the unique features of smart cities, such as how to efficiently deploy SDN controller nodes in a distributed blockchain network architecture; how to deploy cache nodes; and how to filter raw data at the network's edge. Sharma et al. [54] proposed DistBlockNet, a distributed secure SDN architecture that uses blockchain technology for the IoT. The protection manager of the proposed architecture can dynamically adapt to the threat environment without having to include a security manager to manually process a large number of advisories and approvals. The experimental results show that the performance overhead is low and that attacks can be detected in real time on the IoT network while meeting the design principles required for future IoT networks. Li et al. [55] proposed a new distributed host-based collaborative detection (DHCD) method for identifying and mitigating false data injection (FDI) attacks in the Smart Grid CPS. In particular, rule specifications based on real-time collaborative detection systems are designed to identify abnormalities in the measurement data. Zhang et al. [56] proposed a healthcare CPS based on cloud and big data analysis technology for patient-oriented medical applications and services. By using cloud and big data technologies to improve the performance of medical systems, humans can showcase a variety of smart healthcare applications and services. Surveys of CPS security solutions summarize the various solution surveys and analyze the categories, solution types, descriptions and related studies, and show solutions for each environment in Table 2.

Table 2. Summary of CPS security solutions, description, and related studies

Type of solutions	Description	References
Device protection		
Hardware anchor based Ianus solution	HW-SW and SoC architecture with efficiency and security	Jin and Oliveira [41], Oliveira et al. [42]
PUF	A digital fingerprint used as a unique ID of a semiconductor device such as a microprocessor	Al Ibrahim and Nair [43]
WSO2 CEP solution	CPS integration solution modeled as multi-agent systems secured by WSO2 CEP	Vegh and Miclea [44]
DPA	Research the blocking of attacking parties with access to the latest ciphertext and plain text data	Kocher et al. [29]
Network access detection		
SD-CPS	A research on the way SDN motivates without or using SDN switches and controllers	Kathiravelu and Veiga [45]
Wormhole attack detection algorithm	Research method to find wormhole tunnels and update frequency tables using bandwidth as parameters in WSN	Gupta [36]
Control system attack detection	Research on immediate blocking and defense against unauthorized access	Cardenas et al. [46]
Pre-forecast for device management	A research on CPS Simulator and interpolation algorithm based on infinite loop for computing system state sequence in the future	Sánchez et al. [47]

Table 2. (Continued)

Type of solutions	Description	References
Malicious code detection		
Early warning OSN worm detection system	A research on the maximum range algorithm to detect communication between users by adding a bait friend with a legitimate OSN user group	Xu et al. [49]
XSSClassifier	A research on the three functions of URL, Web page and SNS based on XSS attack detection	Rathore et al. [50]
Application solution		
Control CRCPS for HRC	A research on design methodology for human robot collaboration environment for various industrial scenarios enabling solution implementation	Khalid et al. [51]
CF-CloudOrch	A research on container fog node-based cloud orchestration through efficient and simple management type of IoT network	Kim et al. [52]
Smart City	DistArch-SCNet: a research on distributed blockchain network based on SDN controller for Smart City related issues	Sharma et al. [53]
DistBlockNet	A research on distributed security SDN architecture using blockchain technology for IoT networks	Sharma et al. [54]
Smart Grid	Research of new DHCD method to identify and mitigate FDI attacks	Li et al. [55]
Smart Healthcare	Research on the cyber-physical system, health-CPS, based on cloud and big data analysis technology	Zhang et al. [56]

4. CPS Security Research

Research on the security of the CPS has become an integral part of the cyber world, and related projects are under way in various countries. In Korea, the DGIST is studying the CPS security environment in detail, and research in this area is also being conducted at several universities in the United States. In addition, Europe is also carrying out large-scale projects based on cooperation among countries. Thus, active research on CPS security in various environments is being conducted at home and abroad. In this section, there are very few survey data related to domestic and international projects, so we have listed various recent projects of each country. Thus, the latest Korean, American and European project research shows.

Korea: In the smart industry, a cyber-attack on Iran's nuclear facilities control system affected the country's nuclear program. These attacks are characterized by being designed for specific cyber-physical systems. Thus, the security of cyber-physical systems has increased the need for techniques for detecting attacks and protecting the functionality of the system from malicious attacks. The worst-case execution time (WCET) project at Seoul National University involves a control kernel project for CPS, and the stability of the kernel is currently being secured. In order to commercialize CPS technology, ETRI is conducting a CPS core technology development project on a high-reliability autonomous control SW technology, a research technology and an autonomous control technology to ensure the reliability of systems in a complex system environment. International projects have increased the need for the CPS

in various aspects and are focusing on the related research. However, domestic projects include little in the way of CPS security research. Therefore, the CPS security project is summarized in Table 3 for the CPS project and the domestic and overseas project research. And it can be applied to various environments by analyzing recent research by country, institution, and project.

Table 3. The list of latest CPS security projects

Institute	Project	Ref.
Korea		[57]
Seoul National University	A study on guaranteeing high reliability in kernel by executing control kernel project for CPS	
ETRI	Development of CPS core technology for high reliability autonomous control SW with the aim of commercialization of CPS technology	
DGIST	Study on CPS-based energy management system and smart grid-specific security technique	
	Interworking between vehicle simulation tool (AutoSim) based on inter-vehicle communication model and simulated driving system (OpenDS) providing actual vehicle driving environment	
	A study on the improvement of the accuracy by detecting the dangerous situation by applying the experiment and various machine learning algorithms by deploying the connector sensors and developing their own algorithms	
USA		
University of Notre Dam	Towards reliable cyber-physical systems using unreliable human sensors	[58]
Purdue University	Towards secure large-scale networked systems: resilient distributed algorithms for coordination in networks under cyber attacks	[59]
Ohio State University	Hierarchical control for large-scale cyber-physical systems	[60]
EU		
France	EuroCPS (European network of competencies and platforms for enabling SME from any sector building innovative CPS products to sustain demand for European manufacturing)	[61]
Austria	MODESEC (Model-based Design of Secure Cyber-Physical Systems)	[62]
Italy	CPSwarm	[63]

- The DGIST, in collaboration with the University of Pennsylvania, USA, is studying how to protect the core functions of the system, including the sensor, from various threats, including malicious and DoS attacks. To protect the core functions, it is necessary to use extra sensors and infer actual measurements. In addition, there are various studies on noise reduction techniques and methods of implementing the inference process for each sensor in a limited environment [57].
- The DGIST's Smart Grid will implement a CPS-based energy management system and a dedicated smart grid security technology, and build a complete testbed. The testbed consists of integrated DC and AC sources, solar power, load and real-time power hardware in loop simulation (HILS) devices. This smart grid system predicts the change factors based on the collection of energy information and the analysis of smart meters, thereby making it possible to optimize energy use. Smart grid security is one of the fundamental issues that new security issues can cause due to the physical accessibility of smart meters and system openness due to Internet access. Therefore, even if a smart grid system is attacked, the grid must be effectively restored and

remain open and available.

- The DGIST's intelligent transportation system is the first step toward creating the intelligent transportation system of the future. The CPS Global Center is working on a car simulation model (AutoSim) based on a simulation system (OpenDS) that provides the inter-vehicle communication model developed by Carnegie Mellon University and the actual vehicle driving environment. This research can test various CPS elements such as vehicle sensors and communication between vehicles and facilities in a different way from existing methods. It also consists in developing new algorithms and functions in AutoSim which have been extended for the testbed.
- The DGIST's Connected Sensor is a joint research project with the University of Virginia in the United States, and it is being deployed in an actual home environment. It involves research on its accuracy in detecting dangerous situations via the application of various machine learning algorithms. In addition, the connected sensor collects the size, position and distance information of difficult elements by image processing, and analyzes the risk factors to ensure a safe and convenient life for elderly people.

United States of America (USA): According to the recommendations of the American Scientific and Policy Advisory Council, the NSF in computer and information science and engineering recognizes the technical importance of the CPS itself as a key area of maintenance. It includes "American safety and competitiveness", which also include defense, aerospace, space, automotive, chemical, transportation and energy. Therefore, the NSF CPS program is designed to adopt the CPS program support in view of the tremendous ripple effects and to find a common underlying technology that can support a combination of physical and computing elements in all applications.

- The project titled "Towards reliable cyber-physical systems using unreliable human sensors" at the University of Notre Dame Institution analyzed information perceived by humans using estimation theory and CPS technology. The critical information thus analyzed provides the CPS as a human resource in order to provide a reliable social sensing component. The project proposal was rather timely given the increased interest in social networks, big data and human in-loop systems, and the proliferation of computer artifacts that interact with or monitor the physical world [58].
- The project titled "Secure large-scale networked systems" conducted by Purdue University proposes a new algorithm. This algorithm solves the problem, allowing large network components to take optimal action and predict system health in spite of attacks on multiple components. The proposed study established a new metric for measuring elasticity in a distributed optimization algorithm. It is also based on a generalized optimization approach to deriving a flexible and decentralized optimization algorithm [59].
- The goal of the Ohio State University organization's hierarchical control project for large-scale CPS is to establish a new foundation for control and game theory using numerical algorithms. It should be designed to be formal and extensible of a hierarchical population control system. The design approach of the proposed mechanism consists in developing an improved bidirectional optimization algorithm to solve the computational difficulties [60].

European Union (EU): The European Research and Development Information Service (CORDIS) is a project and its related organization funded by the EU under the Horizon 2020 framework program for

research and innovation from 2014 to 2020. This survey focuses on France, Austria, and Italy in Europe.

- The EuroCPS project in France aims to increase the synergy between small and medium-size enterprises and CPS providers as a major CPS platform, and to launch Europe as a network of design centers with the aim of occupying as soon as possible the emerging markets for IoT products. It involves research on CPS development in Europe by significantly reducing the development time and certification efforts by enabling access to a strong value chain of European collaboration and exchanges of knowledge and strategies [61].
- The MODESEC project in Austria includes research on a security development method (SDM) for a secure CPS with the aim of interaction between modeling and security. The project aims to support CPS engineers who are not trained in cybersecurity because of the security of the system under consideration [62].
- The CPSwarm project in Italy entails research on CPS issues including the proposal of new technologies for system integration and tools for supporting Swarm engineering at the CPS. We can also use the CPSwarm tool to easily develop and integrate a heterogeneous CPS that demonstrates collective action to collaborate on local policy and address complex, industry-driven, real-world issues [63].

5. Discussion and Open Issues

CPS security is so extensive and diverse that it must adapt to the threats that arise in these environments. Previous CPS security threats have been classified as physical, communication, and application environments, but researchers are constantly striving to protect the environment. Therefore, this section discusses the proposed solutions to be included in all security threats, and also discusses future open issues and development possibilities. CPS security discusses the recommended solutions for each layer attack based on various threats, as shown in Table 4.

5.1 Discussion

Jin and Oliveira [41] presented a hardware anchor-based solution that can dynamically monitor the overall system operations and enforce dynamic hardware and software security policies using communication channels and collaboration protocols. Therefore, when embedded hardware Trojans and various attacks cause false positives or performance issues, it is possible to remove the security policy and isolate faulty modules. Oliveira et al. [42] analyzed the integrity of down-call and information transfer, the level of protection against kernel-level malware, and the normal operation of benign modules through Ianus security. It stopped everything before the malicious action was performed, executed normally, and evaluated it as the actual kernel rootkit. The system overhead was analyzed through a series of system and CPU benchmarks to be as low as 12%. Al Ibrahim and Nair [43] offered the advantage of combining some PUF elements with biasing elements that are inherently based on a positional approach, resulting in arbitrarily safe and robust system-level PUFs. The fuzzy extractor of the PUF error correction technique is a biometric that can generate a cryptographically secure key. Index-based syndromes can also significantly reduce bit errors in PUFs with real-valued outputs. Vegh and Miclea [44] used ElGamal, an assigned private key, and provided a standard SQL-like query language called SiddhiSQL as the CEP. Without a private key, decryption is almost

impossible. Kathiravelu and Veiga [45] can protect the SD-CPS controller because an unprotected controller could be a vulnerability. SD-CPS controllers mitigate the risk of resource shortages or external attacks on the subnets and intermediate nodes of the system. With application and network awareness, the controller can differentiate the QoS offered to tenant applications. Kocher et al. [29] divided leakage reduction, random integration, and protocol level measurements into DPA prevention. Thus, leakage reduction uses a balanced amount of power to reduce leakage when constructing encryption circuits; randomness integration resists DPA by randomly changing the representation of secret parameters through measurements based on masking or blinding; and protocol-level countermeasures are the most effective and the hardest way of dealing with side-channel attacks is to design a cryptographic protocol for leakage.

Table 4. CPS security threats and their corresponding solutions

	Cryptography threats	Fault attack	Hardware Trojan horse	Node reputation	E2E	Hole attack	Spoofing attack	Buffer overflow	Malicious code	SQL
Hardware anchor based Ianus solution [41,42]	✓	✓	✓	✓			✓	✓	✓	✓
PUF [43]	✓	✓	✓	✓	✓				✓	
WSO2 CEP solution [44]	✓	✓		✓						✓
DPA [29]	✓	✓	✓	✓	✓		✓			
SD-CPS [45]				✓	✓	✓	✓			✓
Wormhole attack detection algorithm [36]				✓	✓	✓				
Control system attack detection [46]	✓	✓		✓	✓				✓	✓
Early warning OSN worm detection system [49]					✓	✓			✓	
XSSClassifier [50]				✓	✓		✓		✓	✓
Control CRCPS for HRC [51]		✓		✓	✓	✓			✓	✓
CF-CloudOrch [52]		✓		✓	✓	✓	✓		✓	
DistArch-SCNet [53]		✓		✓	✓	✓	✓	✓	✓	✓
DistBlockNet [54]			✓	✓	✓	✓	✓		✓	✓
DHCD method solution [55]				✓	✓			✓	✓	✓
Health-CPS [56]	✓	✓		✓	✓				✓	✓

Gupta [36] show a frequency-based algorithm for detecting wormhole attacks in a WSN that creates a secure routing protocol at each node using a broadcast mechanism. Encryption and decryption techniques are used for secure routing. Cardenas et al. [46] aimed to detect modifications to data that are detected or controlled as soon as possible before the system is irreversibly damaged by control system attacks. They also proposed a response mechanism focused on authentication, access control, encryption, or detection. Xu et al. [49] proposed an early-warning OSN worm detection system that

tests the detection system for the propagation of two representative OSN worms, the Koobface worm and the Mikeyy worm. The system consists of a surveillance network built into the OSN website and uses bait buddies to effectively detect OSN worm propagation. Rathore et al. [50] investigated XSS attacks and contributed in two ways to the SNS security domain and proposed an approach to XSS attack detection. The XSS worm is a malicious payload, typically written in JavaScript, which breaks browser security and prevents the propagation of personal information between users of the website. The experimental results showed that access to XSS detection is more effective in the SNS environment.

Khalid et al. [51] integrated communications between the cyber and physical layer overhead control and self-verification approaches to resolving new issues with real-time systems. The individual protection components register the status of workers, machines, factories, and processes and activate the protection mechanisms before a conflict can occur. The system integration approach includes a variety of protection checks and validation schemes based on intelligent sensor fusion technology, intelligent modular synchronization, and acceptable overhead. Kim et al. [52] used CF-CloudOrch to support SDN networking, security services management, scheduling, load balancing, and management services in combination with VM and a container. This architecture improves the performance of IoT networks' high data throughput and enables the rapid detection of various external attacks through real-time management [66]. Sharma et al. [53] proposed a distributed blockchain network architecture model that significantly reduces the end-to-end latency, response time, and processes at the heart of a smart-city network. The proposed model considers difficult issues such as how to deploy the cache node and how to filter the raw data at the network's edge according to the context [64]. It also effectively handles buffer overflow and flooding attacks on flow tables and delivers better performance than other methods in terms of bandwidth. Sharma et al. [54] proposed a secure SDN architecture distributed over an SDN-based network using a blockchain technology that analyzes the issues faced by large-scale IoT networks. The role of this architecture is to create and deploy protective features such as threat prevention, data protection, and access control, cache flooding, ARP spoofing, and DDoS and DoS attacks, and network attack mitigation such as threat detection [65]. Li et al. [55] used a set of rule specifications to identify abnormal measurement data reported by the phasor measurement unit (PMU) using the DHCP scheme. We also considered a reputation system that monitors and evaluates the overall operation of PMUs that use the adaptive reputation updating (ARU) algorithm to further detect corrupted PMUs. Zhang et al. [56] encrypted pre-processed data through the privacy mechanism with the Health CPS to provide hierarchical security. They also applied the distributed file storage (DFS) technology to provide efficient storage, high throughput data upload and download, high data error tolerance, multi-occupant user management, access control lists, and fast data retrieval and exchange for large volumes of medical data.

5.2 Open Issues

IoT open issues in the CPS have high risk in that many devices communicate with the centralized network. Even if hacking only one within thousands of IoT devices, it is connect to the data center network. And there is threat the centralized network that occupies a lot of IoT devices can be used as a tool. A more serious threat is that the IoT can be used as a tool for attacking humans. The open issues of data center in the CPS are the risk of unauthorized use of personal information. This is because data

center in the CPS collect large amounts of data various formats to produce meaningful analysis results. And the information in the data center is information that cannot individually identify a particular individual. Under Korean law, personal information is defined as information that can be used to identify person, either alone or in combination with other information. So we can use big data and data center technology to connect and guess different pieces of information. It can identify specific individuals and increase the risk of personal information leakage. Recently, the open issues of artificial intelligence have emerged as an attack that threatens human beings. This is because artificial intelligence can be a threat to decision-making about clever factory control and medical diagnosis, editing, and creation in everyday life. The Fourth Industrial Revolution can collect large amounts of data through the Internet and receive feedback quickly. It can also be included in CPS based on analysis and learning and use of artificial intelligence with big data. IoT devices are distributed across a physical system outside the boundaries of a specific space. The network connecting IoT collects and controls information. The security threats of the Fourth Industrial Revolution are increasing due to the technical nature of many IoT based on cyber and physical. Threats increase and control expands. The more space CPS uses, the more difficult it is to control the risks. Therefore, the risk analysis associated with the Fourth Industrial Revolution technology should not be applied in a specific environment. If all IoT are inevitably connected and operating, consider performing a risk analysis of the CPS.

6. Conclusion

Limited work has been done in the CPS security field because it is a new area that differs from the current network environment. The CPS is transmission medium can include various sensors, diverse types of data, real-time generated data, process analysis and various application interactions. This paper categorizes the various threats, solutions, and CPS security projects related to the issues and threats facing the CPS, and presents a solution to each threat. The CPS concept and security caused issues and challenges and showed the current security market and CPS related surveys. The CPS security assessed the threats and solutions for each tier and discussed future directions for analysis. We discussed the relationship between the threats and solutions of CPS security and studied open issues.

In the future IT will expand the scope of CPS security by combining the IoT and various sensors. Therefore, we should interact with other systems in various environments to ensure that the system is secure. Since the CPS environment comprises various layers and is associated with field threats, it is concluded that the findings of this paper could improve the security of the entire system. CPS security should be a matter of constant concern because the CPS has been widely applied to various smart environments such as the smart home, smart city, smart industry, smart healthcare, and smart grid. As such, the progressive evolution of CPS security is expected to become increasingly important as the smart environment proliferates.

Acknowledgement

This study was supported by the Research Program funded by Seoul National University of Science and Technology.

References

[1] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: analysis, challenges and solutions," *Computers & Security*, vol. 68, pp. 81-97, 2017.

[2] J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," *International Journal of Computer Applications*, vol. 90, no. 11, pp. 20-26, 2014.

[3] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of Things (IoT) security: current status, challenges and prospective measures," in *Proceedings of 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST),* London, UK, 2015, pp. 336-341.

[4] T. Lu, J. Lin, L. Zhao, Y. Li, and Y. Peng, "A security architecture in cyber-physical systems: security theories, analysis, simulation and application fields," *International Journal of Security and Its Applications*, vol. 9, no. 7, pp. 1-16, 2015.

[5] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in *Proceedings of 2012 10th International Conference on Frontiers of Information Technology (FIT),* Islamabad, India, 2012, pp. 257-260.

[6] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution," in *Proceedings of 2010 47th ACM/IEEE Design Automation Conference (DAC)*, Anaheim, CA, 2010, pp. 731-736.

[7] Y. Peng, T. Lu, J. Liu, Y. Gao, X. Guo, and F. Xie, "Cyber-physical system risk assessment," in *Proceedings of 2013 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing,* Beijing, China, 2013, pp. 442-447.

[8] B. Zhang, X. X. Ma, and Z. G. Qin, "Security architecture on the trusting internet of things," *Journal of Electronic Science and Technology*, vol. 9, no. 4, pp. 364-367, 2011.

[9] L. Wang, M. Torngren, and M. Onori, "Current status and advancement of cyber-physical systems in manufacturing," *Journal of Manufacturing Systems*, vol. 37, pp. 517-527, 2015.

[10] E. R. Griffor, C. Greer, D. A. Wollman, and M. J. Burns, "Framework for cyber-physical systems: Volume 1, overview," National Institute of Standards and Technology, Gaithersburg, MD, *Report No. 1500-201*, 2017.

[11] E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui, and K. P. Chow, "Security issues and challenges for cyber physical system," in *Proceedings of 2010 IEEE/ACM International Conference on Green Computing (GreenCom) and Communications & International Conference on Cyber, Physical and Social Computing (CPSCom)*, Hangzhou, China, 2010, pp. 733-738.

[12] J. Shi, J. Wan, H. Yan, and H. Suo, "A survey of cyber-physical systems," in *Proceedings of 2011 International Conference on Wireless Communications and Signal Processing (WCSP)*, Nanjing, China, 2011, pp. 1-6.

[13] P. Maheshwari, "Security issues of cyber physical system: a review," *International Journal of Computer Applications*, pp. 7-11, 2016.

[14] Ponemon Institute, "2017 cost of data breach study: global overview," 2017 [Online]. Available: https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf.

[15] Gartner, "Gartner says worldwide information security spending will grow 7 percent to reach $86.4 billion in 2017," 2017 [Online]. Available: https://www.gartner.com/newsroom/id/3784965.

[16] C. Konstantinou, M. Maniatakos, F. Saqib, S. Hu, J. Plusquellic, and Y. Jin, "Cyber-physical systems: a security perspective," in *Proceedings of 2015 20th IEEE European Test Symposium (ETS),* Cluj-Napoca, Romania, 2015, pp. 1-8.

[17] J. Al-Jaroodi, N. Mohamed, I. Jawhar, and S. Lazarova-Molnar, "Software engineering issues for cyber-physical systems," in *Proceedings of 2016 IEEE International Conference on Smart Computing (SMARTCOMP),* St. Louis, MO, 2016, pp. 1-6.

[18] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: towards survivable cyber-physical systems," in *Proceedings of 28th International Conference on Distributed Computing Systems Workshops*, Beijing, China, 2008, pp. 495-500.

[19] J. Lee, B. Bagheri, and H. A. Kao, "A cyber-physical systems architecture for industry 4.0-based manufacturing systems," *Manufacturing Letters*, vol. 3, pp. 18-23, 2015.

[20] E. A. Lee and S. A. Seshia, *Introduction to Embedded Systems: A Cyber-Physical Systems Approach*. Cambridge, MA: MIT Press, 2016.

[21] A. Burg, A. Chattopadhyay, and K. Y. Lam, "Wireless communication and security issues for cyber–physical systems and the Internet-of-Things," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 38-60, 2016.

[22] E. Molina and E. Jacob, "Software-defined networking in cyber-physical systems: a survey," *Computers & Electrical Engineering*, vol. 66, pp. 407-419, 2018.

[23] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153-1176, 2016.

[24] K. Sampigethaya and R. Poovendran, "Cyber-physical system framework for future aircraft and air traffic control," in *Proceedings of 2012 IEEE Aerospace Conference*, Big Sky, MT, 2012, pp. 1-9.

[25] G. Denker, N. Dutt, S. Mehrotra, M. O. Stehr, C. Talcott, and N. Venkatasubramanian, "Resilient dependable cyber-physical systems: a middleware perspective," *Journal of Internet Services and Applications*, vol. 3, no. 1, pp. 41-49, 2012.

[26] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210-224, 2012.

[27] Q. Shafi, "Cyber physical systems security: a brief survey," in *Proceedings of 2012 12th International Conference on Computational Science and Its Applications (ICCSA),* Salvador, Brazil, 2012, pp. 146-150.

[28] W. He, J. Breier, S. Bhasin, and A. Chattopadhyay, "Bypassing parity protected cryptography using laser fault injection in cyber-physical system," in *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security*, Xian, China, 2016, pp. 15-21.

[29] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, "Introduction to differential power analysis," *Journal of Cryptographic Engineering*, vol. 1, no. 1, pp. 5-27, 2011.

[30] F. Khelil, M. Hamdi, S. Guilley, J. L. Danger, and N. Selmane, "Fault analysis attack on an FPGA AES implementation," in *Proceedings of 2008 New Technologies, Mobility and Security*, Tangier, Morocco, 2008, pp. 1-5.

[31] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 10-20, 2010.

[32] K. Zhao and L. Ge, "A survey on the internet of things security," in *Proceedings of 2013 9th International Conference on Computational Intelligence and Security (CIS)*, Leshan, China, 2013, pp. 663-667.

[33] R. Bhattacharya, "A comparative study of physical attacks on wireless sensor networks," *International Journal of Research in Engineering and Technology*, vol. 2, no. 1, pp. 72-74, 2013.

[34] Y. Kim, V. Kolesnikov, and M. Thottan, "Resilient end-to-end message protection for cyber-physical system communications," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2478-2487, 2018.

[35] M. Wazid, A. K. Das, S. Kumari, and M. K. Khan, "Design of sinkhole node detection mechanism for hierarchical wireless sensor networks," *Security and Communication Networks*, vol. 9, no. 17, pp. 4596-4614, 2016.

[36] G. Gupta, "Frequency based detection algorithm of wormhole attack in WSNs," *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 4, no. 7, pp. 3057-3060, 2015.

[37] A. A. Pirzada and C. McDonald, "Circumventing sinkholes and wormholes in wireless sensor networks," in *Proceedings of International Workshop on Wireless Ad-hoc Networks*, London, UK, 2005.

[38] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: a review," in *Proceedings of 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE),* Hangzhou, China, 2012, pp. 648-651.

[39] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *Proceedings of 2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing*, Dalian, China, 2011, pp. 380-388.

[40] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits, "A language for describing attacks on cyber-physical systems," *International Journal of Critical Infrastructure Protection*, vol. 8, pp. 40-52, 2015.

[41] Y. Jin and D. Oliveira, "Trustworthy SoC architecture with on-demand security policies and HW-SW cooperation," in *Proceedings of the 5th Workshop on SoCs, Heterogeneous Architectures and Workloads (SHAW-5)*, Orlando, FL, 2015.

[42] D. Oliveira, N. Wetzel, M. Bucci, J. Navarro, D. Sullivan, and Y. Jin, "Hardware-software collaboration for secure coexistence with kernel extensions," *ACM SIGAPP Applied Computing Review*, vol. 14, no. 3, pp. 22-35, 2014.

[43] O. Al Ibrahim and S. Nair, "Cyber-physical security using system-level PUFs," in *Proceedings of 2011 7th International Wireless Communications and Mobile Computing Conference (IWCMC),* Istanbul, Turkey, 2011, pp. 1672-1676.

[44] L. Vegh and L. Miclea, "Secure and efficient communication in cyber-physical systems through cryptography and complex event processing," in *Proceedings of 2016 International Conference on Communications (COMM),* Bucharest, Romania, 2016, pp. 273-276.

[45] P. Kathiravelu and L. Veiga, "SD-CPS: taming the challenges of cyber-physical systems with a software-defined approach," 2017 [Online]. Available: https://arxiv.org/abs/1701.01676.

[46] A. A. Cardenas, S. Amin, Z. S. Lin, Y. L. Huang, C. Y. Huang, and S. Sastry, "Attacks against process control systems: risk assessment, detection, and response," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, Hong Kong, China, 2011, pp. 355-366.

[47] B. B. Sanchez, R. Alcarria, D. S. De Rivera, and A. Sanchez-Picot, "Predictive algorithms for mobility and device lifecycle management in Cyber-Physical Systems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, article no. 228, 2016.

[48] S. Rathore, P. K. Sharma, V. Loia, Y. S. Jeong, and J. H. Park, "Social network security: issues, challenges, threats, and solutions," *Information Sciences*, vol. 421, pp. 43-69, 2017.

[49] W. Xu, F. Zhang, and S. Zhu, "Toward worm detection in online social networks," in *Proceedings of the 26th Annual Computer Security Applications Conference*, Austin, TX, 2010, pp. 11-20.

[50] S. Rathore, P. K. Sharma, and J. H. Park, "XSSClassifier: an efficient XSS attack detection approach based on machine learning classifier on SNSs," *Journal of Information Processing Systems*, vol. 13, no. 4, pp. 1014-1028, 2017.

[51] A. Khalid, P. Kirisci, Z. Ghrairi, K. D. Thoben, and J. Pannek, "A methodology to develop collaborative robotic cyber physical systems for production environments," *Logistics Research*, vol. 9, article no. 23, 2016.

[52] N. Y. Kim, J. H. Ryu, B. W. Kwon, Y. Pan, and J. H. Park, "CF-CloudOrch: container fog node-based cloud orchestration for IoT networks," *The Journal of Supercomputing*, vol. 74, no. 12, pp. 7024-7045, 2018.

[53] P. K. Sharma, S. Rathore, and J. H. Park, "DistArch-SCNet: blockchain-based distributed architecture with Li-Fi communication for a scalable smart city network," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 55-64, 2018.

[54] P. K. Sharma, S. Singh, Y. S. Jeong, and J. H. Park, "DistBlockNet: a distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 78-85, 2017.

[55] B. Li, R. Lu, W. Wang, and K. K. R. Choo, "Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system," *Journal of Parallel and Distributed Computing*, vol. 103, pp. 32-41, 2017.

[56] Y. Zhang, M. Qiu, C. W. Tsai, M. M. Hassan, and A. Alamri, "Health-CPS: healthcare cyber-physical system assisted by cloud and big data," *IEEE Systems Journal*, vol. 11, no. 1, pp. 88-95, 2017.

[57] Y. Eun, K. J. Park, M. Won, T. Park, and S. H. Son, "Recent trends in cyber-physical systems research," *Communications of the Korean Institute of Information Scientists and Engineers*, vol. 31, no. 12, pp. 8-15, 2013.

[58] D. Wang, "CRII: CPS: towards reliable cyber-physical systems using unreliable human sensors," 2017 [Online]. Available: https://cps-vo.org/award/1566465.

[59] S. Sundaram, "CAREER: towards secure large-scale networked systems: resilient distributed algorithms for coordination in networks under cyber attacks," 2017 [Online]. Available: https://cps-vo.org/award/1653648.

[60] W. Zhang, "CAREER: hierarchical control for large-scale cyber-physical systems," 2016 [Online]. Available: https://cps-vo.org/award/1552838.

[61] Community Research and Development Information Service of the European Commission, "European network of competencies and platforms for enabling SME from any sector building innovative CPS products to sustain demand for European manufacturing," [Online]. Available: https://cordis.europa.eu/project/rcn/194150_en.html.

[62] Community Research and Development Information Service of the European Commission, "MODESEC (Model-based Design of Secure Cyber-Physical Systems)," [Online]. Available: https://cordis.europa.eu/result/rcn/195574_en.html.

[63] Community Research and Development Information Service of the European Commission, "CPSwarm," [Online]. Available: https://cordis.europa.eu/project/rcn/206005_en.html.

[64] P. K. Sharma, S. Y. Moon, and J. H. Park, "Block-VN: a distributed blockchain based vehicular network architecture in smart city," *Journal of Information Processing Systems*, vol. 13, no. 1, pp. 184-195, 2017.

[65] Y. Sung, P. K. Sharma, E. M. Lopez, and J. H. Park, "FS-OpenSecurity: a taxonomic modeling of security threats in SDN for future sustainable computing," *Sustainability*, vol. 8, article no. 919, 2016.

[66] N. Y. Kim, K. Y. Park, and J. H. Park, "DOTP-AaaS: dynamic one time password matching-based authentication as a service," in *Advances in Computer Science and Ubiquitous Computing*. Singapore: Springer, 2017, pp. 962-966.

Nam Yong Kim https://orcid.org/0000-0003-0667-6872

He is a M.S. student in the Department of Computer Science at Seoul National University of Science and Technology (SeoulTech.), Seoul, Korea. Currently, he is working in Ubiquitous Computing Security (UCS) Lab under the supervision of Prof. Jong Hyuk Park. His broadly research interest includes information and cyber security, cloud computing, IoT, network security, artificial intelligence. Before joining M.S. at SeoulTech, he received B.Tech. in Computer Engineering from Dongguk University Computer Science Institute, Seoul, Korea.

Shailendra Rathore https://orcid.org/0000-0001-8053-2063

He is a Ph.D. student in the Department of Computer Science at Seoul National University of Science and Technology (SeoulTech.), Seoul, Korea. Currently, he is working in Ubiquitous Computing Security (UCS) Lab under the supervision of Prof. Jong Hyuk Park. His broadly research interest includes Information and Cyber Security, SNS, Digital Forensic, IoT. Previous to joining PhD at SeoulTech, he has worked as an Executive -Technology at Crompton Greaves Global R & D, Mumbai, India from June 2013 to July 2014. He received his M.E. in Information Security from Thapar University, Patiala, India and B.Tech. in Computer Engineering from Rajasthan Technical University, Kota, Rajasthan, India.

Jung Hyun Ryu https://orcid.org/0000-0002-0873-8398

He received B.S. in Department of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech) in 2017. Since September 2017, he is with the Department of Computer Science and Engineering, SeoulTech as Master Course.

Jin Ho Park https://orcid.org/0000-0003-1961-6983

He obtained his Bachelor's degree in Software Engineering at Soongsil University, and Master's and Ph.D. degrees in Software Engineering at Soongsil University. He is currently serving as a professor in the department of software at Soongsil University, and the areas of main interests include SW safety/quality/testing, SW fusion/soft power, Internet of Things, military ISR, IT service, IT technology commercialization/ start-up.

James J. (Jong Hyuk) Park https://orcid.org/0000-0003-1831-0309

Dr. James J. (Jong Hyuk) Park received Ph.D. degrees in Graduate School of Information Security from Korea University, Korea and Graduate School of Human Sciences from Waseda University, Japan. From December 2002 to July 2007, Dr. Park had been a research scientist of R&D Institute, Hanwha S&C Co. Ltd., Korea. From September, 2007 to August, 2009, He had been a professor at the Department of Computer Science and Engineering, Kyungnam University, Korea. He is now a professor at the Department of Computer Science and Engineering and Department of Interdisciplinary Bio IT Materials, Seoul National University of Science and Technology (SeoulTech), Korea. Dr. Park has published about 200 research papers in international journals and conferences. He has been serving as chair, program committee, or organizing committee chair for many international conferences and workshops. He is a steering chair of international conferences–MUE, FutureTech, CSA, CUTE, UCAWSN, World IT Congress-Jeju. He is editor-in-chief of *Human-centric Computing and Information Sciences* (HCIS) by Springer, *The Journal of Information Processing Systems* (JIPS) by KIPS, and *Journal of Convergence* (JoC) by KIPS CSWRG. He is Associate Editor / Editor of 14 international journals including JoS, JNCA, SCN, CJ, and so on. In addition, he has been serving as a Guest Editor for international journals by some publishers: Springer, Elsevier, John Wiley, Oxford Univ. press, Emerald, Inderscience, MDPI. He got the best paper awards from ISA-08 and ITCS-11 conferences and the outstanding leadership awards from IEEE HPCC-09, ICA3PP-10, IEE ISPA-11, PDCAT-11, IEEE AINA-15. Furthermore, he got the outstanding research awards from the SeoulTech, 2014. His research interests include IoT, Human-centric Ubiquitous Computing, Information Security, Digital Forensics, Vehicular Cloud Computing, Multimedia Computing, etc. He is a member of the IEEE, IEEE Computer Society, KIPS, and KMMS.