Critical Usability Challenges and Risk Analysis in CPS: A Focus on STP Management

Takeru Kobayashi
Kyushu University, Nishi-ku, Fukuoka, 819-0395, Japan.
kobayashitakeru@jimu.kyushu-u.ac.jp

Correspondence should be addressed to Takeru Kobayashi : kobayashitakeru@jimu.kyushu-u.ac.jp

Article Info
Journal of Machine and Computing (https://anapub.co.ke/journals/jmc/jmc.html)
Doi : https://doi.org/10.53759/7669/jmc202606029
Received 28 November 2025; Revised from 10 January 2026; Accepted 16 January 2026.
Available online 05 April 2026.
©2026 The Authors. Published by AnaPub Publications.
This is an open access article under the CC BY-NC-ND license. (https://creativecommons.org/licenses/by-nc-nd/4.0/)

Abstract – In a Cyber-Physical System (CPS), multiple embedded subsystems interact with the external environment while operating semi-independently, creating complex contextual relationships, exposure to adversarial conditions, and inherent uncertainty. Ensuring secure communication across CPS infrastructure requires the application of fundamental security principles, supported by a combination of approaches such as social engineering awareness, implementation of security standards, vendor-specific controls, and effective network management. Trust emerges as a critical factor in maintaining the security and reliability of CPS communications. This paper reviews key usability challenges and associated risks in CPS environments, analyzes potential attack vectors across different system layers, and discusses strategies for effective trust management to enhance overall system resilience.

Keywords – Cyber Physical System (CPS), Radio Frequency Identification (RFID), Wireless Sensor Network (WSN), STP Management.

I. INTRODUCTION

Physical objects will soon have built-in networking and telecommunication capabilities, and they will soon be widely available. Their impact on society and the economy will be tremendous if these abilities can be used across time and geography. Computer networks and communication channels, for example, are some of the means through which Cyber-Physical Systems (CPS) link the digital and physical worlds. Physical and technical systems can be monitored, managed, and integrated via a central computer and communication core. From nanoscale to large-scale and wide-area systems, the cyber and physical will be tightly intertwined. Many applications of Cyber-Physical System (CPS) [1] may be found in the manufacturing and construction sectors, where robotics and automation are used. Additionally, medical equipment and systems, aviation systems, transportation vehicles, and smart roadways are all examples of CPS application areas. CPS interact with the physical environment and must operate reliably, safely, securely, and efficiently in real time.

With hypertext, TCP/IP, and graphics as key enablers, the Web has evolved into what we know today as the World Wide Web. This interconnection led to advancements in graphics, connectivity and conceptual webs; infrastructure (such as interconnectivity with intensifying bandwidth) and implementations (such as e-commerce, online auctioning, recreation, digital libraries, social networking sites and virtual communities), as well as a wide range of new services and products. It is also possible to think of CPS as a combination of embedded devices, real-time systems as well as networked radar systems, and controllers. Low-cost sensors, low-power, high-capacity computers in small form factors, the wireless communication revolutions, unlimited network capacity, and energy generation are all driving the potential of CPS forward. A growing number of Cyber-Physical System (CPS) distributors are realizing that the innovation base needed to develop large-scale safety-critical CPS accurately, affordably, conveniently, and on schedule is sorely lacking in fields such as aerospace, construction and ecological control, Critical Infrastructure (CI), control systems, industrial automation, and universal health care.

Cyber-Physical System (CPS) combine the discrete logic of computers with the continuous dynamics of physical and engineering systems to monitor and manage them. The unpredictability and noise in the physical world must be taken into account while computing. It is necessary to address the problem of imperfect time and spatial synchronization. Tolerance or containment of component failures in both the cyber and physical realms is required. In addition, the requirements for data security and privacy must be strictly enforced. It is necessary to consider system dynamics on many timescales. Scale and complexity need to be reined in. In order to meet these demands, new scientific and technical concepts must be developed. Building computer-centric designed systems using a trial-and-error approach is not an option anymore; we

need rigorous procedures, verified systems, and robust tools. Analytics and mathematics must take the place of time-consuming and inefficient methods that need a lot of testing. There must be an end to the occurrence of unforeseen incidents and failures; hence, it is necessary to create new sensors and sensor fusion systems.

The convergence of CPS technologies [2] opens up new avenues for study and presents new obstacles. Connected sensors and actuators will be the building blocks of the CPS, which will consist of linked processing clusters and large-scale wired and wireless networks. Applications and demand will drive the connection between the physical and virtual worlds. Security and privacy will be addressed in new and creative ways in the future. It will be possible to meet the new geographical and temporal restrictions. In addition, communication, computation, and control will have novel interactions. Non-technical users will also be able to utilize CPS, and it will be feasible to integrate and influence beyond organizational boundaries. Because of the wide variety of engineering disciplines involved in CPS, it is essential that computer programmers and network specialists collaborate with experts from a variety of other fields in order to create new and improved features. For this reason, colleges' education of engineers and scientists will be revolutionized. The size, makeup, and skill set of the industrial teams responsible for the conception, development, and implementation of CPS will all undergo significant adjustments. Economic systems that become CPS technology leaders will see a major increase in their international competitiveness.

This paper provides an assessment of the usability issues and risk assessment in the CPS system. In this paper, an evaluation of the attacks within the different CPS layers will be done, and a discussion of trust management of the system provided. The rest of the paper is organized as follows: Section II provides an analysis of CPS security. Section III focusses on the usability issues within the CPS, while Section IV critically assesses the risks in the CPS. Finally, Section V draws conclusions to the research work.

II. CPS SECURITY

Data (information) security and control security are the two most common types of security in CPS, although they are not the only kind. Securing data during large-scale data sharing, data processing and data accumulation in a networking ecosystem, certainly in an open, loosely interconnected network, is an important aspect of data security. Keeping the control system safe against attacks on its estimation and execution algorithms is an important component of control security. Control security, in contrast to information security, is concerned with safeguarding the dynamic behavior of controllers against cyber-attacks. Throughout the rest of this article, information security will be the only topic. Also included in this part is an examination of the most critical security elements and goals for CPS as well as the most common attacks and vulnerability assessments for CPS.

Distinguishing Characteristics

The services provided by IT systems may be restricted or controlled without harming the systems themselves. The physical elements of CPS that typically require real-time responses might be adversely affected or delayed by any IT security measures implemented for CPS. Consolidated technologies, uniform protocols, enhanced connectivity, and open access to information are just a few of the many ICS risk considerations that must be considered. As a result, implementing IT techniques for CPS may have a negative impact on real-time reactions and provide prospective enemies several additional possibilities to potentially disrupt the services rendered by CPSs. Standard IT security techniques and methodologies, on the other hand, are unable to solve the security concerns of the CPS because of the disparities in specifications and connection between the CPS and traditional IT security tactics.

There are three typical IT security goals [3], but in the context of CPS security, a fourth goal is included: authenticity. All communications and transactions between authorized parties should be guaranteed in all the various related processes, e.g., actuating, communications, and sensing, therefore, guaranteeing that the sources of different actions which fundamentally affect the systems were generated from the third party. The goal of CPS's authenticity is to check and authenticate both parties involved in the communication and any connected processes. In contrast to IT systems, CPS prioritizes availability above secrecy and integrity before confidentiality and authenticity. Priority should be given to ensure the proper parties are who they claim to be, since all the other security objectives would be rendered ineffective if it is not possible to verify their authenticity. Suppose an un-authorized (malicious) party gained access to the system and exposed private data. This would compromise system integrity since it is possible for such a party to modify data. Due to the lack of human interaction, a strong authentication method must be included to secure the system and make proper judgments on the acceptance or rejection of incoming instructions and data. A robust authentication mechanism. Because adequate access control is so crucial to CPS security, identity-based IT security is considered the most significant aspect.

Access controls are a fundamental segment of data security since they control who might access and use corporate services and data. As part of access control rules, verification and authorization guarantees that users who they claim to be and have authorized accessibility to corporate information and data. It is also possible to utilize access control to restrict accessibility to campuses and other buildings, as well as datacenters. Passwords, usernames, PINs, biometrics, and other types of security tokens may all be used to identify a user in an access control system. Multifactor authentication (MFA) is a typical feature of various access control frameworks. MFA entails verifying a user's identity using various authentication methods. Once a user's identification and Internet Protocol (IP) [4] address is verified, access controls might allow the required degree of accessibility and authorized activities for specific users. Controlling who has access to what resources is

a complex process that may be broken down into four distinct categories. In most cases, companies choose for the approach that best meets their specific security and regulatory compliance needs. **Table 1** shows the four different access control models.

Table 1. Access Control Models

Models	Details
Discretionary access control (DAC)	As the system administrator or operator, you may control who has access to your protected information or data.
Mandatory access control (MAC)	People are provided access to data in this nondiscretionary paradigm based on a level of data clearance. Based on the degree of security, a central authority controls access permission. In military and government contexts, this approach is often used.
Role-based access control (RBAC)	Instead of providing accessibility based on a user's identification, RBAC bases it on predefined business operations. Users should only have access to information that is relevant to their jobs in the company. One of the most often utilized methods is built on a complicated mix of roles and permissions.
Attribute-based access control (ABAC)	Access is determined by a set of traits and ecological elements, such as timing of day and geography, allocated to both resources and services in this dynamic manner.

Traditional security methodologies in IT and CPS vary in that they target security for particular system component in stead of the interconnection between these elements. As a result, safety (the absence of failure) instead of security (unauthorized physical access) should be the primary focus. Traditional methodologies may give some security and safety assessments and solutions for complex systems. In such systems, it is difficult to take into account new challenges such as network diversity, element interactions and cyber linkages. An example of such a problem is when an authentication attempt fails because a control parameter was changed. Thus, a security breach occurs without any system failures. This means that a system cannot be called secure if it does not have any failures. As a consequence, existing security measures won't be enough to keep CPS safe from hackers. Consequently, the primary security issue is to evaluate interactions between different CPS components.

In order for CPS to function, the three Information Technology (IT) security goals i.e., CIA (Confidentiality, Integrity and Availability) [5] must be met. Physical processes cannot be managed if the cyber-system is unavailable, and the consequences may be disastrous, especially for real-time activities. A lack of proper confidentiality, integrity, and accessibility mechanisms could lead to the deception of critical data; without an authentication methodology, receiving datasets could be sent from the intruder or released from unauthorized parties. CPS's four major security goals may be summed up in these four terms. It is necessary for CPS to carry out a variety of tasks, including securing access to devices, securing data transmissions, securing applications, securing data storage, and securing actuation. These conditions are briefly described in the following sections.

Securing Accessibility to Devices

The first problem is securing access to a device. Unauthorized items will be able to obtain access to and influence the system if authorization is not implemented or is inadequately supported, hence confidence in any fundamental binary codes or functionality at the application levels is not assured. Network security is vital to securing client information and data, assuring reliable accessibility and network performance, and securing networks from cyber threats. In an event of data breach or cyber-attack, well-designed network security solutions save overhead costs and secures users from catastrophic damages. Providing consumers with lawful access to systems, apps, and data is critical to a company's ability to operate and offer goods and services.

Securing Data Transmissions

Detecting and blocking illegal access to CPS communication networks necessitates the use of data transmission security. The physical aspects of system power consumption and timing patterns, for example, are being intercepted by at- tackers in order to examine the data that is provided and received. DoS assaults and routing topology disruptions [6] are two methods used by attackers to disrupt networks. Data processing and transmission capabilities and enough storage capacity are lacking in certain terminal devices that are not part of a computer system. As a result, penetration attacks on these devices are more likely. Although open networking standards may assist increase system performance and minimize operating costs in Industrial Control System terminals, they can also be a disadvantage.

Despite the fact that these terminals allow for more effective and efficient operations, they also expose systems to greater risks of hostile assaults and intrusions, including malware (harmful code), distributed denial of service (DDoS), listening in on conversations, and unauthorized access. Additionally, the de-signing procedure has a limited amount of processing timeframe (speed), power consumption, and hardware resources. This directly causes vulnerabilities. Furthermore, embedded systems are created by professionals who have little or no expertise with security concerns and concentrate more on functionality, error remedies, and efficiency than security. As a result, the system develops flaws that allow unauthorized or undesirable people to access sensitive data.

Securing Applications

There are many distinct applications and security issues on the application layer. Certain security concerns do not exist at the other levels; thus, the privacy protection issues that must be dealt with at this level will not be handled there. As a result, attackers have access to the private data of users, resulting in data leaks and privacy violations. Because this data may include information about previous and current places visited by users, various data security approaches include location camouflage, anonymity space, and space encrypting. There are a lot of social applications on this layer, and they need to be safeguarded.

Securing Dataset Storage

Secret datasets within CPS devices must be safeguarded. Sensors, the most common CPS node, are resource-constrained, remotely linked devices. Cryptographic methods may be used to encrypt data in these devices, but the constrained memory and limited computational power make them insufficient. Lightweight security methods are now required as a consequence of this development.

Securing Actuation

In order to ensure actuation security, only authorized sources are permitted to perform any actuation activities. An adversary will not be able to tamper with the feedback or control instructions provided. It is inevitable that security concerns will arise when utilizing the Web as a transmission layer in CPS connections. As a rule of thumb, security should be applied across the whole system rather than just the functioning security measures at each layer. In addition, any desirable security solution presently requires expensive calculations and huge memory demands.

III. USABILITY ISSUES IN CPS

Attacks on CPS

The physical environment might be severely impacted by attacks against CPS. Each CPS layer is vulnerable to both passive and active assaults. There are more assaults that can be made on a CPS system than on a standard IT system because of the usage of the Web, that is already being utilized to transmit the system's data. There are many different types of assaults that may occur on the perception layer, the transmission layer, and the application layer. These integrate the hazards on the nodes e.g., the sensor and actuator, data damages or leakages, and security vulnerabilities during the transfer of data. As a result, a thorough analysis of potential threats and the development of a solid security architecture are necessary. According to Lamba [7], various assaults may affect all layers at the same time. These include the following (see **Table 2** below):

Table 2. Attacks on the CPS Layers

Attack	Details
Denial of Service (DoS)	Blocks traffic to make the networks and services inaccessible by exploiting a protocol flaw, for example, by overloading a resource with fake requests. As a result of this, the DDoS assault is a frequent one that affects several resources, e.g., infrastructure and end-devices at the same time, limiting accessibility to services and data.
Man-in-the-Middle (MITM)	Unwanted actions, e.g., limiting major functions dependent on the received messages could amount to sending a phony message to a targeted resource, for instance. It is also possible for this sort of assault to be proceeded by eavesdropping on the network layer.
Eavesdropping	Intercepts any datasets sent by systems. In the CPS, for instance, sensor networks might communicate control data to applications, making it vulnerable to eavesdropping. The system's monitoring might potentially lead to users' security being violated.
Spoofing	The user acts as a legal member of a model, then try to participate in the system’s activities. Once accessibility is gained, the intruder will be able to do any action, such as modifying, removing, or adding information.
Replay (playback)	To regain the confidence of the system, a packet acquired from the target node is retransmitted. A spoofing operation is one in which the identification data of one of the devices is altered or responded to.
Compromised Key	Spies on the secret key used to encrypt communications. As a timing (side channel) assault, this may be done by analyzing how long it will take to encrypt the data. Compromise of one secret key will allow unauthorized access to other private keys in the same system, which may then be exploited to alter the data. Sometimes, an attacker may get control of sensors and demand they execute engineering tasks in order to acquire additional internal keys. Once the sensor node is replaced, an attacker might pose as genuine to exchange key with other sensors and get access to all the other private keys of the nodes they're exchanging with.

At every level of the CPS, there are numerous sorts of threats, and the most typical assaults may be categorized as follows.

Attacks at the Perception Layer

The end devices, e.g., RFID sensors and tags, form the perception layer, and are confined by memory capacity and computational resources of their host computers and mobile devices. These devices are often positioned outside, making them vulnerable to physical assaults, such as interfering with or changing their elements. Terminal systems are the most vulnerable to a wide range of cyberattacks, as a result. At the perception layer, prevalent attacks entail equipment malfunction and line malfunction; witch, radio interference; perceptual file corruption; nonlinear power assessment; data breaches; information monitoring; interfering; sensing data leaks; physical harm; and energy depletion. These attacks (in **Table 3**) may take several forms, including:

Table 3. Attacks on the Perception Layer

Attack	Details
Node Capture	After gaining control of the node, the attacker gains access to encrypted data, which is subsequently exploited to compromise the whole system's security. Availability, confidentiality, authenticity, and integrity are the primary goals of this assault.
False Node	Intrudes on the integrity of data by transmitting malicious data via a new node on the network. As a result, the system's nodes might be subjected to a denial-of-service attack (DoS).
Node Outage	Disables the ability to read or collect data from nodes by interrupting their services and launching many additional attacks that compromise the system's integrity and availability.
Path-Based DOS	Depletes the node's battery and causes network disruption by flooding it with high numbers of messages. This reduces its ability to communicate with other devices.
Resonance	Disrupts the resonance frequency of vulnerable detectors or actuators
Integrity	Attempts to interfere with the system by introducing erroneous sensor data and erroneous exterior control inputs.

Attacks at the Transmission Layer

Information leakage during transmission is a common sort of attack on this layer. The accessibility of the transmission medium, particularly in wireless communications, is to blame for this. For example, an attacker may intercept a radio transmission, alter it to seem like the legal user, and then retransmit the message. Because of these and other variables, such as high traffic congestion and remote access techniques, the risk for an attack increase. Traffic analysis, manipulation, exhaustion, collusion, black hole, inundation, hidden passageways, sink node, orientation deceptive sinkhole, wormhole, improper route selection, tunnelling, and unlawful access are some of the most common assaults on this layer. Examples of frequent transmission layer assaults are shown in **Table 4**.

Table 4. Attacks on the Transmission Layer

Attack	Details
Routing	Networking transmission may become more difficult, or the source route may extend, as a consequence of routing loops.
Wormhole	By creating bogus channels via which all signals are routed, it creates data gaps in the system.
Jamming	Signal interference may be introduced into a wireless medium between sensor nodes and a distant base station by jamming the channel. Intentional networking interference might lead to a distributed denial of service (DDoS) attack.
Selective Forwarding	Selected packets will be forwarded from a hacked node. Node compromises might cause packets to cease being sent to their intended destinations and/or reject all other signals whereas this node is regarded to be valid.
Sinkhole	Notifies other nodes of the optimum route to take in order to send traffic to them. There are a variety of ways to use this assault, such as phishing and targeted forwarding.

Attack within the Application Layer

Threats against the application layer might result to security loss, data loss, and unauthorized disclosure to devices, since a substantial quantity of users' information is acquired at this level. This includes user privacy leaks, fraudulent code, databases and controller command forgery threats at the application layer. **Table 5** displays common instances of assaults on this layer.

Table 5. Attacks on the Application Layer

Attack	Details
Buffer Overflow	Attacks are launched by exploiting any software flaws that result to buffer overrun flaws.
Malicious Code	Malicious programs, e.g., worms and viruses, are sent to assault the user application, causing the system to slow back or pose a risk.

IV. RISK ASSESSMENT

Because of the growing prevalence of CPS in so many high-risk industries (such as smart healthcare and home automation), the demand for a reliable technique of risk assessment has never been greater. The concentration of risk evaluation has transformed from computer risk evaluation to network risk assessment, particularly in light of the increasing reliance on the Internet. CPS risk assessment is intended to provide a quantifiable model for future system stability. Many research and efforts have been devoted to enterprise architecture that are not directly connected to CPS. To a large degree, CPS security differs from standard IT systems in terms of the security features. Insecure linkages and the exchange of information are only a few examples of the many dangers associated with ICS. First, the CPS threat assessment framework outlines what will occur to the system; next, it estimates how likely it is that it will happen; and finally, it estimates the implications. In addition, the asset (value), risk, and susceptibility identifications must all be considered when assessing CPS risk.

Asset Identification

As a resource with a monetary or intangible value, an asset must be safeguarded. Examples include medical equipment, industrial facilities, device activities and educational facility operations and information. Intangible assets include, for example, data about the business or an association's public image. In truth, most assets are intangible, and as a result, they should be safeguarded since their worth is directly tied to many everyday transactions and services. The harm caused by direct and indirect financial losses may also be used to determine the value of assets. To determine the system's worth, it is necessary to identify the system's protection layers, vital assets, and essential operations. Cyber assets, physical assets, and interconnections with other networks make up the three main categories of CPS assets. The inter-communications of CPS are complicated, intangible, and intertwined with other networks, which distinguishes them from traditional IT assets.

Threat Identification

Risk identification in the area of CPS is a difficult task, and this phase helps in that process. It is possible to measure the occurrence of the risk using historical information, while sample logs and records in IDS (Intrusion Detection System) [8] are used to evaluate the threat. Authors conducted an analysis that identifies new CPS IDS methodologies, recommends new research goals, and presents an evaluation of most researched CPS IDS methodologies, which is beyond the scope of this work.

Vulnerability Identification

An asset's value may be damaged or eavesdropped on by an opponent if it has a vulnerability that can be exploited for espionage purposes. A circumstance or setting that may be abused by an advertiser to attack or harm systems is also included in the definition. When a system's flaws are identified and documented remedial measures or mitigations are identified and executed, a vulnerability evaluation has been successfully completed. Network, system, and management flaws are the most common types of CPS flaws. Design, hardware, and management flaws all contribute to networking vulnerability. Deficiencies in the platform's setup, software and hardware, and lack of security approaches, are all examples of platform vulnerabilities. The absence of security rules is the most significant contributor to management vulnerabilities. The previous expert evaluation methodologies, comparison with historical data, or best experience in businesses may all be used to arrive at a vulnerability quantification. It is almost impossible to completely eliminate or avoid all dangers. It is for this reason that risk mitigation strategies based on the least number of resources are often used.

As physical and cyber activities become more intertwined, the number of considerations that CPS must make while creating a security approach for such systems increases. A more complex degree of security is required since the ecosystem is typically transforming and devices might be dynamically interlinked in various locations. Because of the challenges in avoiding, detecting, and mitigating threats, setting up a security system may be complex. Since cyber and physical systems interact, stopping the attack is very challenging. It isn't only direct flaws that are exploited by specific attackers. When developing detection algorithms for all levels of the CPS, it's important to think about the application, transmission, and perception layers as well. Detecting assaults is the most difficult part of the job. One of the most pressing issues is how to create a security mechanism that can prevent and detect breaches in the detection or preventive phases of the system

Security Requirements

CPS security difficulties may be divided into two segments: (1) the issues arising from the heterogeneous systems, which are coupled to accomplish appropriate arrangements; and (2) the prominent factors from the functions and components of

applied security to accomplish the needed security objectives. Due to CPS's wide-ranging Internet and Wireless Sensor Network (WSN) connection, CPS's security infrastructure will integrate, for instance, all challenges related to Internet security. Unlike conventional IT, CPS do not have the same level of consistent analytical and execution processing power to meet higher security needs. The dynamic nature of the environment makes it very challenging to implement any form of unified security solutions. At every layer, most of the solutions recommended strive to focus on various security concerns. There may be some benefits to using these methods, but there may also be dangers in other portions of that system. In order to address this concern, a CPS system infrastructure is employed to secure security across all the levels, e.g., data collection, data transmission and data analysis, from the lower layer to the upper one. A bottom-up assessment is presented in the next sections of the security organization of every layer of CPS since there are various security problems at each layer that must be addressed to secure such systems against possible in adversaries. .

Security Assessment within the Perception Layer

This layer's major goal is the perception, identification, and collecting of data about objects. In addition, the increasing number of linked devices creates new security risks. Due to their limited capabilities and frequent use of less secure wireless communications while linked to the Internet, attacks on these types of devices could easily get access to more sensitive information, execute malicious programs, and also restrict accessibility in certain situations. As a result, safeguarding these devices and preventing information leakage is critical. Physical assaults, e.g., tampering with device components or substituting devices with another, may come from attackers exploiting newly installed devices, many of which are placed in external or outdoor locations.

As a result, installing a novel device is a crucial consideration. Unauthorized access and disclosure of sensitive information, as well as the installation of dangerous applications that might destroy the system, are all too common when it comes to physical layer devices. Since, applying authentication to these devices is very difficult because there are so many objects and organizations with restricted capabilities implicated. Encryption is a good authentication method for this tier. However, the limited resources of certain devices (such as sensors, contactless intelligent cards, and health-care equipment) make it impossible to incorporate appropriate cryptographic features. As a consequence, field devices need a proposed authentication system due to their low computing power, which is the emphasis of research now. Therefore, verification and accessibility control procedures prohibit accessibility from unauthorized nodes, protection against physical attacks, data encryption assures confidentiality of information and prevents the publication of private information during the transfer of data, Due to the widespread use of and WSN and RFID techniques [9], the evaluation of these different systems will be examined in detail in the next two subsections.

Remote data storage and retrieval is made possible via the use of Radio Frequency Identification (RFID). The key benefit of employing RFID is the identification of the target device without the need for user intervention. Real-time accuracy is a characteristic of RFID technology; however, most tags do not contain any form of security measure, and those that do not integrate security utilize hashing algorithms or conventional ways owing to power, computing, and storage limits. As widely utilized as RFID has become in recent years, it still presents a number of security concerns. These include uniform coding due to the lack of uniform standards, which could prevent the reader from accessing data; conflict collisions as a result of transmitting data from various RFID identifiers at the same time, which could disable the reader; and data confidentiality due to the use of cost-effective RFID tags, which have scares resources (for example, weaker algorithmic cap).

Despite its many security flaws, RFID is still considered an essential component of CPS because of its wide range of capabilities, which include the detection of environmental and physical alterations, movements and velocity, temperatures, humidity, gases, and illumination sensing. Device verification is an important aim in terms of security, and creating an effective authentication system needs tags with enough processing and storage capacity. On the other hand, low-cost RFID tags other hand, lack the requisite specifications for reliable security measures. As a result, the resource limitations of RFID make it impossible to apply any of the typically utilized security approaches (e.g., Diffie– Hellman key exchange, SSL, PKI, and IPSec). The primary RFID security problems are uniform encoding, dispute collision, data confidentiality, and location privacy. As a result, there is a significant need for consistent encoding formats, conflicts collision avoidance and identification, as well as lightweight dataset security protocols. Lightweight security protocols and input signals technologies, which are well-suited to low resources, may be used in RFID to ensure data integrity, authenticity, and secrecy.

Distributed detectors, such as temperature sensors, chemical sensors, and pressure sensors, make up Wireless Sensor and Actuator Networks, or WSNs. Self-organizing systems with variable network architecture and extensively spread multi-hop cellular networks are also known as "multi-hop" networks. As a result, WSN have a limited number of resources, such as limited data storage, computing capability (e.g., 16-bit or 8-bit processor design, 8 MHz operating frequency), and limited power infrastructure (such as a power supply), which will affect their capabilities to accomplish any security methodology. Due to the fact that an attacker's substituted device may perceive sensor data, existing research focuses on maintaining data authenticity and integrity at the expense of secrecy. In certain circumstances, sensor nodes may be vulnerable to physical assaults if they are put in an open area where they are not regularly monitored; this is one of the security issues associated to sensor nodes. The key pre-distribution technique, key storage and allocation, and

cryptographic algorithms utilizing less energy are the primary difficulties that have yet to be adequately addressed when employing cryptographic algorithms.

Cryptographic techniques, key control, safe routing, as well as trust management could in sequence eliminate or troubleshoot WSN security issues. In WSNs, both symmetric and asymmetric cryptographic techniques have been used. Nevertheless, each form has its own advantages and disadvantages. Even though key exchange protocol problems e.g., complexities of key exchange protocol, and the security of the key data are common in the symmetric encryption community, symmetric encryption is widely employed since it necessitates few computing computations compared to asymmetric encryption. It is also possible to use asymmetric cryptography (public key), which has the following advantages: excellent scaling, correct node authentication, and improved network security. As a result, research will concentrate on improving computational processes as well as parameters (algorithm variables) utilized in public key cryptography.

Sensor nodes have yet to benefit from a lightweight cryptography scheme. In the end, there are advantages to using asymmetric and symmetric encryption, but no one technique can address all of WSN's security concerns. It's possible to use hardware that consumes less power, plus software that has been optimized for both authentication and encryption. WSN devices with little memory and computing power cannot use the 1024-bit keys asymmetric cryptography, which can be employed on the ad hoc network. Most research is focusing on symmetric encryption approaches, which include hashing, as an alternative to hashing. In addition, devices with restricted capabilities may make use of strengthened asymmetric cryptographic algorithms, such as Elliptic Curve Cryptography (ECC) [10].

The second most critical component in WSN security is key management that integrates generating, distributing, storing, updating and removing the secret keys. Encryption protects communication routes between nodes with the use of a secret key. Furthermore, several techniques have been developed for the protection of data integrity and confidentiality using public key cryptography. Numerous key distribution systems have been created employing symmetric cryptography that is dependent on sensor network features. There are four basic methods for distributing keys, which include simpler key exchange protocols, key pre-distribution arrangements and dynamic keys management. The development of asymmetric cryptographic key distribution methodologies as a networking authentication mechanism became necessary as a result.

In wireless networks, a typical routing method is not suitable since most such protocols were originally built for landline networks. SSH and SSL, as two examples of end-to-end authentication protocols, require to include certification across nodes in order to provide WSN. As a consequence, asymmetric cryptography, e.g., NtruEncrypt (an encryption technique) and Elliptic Curve, became the primary emphasis of WSN security. WSN node trust management is primarily used to address open network security concerns. Authentication algorithms for sensors should be combined with implementations of trust privacy and security for sensors and ground stations. Network security and limited resources must be balanced in a manner that includes all network nodes in trust management. For WSN devices with limited storage and computing power, an authentication mechanism must be developed. WSN security is often overlooked in research projects, and a model, which integrates the above-mentioned features of more complex cryptographic methodologies, secure routing methodologies and trust control should be in place to ensure their safety.

Security Analysis at The Transmission Layer

As a result of the widespread usage of networks in linking devices and enhancing user comfort, there are several security risks and vulnerabilities that may be exploited or eavesdropped on. However, although the simplicity of wireless connectivity is appealing to end users, it also allows hackers to engage with the system, potentially resulting in damage or the theft of sensitive data. Machine-to-machine communications in CPS varies significantly from that on the web, which is just human-to-human communication.

Machine-to-machine connections were not the primary focus of the current network security architecture (such as communications between devices within the CPS). Due to the absence of interoperability between linked devices, machine-to-machine data transfer presents a security risk. Current network protocols, which are primarily intended for Internet usage, are unable to address these security concerns. Despite the fact that these protocols still provide some safeguards, they are not the ideal answer. In order to acquire access to users' personal information, attackers might take advantage of any weaknesses in heterogeneously linked devices. It is critical to safeguard the network as a whole in order to safeguard the devices connected to it. To ensure the safety of the system, devices should be able to detect any anomalous behavior or condition. In order to do this, a strong transmission protocol and software with Intrusion Detection must be implemented on the devices. There are two forms of transmission layer security.

Firstly, the linked devices, and secondly, the associated technologies and the ensuing flaws of the defined protocols during the process of implementation. Within wireless networking, nodes might shift dynamically with not initial authentication, hence amounting to more threats that can be fraudulently leveraged to undermine the securing of networks being used.

Ad hoc networks and wireless networks may be used to connect to the internet. This kind of network is known as ad hoc (p2p) or peer-to-peer and does not require a central station for communication between nodes The nodes may be readily altered to some extent in this network. This type of network is vulnerable to attack because of the radio channel that may be tapped by hackers. There are three typical security issues in this network route security, data security, and node

access. Authentication and authorization mechanisms may be used to prevent unauthorized access to nodes. Key management mechanisms for authentication and encryption may be used to provide a suitable solution to the information security problem. Encryption technologies may be used to solve the problem of routing security. The most extensively used wireless network is Wi-Fi, as referred to as IEEE802.11. Nodes communicate with each other through stationary bridges (base station) e.g., WLAN (Wireless Local Area Network) [11]. Wi-Fi networks allow almost any computer or mobile device to connect wirelessly and interact with other apps on the Internet. In spite of the ease of using Wi-Fi, there are a number of security concerns, including DDoS attacks and illegal access. Authentication protocols and networking encryption are employed to address such security problems.

Data may be encrypted in two ways: end-to-end and hop-by-hop. Whereas data is being sent, hop-by—hop encryption methods encrypts it by the same technique. Plaintext should be maintained for every stage in the decryption and encryption processes. To guarantee that only the sender and receiver may access encrypted information during transmission, end-to-end encryption is employed. Employment of hop-by-hop encryption is possible in order to protect just the connections between nodes. This method has several benefits, e.g., low latency and cost, and high efficiency, every node might decrypt datasets; and they should be deemed trustworthy because of this. Moreover, the nodes' application processes are in charge of the system's security in this case. For example, only the sender and receiver can decrypt encrypted data using end-to-end encryption systems, and eavesdroppers cannot get the cryptographic keys needed to do so. However, this method is difficult to put into practice, especially with limited end devices like sensors. Customers and servers may agree on security parameters through SSL/TLS, an example of an end-to-end protocol.

Wireless networks, in particular, pose a significant security risk to CPS networks. An efficient network security system requires key agreement and end-to-end authentication, cross-network authentication, safe routing, and cross-domain authentication mechanisms. Data integrity and confidentiality may be improved by ensuring that nodes cannot be accessed by outsiders and that network routing is secure. In order to secure communication between devices and systems, point-to-point and end-to-end security architectures may be utilized. The former protects hop-by-hop transport security, e.g., mutual authentication and network certification. Secrecy and availability of data may be safeguarded at the first and second sublayers, respectively. Because most standard communication security methods were not designed to handle diverse networks, a new secret technique is needed. Network congestion and redundancy may be caused by connectivity and capacity issues (e.g., address spaces). IP technology is not designated to handle larger numbers of interlinked devices. Resultantly, IPSex, a protocol, which provides both encryption and authentication, is growing in popularity. By implementing this protocol, VPNs may be set up. 6LoWPAN has been suggested and it employed in a compressed IPv6 packet header version owing to the IP protocol's constraints, particularly in CPS. As a result of this added expense, however, the protocol suffers its major weakness. Secure communication may be provided through TLS/SSL and Internet Protocol Security (IPSec) [12], two well-established protocols that enable integrity, authenticity, and confidentiality across several layers.

Security Assessment within the Application Layer

This layer has a large number of apps, each of which contains a flaw that might compromise the security of the CPS. In addition, the application layer has significant hurdles in protecting user privacy and acquiring hierarchical access to sensory data. For example, in Smart Homes and Smart Cities there are services and industrial surveillance applications that may be accessed over this layer. The primary source of worry for system security is the possibility that flaws in the design might be exploited by malicious actors in order to compromise the system. A malicious program may be started to compromise system security this way. If many approaches are integrated, data processing may be hindered and the system become bottlenecked, leading to security concerns. The system's availability and dependability might be negatively impacted by these security problems. Wu, Zhao, Riguidel, Wang and Yi [13], for example, mentions trust as an element of security. A system's security does not require the availability of trust, nor does it necessitate embedding trust within the system.

Information access, user authentication, data privacy, and data link collapsing are all aspects of application layer security. Every application has its own set of security needs, and the need to meet these requirements is expanding as the use of critical systems that must be constantly monitored and controlled grows. When it comes to intricate security challenges, it all relies on the sort of application you're working with. This means that designing applications that can be trusted amongst themselves without considering the system's underlying functions, such as connection and data provided by CPS, is challenging. Another problem is that the CPS applications vary by industry standard. CPS application layer interactions and growth are still ungoverned by any worldwide standard, adding to the lack of security. As a result, the security requirements for various types of applications vary. Various authentication frameworks for diverse applications make integration extremely complicated when assuring identity verification. A substantial number of the devices that are connected and the shared dataset results within the wide-range software overhead that will be mirrored in the accessibility of services issued by such interlinked devices; the majority of individuals; and many other security issues should be taken into consideration when developing CPS applications.

V. CONCLUSION

In a Cyber-Physical System (CPS), a computer network in which a component is managed or regulated by computer-based techniques is known as an intelligent system. To understand cyber-physical systems, it is important to understand how the hardware and virtual components communicate with one another, how they work at various geographical and temporal scales, and how they interact in ways that alter depending on the environment. Cross-disciplinary methods, such as those rooted in cybernetics, mechatronics, and design, are all part of the CPS. Embedded systems are a common term used to describe process control. Embedded systems place a greater focus on the computational aspects than on a close connection between the cognitive and physical parts. There are many similarities between CPS and the Internet of Things (IoT), however CPS has a greater level of coordination and cooperation between physical and computer components. An authenticated user's identity should be a top priority for all other CPS security goals since it provides a foundation for all other security classes to be established. It's impossible to achieve any other security goals unless you can verify that the authorized party is who they say they are. Any cryptographic approach to accomplish security goals ought to be light-weight for it to be cost-effective for the devices, which have restricted capabilities. As a result of this, it is possible to overcome the limitations of these devices. Many security threats may be addressed most effectively and effectively by using authentication.

CRediT Author Statement

The author reviewed the results and approved the final version of the manuscript.

Data Availability

The datasets used and/or analysed during the current study are available from the corresponding author on reasonable request.

Conflicts of Interests

The author declares no conflict of interest

Funding

No funding agency is associated with this research.

Competing Interests

There are no competing interests.

References

[1]. R. Johari, A. Kaur, M. Hashim, P. K. Rai, and K. Gupta, “SEVA: Secure E-Voting Application in Cyber Physical System,” Cyber-Physical Systems, vol. 8, no. 1, pp. 1–31, Nov. 2020, doi: 10.1080/23335777.2020.1837250.

[2]. E. S. Faden, “Assimilating New Technologies Early Cinema, Sound, and Computer Imagery,” Convergence: The International Journal of Research into New Media Technologies, vol. 5, no. 2, pp. 51–79, Jun. 1999, doi: 10.1177/135485659900500205.

[3]. R. Picciotto, “Why the world needs millennium security goals,” Conflict, Security & Development, vol. 6, no. 1, pp. 111–120, Apr. 2006, doi: 10.1080/14678800600590777.

[4]. E.-J. Yoon and K.-Y. Yoo, “An Improvement of the User Identification and Key Agreement Protocol with User Anonymity,” Informatica, vol. 23, no. 1, pp. 155–172, Jan. 2012, doi: 10.15388/informatica.2012.354.

[5]. N. Edwards, S. B. Kiser, and J. B. Haynes, “Answering the Cybersecurity Issues: Confidentiality, Integrity, and Availability,” Journal of Strategic Innovation and Sustainability, vol. 15, no. 4, Aug. 2020, doi: 10.33423/jsis.v15i4.2956.

[6]. G. R. K. RAO, “Preventing Mobile Blockade and DDOS Assaults in ICN Network Communication Using Routing Path Identifiers,” Journal of Research on the Lepidoptera, vol. 51, no. 1, pp. 234–245, Feb. 2020, doi: 10.36872/lepi/v51i1/301020.

[7]. A. Lamba, “A Through Analysis on Protecting Cyber Threats and Attacks on Cps Embedded Subsystems,” SSRN Electronic Journal, 2020, doi: 10.2139/ssrn.3517474.

[8]. S. A. Hussein, A. A. Mahmood, and E. O. Oraby, “Network Intrusion Detection System Using Ensemble Learning Approaches,” Webology, vol. 18, no. SI05, pp. 962–974, Oct. 2021, doi: 10.14704/web/v18si05/web18274.

[9]. С. П. Санников and Э. Ф. Герц, “Method of the monitoring illegal chopping tree with use RFID-device and WSN-network,” Известия СПбЛТА, no. 219(), Sep. 2017, doi: 10.21266/2079-4304.2017.219.173-183.

[10]. A. V. Tsiganov, “Duffing Oscillator and Elliptic Curve Cryptography,” Nelineinaya Dinamika, vol. 14, no. 2, pp. 235–241, 2018, doi: 10.20537/nd180207.

[11]. J. Huang, “Cross layer link adaptation scheme in wireless local area network,” Journal of Computer Applications, vol. 29, no. 2, pp. 518–520, Apr. 2009, doi: 10.3724/sp.j.1087.2009.00518.

[12]. S. Hermann and B. Fabian, “A Comparison of Internet Protocol (IPv6) Security Guidelines,” Future Internet, vol. 6, no. 1, pp. 1–60, Jan. 2014, doi: 10.3390/fi6010001.

[13]. Y. Wu, Y. Zhao, M. Riguidel, G. Wang, and P. Yi, “Security and trust management in opportunistic networks: a survey,” Security and Communication Networks, vol. 8, no. 9, pp. 1812–1827, Sep. 2014, doi: 10.1002/sec.1116.

Publisher’s note: The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations. The content is solely the responsibility of the authors and does not necessarily reflect the views of the publisher.