A Review of CPS Design and Vulnerability Analysis

[1]Andrea Vilan and [2]Pamela Walker
[1,2]American University, Massachusetts Avenue, NW, Washington, DC 20016
[1]vilanandrea@american.edu

Article Info
Journal of Computing and Natural Science (http://anapub.co.ke/journals/jcns/jcns.html)
Doi: https://doi.org/10.53759/181X/JCNS202202014
Received 16 January 2022; Revised form 10 April 2022; Accepted 05 May 2022.
Available online 05 July 2022.
©2022 Published by AnaPub Publications.

Abstract – Cyber-Physical Systems (CPS) offer a wide array of applications. Integration of various heterogeneous infrastructures that generate data for intelligent analysis is discussed. The objective of this article is to review CPS and provide a discussion of the system's security flaws. Many earlier investigations have also been properly explained. Because of the increasing usage of CPS in sensitive organizations (e.g., healthcare and connected homes), the requirement for a risk assessment strategy is essential. The major concentration of risk evaluation has shifted from computer risk evaluation to network-based risk analysis as a result of our substantial dependence on the Internet. The goal of CPS vulnerability analysis is to develop a quantitative model for future system protection.

Keywords – Cyber-Physical Systems (CPS)**,** Denial of Service (DoS), Radio Frequency Identification (RFID)

I. INTRODUCTION

Computer systems, Information and Communication Technology (ICT), and physical phenomena and interplay are all intertwined in Cyber-Physical Systems (CPS). Child protection services abound in today's culture. From the smallest to the greatest sizes, examples are available. According to many experts, the microgrid is one of the most complex and critical CPSs. Consequently, smart grid security receives a lot of attention in study. Among the most current research on smart grid attacks are the following: Research difficulties (majorly from an ICT aspect) and In-depth research on CPS testbeds, focused on a comprehensive list of potential vulnerabilities and assaults. This is presented in two papers: a long survey report that includes an outstanding qualitative discussion and categorization of attack and defensive tactics.

CPS testbeds and the most frequent smart grid vulnerabilities are discussed in this article. Threats in the smart grid may be divided into four categories, as outlined in [1]. developing new methods and methodologies for assessing the danger of smart grid attacks and the systems' ability to withstand such attacks. There are a number of ways to build, detect, identify, and repair smart grids. For smart grids and industrial CPSs, the researchers also give a categorization of attack types, a high-level study of assaults and detection techniques, as well as a comprehensive evaluation of the key control mechanisms. Their discussion focuses on the dangers and weaknesses of Phasor Measuring Units (PMUs) and the GPS.

Because of the fast expansion of the informational network and the increased incorporation of crucial infrastructures and IED (Intelligent Electronic Device) devices into the energy CPS (Cyber-Physical System), electrical power networks are now facing exceptional cyber-attacks. Cyber-attacks are increasingly likely to occur because of the widespread use of ICT (information and communication technology) [2]. When one layer of an interconnected network fails, the whole network is affected, resulting in fragmentation and cascade failures. This results in an anomalous power flow transition. Cascading failures and cyber-attacks will ultimately lead to a blackout like the big blackouts that happened in North America in 2003, Rome in 2004, and Ukraine in 2015.

Small impact and scale-free properties have been found in several investigations on the electric grid. It has a high level of resistance to random strikes, but is very vulnerable to targeted attacks. In [3], Čepin offered ways to increase the power system's reliability. According to Sugiyama in [4], the power grid can remain stable despite most disruptions, but the synchronization capacity of the grid is dramatically weakened when the major power nodes are assaulted. Therefore, detecting and analyzing critical points in the power grid, as well as conducting preventative and corrective measures, are critical to ensuring the power system's long-term viability. Existing node significance assessment approaches include K-shell decomposition technique, closeness centralization, method focused on characteristic vectors such as PageRank, and methods focused on node deletion and contraction.

These methods are all based on local information. The topological architecture of the power grid was used by Taft in [5] to test the possibility of identifying critical nodes using the node contraction approach. Nodes in the electric grid may be identified using a thorough assessment index that considers both electrical and topological features. From a worldwide energy transmission viewpoint, the Geng, Sun, Li and Wu [6] defines key power system nodes based on power flow tracking node connection strength. Using dynamic Bayesian networks, the Shafiee Kamalabad and Grzegorczyk in [7] completely assess the attack impacts of network nodes by analyzing the advantages, losses, expenses, and other elements of network

assaults. CPPS security scenario assessment model that takes threat propagation into account is suggested in [8] using the updated threat propagation tree. When it comes to determining which nodes are most important, this strategy simply takes into account the properties of a single-layer network.

In [9], Wu, Zhang, Wu and Yang studied the cascading failure of interdependent networks and presented a network topology-based cascading failure model. Key nodes in sophisticated power grids may be identified by using an electric range and node electric coupling connection measure provided by the author in [10]. There are two metrics used to determine the effect of a disabled node on a network: average capacity balance of surrounding nodes, as well as network load rate. It's important to note that the above node significance assessment takes into account several characteristics of how disabled nodes affect interdependent networks, but it does not properly examine the aggregate value of nodes in a power CPS under the propagation of cyber-attacks.

Even if we use a single-layer network to evaluate the relevance of the nodes, the resulting value is still dependent on a single property of the system. Without addressing the possible threats of cyber-attack spreading, such fixed indexes can't fulfill the system's requirement to differentiate significant nodes under attack spread eventualities of this kind. Assume a cyber-attack targets a certain information system device at some point between two detections (such as worms, and Trojan Horse). The initial stage of the cyber-attack spreads before the power detects the infected device and takes countermeasures. It's possible that the first assault has spread to other machines that have topological or informational ties to it. For instance, the information detection rate cannot keep up with the data exchange pace, therefore the cyber-attack will propagate over new information equipment before it is detected again.

Detection of a transmitting device in an exposed state is impossible if the assault was successful, but the perpetrator did not carry out any attack actions on the transferred device. After the first assault, the power system identifies and responds to the threat. Although the existing detection failure rate may match the dispatch center's requirements, it cannot be eliminated. As a result, the response plan devised by the dispatching center can only mitigate and prevent some of the damage caused by cyber-attacks. The cyber-attack propagation does not factor into this technique either (1) After the initial step of propagation, there are quite likely vulnerable nodes in the electric grid. (2) The proliferation of cyber-attacks has entered a second stage since the plan was implemented and the next detection was made. (3) Cyber-attacks will continue to widen in reach, even if prior techniques focused on a single device at the beginning of the infection process. (4) Most devices may be attacked after the previous two phases of propagation. It is possible that the power system might be in danger during the time between the two detections of this possible risk.

This paper provides an evaluation of the Cyber-Physical Systems (CPS) and potential attacks on it in a vulnerability evaluation. To illustrate this rationale orderly, this paper has been organized as follows. Section II presents a background analysis of the research. Section III presents a review of the past literature works related to the topic, while Section IV critically evaluates the paper and presents different scopes of the vulnerability evaluation. Lastly, this paper draws conclusion to the research in Section V.

II. BACKGROUND ANALYSIS

In the event of a CPS strike, the physical layout might be severely impacted. Passive and aggressive assaults are possible on each design layer of CPS shown in **Fig. 1**. Additionally, CPS is susceptible to more attacks compared to normal IT models, but to assaults from the used network, notably the web, that is already used as the transmission layer. There are many different types of assaults that may occur at any tier in the system, from the perception layer (such as attacks on sensors and actuators) to the transmission and applications layers (such as data leakage or damage). Analysis of potential threats and development of a strong security infrastructure are thus fundamental. Even though every layer is vulnerable to various assaults, certain assaults could target all dimensions, a discussion of these threats entail:

Denial of Service (DoS)

Changes the features of behavior by restricting traffic to render the service and unavailability, for example, by overloading the capability with illegitimate requests and exploiting the weaknesses of the protocols. DDoS is considered a regular attack, which affects different resources in a simultaneous manner, e.g., infrastructures and end devices, blocking accessibility to services and data.

Man-in-the-Middle (MITM)

An unintended action is taken by sending a falsified message to a specified resource, which in turn causes the resource to do an unwanted activity, such as managing a major function. It is also possible for this sort of assault to be followed by eavesdropping on the network level.

Eavesdropping

The technology detects any data that is sent. In the CPS, for instance, the transmission of control data from sensor nodes to applications might be vulnerable to eavesdropping. It is possible that the monitoring of the system will lead to a violation of user privacy.

Spoofing
A person who makes the effort to seem as if they are an integral part of the organization and then participate in its operations. After achieving expected achievement, the perpetrator will gain accessibility to data and could possibly execute activities e.g., adding, deleting and modifying data.

Replay (playback)
In order to gain the confidence of the network, a packet is retransmitted from the intermediate nodes. A spoof attack is one in which the identification data of one of the machines is altered or responded to Sudheendra and Krishnamurthy [11].

Compromised Key
Attempts to steal the encryption key being used to keep communications secure. In order to do this, it is necessary to analyze the amount of time it takes to encrypt a message, which is identified as side channel/timing attack. It will be utilized to alter gathered data and complete computer evaluation to promise more private keys in the similar system, which will be compromised. When an enemy gains control of a sensor, they may have it execute engineering activities so that additional internal keys can be extracted. In another scenario, an attacker may replace sensor nodes and act as a legitimate version to the interchange key with other sites, therefore finding additional secret keys of the connected nodes. At each stage of the CPS, there are many threats, and they may be categorized as follows depending on the CPS structure.

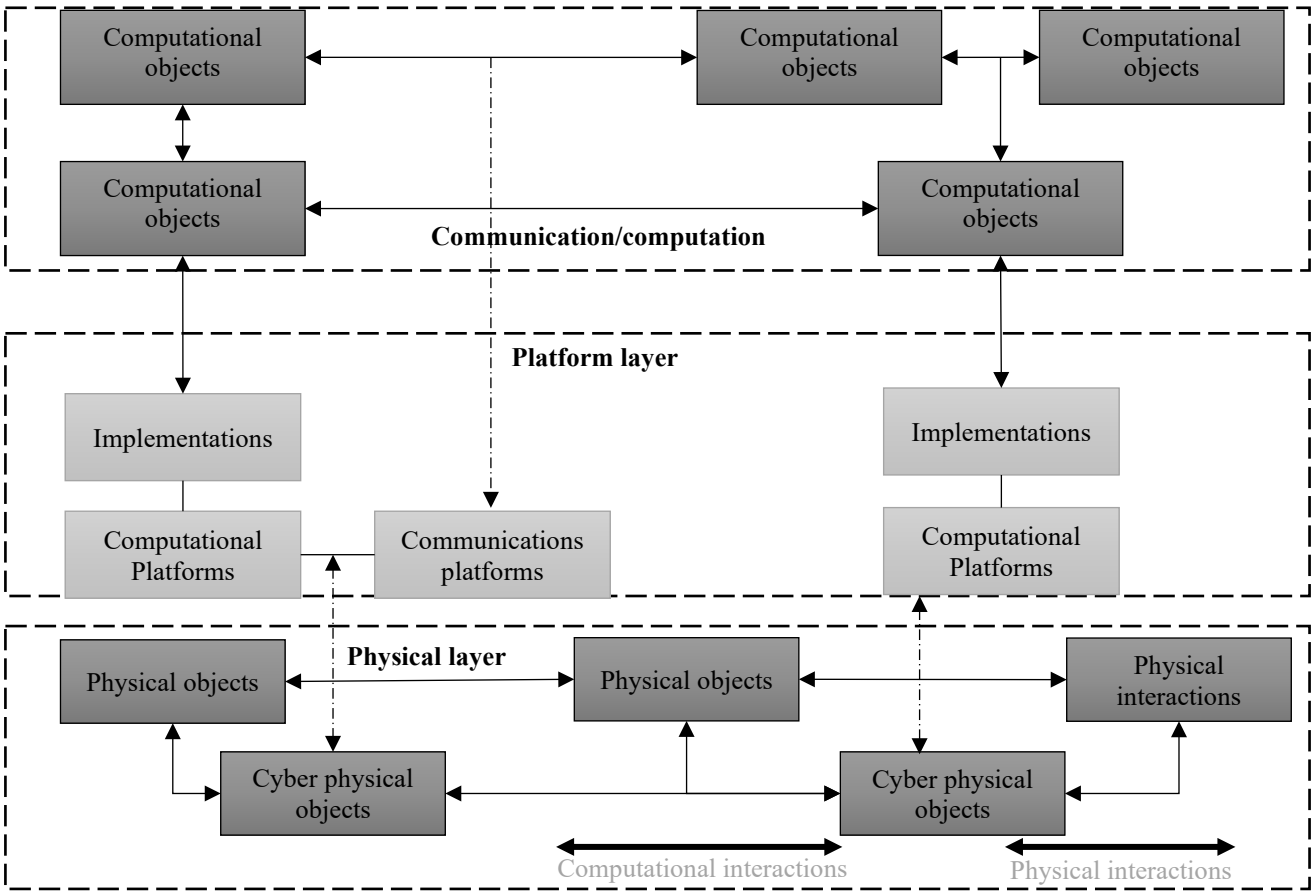

Fig 1. Design layers for CPS

Attacks at the Perception Layer
The perceptive layer integrates the edge devices, like Radio Frequency Identification (RFID) tags and detectors, which are hampered by the limited computer resources and storage capacity. As a consequence, these devices are often exposed to physical assaults, such as altering with the devices' elements or replacing them. As a result, a wide range of assaults may target such terminal devices. The perception layer is commonly attacked by equipment disappointment, line failure, witchcraft, electromagnetic fields, perceptual data bribery, differential energy analyzation, data leakage, in-formation monitoring, interfering, sensing data leakage, physiological destruction, and energy exhaustion attacks. These assaults may take many different forms, including but not limited to depiction in **Table 1**.

Table 1. Attacks on the perception layer

Attack	Details
Node Capture	Takes control of the nodes and obtains and divulges sensitive information, such as encryption keys, in order to put the whole system at risk. Security, accessibility, authenticity and integrity are all targets in this assault.
False Node	By adding another connection to the network, harmful data is sent that threatens the integrity of the data. As a result of this, the program's nodes may be consumed by a DoS assault.
Node Outage	In addition to launching a range of assaults that damage the integrity and availability of nodes, it shuts down their services, rendering it challenging to acquire and read data from nodes.
Path-Based DoS	As a result, the nodes' battery capacity is depleted and network disruptions occur, resulting in a decrease in the node's operational time and capacity.
Resonance	When sensors or controllers are affected, they must function at a new rate.
Integrity	Attempts to include outer control data and illegitimate sensor dataset to possibly destabilize systems.

Attacks at the Transmission Layer

Information leakage during transfer is a common sort of assault on this layer. The transparency of the transmission medium, particularly in communication technology, is to blame for this. It is possible to intercept a radio transmission, edit it, and then send it out again, all the while pretending to be the original sender of the data. Another element that increases the likelihood of an attack is the large number of network nodes that might generate traffic congestion. Assaults at this layer integrates feedbacks and sybil, collusion, manipulation and analysis of traffic, including exhaustion and trap doors, floods and black holes and sink nodes. Attacks on the transmission layer have been presented in **Table 2**:

Table 2. Attacks on the transmission layer

Attack	Details
Routing	As an end consequence, a network with more resistance, longer transmit times, or longer sources of transmission may be created by this technique.
Wormhole	Gaps in the network's informational flow by the introduction of fake pathways for packets to follow.
Jamming	Presents signals and noise of similar wavelengths into the wireless system among the sensor node and the remote Base Stations (BS). It is possible that this assault might result in a Denial of Service (DoS) because of the purposeful network disruptions it causes.
Selective Forwarding	Drop and reject packets from a vulnerable node and forward chosen packets. As long as the malicious node is deemed a valid node, it may cease sending packet to the projected target or send chosen messages and ignore the rest.
Sinkhole	The optimum routing path to apply to route a connection to the remaining nodes is announced here. Selective forwarding and spoofing might also be employed in conjunction with this attack.

Attacks at the Application Layer

Because so much personal data is collected at this level of security, an assault here may lead to data loss, privacy loss, and illegal access to devices, among other things. Malicious code, database corruption, and forged controlling command injection are all common app-layer attack vectors. Typical instances of assaults on this layer are shown in **Table 3** below.

Table 3. Attacks on the application layer

Attack	Detail
Buffer Overflow	A vulnerability in the program that causes buffer overflows may be used to launch attacks on the system.
Malicious Code	A virus is used to attack the user program, slowing it down or damaging it completely.

III. LITERATURE REVIEW

As per Naseri, Lucia and Youssef in [12], Cyber-Physical Systems (CPS) are a brand-new area of research with the potential to link the physical and digital domains in meaningful ways. These systems depend on a network of linked components to link the physical and digital domains. Because of the spread of the Internet of Things (IoT) and the complexity of occupations, it is essential to build interoperable CPSs that can provide timely services. Physical item monitoring and control may be efficiently, reliably, safely and securely administered using a distributed CPS with multi-scale dynamics and networking.

As per Sakurai [13], the combination of CPSs with IoT has resulted in new innovations such as service-oriented architecture (SOA), collaborative systems, and cloud computing. Service-oriented CPSs so far seem to be capable of interoperability at both the cyber and physical levels, which is a positive sign. Creating distributed real-time CPSs, which consider the intricate interdependencies between the physical and cyber systems requires a service-oriented approach combined with the most efficient possible use of available resources. Agents that are aware of their surroundings make

distributed pervasive computing more attractive since it is possible to combine a wide range of qualities into them and accomplish distributed pervasive computation with enhanced interoperability and coordination across heterogeneous and autonomous devices. The new technology depends largely on sensors, resources, flexibility, and augmentation, hence CPSs must have context awareness. Partial observability is inherent to CPSs because of the dynamic nature of distributed CPS domains. For ontology-based semantic technology to achieve high model performance, uncertainty modeling approaches must be used.

In [14], an interoperable CPS must be achieved in order to suit the needs of both physical and cyber components. The lack of a robust theoretical framework has contributed to this constraint, even though most methods can model either cyber and physical components of a CPS. A number of approaches, including the creation of complete CPS models, may make use of service-oriented computing to promote interoperability in CPSs. We need more than simply a service-oriented strategy to depict distributed CPSs with real-time multiscale dynamics and networking. When it comes to distributed, complicated systems, such as CPSs, agent-based modeling is a better fit.

Since CPSs have a built-in sensor network, our approach is closely related to semantic agent technology. Information fusion techniques are used in real-time context-based reasoning to integrate sensor networks in the battlefield information system, which has been referred to as semantic agent technology. The creation of a service-oriented sensor information platform and its architecture and programming paradigm has enabled scalable sensor information access. This approach maximizes the use of data gathering and storage resources by using an ontological abstraction of information. The responsiveness and concurrency of distributed processing environments may also be improved by the employment of autonomous software agents. Software paradigms that use autonomous semantic agents in distributed computing systems have been proposed.

These examples include the Internet of Things (IoT) and smart cities, transportation systems, and "smart things" (e.g., homes and hospitals). These systems need various levels of security and protection, depending on the sensitivity of the data. In spite of this, cyberattacks, privacy violations, phishing tactics, and data breaches continue to haunt us. Because of the flaws in present computer and communication technologies, smart CPSs are similarly subject to security breaches and privacy invasions. There will also be more vulnerabilities as smart CPSs get more complex. Future cyberattacks will be more complex because of the ever-changing cyber-physical environment. A new generation of smart CPSs requires cutting-edge research to ensure the security and privacy of new architectures, system designs and cryptographic protocols.

Computers and physical processes are increasingly intertwined in CYBER-Physical Systems (CPSs). It is often required to employ the complete spectrum of sensors to monitor a CPS because of the enormous number of variables in the system. Sensor location, sensor assignment, and sensor coordination are all important concerns when using a large number of sensors. System feedback needs must be addressed without losing overall system reliability or performance; these qualities are driven by these two (sometimes conflicting) aims in the design of the system. Because of this, a criterion-based sensor management framework is needed to aid in the selection and use of sensing resources as they become available.

As per Cheng, Du, Wang and Xu [15], in the context of wireless sensor networks, you're presumably thinking about how to deal with difficulties like energy usage, bandwidth restrictions, and so on. The easiest way to achieve the greatest results from a target tracking system is to use the proper sensors. These criteria were used to identify which sensors should be utilized, at what time, and for what purpose in all of the aforementioned cases. A few examples of information theory criteria and norms used in combination with estimate theory are entropy, reciprocity, and Kullback-Leiber-Reneyi divergence (Kalman filter, particle filters, etc.) It's been found that researchers have also looked into other methods to sensor control, e.g., utilizing computational interaction between environment and sensor integrated with Bayes reasoning for the selection of sensors within the robotic framework, the application of neural database and networks to potentially estimate the dependability of sensor messages and sensor application in the surface grinding procedure based on the application of empirical approaches.

In order to identify and isolate defects, analytical redundancy has been employed in a number of methods. Fuzzy logic and the Nadaraya Watson statistical estimator may be used to find subspace models. This work will focus on using the Bayesian approach, which is capable of detecting multiple sensor faults and differentiating between system and sensor faults, including integrating various approaches together in one application to accomplish different tasks like model-based fa, despite the fact that each method has its own benefits and drawbacks (accelerated implementation and accurate results, ease of implementation, etc.). With this method, it is possible to combine both the duty of isolating and accommodating faults with the task of correlating system variables in a way that is physically relevant (and that can be depicted visually for intuitive comprehension). To account for the problem's intrinsic nonlinearities and uncertainties, probabilistic computation is useful. [16] is an excellent illustration of this method in action.

This emphasis on attack graph building and simulation in security research was stressed by Zhang, Li, Chen and Fan [17]. They were mostly engaged in the development of new assault tools. According to the findings of this research, the impact of an assault may be directly related to the attack's characteristics. Jadhav [18] explains the importance of Unified Threat Management in his work. For the purpose of anticipating cyberattacks, Liu [19] used an attack graph and ambient data, together with a Bayesian network. Researchers say that environmental data is crucial in establishing the safety of a product. According to this article, the characteristics and outcomes of an assault may be influenced by environmental information. Using uni- and multi-model models, the researchers at Sun, Zhao and Cheng [20] investigated the possibility of enhancing security. Prior to starting the exam, a short lecture about authentication and security took place. Insider threats

may be predicted using a Bayesian network model, according to research by WU, HE and FANG [21]. Attack frequency and susceptibility were discovered to be linked by [22]. Nonetheless, an aggregate effect of the assault setting elements on the attack was not discovered. Le and Zincir-Heywood [23] develop an approach for assessing the effectiveness of insider threat identification frameworks centered on the system dynamics methodology. The research evaluates the aspect of risk management and early identification of insider risks.

The three-impact CVSS metrics are used to assess the effect of a vulnerability on an IT asset. Along with Access Vector and Complexity, authentication is one of the metrics. Vulnerability effects the integrity, confidentiality, and accessibility of these attributes. Depending on the source of measurement, cyber security metrics may be divided into two broad groups. An attacker or group of attackers may do a range of actions on the network. Additionally, the host/victim may conduct specific actions. Users with malicious intent have the potential to select the attack's strength, secrecy and timing. Employees' technical and cyber skill is also evaluated from the point of view of the hostile user/group. A program like as X-Force may be used to find out how much power is being utilized to secure a system over a certain length of time, as well as what type of faults are there in the tool. Using these two categories, a prediction model is developed, but no precautions are taken for hazardous users or groups. Complexity in assaults of this kind has rendered accurate measurements difficult. If the target applications are hosted by an organization, such efforts originating from attackers' end as of scare use.

For data analysis and decision support systems, Cyber-Physical Systems (CPS) are being employed in a wide range of industries. Intelligent analysis relies on the integration of a variety of heterogeneity infrastructures. This article's goal is to provide a quick review of CPS and to point out some of its attacks under vulnerability assessment.

IV. VULNERABILITY ANALYSIS

For most vulnerable entities (such as smart homes and medical facilities), the need for a risk assessment approach is critical because of the rising use of CPS. Because of our heavy reliance on the Internet, computer risk analysis has shifted to network risk analysis as the primary emphasis of risk assessment. CPS risk assessment is intended to provide a quantifiable model for future system defense. Many research and efforts, however, are devoted to business systems that are not directly linked to CPS. As a result, the security mechanisms for CPS vary greatly from those found in standard IT systems. As an example, Alavi, Islam and Mouratidis [24] found that ICS risk factors include standardized protocols and techniques, unsecured interconnections, and interchanged data.

It is possible to break down the CPS risk evaluation model into three stages: (1) specifying what will occur to the network; (2) assessing the likelihood of the incident; and (3) evaluating the implications of the occurrence. CPS risk assessments should also include three other factors: asset (value), threat, and susceptibility descriptors. From immediate and indirect commercial losses, as well as damages, asset quantification may be assessed. Identification of defensive layers, important assets and core (essential) system operations as well as asset value rating are all part of the value evaluation process. There are three types of CPS assets: physical assets, digital assets, and assets that interface with other systems. It is the complex, intangible, and interrelated nature of CPS assets that distinguishes them from traditional IT assets.

Threat Identification

Using this process, which may be challenging in the realm of child protective services, we can uncover concerns that need immediate attention. Sample recordings and logging in the Intrusion Detection System (IDS) may be used to calculate the frequency of the danger, as can historical data. Logs and many other approaches can also be employed. However, Poltavtseva [25] provide a critical analysis, which categorizes CPS IDS methods, recommends research objectives, and provides an analysis of most studied CPS IDS methods in the domain. It is possible for an enemy to listen in on or damage the value of assets by taking advantage of a vulnerability that already exists. An adversary would use it as a state or environment to attack or harm devices. Weaknesses and appropriate corrective measures or mitigations to mitigate or eradicate any vulnerabilities are identified via a vulnerability evaluation of a system and its functionality.

CPS threats may be broken down into three groups: management, platforms, and network. There are monitoring, hardware, and configuration vulnerabilities, which could amount to network security breaches. Software, hardware and configuration vulnerabilities, including a lack of protective mechanisms, all contribute to platform vulnerability. The most common cause of management vulnerability is a lack of security rules. Expert evaluations, historical data, or the best practices of other sectors may all be used to quantify a company's vulnerability.

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. The number of issues that CPS must take into account when developing a security feature for such systems grows as it integrates cyber and physical activities. To make matters more complicated, the setting is always transforming and devices linked could be dynamically linked in various locations. The design of a security mechanism may confront difficulties in preventing, detecting, and mitigating security breaches. Cyber and physiological systems interact in a complex way, making pre-venting an assault difficult. When attempting an attack, an attacker may not just rely on known direct weaknesses, but also attempt an assault that cuts over many layers of defense. Because of the interplay between cyber and physical space, detecting algorithms must be developed for various levels of CPS, e.g., perception, transmission and application layers. It is fundamental establish a security element, which is capable of minimizing the impacts of a breach in the event that pre- and detecting security are exceeded.

Security Requirements

In CPS, security issues may be divided into two categories: (1) those emerging from the integration of diverse technologies to execute the required functions, and (2) those from the implementation of security elements for attain the required security. CPS security infrastructure will integrate, for example, the require security problems within the WSN, Web and Mobile Communications Systems because of its extensive access to the Internet. In contrast to conventional IT, CPS lacks the consistent execution and computing process capacities essential to accomplish complex security standards. As a result, implementing a unified security system in a constantly shifting environment is very difficult.

At each tier, most of the privacy solutions suggested strive to address different security concerns. Using these methods, a portion of the system may be secured, but there is a possibility that other sections of the system might be vulnerable. Through all levels of the system (such as collecting, transmission, and processing), a CPS security architecture is employed to ensure the safety of information. A bottom-up analysis is presented in the next sections of the security needs for every CPS level, as there are various security issues at every level, which have to be mitigated to potentially defend these systems from potential intrusion.

Security analysis at the perception layer

Data gathering and identification are the key goals of this layer. However, as more devices become interconnected, the risk of a security breach increases. It is possible for attackers to obtain access to sensitive information, install malicious programs, and even restrict access to the Internet using these devices, which have limited abilities and are often linked to the Internet over less secure network media. As a result, it is crucial to safeguard these devices and prevent the leakage of sensitive data. Physical assaults, e.g., altering the functioning of the device components or transforming a device, may come from attackers exploiting newly installed devices, many of which are placed in external or outdoor locations. As a result, the addition of each new device must be taken into account.

As a result of a lack of authentication functionality in many physical layer devices, rogue software might get access to sensitive data and corrupt the systems. Since of this, applying authentication to these devices is quite difficult because there are many items and organizations with restricted capabilities. Encryption is a good way to provide authentication at this level. Constrained devices (e.g., smart cards, sensors) may not be able to perform appropriate cryptographic operations owing to the limited resources of these devices. This necessitates the development of a light-weight authentication system, which is the subject of current study. Therefore, identification and access controlling procedures prohibit accessibility from unpermitted nodes, defence against potential physical attacks; data encryption protects and assures confidentiality prevents the publication of personal information during data transfer. As the most extensively used communication technology at the perception layer, RFID and WSN security analysis is the subject of the next two subsections.

RFID security analysis.

RFID represents a wireless approach, which is capable of storing and retrieving data remotely from devices. Because RFID does not need any human input, it is a very advantageous technology. Aside from the accurate real-time properties of RFID technology, various RFID tags do not have any form of security approach, and those that do apply hashing approaches or conventional symmetric methods owing to the limitations of power constraints. Because of this lack of standardization in RFID, it is vulnerable to a variety of security issues. These include uniform coding that could prevent readers from reading data, conflict collisions that can disable readers, and privacy protections that are compromised due to RFID tags with limited re-sources (e.g., computational capacity).

CPS cannot function without RFID, despite the fact that it has the security flaws listed above, because of the wide range of activities it can do, including the detection of physical and environmental item changes, motion and velocity, as well as temp, humid, gas and light changes. An important aim in the area of security and device authentication is to have tags with sufficient storage and computing capabilities to establish an effective authentication method. Due to that, low-value RFID tags lack the specifications needed to build effective security methods. Due to the limited resources of RFID, it is unable to apply any typically applied security approaches (such as Diffie– Hellman key exchanges, PKI, IPSec, and SSL). Four RFID security issues include location privacy, privacy protection, conflict collision, and coding uniformity. Consequently, a standard encoding, conflict collision detection and avoidance, and light-weight data personal privacy is needed. A cryptographic approach that is lightweight and transmission protocol approach is ideal for limited assets in RFID to ensure the authenticity, authentication, and secrecy of data.

WSN security analysis.

Decentralized sensors are used to monitor the physical setting or factors such as gas indicators, pressure and temperature. WSNs, also known as Wireless Sensor and Actuator Networks, are dispersed sensors. Self-organizing connections with dynamic topology of the network and widely spread multi-hop wireless systems are also known as "multi-hop" networks. In conjunction to the fact that WSN have limited resources (e.g., 16-bit or 8-bit processor infrastructure, 8 MHz clock frequencies), susceptible radio circumstances, and little direct human involvement, this will be reflected in the capacity to conduct any safety mechanisms.

Due to the fact that an attacker's replacement device may detect the data, current research concentrates on ensuring sensor data authenticity and integrity at the expense of secrecy. An important security risk for sensor nodes is their ability to

communicate securely with one other; in certain circumstances, sensor nodes may be vulnerable to physical assaults since they are installed in an unmonitored environment. Key pre-distribution, key storage, and energy consumption are the three fundamental problems of cryptographic algorithms that have yet to be fully resolved after decades of research.

Cryptographic technologies, key management, secure routing, and trust maintenance may all be used sequentially to address WSN security concerns and meet the CPS security goals. In WSN, both symmetric and asymmetric cryptographic algorithms have been used. To be sure, there are advantages and disadvantages to every one of these sorts of strategies. Symmetric encryption is extensively used since it requires fewer computing computations compared to the asymmetric encryption, even though key exchange protocols have problems like complexities of the protocols as well as key secrecy. There are many advantages to using asymmetric cryptography (public key), including greater scalability, correct node authentication, and increased security for chosen networks. As a result, research will concentrate on improving computational tasks as well as parameters (algorithm parameters) utilized in public key cryptography.

There has yet to be developed a sensor node-friendly cryptographic algorithm. Ultimately, each of the non - symmetric and symmetric approaches to WSN security has its own advantages; however, only one of these approaches can be used to overcome all of the security problems in WSN. Devices with low power consumption with software identification and symmetric encryption algorithms that are well-developed may be appropriate. However, even if asymmetric encryption with 1024-bit keys could be utilized to Ad Hoc networks, WSN gadgets with computational capacity and low memory are not suitable. Lightweight symmetric encryption methods may be used instead of hashing and are the subject of the majority of research. Even with restricted capabilities, certain advanced asymmetric encryption methods (e.g., Elliptic Curve Cryptography (ECC)) may be used.

The second major WSN security component is key management. This comprises producing, disseminating and maintaining the secret key. The encryption procedure uses the secret key to safeguard the communication routes between the nodes. Numerous protocols have been developed for public key cryptography, which is primarily responsible for protecting data secrecy and integrity. The key distribution frameworks centred on symmetric cryptography and the sensor network element have been established based on the application of various key distribution methods. Simplified key distribution, dynamic management, pre-distribution and hierarchical key control are the four basic key distribution techniques. An urgent need for cryptographic key distribution techniques that use the Asymmetric Cryptography Protocol (ACP) has evolved.

Due to the fact that most of these protocols were originally built for wired networks, they will not operate in wireless networks. SSH and SSL protocols, for example, must involve certification among WSN nodes in order to be secure. Consequently, the emphasis of safety in WSN was transferred to applying asymmetric encryption such as NtruEncrypt and Elliptic Curve. Open networks' security vulnerabilities are mostly addressed by WSN node trust management. The implementation of security, privacy and trust amount identifiers and the BS should work hand in hand with any authentication technique for sensors. All network nodes will be included in the trust management process in this fashion, which means that network security will be prioritized above resource constraints. It is necessary to utilize authentication processes, which are optimized for WSN with less processing power and storage. WSN security is often studied from a single angle, but a comprehensive approach that considers all four of the above-mentioned aspects, as well as safe routing protocols and trust management, would be more effective. This framework would be ideal for future study on WSN security.

Security Examination at the Transmission Layer

As a result of the widespread usage of networks in a variety of industries, they reveal a broad range of security risks and are vulnerable to assault or eavesdropping. For example, wireless accessibility gives great convenience to consumers, but it also allows attackers to engage with the system and inflict harm or steal vital information. Machine-to-machine communications in CPS varies from that on the Internet, which is just human-to-human communication. In order to protect machine interactions, the current network privacy infrastructure was not initially intended. (e.g., communications between CPS devices). Due to the absence of interoperability between linked devices, machine-to-machine data transfer presents a security risk.

The present network protocols built for the Internet cannot address these security concerns. Despite the fact that these protocols still provide some safeguards, they are not the ideal answer. In order to obtain access to users' personal information, attackers might take advantage of any vulnerabilities in heterogeneously linked. It is critical to safeguard the network itself in order to protect the devices that are connected to it. To ensure the safety of the system, devices should be able to identify any anomalous behavior or condition. Software with Intrusion Monitoring must be installed on the devices that will be transmitting data. There are two forms of safety at the transmission layer. Devices that are linked to a network generate the first sort of attack, while other technologies and implementation flaws introduce the second. There are additional vulnerabilities in wireless networks since nodes may move dynamically without prior authentication, posing a security risk to the network as a whole.

Network Access

With an ad hoc networking or wireless connections, network access may be made possible. For communication to take place, there is not any central hub, which is known as a 'base station,' in a "peer-to-peer" network. Adapting node modifications is simple with this network type. Attackers may eavesdrop on the radio channel in this type of network and so pose the greatest

danger to its security. Data security, network routing, and illegal node access are some of the most prevalent security threats in this network. Authentication and authorization approaches may be used to solve the problem of illegal access to nodes. Identification and encryption are important management mechanisms that may provide a suitable answer to the data security problem. It is possible to employ encryption methods in order to secure routing.

IEEE 802.11 (or Wi-Fi) is the most commonly utilized wireless network in the world. WLANs, or wireless local area networks, use stationary bridges (called "base stations") to connect nodes together. Wi-Fi networks may be used by any kind of device to connect to the Internet and interact with apps. There are several security difficulties, even though Wi-Fi technology is convenient, involving DoS and unrestricted access attacks. Access monitoring and network encryption are used to alleviate these security problems.

Network Encryption Approaches

End-to-end encryption and hop-to-hop encryption are the two primary methods of encoding data. It's encrypted as it travels via the network in a hop-by-hop encryption technique. Keeping plaintext in each node is a requirement for both encryption and decryption in this strategy. The transmitter and receiver are the only two parties who can decipher the data sent using end-to-end encryption, which encrypts it at every step of the way, from transmission to reception. To safeguard just the connections between nodes, the hop-by-hop encryption method may be used. Although this technique has several advantages, such as cheap cost and latency and great efficiency, each node can decrypt the data. Hence, it is necessary to have faith in these nodes.

This also places responsibility for security on the nodes' application processes. It is impossible for eavesdroppers to decipher the encrypted datasets utilizing the end-to-end encryption since only the message sender and recipient have access to the cryptographic keys required. However, implementing this strategy is very difficult, particularly with constrained end devices like sensors. SSL/TLS, for instance, is an end-to-end protocol that enables clients and servers to establish certain needed security characteristics. A multi-layered surveillance system is used to protect networks, and wireless devices pose the greatest threat to CPS's network security. End-to-end consensus and authentication mechanism, encryption routing, cross-network verification and cross-domain identification techniques are all necessary to establish a comprehensive network security system. Personality identification should be considered to improve data confidentiality and integrity by preventing unauthorized access to nodes and ensuring safe network routing.

For example, point-to-point and end-to-end security are two sublayers of a security architecture that may be used to secure hop-to-hop transportation security such as mutual authentication and across network certification. The first sublayer could safeguard hop transmission data, while the second layer could guarantee data secrecy and network availability. We need a novel secret strategy for diverse applications since most conventional communication security solutions are not built for heterogeneous programs. Concerns about network capacity and connection (e.g., address space) must be considered in order to avoid congestion and redundancy difficulties. The IP protocol isn't designed to handle a huge number of interconnected nodes. With this, the IPSec protocol has been extensively used since it includes authentication and encryption capabilities.

Network partners often utilize this protocol to build secure Virtual Private Networks. 6LoWPAN has been considered as a replacement for IP, notably in CPS, because of the limitations of the IP protocol. A more serious problem with this protocol remains, however: the additional overhead caused by the remaining overhead. TLS/SSL that could provide confidentiality, authenticity, and integrity, and Internet Protocol Security (IPSec) that could provide confidentiality, authenticity and integrity at each layer, are two well-established options for communication security.

Security analysis at the application layer

Multiple programs make up this layer, and as a result, the CPS's security may be compromised in several ways. In addition, the application layer has major issues in securing user privacy and accessing sensory information in a hierarchical fashion. In Smart Homes and Smart Cities, this layer may incorporate a variety of implementations, such as operations and monitoring for industry. Design flaws that might be exploited by attackers are the key security worry here. Therefore, malicious software or code might be utilized to disrupt the security of system, Integrating a variety of methodologies raises another question about security since it might slow down data processing and cause bottlenecks in the operation. System uptime and dependability may be compromised as a result of these security vulnerabilities. Fournaris, Lampropoulos and Koufopavlou [26], for instance, mentions the aspect of trust, and integrating trust into systems is expensive undertaking and time-consuming

Information access, user authentication, data privacy, and data link collapsing are all part of the application layer's security. As a result, there is an increasing need for providing security requirements for each application, as the use of critical and sensitive technologies, which are controlled and monitored in real time, is increasing in importance and volume. On the contrary, there are a wide range of sophisticated security challenges that need to be taken into account based on the kind of program. Consequently, it is impossible to create applications that are completely recognized amongst themselves without taking into consideration the system's underlying processes, such as connection and the data provided by CPS. Another problem is that CPS is used in a variety of ways in various industries. Because there isn't a single universal standard for CPS application layer applications, the lack of security is worsened. This implies that various security requirements are needed for different application contexts. When constructing CPS implementations, there are a number of security problems that

must be taken into consideration, such as: different authentication processes for variety of application that make integration challenging when assuring identification authentication; a greater portion of connected devices and shared dataset, which results to higher application costs that will be conveyed in service accessibility provided by devices; the greater number of clients using CPS.

V. CONCLUSION

For data processing and decision support systems, Cyber-Physical Systems (CPS) offer a wide range of applications. Integration of various heterogeneous infrastructures that generate data for intelligent analysis is discussed. This study has given an overview of CPS, as well as a discussion of the CPS vulnerabilities. The threat of cyber-attacks is a major concern for all enterprises. It is imperative that computer systems be kept secure. Predicting assaults on an ecosystem is critical for organizations. Risk management should include the ability to predict assaults statistically. Worms, viruses, and other harmful software may have a substantial financial effect. This article has highlighted the necessity for CPS systems to be assessed for vulnerabilities. Risk assessment is crucial for many sensitive companies (such as healthcare and smart homes) because to the increasing usage of CPS. The goal of CPS risk evaluation is to develop a quantitative model for prospective system protection.

References

[1]. G. Koutitas, "Control of Flexible Smart Devices in the Smart Grid", IEEE Transactions on Smart Grid, vol. 3, no. 3, pp. 1333-1343, 2012. Doi: 10.1109/tsg.2012.2204410.

[2]. S. Shackelford, "Toward Cyber Peace: Managing Cyber Attacks Through Polycentric Governance", SSRN Electronic Journal, 2012. Doi: 10.2139/ssrn.2132526.

[3]. M. Čepin, "Evaluation of the power system reliability if a nuclear power plant is replaced with wind power plants", Reliability Engineering & System Safety, vol. 185, pp. 455-464, 2019. Doi: 10.1016/j.ress.2019.01.010.

[4]. H. Sugiyama, "Pulsed power network with potential gradient method for scalable power grid based on distributed generations", IET Smart Grid, vol. 3, no. 6, pp. 906-913, 2020. Doi: 10.1049/iet-stg.2019.0245.

[5]. J. Taft, "Grid Architecture: A Core Discipline for Grid Modernization", IEEE Power and Energy Magazine, vol. 17, no. 5, pp. 18-28, 2019. Doi: 10.1109/mpe.2019.2921739.

[6]. J. Geng, X. Sun, F. Li and X. Wu, "Prediction method of important nodes and transmission lines in power system transactive management", Electric Power Systems Research, vol. 208, p. 107898, 2022. Doi: 10.1016/j.epsr.2022.107898.

[7]. M. Shafiee Kamalabad and M. Grzegorczyk, "Improving nonhomogeneous dynamic Bayesian networks with sequentially coupled parameters", Statistica Neerlandica, vol. 72, no. 3, pp. 281-305, 2018. Doi: 10.1111/stan.12136.

[8]. F. Nian, S. Ren and Z. Dang, "The propagation-weighted priority immunization strategy based on propagation tree", Chaos, Solitons & Fractals, vol. 99, pp. 72-78, 2017. Doi: 10.1016/j.chaos.2017.03.049.

[9]. R. Wu, B. Zhang, H. Wu and X. Yang, "Cascading Failure Model of Interdependent Power Networks Based on Load Redistribution", Applied Mechanics and Materials, vol. 602-605, pp. 2995-3000, 2014. Doi: 10.4028/www.scientific.net/amm.602-605.2995.

[10]. "The Model of Electric Connection of a Low-Conducting Liquid in High-Frequency Electric Field", Прикладная механика и техническая физика, no. 2, 2018. Doi: 10.15372/pmtf20180202.

[11]. P. Sudheendra and D. Krishnamurthy, "Novel Promising Algorithm to suppress Spoof Attack by Cryptography Firewall2014", International Journal of Trend in Scientific Research and Development, vol. -2, no. -5, pp. 102-109, 2018. Doi: 10.31142/ijtsrd15801.

[12]. A. Naseri, W. Lucia and A. Youssef, "Confidentiality attacks against encrypted control systems", Cyber-Physical Systems, pp. 1-20, 2022. Doi: 10.1080/23335777.2022.2051209.

[13]. T. Sakurai, "Trillion-node engine: open-innovation IoT/CPS platform—pioneering future of IoT/CPS for everyone, by everyone", Japanese Journal of Applied Physics, vol. 59, no., p. SG0804, 2020. Doi: 10.35848/1347-4065/ab7412.

[14]. S. Stall, "Enabling Findable, Accessible, Interoperable, and Reusable Data", Eos, vol. 98, 2017. Doi: 10.1029/2018eo081907

[15]. X. Cheng, D. Du, L. Wang and B. Xu, "Relay sensor placement in wireless sensor networks", Wireless Networks, vol. 14, no. 3, pp. 347-355, 2007. Doi: 10.1007/s11276-006-0724-8.

[16]. V. Danos and T. Ehrhard, "Probabilistic coherence spaces as a model of higher-order probabilistic computation", Information and Computation, vol. 209, no. 6, pp. 966-991, 2011. Doi: 10.1016/j.ic.2011.02.001.

[17]. S. Zhang, J. Li, X. Chen and L. Fan, "Building network attack graph for alert causal correlation", Computers & Security, vol. 27, no. 5-6, pp. 188-196, 2008. Doi: 10.1016/j.cose.2008.05.005.

[18]. P. Jadhav, "Cloud Unified Threat Management System", International Journal for Research in Applied Science and Engineering Technology, vol. 6, no. 4, pp. 1712-1715, 2018. Doi: 10.22214/ijraset.2018.4288.

[19]. X. Liu, "A network attack path prediction method using attack graph", Journal of Ambient Intelligence and Humanized Computing, 2020. Doi: 10.1007/s12652-020-02206-5.

[20]. D. Sun, H. Zhao and S. Cheng, "A novel membership cloud model-based trust evaluation model for vehicular ad hoc network of T-CPS", Security and Communication Networks, vol. 9, no. 18, pp. 5710-5723, 2016. Doi: 10.1002/sec.1730.

[21]. J. WU, L. HE and Y. FANG, "Social network matching model using dynamic Bayesian network", Journal of Computer Applications, vol. 28, no. 12, pp. 3102-3104, 2009. Doi: 10.3724/sp.j.1087.2008.03102.

[22]. Amseh "TNF-Pathway Proteins Modulate Tumor Susceptibility to T-cell Attack", Cancer Discovery, vol. 9, no. 9, pp. 1157.2-1157, 2019. Doi: 10.1158/2159-8290.cd-rw2019-110.

[23]. D. Le and N. Zincir-Heywood, "Exploring anomalous behaviour detection and classification for insider threat identification", International Journal of Network Management, p. e2109, 2020. Doi: 10.1002/nem.2109.

[24]. R. Alavi, S. Islam and H. Mouratidis, "An information security risk-driven investment model for analysing human factors", Information & Computer Security, vol. 24, no. 2, pp. 205-227, 2016. Doi: 10.1108/ics-01-2016-0006.

[25]. M. Poltavtseva, "Heterogeneous Data Aggregation and Normalization in Information Security Monitoring and Intrusion Detection Systems of Large-scale Industrial CPS", Proceedings of the Institute for System Programming of the RAS, vol. 32, no. 5, pp. 131-142, 2020. Doi: 10.15514/ispras-2020-32(5)-10.

[26]. A. Fournaris, K. Lampropoulos and O. Koufopavlou, "End Node Security and Trust vulnerabilities in the Smart City Infrastructure", MATEC Web of Conferences, vol. 188, p. 05005, 2018. Doi: 10.1051/matecconf/201818805005.