Cyber-Physical Systems & its challenges for smart home/ smart city

AUD: 15697
Name: Jaden Ade

Introduction

Cyber-Physical system could potentially link both our physical and cyber world. Cyber-Physical Systems (CPS) is a collection of networking, computational and physical processes. It is a system in which the mechanism is controlled or monitored by computer-based algorithms. It integrates networking, computation and much more into physical devices thereby connecting them online and with each other. In the physical world, the system works through the means of sensors and Internet of Things (IoT) devices. Whereas in the virtual world, it connects the physical system to the virtual world with the help of computing element and computer-based algorithms. Currently, reliance on Cyber-Physical systems is gradually increasing in various fields such as medical, transportation, manufacturing and much more. Although CPS could potentially help bridge the virtual and physical world, there are still the cons to consider which is hampering its implementation. One of the biggest problems of Cyber-Physical Systems is their security and privacy. The reasons for these concerns are since any vulnerability or loophole in the system could have a direct threat to our lives. In recent times, cybercrimes have increased at an exponential rate and are becoming more unpredictable every day. Although companies invest a lot of money in cybersecurity and protecting privacy, there are still security breaches and vulnerabilities which not only leads to issues with data security but also causes a lot of damage to companies financially and reputationally. As CPS gets more popular and widely used, it is also necessary to improve its security day by day. However, most of these issues could be solved with robust testing and updated security measures. Also, implementation of software script detection methods such as Malicious Code detections, network access detection, device detection and so on could potentially reduce this risk. Another aspect is Researching current security threats and issues. Research on CPS and its security is currently ongoing in many countries. For example, Research on CPS Security is currently going on with DGIST. Similarly, universities in the US are also researching this field. A Korean project on CPS Security researched the cyber-attack on Iran's Nuclear control system which affected the nuclear program of Iran. Therefore, CPS require systems and measures in place to ensure detection of these kinds of attacks and try to avoid or notify the respective body of the breach. Additionally, organizations dealing with CPS must ensure that not only the sensor is secure but also that there are provisions in place for security in the data centers as these devices are interconnected from a central server. However, we must welcome these innovations and technologies in CPS as these improve not only the standard of living but makes it easier for us to access and control devices around us and change the way we live our lives. This also paves away and leads to the

creation of a ‘Smart City. We will discuss more on Cyber-Physical System in this paper which addresses the above issues and solutions along with certain research from other countries.

Purpose & Motivation

Cyber-Physical system could potentially link both our physical and cyber world. Cyber-Physical Systems (CPS) is a collection of networking, computational and physical processes. It is a system in which the mechanism is controlled or monitored by computer-based algorithms. It integrates networking, computation and much more into physical devices thereby connecting them online and with each other. In the virtual world, it is an environment in where computing, communication and management are being taken up by programs or machine-driven algorithms. Whereas the Physical World is an environment in which sensors and IoT devices are connected. Due to CPS being a technology that uses next-gen control systems and a combination of physical systems like sensors, actuators, etc.; and all these being connected to an algorithm or an element that controls it, CPS demand and dependence on it by Energy, transportation, medicine, and many other industries, has increased. The development of CPS may lead to improvement in lifestyle and quality of life, but at the same time, the risks in terms of security are increasing due to new loopholes and new protocols. The real security issue is identifying the source. This is because there are many components in CPS and a targeted breach/attack on a component may expose data of other components to the attacker. In 2014, 54% of the world’s population lived in urban areas. That number is expected to reach 66% by 2050. Cities these days are looking for ways to be sustainable, comfortable, and economically stable for their citizens; in other words, these cities want to become “Smart”. So, what is a smart city, exactly? A smart city is one in which new ideas and methods are employed to enhance and enhance services in areas such as transportation, energy, healthcare, the environment, business, commerce, disaster response, and social activities. A Smart City's infrastructure is made up of numerous sensors and actuators placed around the city and connected to wireless devices and the Internet through a cloud service. The Cyber-Physical Systems may collect data such as air and water quality in the city, the structural integrity of bridges and roadways, status of city resources such as police, transport, etc. A lot of these Cyber-Physical Systems are already in service. For example, when you visit a mall, in the parking lot, you will see these devices with either red or green lights above which indicate whether the parking space in front of it is occupied or free. Another example could be, in Dubai when we commute with Roads and Transport Authority (RTA) Transport. At the bus stop or in the metro station, we see the timing of when we can expect our bus or metro to arrive. Both these examples are CPS in play. Currently, these systems are widely seen in Cities with a huge spending capability. But day by day, we see it emerging in other areas of the world as well with the decreasing cost of this technology and the increase in its popularity and ease of use. Utilizing such devices in ‘Smart Cities’ requires a cyber-physical infrastructure combined with state of the art and new software and better mobility, security, privacy and procession of data. This requires a proper understanding of the physical and virtual components with the use of proper energy usage and better security of the wireless and wired data transferred via these CPS devices and components. In this era, the internet will no longer be just a medium for

transferring packets from one location to another but, it will help data flow from components or IoT to central servers and sending of commands to actuating devices that perform real-time operations (e.g., Traffic Light Controller, HVAC Systems, etc.).

Problem / Issue to be Addressed

Over the last couple of years, Cyber-attacks have been more sinister and have a bigger risk and breach in terms of data and security. The biggest and most discussed Problem of CPS is its Security Issues, Vulnerabilities and Data Privacy. As of writing this, there are three types of CPS Security Threats:

- **Perception Threats:**
  This layer is limited to and consists of the devices and memory functions in the physical environment like RFID scanners. These devices are placed in outdoor areas which can cause physical attacks in which device components could be changed, altered, or the entire device could be replaced or tampered with. Most security researchers and testers, focus on the cyber environment thereby ignoring or omitting the vulnerabilities of the physical layer which is why the importance of researching and testing on this layer is needed. This layer includes threats such as:
  Cryptography Threat: The security data of CPS are always at risk of being hacked on the cyber or physical layer. Security data is collected, processed, transmitted, and stored on physical devices. The unmanaged/unmonitored status of these endpoint devices makes it probable to hardware-based attacks.
  Fault Attack: This is when an attacker intentionally triggers faults on the devices to reset the data password and remake in the internal mechanism. It is generally known, that when these kinds of attacks are triggered, all major pathways in the system come across the problem of circuit control.
  Node Reputation: There are several forms of assaults that fall under the category of Node Reputation, including node capture, false nodes, and node outages. When an attacker obtains information about encryption keys on behalf of a node, this is known as node capture. This jeopardizes the system's overall security. When an attacker adds a fake node to the system, they send malicious data to the system. This results in DoS attacks that consume the node's energy and compromise the data's readability or integrity. When an attacker compromises the availability and integrity of a node, it is known as a node outage. This makes it harder for the node to collect and evaluate data because the node service is interrupted.
  All these different dangers are aimed at maintaining confidentiality, stability, integrity, and availability.

- **Communication Threats:**
  This layer needs proper protection the prevent vulnerabilities in the CPS Infrastructure. The CPS Structure must be able to provide control over all the devices connected in the environment under a lightweight and resilient protection scheme. The risks in this layer

are routing attacks, DoS or DDoS attacks, control attacks, flood attacks, trap doors and many more. There are many different threats to this layer. Few of which are discussed below:

End To End (E2E): These kinds of attacks pose threats to the end-to-end authentication and the core contacts, key management, encryption algorithm and DoS/DDoS attacks. Distributed devices that have been placed in the environments may be exposed to third parties which may pose some security risks which is why secure communication is required. Thereby, all information being exchanged between devices and servers must be protected with the highest standards and protocols. With E2E, the reliability of devices and large-scale CPS are at risk.

Hole Attack: There are a variety of assaults that fall under the category of hole assaults. Wormhole attacks, sinkhole attacks, black hole attacks, and grey hole assaults are only a few examples. A wormhole attack on the Wireless Sensor Network protocol is very serious and dangerous, and it consists of two main attacks. The way it works is that two illegal nodes create temporary wormhole tunnels for the legitimate nodes. This gives the impression of being quite close. As a result, attackers can take control of network pathways and send in false routing protocols and data. The sinkhole assault gives the best pathway to the base station for the attacker. Before the data is erased or received at the destination, the sinkhole attack node alters it. This causes unneeded and unwelcome delays in the network path.

Spoofing: This is when an attacker acts or portrays himself as an authorized or legitimate part of the system and tries to interfere with its operation. If the attacker is successful, this not only gives access to the data to them but also allows them to delete, modify or update data with false or invalid data. Furthermore, this may also lead to incorrect functioning/malfunctioning of the system thereby delaying services and raising threats. During this attack, the system is unaware of the attacker and accepts all data fed by the attacker as legitimate thinking it is coming from an authorized/legitimate source. A subpart of this is Man-in-the-middle.

- **Application Threats:**

  Application threat occurs when there is an attack on the information and data of users. Data loss, loss of personal information such as user preferences, and illegal access to the device are all consequences of these types of assaults. To mention a few, this layer includes user privacy disclosure, illegal access, harmful code, database assaults, and more. Below are a few of the application threats discussed in brief:

  Buffer overflow: This type of attack occurs when an attacker interferes with the program's or application's regular operation and prevents it from working properly. Stack smashing and function pointing manipulation are two typical approaches for these assaults. Password resets, data and content manipulation, the execution/running of malicious code, and the exploitation of software vulnerabilities are all common outcomes of these assaults.

  Malicious Code: This attack occurs when various malicious codes filled with viruses and bugs, attack an application thereby causing damage to the network. Depending on the

load of the virus attack, it may cause the application to crash or execute even more malicious code.

Structure Query Language (SQL): Most organizations data can be accessed via database applications on SQL. The usage of SQL commands and statements for this attack may lead to structural changes and data manipulation in the Database. Another term is SQL Injection. SQL Injection is when another entity manipulates the data but prevents the user from deleting it and inserting unwanted/unexpected SQL commands in the database. In the recent study, the SCADA system (Supervisory control and data acquisition system) was proven to be one of the best countermeasures on SQL Injections with a very superior security mechanism of the SCADA System.

Every year, big tech companies and governments spend millions of dollars trying to counteract data breaches as well as reducing the impact/damage caused due to the leak of data by the data breach. It is necessary to keep a close eye on the security of CPS as Cyber Security grows and so does the threats. The security of CPS is divided into three parts: namely, physical security, communication security and, control and operational security. Physical security is governed by the task of protecting data on physical devices like sensors and ensuring there is no unauthorized access given to an attacker as discussed in the attacks above. Communication security is tasked with protecting the data when it is being transmitted and received so that there is no data manipulation in between or data loss. And finally, control and operational security are governed to protect the cyber environment from attacks on the central systems, control algorithms and control systems.

We've now discussed the crucial and important issue of CPS. But for every problem, there must be a solution. We will discuss the approach for the CPS problems in the next section.

Approach:

CPS is mostly used in smart grids, health care, autonomous industries, smart transportation, home energy management system, deep-sea exploration and many more. But even though they are used in these scenarios, they face many challenges as discussed in the previous section. In this section, we discuss the solutions to overcome these problems and possibly solve them. Following are the design principles and requirements that should be followed to ensure that no security attacks or structural failure occur:

Test and Analysis Complexity: There are diverse fields in CPS right from software engineering, mechanical engineering to systems engineering and network engineering. Due to the diversity of these fields, it is difficult to collect, test and analyze software and hardware requirements. Even testing has become difficult due to there being no effective testing tools or approaches. Therefore development and testing should work with various clients and be able to communicate with the various fields.

Design & Implementation Complexity: The design of software for CPS is very complex, due to the security issues and vulnerabilities of CPS. Additionally, CPS must also meet many requirements by components, applications, programming languages and external environments.

Safety: This is necessary for every CPS device and node and is an asset in applications that have control systems. CPS Devices and systems must be designed and created so that it safeguards and does not cause any harm to life or lead to financial losses.

Security: In CPS, Security is classified into three main parts. Namely, Encryption, data and its information security and control system security. These measures are required so that the User's Personal Information is safe and not compromised. CPS manufacturers and developers must also ensure that network attacks on the communication between sensors, actuators and controllers are prevented, detected, and blocked. The main aim of CPS is to provide uninterrupted service and avoid issues of computing, control, and communication.

CPS Security needs to be designed in a way to protect the data, network security and privacy in both the physical and cyber environments. There are various security schemes in CPS which have been categorized as below. Following are the solutions to solving the issues of CPS:

- **Device Protection:**
  Designing a safe hardware platform with robust architecture to defend against cyber-attacks is the best technique to establish a secure hardware infrastructure. Based on hardware anchors, Jin and Oliveira suggested an OS-to-hardware communication-based high-security SoC architecture. Hardware anchors are regularly verified, and bus activity is tracked to avoid unwanted manipulation. The design they provided was effective and had a low performance overhead. Oliveira et al. created a HW/SW design that allows the OS to be extended safely. Ianus, an emulator-based prototype, was constructed by them. All malicious rootkits were disabled because of this test, and no false positives for positive modules were detected. Al Ibrahim and Nair created a breakthrough CPS security architecture based on PUFs. Synthetic techniques that incorporated the security aspects of complex PUF elements were investigated using the framework. A physical unclonable function is a digital fingerprint used to identify a semiconductor device, such as a microprocessor (PUF). It is distinguished from other semiconductors by physical changes that occur spontaneously throughout the semiconductor production process. The PUF is a widely used encryption algorithm that is now being implemented in integrated circuits for high-security applications. The WSO2 complex event processor served as the security layer in Vegh and Miclea's integrated CPS solution, which was developed as a multi-agent system (CEP). The solution evaluates each communication and can tell you if it is encrypted or not. It also epitomises the ideal CPS by ensuring safe, efficient, and reliable secrecy, privacy, and accessibility. Kocher et al. suggested employing the most up-to-date cryptographic primitives, such as AES, RSA, ECC, and HMAC, to protect against attacks by adversaries utilising plain text and cypher text data.

This way of preventing assaults, rather than indiscriminate attacks, is considered to provide a mechanism that can protect against assaults that are outside of the conventional range while also improving cryptanalysis findings.

- **Network Access Detection:**
  Using software-defined network (SDN) and control system detection techniques, network and system access defence covers defence and wormhole attack detection measures. The SD-CPS was presented by Kathiravelu and Veiga as a solution and architecture for dealing with the CPS' application and design challenges. As a result, the SD-CPS is compatible with existing CPS implementations that do not require SDN and can be used in conjunction with them. As a result, several research methodologies for SDN deployment, design, and enhancement were made accessible for alternate evaluation. In the WSN, Gupta devised a new method for identifying wormhole assaults. This method identifies wormhole tunnels using a basic search methodology and updates the frequency table with bandwidth as a WSN parameter, consuming less data. According to Cardenas et al., it is possible to identify a computer assault that alters the function of the target control system by altering the physical system. Previously, interactions between control and security experts in the physical environment and control domain were essentially unimportant, and there were worries about control algorithms and target assaults. As a result, anytime a physical device is upgraded, new interfaces and compatibility are added to re-test it and detect and resolve any vulnerabilities. Furthermore, authorized workers can acquire rapid and easy access to vital systems to update the CPS's components, but unlawful access should be instantly stopped and defeated. To meet all the CPS standards, Sanchez et al. created a predictive system to manage mobility and device lifecycles. To generate future system state sequences, the approach used CPS simulators and interpolation methods based on endless loops. It also served as an experimental validation for the suggested solution's performance.

- **Malicious Code Detection:**
  On the internet, various malware detection techniques have been described. However, because these technologies only detect hazardous code on the web, they can't be used to prevent unsafe code from propagating in the CPS. By integrating all of an OSN's features, Xu et al. created an early warning online social network (OSN) worm detection approach. The system employs the maximum range algorithm to identify user communication and produces a "bait friend" with a real OSN user group. The detection system uses network and local methods to separate harmful propagation from permitted users when evidence from the "bait buddy" suggests that a suspected malicious code has been transmitted to the connection. Rathore demonstrated a machine learning-based XSS threat detection solution for the Social Networking Service. XSS assaults are identified utilizing three functions in this strategy: URL, Web page, and SNS, and the recommended methodology's efficacy is compared to previous ways.

- **Application Support:**

Application solutions span all aspects of smart buildings, smart cities, smart industries, smart healthcare, smart grids, and related solutions. Khalid et al. created a collaborative robotic CPS (CRCPS) framework for human-robot collaboration (HRC). Humans may use it to integrate and deploy a wide range of interactive technologies. Kim and colleagues demonstrated CF-CloudOrch, a cloud orchestration system built on lightweight container technology and a basic network management architecture. The fog nodes were setup, and Docker Swarm and Container Docker were used to enable full managed services cloud orchestration. IoT network administration is crucial because if the network is maintained properly and easily, it may be used for future IT. Sharma et al. created a scalable distributed smart-city architecture to satisfy the design goals for a sustainable smart city. The deployment of SDN controller nodes in a distributed blockchain network architecture, the deployment of cache nodes, and the filtering of raw data at the network's edge, on the other hand, provide a number of obstacles. Sharma et al. presented DistBlockNet, a distributed safe SDN architecture for the Internet of Things that incorporates blockchain technology. The protection manager can react dynamically to threats, eliminating the need for a security manager to manually examine a high number of warnings and approvals. According to the findings, the performance overhead is modest, and IoT network attacks may be detected in real time while conforming to the architectural principles required for future IoT networks. Li et al. introduced a new distributed host-based collaborative detection (DHCD) methodology for detecting and mitigating false data injection (FDI) risks in the Smart Grid CPS. Anomalies in measurement data are detected using rule specifications based on real-time collaborative detection systems. By leveraging cloud and big data technologies to improve the operation of medical equipment, humans may exhibit a variety of smart healthcare applications and services.

Conclusion:

Because many devices interface with the centralized network, IoT open issues in the CPS pose a high danger. Even if only one IoT device out of thousands is hacked, it is connected to the data center network. Furthermore, there is a risk that the centralized network that connects many IoT devices will be utilized as a tool. The IoT can also be used to attack humans, which is a more significant concern. The possibility of illegal use of personal information is one of the data center's unresolved challenges in the CPS. This is since the CPS's data center collects vast amounts of data in a variety of forms to deliver useful analytical results. The open issues of artificial intelligence have recently arisen as a threat to human beings. This is because artificial intelligence poses a danger to ordinary decision-making in areas such as intelligent industrial control, medical diagnosis, editing, and creativity. The Internet allows the Fourth Industrial Revolution to collect vast volumes of data and receive responses swiftly. Based on analysis and learning, as well as the application of artificial intelligence with large data, it can also be integrated in CPS. The threat level rises, and the scope of control grows. The more room CPS takes up, the more difficult it is to keep the hazards under control. As a result, the risk assessment linked with Fourth Industrial Revolution technology should not be used in a specific setting. Consider completing a risk analysis of the CPS if all IoT are inexorably connected and operational.

Because CPS security is a new domain that differs from the present network environment, little work has been done in this area. The CPS handles data from a variety of sensors, data kinds, real-time produced data, process analysis, and application interfaces. This page organizes the multiple dangers, solutions, and CPS security initiatives connected to the CPS's issues and hazards and offers a solution for each issue. The CPS notion and security produced problems and challenges, as well as displaying the existing security market and CPS-related surveys. The CPS security team evaluated each layer's hazards and remedies, as well as future research prospects. We investigated the connections between CPS security threats and remedies, as well as any lingering issues. By merging IoT and other sensors, IT will be able to expand the scope of CPS security in the future. To guarantee that the system is safe, we should connect with other systems in a variety of scenarios. The findings of this study might assist to improve the overall security of the system because the CPS environment is made up of various layers and is related to field dangers. Because the CPS is extensively utilized in many smart settings, such as the smart home, smart city, smart industry, smart healthcare, and smart grid, CPS security should be a continual worry. As a result, as the smart environment evolves, the growth of CPS security is projected to become increasingly significant.

References:

1. N. Y. Kim, S. Rathore, J. H. Ryu, J. H. Park and J. H. Park, "A Survey on Cyber Physical System Security for IoT: Issues, Challenges, Threats, Solutions," Journal of Information Processing Systems, vol. 14, no. 6, pp. 1361-1384, 2018.

2. Cassandras, Christos G. “Smart Cities as Cyber-Physical Social Systems.”. In Engineering 2, 2nd ed., 2:156–58. Engineering Sciences Press, 2016.

3. Venkatasubramanian, K.K., 2009. *Security solutions for cyber-physical systems*. Tempe: Arizona State University.

4. Keerthi, C.K., Jabbar, M.A. and Seetharamulu, B., 2017, December. Cyber physical systems (CPS): Security issues, challenges and solutions. In *2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)* (pp. 1-4). IEEE.