iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** I **Month of publication:** January 2022

DOI: https://doi.org/10.22214/ijraset.2022.39734

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue I Jan 2022- Available at www.ijraset.com

Attack Taxonomy for Cyber-Physical System

Ms. Keerti Dixit[1], Dr. Umesh Kumar Singh[2], Dr. Bhupendra Kumar Pandya[3], Mr. Shekhar Disawal[4]
[1, 2, 3, 4]*Institute of Computer Science, Vikram University, Ujjain*

Abstract: Cyber-physical systems are the systems that combine the physical world with the world of information processing. CPS involves interaction between heterogeneous components that include electronic chips, software systems, sensors and actuators. It makes the CPS vulnerable to attacks. How to deal with the attacks in CPSs has become a research hotspot. In this paper we have study the Architecture of CPS and various security threats at each layer of the archicture of CPS. We have also developed attack taxonomy for CPS.

Keywords: Cyber Physical System, Threat, Attack.

I. INTRODUCTION

CPS are similar to Internet-of-Things (IoT) systems, but they have more physical and computational coordination [1] [2]. Users, the physical environment, and a variety of hardware and software-based systems all interact with cyber-physical systems. Integration, interoperability, monitoring, and control of cyber-physical system components are all part of this. In contrast to stand-alone devices, CPS feature a chain of inputs and outputs linked to interacting elements. Furthermore, the application of CPS cannot be limited to a single field; rather their applications extend to almost every field [3]. These systems will enable advanced customisation of health care, traffic control, banking, and the smart grid, etc. A CPS is characterized by the wide range of deployed technologies and a varying scale between such systems [4]. Computing devices, embedded systems, sensors, control units, and other devices that accomplish different tasks can all be deployed in a CPS. One CPS, for example, can mainly consist of a few sensor and actuator nodes for monitoring and adjusting the room temperature. A CPS, on the other hand, can evolve into a network of enormous heterogeneous and decentralised distributed subsystems that can, for example, conduct various autonomous activities on a solar energy plant [5]. CPSs have adaptive skills to handle both this complexity and changes in system scale. In most cases, the scale and diversity of deployed components define the complexity of a CPS. In addition, the majority of CPS use powerful feedback control technology. The ability to govern cyber-physical events in reaction to changes in the physical environment is referred to as feedback control [6].

II. ARCHITECTURE OF CYBER PHYSICAL SYSTEM

CPSs are usually composed of three layers:

A. The Physical Layer

Sensors, actuators, and a range of additional devices and subsystems with sensing, processing, and communication capabilities make up a physical layer [7]. Physical phenomena in the system's physical environment are recorded by sensors in this layer. This layer also includes actuator units, which react to real-time event monitoring and interact with the application layer to allow data processing [8] [9]. The actuator units have the ability to change the properties of physical objects and occurrences in the real world [10]. Cyber-physical events are formed as a result of the information processed in the system, and they cause actuation in a physical process. The capacity of its components to interface with external networks such as the internet via a gateway node is an important aspect of this layer. Because this layer is so sensitive to cyber-attacks, setting security standards is crucial.

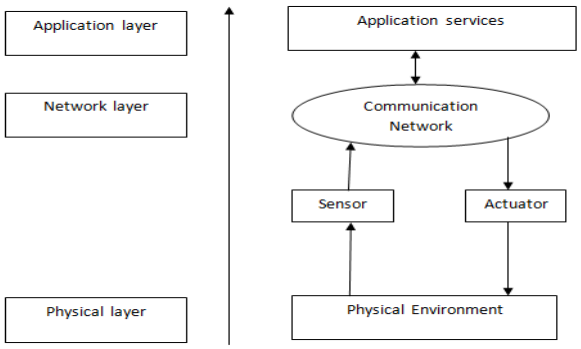


Figure 1: Architecture of Cyber Physical System

B. The Network Layer

The purpose of the network layer is to transmit control commands and sensory data between the application layer and the physical layer. The large number of different heterogeneous networks connected means that special security protocols have to be taken into account.

The network layer is critical for CPS operation because it serves as a link between the physical and application levels as well as a channel between sensors and actuators [11] [12]. The network layer is the route over which data, measurements from sensors, and commands to actuators are exchanged. Some of the network layer's communication protocols include: Ethernet, Distributed Network Protocol (DNP), Recommended Standard 16 (RS-232), Transmission Control Protocol/Internet Protocol (TCP/IP), dial-up modem, and other wireless protocols [13].

Because of their scattered nature, wireless communication is the most popular mode for sensor and actuator communication. The cloud or a physical server are frequently utilised for wireless communication. The network layer connects the application and physical layers, allowing them to operate together closely.

C. The Application Layer

The application layer is made up of many components such as controllers, databases, and a user interface. This layer takes data from the network layer and generates control orders to control physical devices and processes [14]. The application layer is responsible for a variety of services, including user access, precision agriculture, environmental monitoring, intelligent transportation, smart grid, and other application-specific roles involving data reporting and representation, acting as a control panel for end users, and providing a mostly graphical user interface for a variety of applications and services, including user access, precision agriculture, environment monitoring, intelligent transportation, smart grid, and others. It also provides an interface and services to the end users for accessing sensory data via mobile devices or terminals, which might take many various forms and have highly unique security requirements.

III. SECURITY THREATS IN CYBER PHYSICAL SYSTEM:

A. Threats in Physical layer

The physical layer is a key source of perception data and the execution venue for control commands in the three-layer architecture of cyber-physical systems. The majority of physical layer network nodes are placed in unsupervised environments, making them easy targets for attackers. Because the nodes' data processing, communications, and storage capacity are restricted, typical security techniques cannot be directly applied to the physical layer's perception network. The physical layer's key security threats are described below:

1) *Physical Attack:* Physical attack mainly refers to the physical damage for the nodes.
2) *Equipment Failure:* Equipments reduce or lose performance due to external forces, environment or aging.
3) *Line Fault:* The failure of power lines on nodes is referred to as line failure.
4) *Electromagnetic Leakage:* By processing electromagnetic signal equipments at work radiated out, attackers can restore the original data.
5) *Electromagnetic Interference:* Unwanted electromagnetic signals or commotions make negative impacts on useful signals, resulting in system Performance degradation.
6) *Denial of Service (DoS):* Through network bandwidth consumption, the attacker causes the target machine to discontinue offering services.
7) *Channel Blocking:* Data cannot be transmitted for communication channel has been occupied for a long time.
8) *Sybil Attack:* To attack the system by controlling the majority of nodes, a single malicious node uses numerous identities.
9) *Replay Attack:* Attacker resends the legitimate data obtained before, to get the trust of the system.
10) *Perception Data Destruction:* The unauthorized addition, deletion, modification and destruction of perception data.
11) *Data Intercept:* Illegal access to the data resources through intercepting the communication channel.
12) *Data Tampering:* Attacker intercepts and modifies the data, then sends modified data to the recipient.
13) *Unauthorized Access:* Resources are accessed by unauthorized users.
14) *Passive Attack:* Attacker passively collects data by sniffing and information collection.
15) *Node Capture:* Gateway node or ordinary node is controlled by attackers.

Physical layer security concerns include the physical security of each node's infrastructure, the acquisition of perception data, and the execution of control commands. This layer's security mechanisms should assure the safety of sensors, actuators, RFID devices, image capture devices, and other devices. The physical layer's security is the foundation for the security of cyber-physical systems. The following are the main security measures for the physical layer:

a) Enhance the management and protection of the identity of the node. To some extent, this will lengthen the time it takes for a node to be certified. Administrators can weigh the system's security and efficiency to design a better balanced node authentication method in practical applications.
b) To provide better protection of perception data by applying biometric technology and near-field communications technology.
c) Strengthen the legislation. Make clear the cost for the illegal behaviors concerning cyber-physical systems.
d) Research on the technologies of cryptographic [10-11], privacy protection [12-14], security routing [15], security data fusion [16] and safety positioning [17] combining with cyber-physical systems.

B. Threats in Network Layer

The "next-generation network" serves as the fundamental bearer network for the network layer of cyber-physical systems. CPS will face a number of security vulnerabilities as a result of the architecture, access methods, and network equipment of the "next-generation network." On the network layer, the large number of nodes and large amounts of data may generate network congestion, making the system vulnerable to DoS/DDoS attacks. New security concerns for the network layer of cyber-physical systems will arise as a result of data interchange, gateway authentication, and convergence of security policies amongst diverse networks. The following are the main network layer security threats:

1) DDoS: Plenty of malicious nodes attack target server as the sources of DoS at the same time.
2) Routing Attack: Attacker interferes with the normal routing process by sending forged routing information.
3) Sink Node Attack: Interrupting data transmission between physical layer and network layer by attacking the sink node.
4) Direction Misleading Attack: Malicious node modifies the source and destination addresses of data packets then sends it to a wrong path, resulting in network routing confusion.
5) Black Hole Attack: Malicious node cheats other nodes to establish routing connections with it, and then discard the packet should be forwarded, causing packet loss.
6) Flooding Attack: Exhausting the resources of the network servers on network layer by Smurf and DDoS.
7) Trapdoor: Allow the exception of security policy when specific data transporting.
8) Sybil Attack: By controlling the majority of the nodes, the malicious node uses numerous identities to obstruct data transit.
9) Sinkhole Attack: Malicious node attracts normal nodes around as a point in the routing path, so that all data will flow through it.
10) Wormhole Attack: Malicious nodes attack together to get the routing right by the less routing hops between the malicious nodes.
11) Routing loop Attack: Malicious node modifies the data path to cause an infinite routing loop.
12) HELLO Flooding Attack: By broadcasting routing information via a powerful signal, the malicious node alerts other nodes in the network that it is their direct neighbour.
13) Spoofing Attack: A malicious node pretends to be a genuine node in order to transfer data down a slow path or to a failed node.
14) Selective Forwarding: Malicious node deliberately loses some or all of the key information in the forwarding.
15) Tunnel attack: Malicious nodes hide the real link distance between them to lure the other nodes to establish routing path through them.
16) False Routing Information: Malicious node attacks network layer network by tampering with the routing information.

Security measures for the network layer of cyber-physical systems maintain the integrity, confidentiality, and consistency of communication data in the system. Both point-to-point and end-to-end encryption mechanisms can be used for network layer security [18].

a) The security of data during hop-by-hop transmission is ensured by a point-to-point encryption technique. Because each node in the chain can obtain plaintext data, this technique necessitates a higher level of node reliability. Node authentication, hop-by-hop encryption, and inter-network authentication are some of the security measures.
b) End-to-end encryption ensures data secrecy from beginning to end, as well as providing adaptable security rules for various security levels. End-to-end encryption, on the other hand, cannot conceal the data's source and destination, and attackers could exploit this information. End-to-end authentication, key negotiation, and key management are some of the security mechanisms.

C. Threats in Application Layer

Because some programmes on the application layer capture personal information from users, such as their health and consumption habits, privacy protection of information on the application layer is important in cyber-physical systems. Because there are so many different applications in the system, each with its own set of security requirements, developing security measures for the application layer is extremely difficult. The major application layer security threats are outlined below:

1) *Privacy daTa Leaking:* Due to insecure data transmission, storage, and presentation, consumers' personal information gets leaked.
2) *Unauthorized Access:* Unauthorized access to network and system data.
3) *Malicious Code:* There is code in the system that has no effect but could be a security concern.
4) *Forged Control Commands:* By altering control commands, attackers maliciously use or harm the system.
5) *Loophole:* Using application layer loopholes to attack the system
6) *Viruses, Trojan horses:* Viruses and Trojan horses are the most common security threats to application layer security.
7) *SQL Injection Attack:* SQL injection is a common technique of attacking a system's database.

The application layer is the central component of cyber-physical systems, and it is in charge of making decisions and issuing control commands. Massive volumes of data on the application layer of cyber-physical systems necessitate powerful data processing capabilities on this layer, as well as extensive user privacy data protection. The following are the main security measures for the physical layer:

a) Strengthen access control policy of the system.
b) Strengthen the authentication mechanism and encryption mechanism in different scenarios.
c) Improve network forensics mechanism to strengthen the capacity of network forensics [19].
d) Establish a centralized, efficient security management platform for the various applications of cyber-physical systems.

IV. ATTACKS ON CYBER PHYSICAL SYSTEM:

Attacks on CPS could cause significant physical damage to the environment. Each layer of the CPS can be attacked passively or actively. Furthermore, CPS is more vulnerable to attacks than typical IT systems. These attacks are not specific to CPS, but also include attacks on the network itself, particularly the Internet [20], which is already used as the transmission layer. Attacks on nodes such as sensors and actuators are examples of physical layer attacks; data leakage or destruction, as well as security vulnerabilities during data transmission are examples of network layer attacks; and application layer attacks include unauthorised access that compromises user privacy [21]. As a result, assessing potential threats and constructing a strong security architecture are essential. Despite the fact that each layer is vulnerable to various types of attacks, some attacks may target all layers, and according to [21], [20], [18], and [22] examples of these attacks include:

1) *Denial of Service (DoS):* It modifies behaviour characteristics by restricting traffic in order to make the network and service unavailable, for example, by flooding a resource with fake requests and exploiting a protocol vulnerability. Furthermore, DDoS is a frequent attack that simultaneously targets many resources, such as end devices and networks, blocking access to information and services[22].
2) *Man-in-the-Middle (MITM):* It sends a fake message to a targeted resource, which then performs unwanted activities, such as controlling a primary function, in response to the received message, which could result in an undesirable event. This type of attack can also affect the network layer, which can be followed by eavesdropping in some situations [23].
3) *Eavesdropping:* Any data sent by the system is intercepted. For example, transferring control information from sensor networks to applications in the CPS for monitoring purposes could be vulnerable to eavesdropping. Furthermore, because the system is being monitored, user privacy may be compromised [23].
4) *Spoofing:* Pretends to be a legitimate user of the system before attempting to participate in system activities. After successfully gaining access, the attacker will have access to information and will be able to alter, delete, or insert information [23].
5) *Replay (playback):* Retransmits a received packet from the target node to acquire the system's trust [22]. This type of attack can be launched by spoofing and altering or responding the identifying information of one of the devices.
6) *Compromised Key:* The secret key that is used to secure communication is the target of this attack. This is accomplished by a timing (side channel) attack, which involves evaluating the required encryption time [22]. The stolen key will then be utilised to alter collected data and perform computer analysis in order to decrypt other secret keys in the same system. An adversary could gain access to sensors in some situations and force them to execute engineering activities in order to retrieve other internal keys.

In another scenario, an attacker might be able to replace a sensor node and pertain as the legitimate version while exchanging keys with other nodes [18, 19], thereby, discovering other secret keys of the involved nodes.

There are numerous types of risks at each level of the CPS, and frequent attacks for each layer can be classified as follows depending on the CPS architecture.

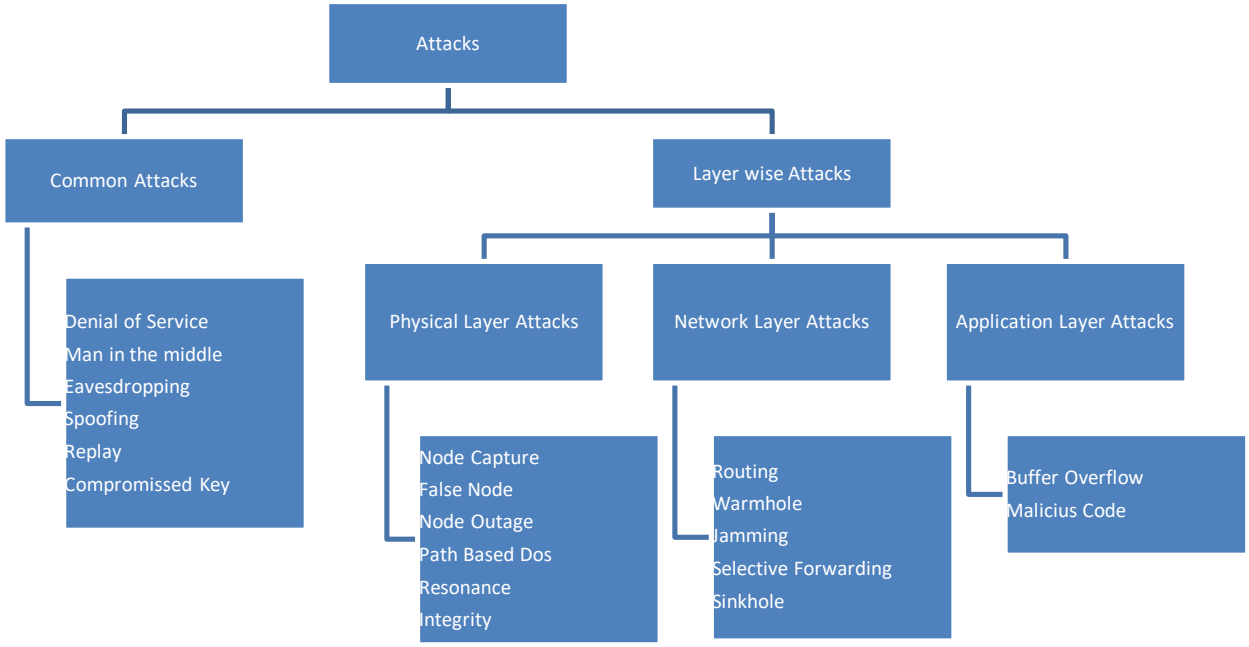


Figure 2: Attack Taxonomy of CPS

A. Attacks at the Physical layer

End devices, such as RFID tags and sensors, make up the physical layer, which are confined by computational resources and memory capacity. Furthermore, because these devices are primarily found in external and outdoor areas, they are vulnerable to physical attacks such as tampering with their components or replacing them. As a result, those terminal devices are the most vulnerable to various attacks [23]. The following are examples of common types of attacks:

1) *Node Capture:* Takes control of the node and obtains and leaks information that may include encryption keys, which is subsequently used to threaten the entire system's security. This form of attack targets confidentiality, availability, integrity, and authenticity [22, 24].
2) *False Node:* To threaten data integrity, it adds a new node to the network and sends malicious data. This, in turn, could result in a DoS attack by exhausting the system's node's energy [22].
3) *Node Outage:* Stops node services, making it hard to read and acquire information from them, and launches a variety of additional attacks that compromise the availability and integrity of the network [24].
4) *Path-Based DOS:* Sends a large number of packets, known as flooding packets, along the routing path to the base station, draining node batteries and disrupting the network, lowering node availability [24].
5) *Resonance:* Forces sensors or controllers that have been compromised to operate at a different resonance frequency [25].
6) *Integrity:* Attempts to destabilise the system by injecting external control inputs and misleading sensor data [26].

B. Attacks at the Network layer

Data leakage during information transfer is one type of attack on this layer. This occurs as a result of the transmission media's openness, particularly in wireless communication. Such attacks impersonate a legitimate user by capturing a sent message through a radio interface, modifying and retransmitting it, or exchanging information between heterogeneous networks. Other elements, such as remote access techniques among a large number of network nodes, which could generate traffic congestion, would also enhance the likelihood of being attacked [20, 23].

The following are some examples of popular network layer attacks:

1) *Routing:* Creates routing loops, which can lead to network transmission resistance, increased transmitting delay, or an extended source path [18, 22].
2) *Wormhole:* By establishing false paths through which all packets are sent, it creates information gaps in the network [27].
3) *Jamming:* The wireless channel between sensor nodes and the remote base station is jammed when noise or a signal with the same frequency is introduced. This attack could result in DoS [18] by introducing purposeful network interference.
4) *Selective Forwarding:* Makes a hacked node to drop and reject packets while forwarding chosen packets. While the compromised node is still regarded genuine, it may stop delivering packets to the intended destination or only forward selected messages while discarding all others [18].
5) *Sinkhole:* It is announced which routing path should be used for traffic routing to other nodes. Other attacks, such as selective forwarding and spoofing, could be launched using this method [18].

C. *Attacks at the Application layer*

Because this layer collects a huge amount of user data, attacks here result in data loss, privacy loss (such as user habits and health conditions), and unauthorised access to devices [20]. At this layer, common examples of attacks include:

1) *Buffer Overflow:* Takes advantage of any vulnerabilities that result in buffer overflow vulnerabilities and uses them to conduct attacks [22].
2) *Malicious Code:* Attacks the user application by launching malicious code such as viruses and worms, which slows down or damages the network [28].

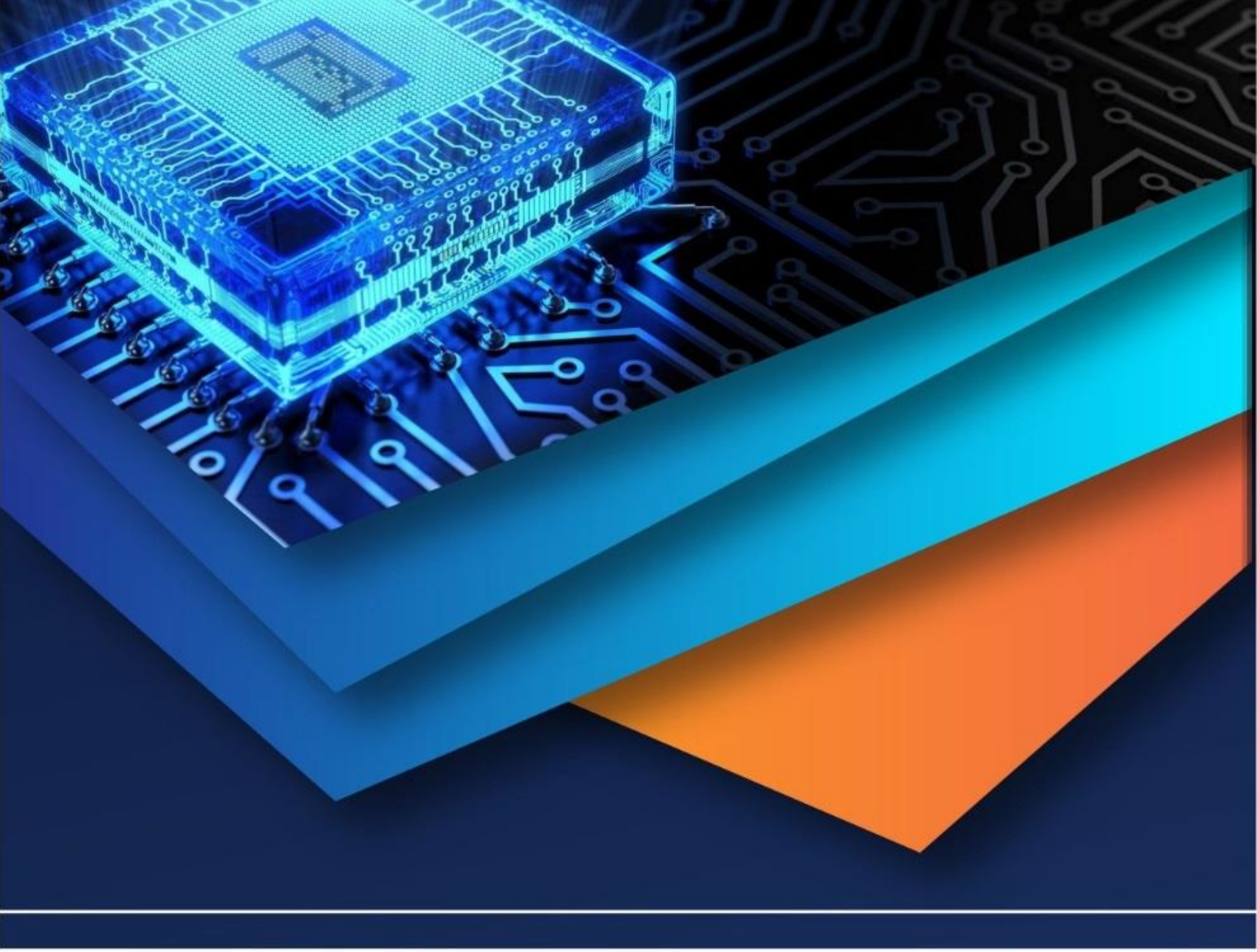
V. CONCLUSION

Complex systems based on the convergence of physical or hardware and cyber or software components are known as Cyber Physical Systems (CPS). CPS offers a wide range of applications. The number of deployed CPS is continuously increasing, raising a number of security and safety issues. In this work we have provides an overview of the definition and architecture of Cyber Physical Systems, and analyzes the security threats and attacks of the three layers of Cyber Physical Systems. We have also developed the attack taxonomy for CPS.

REFERENCES

[1] R. Rajkumar, I. Lee, L. Sha and J. Stankovic, “Cyber-physical systems: the next computing revolution,” in Design Automation Conference (DAC), 2010 47th ACM/IEEE (pp. 731-736). IEEE., 2010.
[2] L. Da Xu, W. He and S. Li, "Internet of things in industries: A survey," IEEE Transactions on industrial informatics, 10(4), 2233-2243., 2014.
[3] J. Gubbi, R. Buyya and S. P. M. Marusic, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, 29(7), pp.1645- 1660, 2013.
[4] J. Wan, H. Yan, H. Suo and F. Li, "Advances in Cyber-Physical Systems Research.," KSII Transactions on Internet & Information Systems,, p. 5(11), 2011.
[5] M. E. Brak, S. E. Brak, M. Essaaidi and D. Benhaddou, "Wireless Sensor Network applications in smart grid," in International Renewable and Sustainable Energy Conference (IRSEC) (pp. 587-592). IEEE., 2014.
[6] B. Bordel, R. Alcarria, T. Robles and D. Martín, "Cyber–physical systems: Extending pervasive sensing from control theory to the Internet of Things," in Pervasive and mobile computing, 40, 156-184., 2017.
[7] D. Estrin, D. Culler, K. Pister and G. Sukhatme, "Connecting the physical world with pervasive networks," in IEEE pervasive computing, 1(1), 59-69., 2002.
[8] L. M. Oliveira and J. J. Rodrigues, "Wireless Sensor Networks: A Survey on Environmental Monitoring," in JCM, 6(2), 143-151., 2011. 168
[9] S. Wang, J. Wan, D. Li and C. Zhang, "Implementing smart factory of industrie 4.0: an outlook," in International Journal of Distributed Sensor Networks, 12(1), 3159805., 2016.
[10] W. Dargie and M. Zimmerling, "Wireless sensor networks in the context of developing countries," in In IFIP World IT Forum (WITFOR)., 2007.
[11] N. Jazdi, "Cyber physical systems in the context of Industry 4.0," in 2014 IEEE international conference on automation, quality and testing, robotics (pp. 1-4). IEEE., 2014.
[12] Y. Tan, S. Goddard and L. Perez, "A prototype architecture for cyber-physical systems," in ACM Sigbed Review, 5(1), p.26, 2008.
[13] S. Han, M. Xie, H. Chen and Y. Ling, "Intrusion detection in cyber-physical systems: Techniques and challenges," in IEEE systems journal, 8(4), pp.1052-1062, 2014.
[14] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," in IEEE Internet of Things Journal, 4(5), 1125-1142, 2017.
[15] Lo’ai, A.T., Mehmood, R., Benkhlifa, E. and Song, H. (2016) Mobile Cloud Compu- ting Model and Big Data Analysis for Healthcare Applications. IEEE Access, 4, 6171-6180. https://doi.org/10.1109/ACCESS.2016.2613278
[16] Kocher, P.C. (1996) Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. Proceedings of CRYPTO, Santa Barbara, August 1996, 104-113. https://doi.org/10.1007/3-540-68697-5_9
[17] T. Lu, J. Lin, L. Zhao, Y. Li and Y. Peng, "A Security Architecture in Cyber-Physical Systems. Security Theories, Analysis, Simulation and Application Fields," IJSIA (International Journal of Security and Its Applications) 9 (7), 2015.
[18] Raza S. Lightweight security solutions for the Internet of Things, Mälardalen University Press Dissertations, Mälardalen University, Västerås, Sweden, 2013.

[19] Wang EK, Ye Y, Xu X, Yiu SM, Hui LCK, Chow KP. Security issues and challenges for cyber physical system, Proc. IEEE/ACM Int'l Conf. Green Comput. Commun. Int'l Conf. Cyber, Phys. Soc. Comput., pp. 733–738, 2010.
[20] Peng Y, Lu T, Liu J, Gao Y, Guo X, Xie F. Cyber-physical system risk assessment, Ninth Int. Conf. Intell. Inf. Hiding Multimed. Signal Process., pp. 442–447, 2013.
[21] Lu T, Lin J, Zhao L, Li Y, Peng Y. A security architecture in cyber- physical systems: security theories, analysis, simulation and application fields. Int J Secur Appl 2015;9(7):1–16.
[22] Zhao K, Ge L. A survey on the Internet of Things security, Ninth Int. Conf. Comput. Intell. Secur., pp. 663–667, 2013.
[23] Shafi Q. Cyber physical systems security: a brief survey, Comput.Sci. Its Appl. (ICCSA), 12th Int. Conf. IEEE, pp. 146–150, 2012.
[24] Bhattacharya R. A comparative study of physical attacks on wireless sensor networks. Int J Res Eng Technol 2013;72–4.
[25] Alvaro C, Amin S, Sinopoli B, Giani A, Perrig A, Sastry S. Challenges for securing cyber physical systems. Work Futur Dir Cyber-Phys Syst Secur 2009;5.
[26] Mo Y, Sinopoli B. Integrity attacks on cyber-physical systems, Proc. 1st Int. Conf. High Confid. Networked Syst., pp. 47–54, 2012.
[27] Gaddam N, Kumar GSA, Somani AK. Securing physical processes against cyber attacks in cyber-physical systems, Natl. Work. Res. High-Confidence Transp. Cyber-Physical Syst. Automotive, Aviat. Rail, Washingt. DC, pp. 2–4, 2008.
[28] Suo H, Liu Z, Wan J, Zhou K. Security and privacy in mobile cloud computing, 9th Int. Wirel. Commun. Mob. Comput. Conf. (IWCMC), IEEE, pp. 655–659, 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY