Security and Privacy in CPS: Healthcare Perspective

Swapnil Naresh

Department of Computer Science, DIT University, Dehradun, India
E-mail: 1000013908@dit.edu.in

Abstract: The latest epidemic has necessitated the development of a powerful and intelligent healthcare system capable of effectively monitoring patients and managing the situation that occurs as a result of the illness's emergence. Healthcare Cyber-Physical Systems (HCPS) are sophisticated, connected systems used in healthcare facilities of healthcare equipment that may be used in a treatment center to deliver the best possible clinical treatment to patients. They blend psychological, cybernetic, and physical aspects as a result. Even though they are life-critical and context-aware, HCPSs are crucial to the healthcare industry, which is subject to data breaches and cyber-attacks. As a novel research area, HCPS has various challenges in terms of system dependability, confidence, independence and security, and confidentiality. Technologies like the Web of Things, Advanced Analytics, and Intelligent Systems have been used to construct integrated CPS including Integrated Healthcare Systems, Combined Vehicular Structures, and Consolidated Networks. These systems are multidisciplinary and rely on a variety of technologies to function properly. The characteristics, security problems, HCPS reliability, and security challenges in CPS, as well as HCPS, are discussed in this article.

Keywords: Cyber Security; Healthcare; Security and privacy; Cyber Physical System; Smart Health

Introduction

Healthcare stands for a service that involves a variety of stakeholders and players, including doctors, patients, hospitals, and medical research institutes. Its introduction has ushered in a revolution in the field of health; it has permitted a highly effective evolution for humanity's health, allowing us to combat a variety of diseases and deal with a variety of limits where even detection was previously impossible. In the healthcare industry, the usage of gadgets that stand alone to diagnose and patients to be treated is increasingly being phased away. It is quickly heading toward the use of complex systems that can track, evaluate, and manage several elements of a patient's health at the same time. To bring tremendous and more economical effective solutions to its patrons, the healthcare sector has employed modern information and communication technologies to computerized medical health record systems should be used to replace paper-based systems (Sztipanovits *et al.*, 2012). Computerized medical health records improve patient care by encouraging patient collaboration, improving illness diagnosis, increasing practice efficiency, and providing continual access to patient health information (Janett and Yeracaris, 2020). Healthcare data has become more electronic, dispersed, and adaptable in recent years. The m-health has also played a significant role in this regard. Healthcare organizations collect responsive. Information from their clients and keep it on network servers so that it is always available and may be used to help patients. However, every good thing has a bad side, and this is no exception. Cell phones and other smooth gadgets have also developed a significant cause of data breaches.

These systems are occasionally accessed by unauthorized people and are vulnerable to insider assaults as a result of software flaws, security flaws, and human error. As a result of data infractions, sensitive information is exposed. By inflicting harm to guarded health records, it leads to the lost, misuse, or breaches of confidentiality healthcare data [24]. According to numerous experts, the total number of persons impacted by healthcare data breaches from 2005 to 2020 was 249.09 million. In the previous five years alone, 157.40 million people have been affected (Seh *et al.*, 2020). Individuals and businesses alike are concerned about data privacy and confidentiality. Because tampering with healthcare data might result in ineffective treatment, it is more vulnerable than other forms of data, which could end in tragic and irreversible patient losses. As a result of this evolution, a better solution for health and management has been developed. Using Occupational health and safety solutions, data may be translated into the right information and knowledge about unobserved aspects of asset deterioration, as well as inaccuracy and inefficiency in operations (Dey *et al.*, 2018).

Data security is a critical requirement in healthcare since the primary focus is the well-being of patients. The likelihood of security threats and adversary assaults is substantially higher as the number of devices linked to the Internet in such systems grows. Furthermore, the obtained data is extremely sensitive because it contains the patients' personal information, making it subject to various forms of assault.

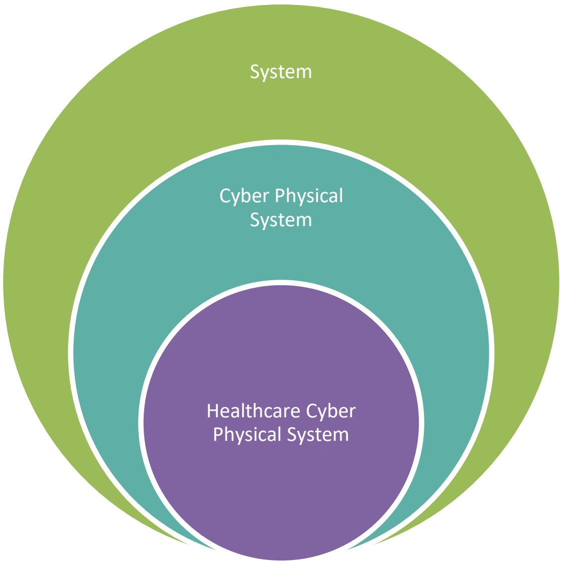

Figure 1: Mapping of Cyber-Physical System

To avoid significant packet delay in important applications, any security mechanism for wireless sensor systems employed in these systems should satisfy system criteria (i.e., energy efficiency, quick operation, low bandwidth consumption, and low memory utilization). Furthermore, data transfer extends well beyond local networks, necessitating the development of robust authentication and authorization methods (Chen, 2017).

Existing security solutions are frequently unable to meet the demands, necessitating additional research in this field. The major focus is on data security and privacy on existing approaches to acquire a deeper understanding of existing healthcare solutions and their security-related challenges. The HCPS, this research is focused on a sub-domain of CPS. HCPS refers to the network of healthcare devices (components) that work together to improve healthcare quality. HCPS are shown in this diagram, which comprises physical equipment and physical structure (Fig.1). The physical aspects of the system are brought together to form an overall system. The combined functionality and performance of these task-specific systems are about the sum of their parts (Lu, 2017). CPS is data management system that brings the physical and electronic worlds closer together. Sensors and actuators may make up the physical environment (Sridhar, Hahn and Govindarasu, 2012). Several CPS constituents work together to carry out some sort of global behavior. Sensors and actuators, software solutions, communication technologies and other components that interact with the physical are examples of these constituents. The HCPS, this research focuses on a sub-domain of CPS. The healthcare essential integration of a network of healthcare devices targeted at enhancing healthcare quality is referred to as HCPS (Haque, Aziz and Rahman, 2014).

Cyber-Physical System (CPS)

To establish proficient and operative systems for the excellence of service, CPS was created in response to the need for constant communication, control, and cooperation. The concept "Cyber-Physical System" was proposed by Helen Gill of the National Science Foundation in the United States in 2006. Sensors that act as data collectors collect data such as temperature, pressure, and transmission to the cyber world and storing in servers to connect the cyber and physical worlds, speed/activity time is required (Lu, 2017).

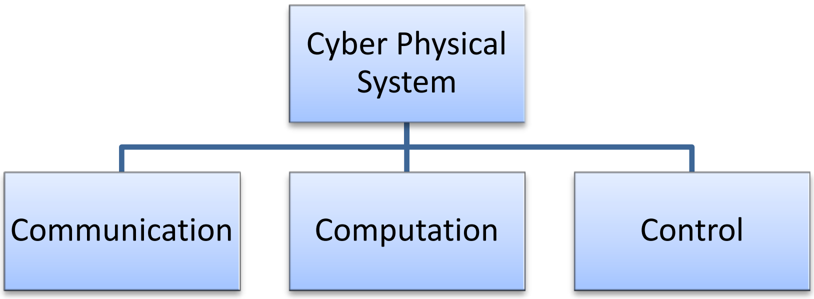

Figure 2: Capabilities of Cyber Physical System

Physical processes in any CPS will be governed and well-ordered by implanted processors and systems, with planned feedback mechanisms that connect to physical methods and effect computation and then provide information on how to control the physical processes in the future (Nadeem *et al.*, 2022). Transmission, processing, and control are all capabilities of a CPS (Fig. 2).

Physical and software components are closely linked in cyber-physical systems, allowing them to function on diverse spatial and temporal dimensions, display multiple and unique behavioural modalities, and engage with one another in context-dependent ways (Chandra, Agarwal and Shukla, 2020). CPS combines cybernetics, microelectronics, design, and process science in a Trans disciplinary approach. Embedded systems are a term used to describe process control (Lu, 2017). The emphasis of embedded systems tends to be on the computational parts, rather than a strong relationship between the computational and physical aspects (Pereira *et al.*, 2013).

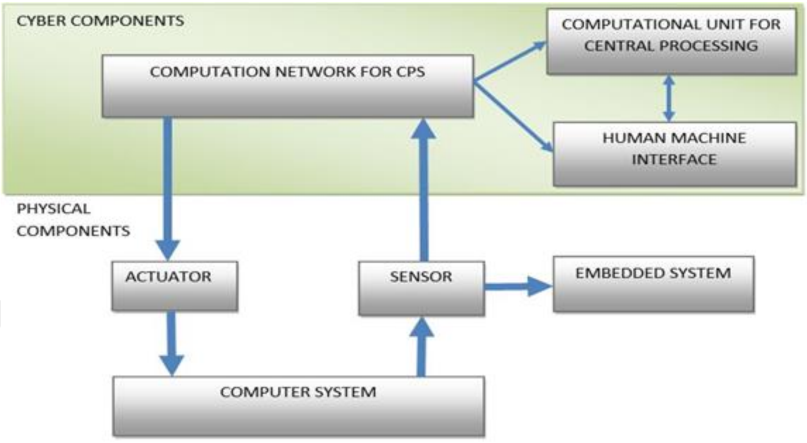

Figure 3: Component of CPS

In (Fig.3) shows that how the cyber component and physical component communicate with each other. Sensors and Actuators are used by the computer system to interact with the physical world in the illustration. These embedded systems are no longer stand-alone; they instead exchange their data over communication networks such as the internet, where data from several embedded systems may be gathered and analysed using cloud computing. As a result, a system of systems is created. A computational unit can control and decentralize connected embedded systems. The information gathered can be processed manually or using a Human Machine Interface (HMI). Sensor networks and embedded computers are commonly used in CPS to monitor and regulate the physical environment, with feedback loops that allow this external stimulus to self-activate transmission, operate, or computing (Wang *et al.*, 2010).

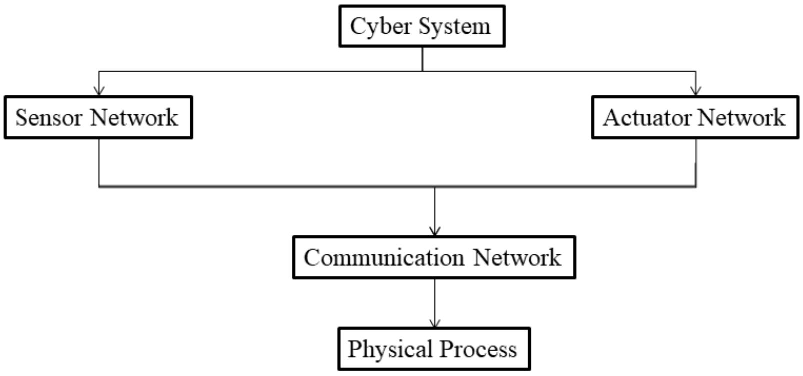

Figure 4: structure of CPS

The physical systems are added to generate a multi-system overarching system. These specialized task-oriented systems are greater than the sum of their parts in terms of capability and efficiency (Chandra, Agarwal and Shukla, 2019). CPSs are data processing systems that bridge the chasm that exists between the real and virtual worlds. Sensors and actuators may make up the physical environment. Several CPS constituents work together to carry out some class of universal comportment. Software systems are among the elements, wireless communications, instruments and actuators, and other elements that connect through the actual world (Ansar *et al.*, 2020a). Due to the huge quantity of devices involved, communication and management are binary key jobs for any CPS (Canedo, Schwarzenbach and Al Faruque, 2013). Physical components, human interfaces, and cyberspace systems make up CPS (Fig. 4). The physical world's components ensure that linked technology is monitored and maintained. As calculating devices have emerged as light weight, transportable, and able to be linked with the factual international, CPS additives can be interrelated thru the Internet by the proficiency of gadget observing and supervisory with the right process and instantaneous reaction (Majumdar, Saha and Zamani, 2011). CPS offers a coupled atmosphere that incorporates the inter connectivity of hundreds of gadgets, offering extra comfort in supervision and control.

CPS architecture

The CPS is the combination of figuring, verbal exchange, and manipulating competencies that reveal and control the substances within the bodily global. The bodily techniques are managed and observed by virtual systems, which can be systems with feedback loops (Ansar *et al.*, 2020b). There is global consensus on the definition of CPS, but there is no consensus on the vital elements of the CPS and its communiqué fashions. The CPS building usually stated essential layers of the physical and cyber. The corporal layer takes identified records and plays the commands of cyber layers, while the cyber layer explore and techniques the corporeal layer records and reveals the right instructions as a consequence. The CPS operates at 3 layers: perception, transmission, and application (Zhang *et al.*, 2013).

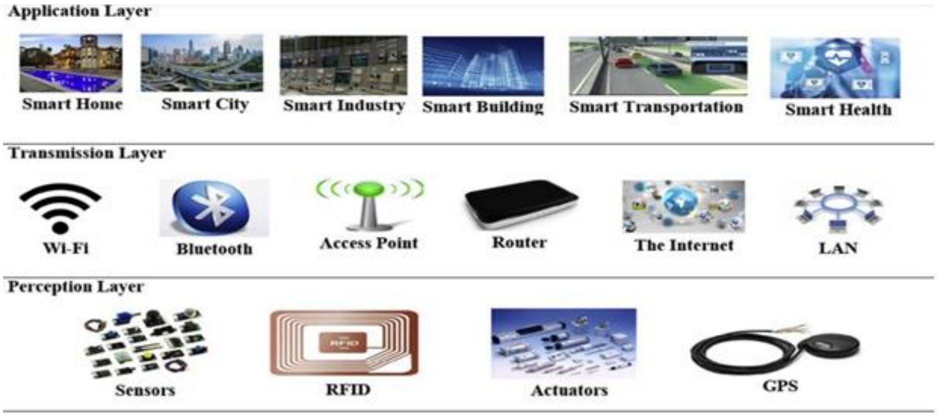

Figure 5: layers of Cyber Physical System

In (Fig.5), each of those layers is described with the aid of the gadgets inside it and the associated features that have to be applied perception on physical, information transmission on network, and alertness on cyber layer. The 1st layer represented as notion layer, additionally known as the popularity layer or sensors layer. This layer has a couple of terminal equipment which includes laser scanners, actuators, Global Position Systems (GPSs), sensors, cameras, clever gadgets, RFID tags with 2-D bar cipher readers. Devices at this residue can collect real-time records that are wished for distinctive functions, construe what they acquire from the bodily international and accomplish instructions from the utility level (Alharbi *et al.*, 2021). The accumulated information can consist of chemistry, light, mechanics, sound, warmth, power, biology, or vicinity. Sensors can work with nodes to generate real-time data in distant and near network domains, allowing data to be aggregated and analysed at application level. The 2nd level is the transmission layer additionally called the shipping level or network layer, that's accountable for switching and handling information among the notion and the utility. The collaboration and broadcasting of information at this layer varies depending on the sensors, using many technologies such as short-range networks, the Internet, or 4G, and 5G, UMTS, Wi-Fi, Bluetooth, Electromagnetic, and ZigBee, gadgets it is done over the current network. Although, most connections are made over the Internet for a variety of reason, including availability and cost-effective. In this way, you need to support the actual operation on your network. As it's far crucial to control and manner large facts, the transmission layer can start with procedure and manipulate a widespread amount of facts and recognize real-time transmission with obligation for reliable verbal exchange aid. Many protocols and capabilities may be determined at this accretion to address an increased quantity of items together with Internet Protocol version 6 (IPv6). Furthermore, the function of this deposit consists of information steering and broadcasting via numerous procedures and hubs over the used systems. Cloud calculating systems, steering gadgets, exchanging, and web Gateways paintings as nicely at this level use technologies along with ZigBee, 4G/5G, Bluetooth, Wi-Fi, LTE. The network gateway works for the connector factors of different nodes to collect, filter, receive and transmit facts from some and different layers of CPS (Ferrag *et al.*, 2022). The improved quantity of linked devices poses some other problems in CPS that as site visitors and garage. This affects safety within the CPS. Although these site visitors can be controlled by way of protocols consisting of firewalls, the security limited features gadgets are not guaranteed due to their very limited computing abilities and storage capacity. The largest interactive layer at 0.33 is the request layer. Its task is to calculate the recorded statistics from the degree of broadcasting of the record and issue orders to be implemented via actuators and sensors. This layer mechanism (via imposing multifaceted choice-making algorithms) is at the amassed information to produce accurate selections and manipulate instructions to be utilized in corrective moves (Lu, 2017). Thus, this layer gets and approaches facts from the belief layer to determine what desired automated moves are being called. Aggregation of data from unique sources and wise processing of large information is achieved with this aggregation using object manipulation and control. Cloud figuring, middleware, and records excavating procedures can also be utilized to implement at the physical layer of connected devices (Derler *et al.*, 2013). The system is also monitored at this layer, whose role is to monitor the performance of physical strategies and problem commands, replace the performance of physical policies, and ensure that the working atmosphere is functioning properly and optimally. The request layer also saves beyond movements, providing feedback on previous actions and ensuring that fortune operations are improved. The goal of this residue is to ensure a clever environment and imposed CPS with industry-specific applications. This has brought about vast and clever applications in areas that could consist of non-public and secure statistics, which include: Smart Control Grid; Nifty Homes and Towns; Intellectual Conveyance; Smart Auto; environmental tracking; industry control, Smart Fitness; and Smart Agricultural. Such programs may accumulate customers' non-public records, which include fitness information and behaviours. Therefore, it is essential to use apparatuses to defend the information (Zhang *et al.*, 2013).

Healthcare Cyber Physical System (HCPS)

Communication, computation, and monitoring are all capabilities of a Cyber-Physical System. Any CPS's major purpose is towards link automation and sensor systems to data collected from additional CPS elements, all of which are then processed using computational expertise to get a conclusion. As a result, they serve as the foundation for HCPS, Including physical and computational characteristics that allow for human contact. The HCPS, like the CPS, combines physical operations with applications and system administration to generate feedback systems as a single entity. These devices are used in a variety of industries, including energy, infrastructure, manufacturing, military, robotics, and transportation (Derler *et al.*, 2013). As a result, CPSs must have variety, independence, competency, utility, unwavering quality, security, and ease of use (Khurana, 2022).

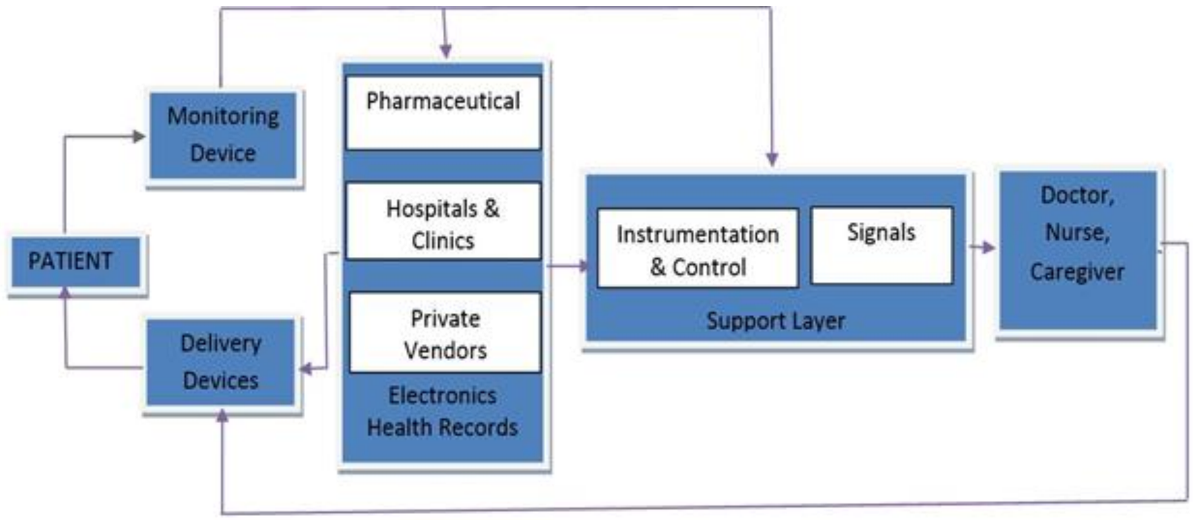

Figure 6: Network in Healthcare CPS

Patient data is handled by a range of medical equipment in the health care cyber-physical system, which is increasingly linked and communicated via the internet (Fig.6). It is critical to maintaining appropriate communication scheduling between interoperating therapeutic equipment such as help minimize the load on patients in terms of general health expenses (Huq, 2000) (Sahu *et al.*, 2021).

Reliability of Healthcare Cyber-Physical System

For virtual-physical systems, notably in the healthcare industry, reliability is an important element (Ansar, Alka and Khan, 2018). System components such as medical sensors and devices, software dependability in software applications that evaluate the patient's health state, and availability in network technologies that transport patient records define the reliability of healthcare cyber-physical systems (Fig.8) (Yang and Xie, 2000).

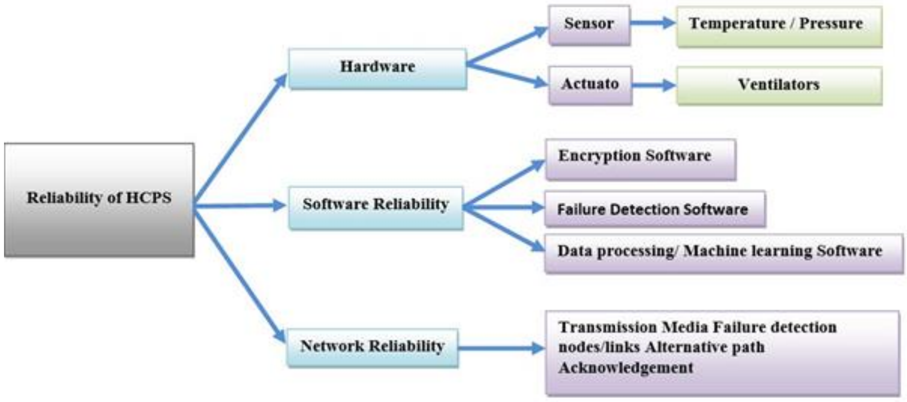

Figure 8: Reliability of Healthcare CPS

For efficient, dependable, and better services, the emergence of cyber-physical systems necessitates resource optimization and a self-adaptive behavior (Canedo, Schwarzenbach and Al Faruque, 2013). In a closed-loop system, an autonomous system must be able to recognize failures of multiple elements and correct them in terms of job execution. Cyber-physical systems' self-adaptive components learn from previous data and change their behavior to the present situation. Healthcare robots, for example, can self-organize in a vibrant setting to tackle the problem of overhaul value.

Solution and Opportunities towards HPCS

Getting a Virtual Private Network (VPN) is one of the most contemporary ways to combat HCPS threats (VPN). To enable secure communications across an open physical network, VPN virtualizes a private network and applies sophisticated security mechanisms. A virtual private network (VPN) is a service that may be used instead of a private network or a private leased line. The EDADT algorithm, the dual IDS model, the semi-supervised method, and the evolving HOPERAA Algorithm (Ong *et al.*, 2020) are examples of new methodologies, have been projected to discourse the challenge of the Intrusion Detection System (IDS). In addition, a new method (Ajagekar and You, 2019) for identifying normal behavioural patterns for each given medical device or machine is based on behavioural rule subtleties and complexities. They can test medical sensor data and actuator settings to find out if physical qualities are malfunctioning as a result of attacks.

Healthcare Cyber-Physical System Opportunities: The fact that CPS is still in its early stages of development in the medical industry makes it one of the most important venues for generating and innovative ideas in this field. The multidisciplinary method, which combines robotics, artificial intelligence (AI), and medical knowledge, improves precision and accuracy rates while also enhancing CPS efficiency. Future research in CPS could include things like achieving dependability through specialized Portable agents, gateways, and segment reasoning for performance improvement and flexibility through the usage of the aspect-oriented instruction set. Furthermore, the majority of the research difficulties are mostly unaddressed, and we feel that further research in these areas can provide an extra level of security to the respective CPS/ HCPS.

Conclusion

The epidemic has offered us a valuable lesson that health services are a nation's capillaries, and that an effective and efficient HCPS creates an atmosphere that combines the virtual and real worlds, New devices, Internet, cloud solutions, AI, deep learning, and advanced data analytics are all linked by a closed - loop system and guided by a variety of technologies, all of these factors contribute to the smooth running of the system. There are various challenges to working and executing in a physical environment regulated by cyberspace, such as the variety of physical elements, inconsistent data formats transmitted between elements, resource limits, and device vulnerability to attacks. Aside from digital concerns, waste management is also a major physical challenge. The expanding usage of HCPS technology in the healthcare business was examined in this study, which included a broad overview of HCPS, categorization, benefits, obstacles, and security considerations, as well as the reliability of the Healthcare Cyber-Physical System to create a reliable and secure Health Care Cyber-Physical System.

References

Ajagekar, A. and You, F. (2019) ‘Quantum computing for energy systems optimization: Challenges and opportunities’, *Energy*, 179, pp. 76–89. doi: https://doi.org/10.1016/j.energy.2019.04.186.

Alharbi, A. *et al.* (2021) ‘Managing Software Security Risks through an Integrated Computational Method’, *Intelligent Automation & Soft Computing*, 28(1), p. 179. doi: 10.32604/IASC.2021.016646.

Ansar, S. A. *et al.* (2020a) ‘Enhancement of Two-Tier ATM Security Mechanism: Towards Providing a Real-Time Solution for Network Issues’, *International Journal of Advanced Computer Science and Applications*, 11(7), pp. 123–130. doi: 10.14569/IJACSA.2020.0110717.

Ansar, S. A. *et al.* (2020b) ‘Enhancement of Two-Tier ATM Security Mechanism: Towards Providing a Real-Time Solution for Network Issues’, *undefined*, 11(7), pp. 123–130. doi: 10.14569/IJACSA.2020.0110717.

Ansar, S. A., Alka and Khan, R. A. (2018) ‘A phase-wise review of software security metrics’, *Lecture Notes on Data Engineering and Communications Technologies*, 4, pp. 15–25. doi: 10.1007/978-981-10-4600-1_2/COVER.

Canedo, A., Schwarzenbach, E. and Al Faruque, M. A. (2013) ‘Context-sensitive synthesis of executable functional models of cyber-physical systems’, *Proceedings of the ACM/IEEE 4th International Conference on Cyber-Physical Systems, ICCPS 2013*, pp. 99–108. doi: 10.1145/2502524.2502539.

Chandra, P., Agarwal, D. and Shukla, P. K. (2019) ‘Mobi-class: A fuzzy knowledge-based system for mobile handset classification’, *Advances in Intelligent Systems and Computing*, 817, pp. 979–987. doi: 10.1007/978-981-13-1595-4_77/COVER.

Chandra, P., Agarwal, D. and Shukla, P. K. (2020) ‘A review on the interval type-2 fuzzy systems’, *International Journal of Intelligent Systems Design and Computing*, 3(2), p. 117. doi: 10.1504/IJISDC.2020.115168.

Chen, H. (2017) ‘Applications of Cyber-Physical System: A Literature Review’, *https://doi.org/10.1142/S2424862217500129*, 02(03), p. 1750012. doi: 10.1142/S2424862217500129.

Derler, P. *et al.* (2013) ‘Cyber-physical system design contracts’, *Proceedings of the ACM/IEEE 4th International Conference on Cyber-Physical Systems, ICCPS 2013*, pp. 109–118. doi: 10.1145/2502524.2502540.

Dey, N. *et al.* (2018) ‘Medical cyber-physical systems: A survey’, *Journal of Medical Systems*, 42(4), pp. 1–13. doi: 10.1007/S10916-018-0921-X/FIGURES/4.

Ferrag, A. *et al.* (2022) ‘A Systematic Review of Radio Frequency Threats in IoMT’, *Journal of Sensor and Actuator Networks 2022, Vol. 11, Page 62*, 11(4), p. 62. doi: 10.3390/JSAN11040062.

Haque, S. A., Aziz, S. M. and Rahman, M. (2014) ‘Review of Cyber-Physical System in Healthcare’, *http://dx.doi.org/10.1155/2014/217415*, 2014. doi: 10.1155/2014/217415.

Huq, F. (2000) ‘Testing in the software development life-cycle: now or later’, *International Journal of Project Management*, 18(4), pp. 243–250. doi: 10.1016/S0263-7863(99)00024-1.

Janett, R. S. and Yeracaris, P. P. (2020) ‘Electronic Medical Records in the American Health System: challenges and lessons learned’, *Ciência & Saúde Coletiva*, 25(4), pp. 1293–1304. doi: 10.1590/1413-81232020254.28922019.

Khurana, M. (2022) ‘Secure Coding and Software Vulnerabilities in Implementation Phase of Software Development’, *ECS Transactions*, 107(1), pp. 7037–7045. doi: 10.1149/10701.7037ECST/XML.

Lu, Y. (2017) 'Cyber Physical System (CPS)-Based Industry 4.0: A Survey', *https://doi.org/10.1142/S2424862217500142*, 02(03), p. 1750014. doi: 10.1142/S2424862217500142.

Majumdar, R., Saha, I. and Zamani, M. (2011) 'Performance-aware scheduler synthesis for control systems', *Embedded Systems Week 2011, ESWEEK 2011 - Proceedings of the 9th ACM International Conference on Embedded Software, EMSOFT'11*, pp. 299–308. doi: 10.1145/2038642.2038689.

Nadeem, M. *et al.* (2022) 'Multi-level hesitant fuzzy based model for usable-security assessment', *Intelligent Automation and Soft Computing*, 31(1). doi: 10.32604/IASC.2022.019624.

Ong, L. M. T. *et al.* (2020) 'Cyber physical system: Achievements and challenges', *ACM International Conference Proceeding Series*, pp. 129–133. doi: 10.1145/3380688.3380695.

Pereira, E. *et al.* (2013) 'Bigactors - A model for structure-aware computation', *2013 ACM/IEEE International Conference on Cyber-Physical Systems, ICCPS 2013*, pp. 199–208. doi: 10.1109/ICCPS.2013.6604014.

Sahu, K. *et al.* (2021) 'Evaluating the Impact of Prediction Techniques: Software Reliability Perspective', *Computers, Materials & Continua*, 67(2), p. 1471. doi: 10.32604/CMC.2021.014868.

Seh, A. H. *et al.* (2020) 'Healthcare Data Breaches: Insights and Implications', *Healthcare*, 8(2). doi: 10.3390/HEALTHCARE8020133.

Sridhar, S., Hahn, A. and Govindarasu, M. (2012) 'Cyber-physical system security for the electric power grid', *Proceedings of the IEEE*, 100(1), pp. 210–224. doi: 10.1109/JPROC.2011.2165269.

Sztipanovits, J. *et al.* (2012) 'Toward a science of cyber-physical system integration', *Proceedings of the IEEE*, 100(1), pp. 29–44. doi: 10.1109/JPROC.2011.2161529.

Wang, E. K. *et al.* (2010) 'Security issues and challenges for cyber physical system', *Proceedings - 2010 IEEE/ACM International Conference on Green Computing and Communications, GreenCom 2010, 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing, CPSCom 2010*, pp. 733–738. doi: 10.1109/GREENCOM-CPSCOM.2010.36.

Yang, B. and Xie, M. (2000) 'A study of operational and testing reliability in software reliability analysis', *Reliability Engineering & System Safety*, 70(3), pp. 323–329. doi: 10.1016/S0951-8320(00)00069-7.

Zhang, Z. *et al.* (2013) 'Co-simulation framework for design of time-triggered cyber physical systems', *Proceedings of the ACM/IEEE 4th International Conference on Cyber-Physical Systems, ICCPS 2013*, pp. 119–128. doi: 10.1145/2502524.2502541.