Chapter 5
Security Issues and Privacy Challenges of Cyber-Physical System in Smart Healthcare Applications

Soumya Samarpita, Ritunsa Mishra, Rabinarayan Satpathy, and Bibudhendu Pati

5.1 Introduction

One of the most significant research fields for technology developers and designers is emerging as the healthcare sector. More security is being included into networks by researchers for data and communication. Any one alteration in a patient's data could have drastic effects on the patient's life. Researchers are motivated to examine different security solutions including multi-layered data cryptography, cryptosystem, and other techniques because of cyber-attacks on medical data. Medical device development has changed quickly as a result of advances in embedded network and software connectivity. The use of standalone devices to independently track and manage patients is being phased out in the healthcare sector. Therapeutic healthcare appliance systems, also known as Healthcare Cyber-Physical Systems (HCPS), are created by the combination of embedded technology monitoring devices, networking capabilities of healthcare equipment, and the complicated physical features shown by patients' bodies (Priyadarshini et al. 2021). IoT also has many uses in the healthcare sector, including remote healthcare monitoring, hardware accessibility and availability, patient inventory tracking, and utilization of health services.

S. Samarpita
FOS, Sri Sri University, Cuttack, Odisha, India

R. Mishra (✉)
FET, Sri Sri University, Cuttack, Odisha, India
e-mail: ritunsa.m@srisriuniversity.edu.in

R. Satpathy
FET, FOS, Sri Sri Univeristy, Cuttack, Odisha, India

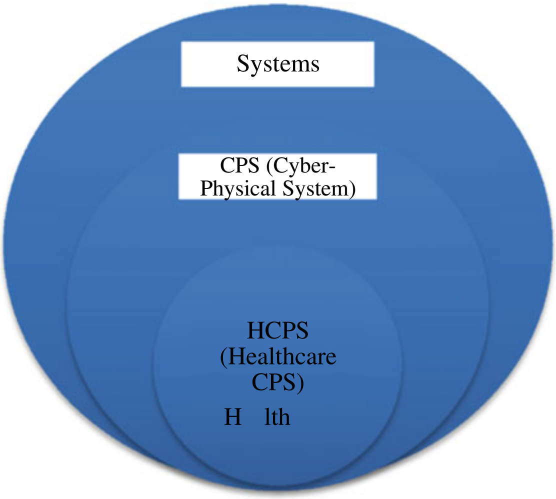
B. Pati
Department of CS, Rama Devi Women's University, Bhubaneswar, Odisha, India

N. Sharma et al. (eds.), *Big Data Analytics in Intelligent IoT and Cyber-Physical Systems*, Transactions on Computer Systems and Networks,
https://doi.org/10.1007/978-981-99-4518-4_5

The idea of a smart factory is based on artificial intelligence (AI) and the IoT, and it results from industrial automation. Examples of industrial automation and CPSs include adaptive supply chain management, human–robot interaction, production quality, and predictive maintenance (Latif et al. 2022). A creative span known as Industry 4.0 that introduces CPSs has been brought about by the necessity for consistent communication, management, and coordination for streamlined and efficient systems for quality of service. Helen Gill of the NSF in the US first used the term CPS in 2006 (Verma, 2022).The latest technology providing cyber security for physical systems and processes is known as the CPS, or cyber system merged with physical phenomena (Kurde et al. 2019). A cyber physical system is a system that combines different physical components with computational components and operations. CPS is also referred to as the Industry Internet, Embedded Systems, and the Internet of Everything. Although cyber physical systems have long existed, a new intellectual system has emerged in recent years. As we cannot simply link physical processes and cyber computer components directly, CPS design and incorporation must be restricted.

The terms healthcare and medicine refer to the problems defining various physiologic elements of the patient. Since they present important research opportunities for the CPS community, medical applications in CPS research are given particular attention (Gunes et al. 2014). Systems known as "CPS" link the real environment with the digital world of cognitive processing. It's possible that sensors and actuators make up the physical universe. The HCPS is the network of healthcare systems brought together to achieve high-quality healthcare. An overview of HCPS, which includes physical systems and devices, is shown by Fig. 5.1. An overarching system of various physical systems is created by combining the physical systems.

Fig. 5.1 The mapping procedure



CPS is a novel method for examining digital systems. Actually, CPS is the latest era of digital systems, focusing primarily on complex interdependencies and interconnections between cyberspace and physical reality (Jamal et al. 2021). With regard to communications, computational resources, sensors, and physical aspects, CPS takes an integrated perspective. In such a scenario, cyberattacks might put underlying systems in danger. Conventional approaches to CPS security design looked at the cyber and physical systems separately and were unable to define network-related risks. Big Data analytics can aid in the government's ability to provide its residents with improved services. Big Data can help governments enhance vital industries like healthcare and public transportation, thereby assisting in the creation of a more effective modern society. Big Data analytics and techniques of machine learning, for instance, can offer inventive solutions for complex issues like health stress prediction or improvement of the transportation services provided by the government to the general public (Iqbal et al. 2020).

5.1.1 Cyber-Physical System (CPS)

Primarily CPS is an intelligent system that is related to computer intelligence which may accommodate some enhanced applications than human intelligence. The basic structure of CPS may include design, modelling, and simulation of information. CPSs' are physical assets or manual systems with a computing and interaction centre that manage, synchronize, merge, and give commands to the operations of the said system (Cabello et al. 2020). CPS implemented in different sectors i.e. Economical, Industrial, and in healthcare units as well to control and monitor networks, clients, patients, and system. CPS can be characterized as systems that involve computational things that are in close contact with the physical environment and its ongoing activities while simultaneously providing and utilizing services for data access and processing (Liu & Wang, 2020).

CPS involves different emerging technologies for the future trends such as: big data architecture, IoT, Machine Learning, human machine communication as well as machine to machine communication (Mishra et al. 2022). Water, smart grid systems, transport, gas, energy, and healthcare, which are critical infrastructure, depend on CPS. These systems contain IoT devices, which produce enormous amounts of data and transfer that data to a centralized server. The qualities of blockchain, including as decentralization, data integrity, decentralized trust, enhanced security, cryptographic protocols, cryptocurrency, quicker settlements, and minting, can all be used to address various CPS concerns (Khalil et al. 2022).

Now a days our day to day life is transformed over internet revolutionization and semi conduction for the interaction and which may lead to the growth of information technology. HCPSs' are used in various fields to enable process optimization and some enhanced functionality (Rho et al. 2016). Neither cyber security nor physical security can save CPS because the vulnerability can never be introduced by removing patient variation and allow the responses with subject to one treatment (Fink et al.

2017). CPSs' are named as the cyber network system that include communication, computation, and cyber physical system itself considered the actuators and sensors (Ashibani & Mahmoud, 2017).

This chapter has the following structure: By using an illustration, Sect. 2 explores the concepts of SHCPS. The characteristics of HCPS are illustrated in Sect. 3. Modern HCPS technologies are provided in Sect. 4. In Sect. 5, we discuss the challenges of HCPS. Security mechanisms are elaborated in Sect. 6, and in Sect. 7, we draw a conclusion.

5.2 Smart Healthcare Cyber-Physical System (SHCPS)

CPSs are created as integrated systems that incorporate physical, networking, and computing processes. This provides convenient interaction between physical objects and cyber services. A CPS is a tool that uses computer-based algorithms to monitor and manage a system (AlZubi et al. 2021). A contemporary context-aware network for healthcare Cloud storage, IoT technology, and integrated devices are all included in CPS. The healthcare system was changed into a class of CPSs known as HCPS thanks to the integration of integrated medical equipment, networking capabilities, and complicated physical dynamics.

The health sector has advanced significantly recently as a result of the rise of modern technologies. HCPS is an expeditious emerging field, which may reach every characteristics of life from now on. A crucial part in this is played by the SHCPS. It is made up of numerous healthcare gadgets that are connected via a network to ensure flawless operation. Doctors have easy access to the patient's electronic health record (EHR) after it is collected and stored on the cloud. Cyberattack awareness has always been high in the healthcare sector. In the healthcare field, it is essential for systems to be dependable, secure, and cost-effectively store and share patient and institution-specific data. In CPS, the combination of passive and active user input, such as sensing devices and/or smart devices in healthcare facilities, can enable the data collection for effective decision-making (Haque et al. 2014). This combination of data collection and a decision-making system has not yet been thoroughly investigated in healthcare applications, hence it is a topic of great research interest. The emergence of synchronized interoperation of self-governing and adaptive devices, set trends for directing and functioning healthcare systems using computation and regulation, miniature implantable smart devices, body area networks, programmable equipment, and novel fabrication techniques are, for instance, opportunities for using CPS in healthcare.

A SHCPS is a special CPS that combines the complicated physical dynamics of patients in the modern medical field with networking capabilities and application security control devices. HCPS's data are created digitally, maintained electronically, and used remotely by healthcare professionals or patients as part of the communication, gadget, and communications system interaction of the HCPS, which is shown in Fig. 5.2.

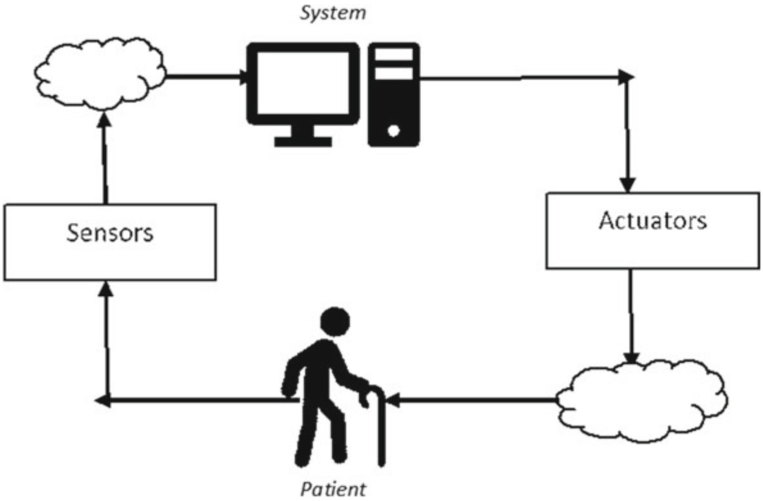


Fig. 5.2 CPS in smart healthcare

With the use of visualization techniques, the CPS, which is made up of sensors and actuators, assists humans in the majority of their daily activities. Pacemakers for humans and robot-controlled medical procedures are among the functions (Krishna et al. 2021).

As a result, HCPS emerges as an unstoppable force that have a significant impact on the medical industry, particularly in light of the development of the market for medical devices that uses integrated software and networking interface. With the development of medical technology, it became intriguing to integrate devices using cloud applications that simultaneously analyse the patient's various physiological features in place of equipment that were created to treat patients independently of one another (Dey et al. 2018).

5.3 Characteristics of Healthcare Cyber-Physical System (HCPS)

Future systems called SHCPS will help the medical community effectively manage pandemic situations. The integration of technologies, organizational domains, life cycles, and "smartness" are characteristics of CPSs. The following characteristics—technical specialization, cross-cutting elements, degree of automation, and life-cycle integration—can be used to describe CPS. CPS in healthcare offers a variety of applications, including care for the elderly, assisted living, and hospitals. The particular application has a big impact on the system complexity. Depending on the relevant area, certain organization of architectural elements may be required. Architecture may have managed aspects in a controlled environment, like an intensive care unit in a medical. Contrarily, it can be necessary to incorporate several automated features in the architecture of an assisted living facility. The two categories of CPS in healthcare applications are controlled and aided (Haque et al. 2014).

HCPS can be categorized at different levels (Verma, 2022). These are as follows.

(a) Unit Level: −Patient monitoring and control are provided by fundamental cyber-physical healthcare systems at the hospital or unit level for patients who are hospitalized. It continuously keeps track of the patients' physiological parameters, including their pulse, hypertension, respiratory rate, etc.
(b) Integration Level: −It is the second level of HCPS. At this level, hospitals connect with smart homes to offer patients remote controlling and medical services.
(c) System Level: −Third level of HCPS is the system level. A Smart City HCPS is formed at this level by a variety of automated systems that assist the HCPS.
(d) Acceptance Level: −Researchers, technicians, engineers, and health professionals collaborate at this level to execute the health sector and make the healthcare system effective.
(e) Evolutionary Level: −Future HCPS systems that have the characteristics of autonomy and personality are evolutionary level HCPS systems.

5.4 Modern HCPS Technologies

HCPS integrates a network of medical equipment, which is essential to healthcare. Hospitals employ these systems more and more to provide consistent, high-quality healthcare. The healthcare network's verification and validation of various devices, followed by encrypted transmission, is an essential component since it validates the credentials of the users (Adil et al. 2022).

The involvement of numerous technologies, including IOT, robotics, artificial intelligence, machine learning, blockchain, cloud computing, and big data in the field of HCPSs is presented in this section. This is illustrated in Fig. 5.3.

5.4.1 Internet of Things (IoT)

The IOT ushered in a novel age of machine-to-machine (M2M) communication, that can be done via Bluetooth, wireless networks, Near Field Transmission, radio communication, and other technologies (Aceto et al. 2019). The IoT enables smart, cyber-physical healthcare systems at the integration level where sensor networks produce large volumes of data that are then sent to distant computers for control and monitoring functions. There are some gadgets linked to mobile devices, which transmit data to cloud servers for healthcare (Verma, 2022).

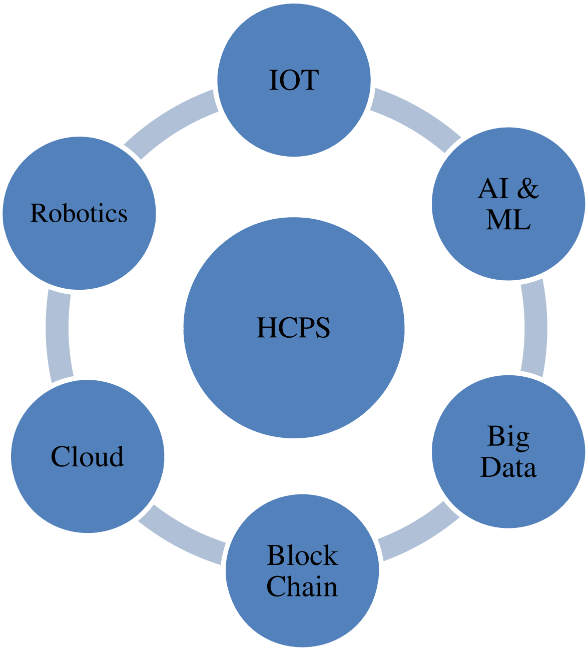


Fig. 5.3 Technologies of HCPS

5.4.2 *Artificial Intelligence & Machine Learning (AI & ML)*

A variety of areas of healthcare, such as medications, healthcare implants, patients, and diseases, can be improved by AI & ML (Verma 2022). ML-based solutions are used to offer different treatment options, personalize therapies, increase the general effectiveness of hospitals and healthcare systems, and reduce overall healthcare costs. (Pourhomayoun & Shakibi, 2021). Symptoms, pre-health condition, and demographic elements that crucially affect the disease activity of different patients.

5.4.3 *Big Data Analysis*

Healthcare CPSs can now discover hidden samples and linkages in massive amounts of information that have been obtained from multiple sources using latest computing paradigms with excessive processing power and big data technology (Verma 2022). High-end computer tools and deep learning models make it possible to analyze huge datasets and find these obscure patterns. Deep learning, machine learning, and statistical methods can be used to reveal these underlying patterns.

5.4.4 Blockchain

Blockchain technology has been investigated for use in a range of applications, including smart cities, smart agriculture, and smart healthcare. Different approaches have been suggested to deal with the difficulties and issues, whether they relate to contract tracing records, medical data coming from the Internet of Medical Things (IoMT), mobile gadgets, or any other smart device. Electronic health records (EHR) kept on cloud servers may be accessed securely and authentically, thanks to blockchain technology, which offers a decentralized distributed database (Xu et al. 2019).

5.4.5 Cloud Computing

Combining and storing IoMT data for analysis and processing is its main goal. Users and cloud servers are authenticated to IoMT devices utilizing OTP validation techniques and user-id or password generation (Vangipuram et al. 2021). The difficult problem is ensuring the confidentiality depending on the security environment of patient healthcare records used to protect the key generation center, which keeps the secret keys of all genuine users (Xu et al. 2019).

5.4.6 Robotics

CPSs use robots extensively, including robotic surgery to aid with operations and patient care, industrial robots to carry out production activities, and monitoring robots to ensure safety and protection. Robots like Moxi carry out a variety of tasks during pandemics (Verma 2022), including distributing PPE kits, carrying out COVID 19 tests, and picking up and dropping off patients. By taking patients' temperatures and facilitating video conferences between patients and their loved ones, the robot Mitra supports medical staff.

5.5 Challenges in HCPS

Potential issues are linked to various systems, including CPS connected to healthcare and IoT, embedded software and green crypto, smart building safety, privacy concerns in CPS, confidence and protection in CPS, emerging security schemes for embedded security, sensitive information handling in CPS, and other unresolved issues brought on by the diversity of technologies used in IoT integrated CPS (Jamal et al. 2021). Healthcare cyber physical system (HCPS) is the combination of a network of critical

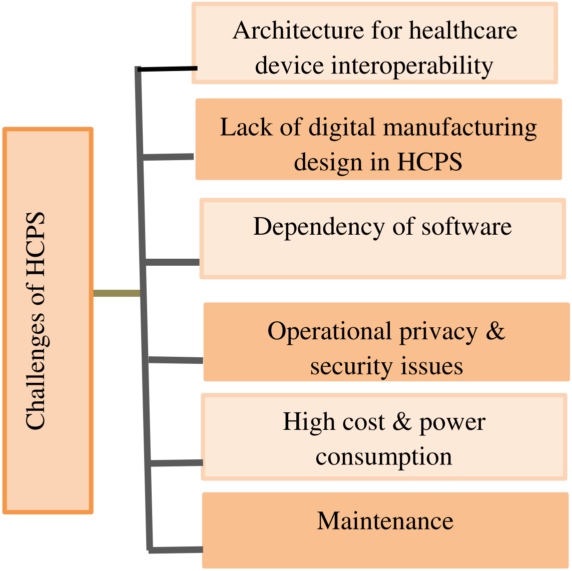

Challenges of HCPS
Architecture for healthcare device interoperability
Lack of digital manufacturing design in HCPS
Dependency of software
Operational privacy & security issues
High cost & power consumption
Maintenance

Fig. 5.4 Challenges of HCPS

medical gadgets. These systems are progressively used in different healthcare sectors to achieve very high quality outcomes by adding more intelligence and providing an ability to process major factors for CPS application. Here some issues and challenges described below which may provide some better opportunities to the healthcare world.

Designing a cost-effective healthcare system is a challenge. The goal of CPS research in this field is to create a smart sensing system that can control health, anticipate a patient's future condition, provide treatments depending on that patient's condition, provide virtual healthcare, use semi-automated robots to help patients with physical activities, and more (Kurde et al. 2019). Different challenges of HCPS are represented in Fig. 5.4.

5.5.1 Architecture for Healthcare Device Interoperability

Recently this distributed HCPS are built by integrating different inter-device communication protocols along with healthcare professionals. CPS faces so many limitations of the computational complexity and physical dynamics such as time and cost management, system and process integration, correctness of data, and structural standards (Giansanti 2021). The architecture of HCPS is highly dominant for the performance and feature of the system. The basic model of HCPS needs to be developed based on the concern of the application and integration of the system, and required information for the user. The HCPS based architecture for healthcare can be derived from the point of infrastructures such as server based architecture which is small and maintained individually. Another one is about the cloud based model which may use in recent works for scalability and easy accessibility.

5.5.2 Lack of Digital Manufacturing Design in HCPS

Now-a-days different healthcare sectors focus on different cyber security applications for their data confidentiality and manage information. The healthcare application needs to pay particular attention for some healthcare networks, communication system, user interaction system, pictorial archiving, and some wearable healthcare tools & devices (Giansanti 2021). In digital designing model this may go through several digital applications like digital health records, digital work station, image uploading, downloading and editing etc. As we know in today's world cyber risks are increasing rapidly due to this increasing digital technologies. We need to focus on this.

5.5.3 Dependency of Software

Dependency consists of two other factors namely safety and reliability which ensures the rights of Quality of Services (QoS). Dependency of a software mainly involves digital affliction, cyber vulnerabilities, consequences' & professional repercussion, digital security and digital everything. To understand the dependency of software regarding data collection and assessment, the network security may go through several steps like: IT software and hardware, level of deployment, risk assessment and establish many strategies (Tong 2022).

5.5.4 Operational Privacy and Security Issues

In healthcare, security and privacy is an essential discussion for patient-data & patient-doctor confidentiality from legal and ethical perspectives. As a matter of fact it is an important task to make sure the confidentiality of collected healthcare information along with patient data. Operational security was taken into consideration for an analytical process, rival collection capabilities, and accentuate the value of sensitive and critical information.

Different levels of security are co-related with higher computational costs, which are not only involved some training programs, up-gradations, and several operational phases, but also restricted to spending for improvement of any properties. So to secure, the security of information is an important matter of question from information and application level that can be considered by encoding the data and privacy setting.

5.5.5 High Cost and Power Consumption

The assumption of security measures in healthcare has many advantages when it associated with the protection of CPS components, levels and areas. But apart from that there are some limitations regarding the performance of the system due to time complexity which was associated with higher power consumption along with high cost as well. Power consumption is an important factor, especially for battery backup and resource constrains, which may affect the system performance and reduce it. The more power consumption means a shorter lifespan of battery life and a higher cost to maintain their availability. More power consumption and higher cost are corresponded to each other. When it consumes more power, then it may increase the cost for access and maintenance. Security measures are associated with more estimation costs, which may never be confined with initial phase of security operations, but also include restore, prepare and upgrade for operations (Yaacoub et al. 2020).

5.5.6 Maintenance

In Computer network management, security and maintenance, systems are still facing many inconsistencies' and safety contradictions. The maintenance of the HCPS basically focuses on risk assessment of medical information, establishment of enhanced approaches and also management of hardware equipment's. The healthcare units incorporate with network security and maintenance into the information construction system and need to focus on the possible risk factors to innovate and renovate the computer network management system and manage it.

5.6 HCPS Security Mechanisms

The security and privacy issue has facinated a lot of awareness and has been creating a lot of issues and controversies now often. Here some of the security mechanisms that were identified in the smart and digital healthcare system (Nasiri et al, 2019). In today's healthcare systems EHR is an enhanced and a necessary model of security mechanism for the patients' data storage, access, and retrival. The basic structure of security in EHR is based on the cloud storage system. All kinds of informations regarding patients particulars, physicians, and healthcare professionals are stored in the cloud based cyber physical system. That can be accessed by some specific users who were having the cyber security access. All these database services are managed by the EHR manager.

Security of the healthcare devices and medical data is analyzed by the "Integrated Fuzzy AHP-TOPSIS" technique (Alzahrani et al. 2022). Security mechanism in healthcare is functioning a design and process it to provide several security services

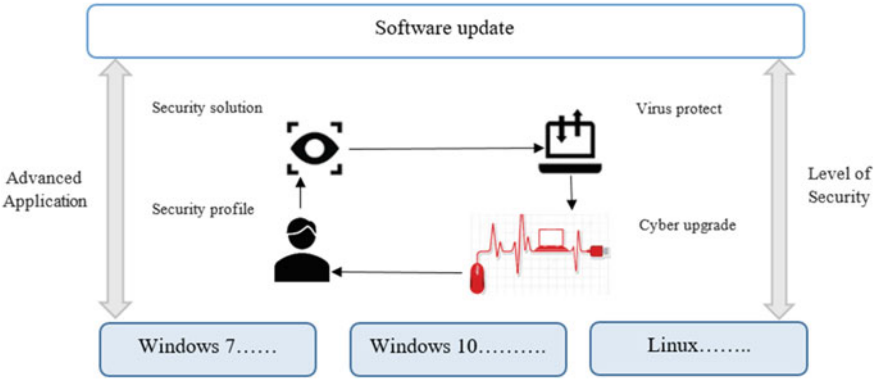


Fig. 5.5 Mechanism of healthcare security

for a particular result in terms of accuracy, assurance, and strength of a system. The Fig. 5.5 represents the basic workflow structure of security mechanism. This may include different types of operating system which can be accessed by the user. For the porpose of data privacy we need to focus on some advanced applications that are based on the security profile of the user and it's solution if any theft arises. The solution of cyber theft can be reduced by upgradation of cyber security applications and protection from any unethical accessses.

5.6.1 Security Mechanism in Block Chain Scheme

There are some security mechanisms corresponding to the block chain mechanism which is based on different assumptions such as: cryptography, fingerprint optimization, data encryption, management system in healthcare database. Block chain technology has emerged rapidly associated with the cloud domain and internet of healthcare security (IoHS) (Pelekoudas-Oikonomou et al. 2022). The healthcare units and tools are correlated in such a way that anyone can access the information whenever they need from any location. IoHS based healthcare management system provides customized and costumer focused healthcare duties by reducing the limitations as: Time, Power, Cost, Maintenance, and Locality. The computational work for digital and smart healthcare system can be reduced in terms of block chain technology. In the field of healthcare the block chain based application needs to be deployed. Edge networking is a frequent type of block chain based security mechanism specially designed for the server based security application (Fig. 5.6).

Block chain system may be considered in two types. First one is the Public block chain mechanism and the other one is the Private block chain mechanism. For todays' healthcare sectors and other organizations as well private block chain is primarily used for the data security and the unauthorized access from the EHR is blocked.

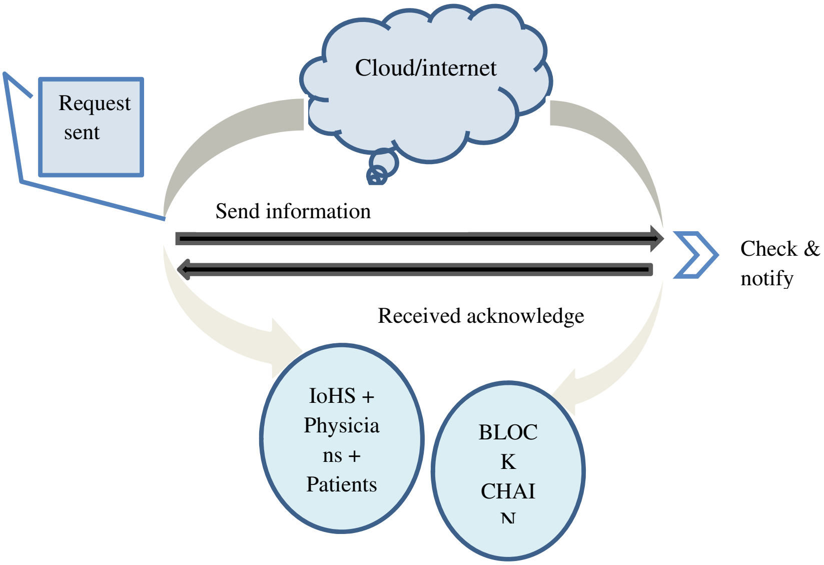


Fig. 5.6 Block chain based mechanism

5.7 Conclusion

Hospital facilities include the use of healthcare equipment and tools. Healthcare gadgets are the main resources for both patients and medical professionals, from patient health scanning and disease diagnosis to report and treatment. The healthcare facility must integrate computer network security into the creation of the system for storing medical and patient information as part of a specified implementation process. IoT and CPS devices are targets for fraudsters, attackers, and other unethical users that are captivated by the vast amount of information disseminated across medical devices. This information might be extremely harmful to anyone involved if it ends up in the wrong hands. IoT-CPS security considered AI-enabled algorithm is therefore required for the future. The security and privacy concerns of CPS in healthcare applications are examined in this chapter. We assume that these issues and challenges will provide enough inspiration for future discussions and an interest in research on security issues for CPS in healthcare applications.

References

Aceto G, Persico V, Pescapé A (2019) A survey on information and communication technologies for industry 4.0: state-of-the-art, taxonomies, perspectives, and challenges. IEEE Commun Surv & Tutor 21(4):3467–3501.

Adil M, Khan MK, Jadoon MM, Attique M, Song H, Farouk A (2022) An AI-enabled hybrid lightweight authentication scheme for intelligent IoMT based cyber-physical systems. IEEE Trans Netw Sci Eng.

Alzahrani FA, Ahmad M, Ansari MTJ (2022) Towards design and development of security assessment framework for internet of medical things. Appl Sci 12(16):8148

AlZubi AA, Al-Maitah M, Alarifi A (2021) Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. Soft Comput 25(18):12319–12332

Ashibani Y, Mahmoud QH (2017) Cyber physical systems security: analysis, challenges and solutions. Comput Secur 68:81–97

Cabello JC, Karimipour H, Jahromi AN, Dehghantanha A, Parizi RM (2020) Big-data and cyber-physical systems in healthcare: Challenges and opportunities. In: Handbook of Big Data Privacy. pp 255–283

Dey N, Ashour AS, Shi F, Fong SJ, Tavares JMR (2018) Medical cyber-physical systems: a survey. J Med Syst 42(4):1–13

Fink GA, Edgar TW, Rice TR, MacDonald DG, Crawford CE (2017) Security and privacy in cyber-physical systems. In Cyber-physical systems. Academic Press, pp 129–141.

Giansanti D (2021) Cybersecurity and the digital-health: the challenge of this millennium. Healthcare 2021(9):62

Gunes V, Peter S, Givargis T, Vahid F (2014) A survey on concepts, applications, and challenges in cyber-physical systems. KSII Trans Internet Inf Syst (TIIS) 8(12):4242–4268

Haque SA, Aziz SM, Rahman M (2014) Review of cyber-physical system in healthcare. Int J Distrib Sens Netw 10(4):217415

Iqbal R, Doctor F, More B, Mahmud S, Yousuf U (2020) Big data analytics and computational intelligence for cyber-physical systems: recent trends and state of the art applications. Futur Gener Comput Syst 105:766–778

Jamal AA, Majid AAM, Konev A, Kosachenko T, Shelupanov A (2021) A review on security analysis of cyber physical systems using Machine learning. Mater Today: Proc.

Khalil AA, Franco J, Parvez I, Uluagac S, Shahriar H, Rahman MA (2022) A literature review on blockchain-enabled security and operation of cyber-physical systems. In: 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC). IEEE, pp 1774–1779.

Krishna M, Chowdary SMB, Nancy P, Arulkumar V (2021) A survey on multimedia analytics in security systems of cyber physical systems and IoT. In: 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC). IEEE, pp 1–7.

Kurde S, Shimpi J, Pawar R, Tingare B (2019) Cyber physical systems (CPS) and design automation for healthcare system: a new era of cyber computation for healthcare system. Structure 6(12).

Latif SA, Wen FBX, Iwendi C, Li-li FW, Mohsin SM, Han Z, Band SS (2022) AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. Comput Commun 181:274–283

Liu H, Wang L (2020) Remote human–robot collaboration: a cyber–physical system application for hazard manufacturing environment. J Manuf Syst 54:24–34

Mishra A, Jha AV, Appasani B, Ray AK, Gupta DK, Ghazali AN (2022) Emerging technologies and design aspects of next generation cyber physical system with a smart city application perspective. Int J Syst Assur Eng Manag 1–23.

Nasiri S, Sadoughi F, Tadayon MH, Dehnad A (2019) Security and privacy mechanisms of internet of things in healthcare and non-healthcare industry. J Health Adm 22(4):86–105

Pelekoudas-Oikonomou F, Zachos G, Papaioannou M, de Ree M, Ribeiro JC, Mantas G, Rodriguez J (2022) Blockchain-based security mechanisms for IoMT Edge networks in IoMT-based healthcare monitoring systems. Sensors 22(7):2449

Pourhomayoun M, Shakibi M (2021) Predicting mortality risk in patients with COVID-19 using machine learning to help medical decision-making. Smart Health 20:100178

Priyadarshini I, Kumar R, Tuan LM, Son LH, Long HV, Sharma R, Rai S (2021) A new enhanced cyber security framework for medical cyber physical systems. SICS Softw-Intensiv Cyber-Phys Syst 35(3):159–183

Rho S, Vasilakos AV, Chen W (2016) Cyber physical systems technologies and applications. Futur Gener Comput Syst 56:436–437

Tong H (2022) Maintenance of network security in hospital information construction based on the internet of things. Int Trans Electr Energy Syst.

Vangipuram SL, Mohanty SP, Kougianos E (2021) CoviChain: a blockchain based framework for nonrepudiable contact tracing in healthcare cyber-physical systems during pandemic outbreaks. SN Comput Sci 2(5):1–16

Verma R (2022) Smart city healthcare cyber physical system: characteristics, technologies and challenges. Wireless Pers Commun 122(2):1413–1433

Xu J, Xue K, Li S, Tian H, Hong J, Hong P, Yu N (2019) Healthchain: a blockchain-based privacy preserving scheme for large-scale health data. IEEE Internet Things J 6(5):8770–8781

Yaacoub JPA, Noura M, Noura HN, Salman O, Yaacoub E, Couturier R, Chehab A (2020) Securing internet of medical things systems: limitations, issues and recommendations. Futur Gener Comput Syst 105:581–606