International Journal of Pure and Applied Mathematics
Volume 117 No. 20 2017, 319-324
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Security Issues in Medical Cyber Physical Systems (MCPS) - A Survey

P. Vimala Devi, Dr.V.Kalaichelvi
Assistant Professor, SASTRA University, Kumbakonam, India
Email: vimalasarathi@src.sastra.edu

Abstract

Cyber Physical Systems (CPS) bridging the cyber world with the physical world. The exploitation of such systems has extensively augmented in the recent years. CPS is used in variety of applications such as Healthcare, Transportation, Process control, Large scale infrastructure and in Defense system. According to World Health Organization (WHO), Cardio Vascular Disease (ie., heart disease and heart stroke) is the prime cause of death. These types of deaths will reach upto 23.3 million by 2030. To give attention to these issues, CPS is combined with Healthcare field. So, CPS in Healthcare is often referred to as Medical Cyber Physical System. In this, Sensor nodes are embedded in, on or around the patient's body to measure patient's physiological vital signs such as temperature, blood pressure, heart rate, respiration rate, ECG, EEG, etc., If these sensitive information are interrupted could lead to several consequences like mental instability, relationship issues, even job loss and wrong treatments leads to patient death. Due to this, more attention should be given and taken to provide security and privacy to the data. This paper discuss various issues that need to be taken into account to fulfilling the security and privacy requirements and also discuss about the relevant mechanisms and terminologies used by the various researchers to solve those issues.

Keywords: Cyber physical system, Security, Privacy, Health care system.

1.0 Introduction

Cyber physical systems is an emerging technology which connects physical environment into virtual. It integrates the physical components known as cameras, sensors with cloud and continuously monitors the changes in the physical environment. The applications of cyber physical systems are smart grid, healthcare, automotive systems and aerospace. In this modern world healthcare is very important one. Old age people and people suffered by chronic diseases require continuous monitoring. One type of cyber physical system known as Medical Cyber Physical System is used for this. It consists of medical devices, sensors and networking components. Sensors are used to measure the various signs of a patient such as temperature, electrocardiogram, blood pressure etc. These measurements can be transferred to the specialists via network. There are some issues occur while forming a sensor network and moving from sensor network to cyber world. The sensors implanted on the patient body is known as implantable medical devices and these devices having the issues such as computing power, storage and energy. The information collected from these devices can be processed in the form of e-health records. These e-health records reduce healthcare costs and also having some security issues. The sensors have the limited storage, so to process large information cloud platform is required. Encryption methods are used to encrypt the data before storing. These methods cannot allow calculations, so homomorphic encryption techniques are used. The cloud platform also have advantages and challenges. This paper summarizes the challenges related to cloud and healthcare.

2.0 Requirements / Properties of Medical Cyber Physical System:

The following are the requirements of Medical Cyber Physical System to build an efficient Health Care system

Security: The physiological signals which are collected from the patients must be well protected from intentional attacks.

Privacy: Medical data collected and managed by MCPSs is very significant. Tampering of this information leads to several consequences to the patient in the form of privacy loss, abuse and physical harm. So, safeguarding the security of MCPS is very vital.

Data Integrity: The physiological data collected from the patient should be accurate and reliable for making correct treatments.

Data Access Control: The patient's data should be accessed only by the authorized person.

Availability: It is expected that the operation of medical devices is available uninterruptedly for a long period of time.

Interoperability: In MCPS, medical devices will communicate with other devices. It is essential to ensure that the integrated devices are safe and secure.

3.0 Literature Survey

Buket Yuksel et al. explained the characteristics of e-health records [1].They also discussed about the design architecture and various access control techniques and encryption methods. The results show that the access control techniques have less performance and extra security is required. Uthpala Premarathne et al. used three techniques to process the data in secured manner [2]. In this biometrics is used to authenticate the user location. The EHR information is encrypted using role based method and embedded into ECG signals using steganography. Ji-Jiang Yanga et al. reviewed about the various techniques used to process health care data [3]. The techniques involved in this journal are big data, cloud and data mining. Mohd Anwar et al. discussed privacy and security challenges in healthcare [4]. They categorized these challenges based on devices used, communication techniques and applications.

José Luis Fernández-Alemán et al. discussed various techniques used to achieve privacy and security of e-health records [5].E-health records maintains the patient medical history and personal details. So, it is necessary to protect the information without leaking to unauthorized persons. Sebastian Haas et al. used a system to protect the privacy for patient information by logon process [6]. Patients have separate logins to verify their details. The authors not specified the methods for authentication and access control. ZHANG Li et al. explained the concepts of attacks in cyber physical systems, design and required measures [7].They also explained the attacks at various layers. Junbeom Hur and Kyungtae Kang developed a system to transmit between the devices and it is controlled by a controller [8].The information is encrypted using the attributes. This system helps to achieve enhanced security and privacy and fails to adapt emergency situation. Khin Than Win et al. reviewed about different types of threats and mechanisms to protect the personal health records [9].They explained pin and password based methods. These methods provide poor security.

Sensors play an important role to gather information from the patient body. Mamta and Shivaprakash et al., reviewed about the security attacks and their requirements for wireless sensor networks to solve health issues [10]. They also compared the protocols used in sensor network. With the advancement of networking and communication technologies, wireless body area networks plays an important part to monitor the patients. Chunqiang Hu et al. proposed a method that combines signature and encryption to transfer data from source to sink node [11]. Pallavi Meharia and Dharma P. Agrawal described public key encryption technique that authenticates the user [12].Hua-Pei Chiang et al. developed a system with help of cloud. The system adjusts the signal frequency and sleep time of sensor nodes to monitor the vital signs of the patient [13].Wireless sensors are used to collect information from patient body. But sensor nodes have limited storage, so cloud is required to store large information. Chandrani Ray Chowdhury surveyed about how to integrate sensors and cloud [14]. She also explained about the data bases and the techniques used for processing the data.

People in rural areas do not have facilities for proper medicine. They are not able to meet the specialists. Shah J. Miaha et al. developed a cloud based system to help rural people. Intermediate workers help the patients to communicate with specialists [15]. Patient's details stored in a database and transmitted to the destination. The authors not specified any methods to ensure availability, confidentiality and integrity of data. Kashfia Sailunaz et al. also developed a system for rural people using cloud [16].The authors used private cloud to process the data. Integrity of data is not achieved using this method. Charalampos Doukas and Ilias Maglogiannis collected the heart beat and movement of the patient continuously and stored to a cloud [17]. The authors used motion and ECG sensor to acquire the data and a microcontroller is used to process the data. This data can be used for emergency situations. Internet of things allows the sensors to communicate directly with cloud. The authors also combined cloud and internet of things to process bulk data [18]. Other than the security issues, types of sensors, standards used are discussed by Mona A. Alhumud et al [19] .The authors also provides an architecture that gives combined view of sharing data, analysis and making decisions. Sonith Raveendran Poyyeri et al. also used Google platform to store information about the patient and they gave the alert messages to patients about their health [20].

4.0 Conclusion

MCPS is a convergence technology useful to monitor the medical situation of patients at anytime, anywhere without limitations. This paper reviewed about the various techniques used in Medical Cyber Physical Systems such as wireless body area networks, cloud, electronic health record, big data, internet of things etc. The security requirements of MCPS are also discussed. Inferences from the various techniques, required knowledge about the challenges and mechanisms will be useful to build an efficient Healthcare System.

References

[1] Buket Yuksel, Alptein kupcu,Oznur Ozkasap , Research Issues for privacy and security of electronic health services, Future Generation Computer Systems,(2017),pp. 1-13.

[2] Uthpala Premarathne, Alsharif Abuadbba, Abdulatif Alabdulatif, Ibrahim Khalil, Zahir Tari,Albert Zomaya, Rajkumar Buyya, Hybrid Cryptographic Access Control for Cloud-Based EHR Systems, IEEE (2016).

[3] Ji-Jiang Yanga,Jianqiang Lic,Jacob Mulderd, Yongcai Wange, Shi Chenf,Hong Wu,Qing Wang,Hui Pan, Emerging information technologies for enhanced healthcare,2015, Computers in Industry, pp. 6-11.

[4]Mohd Anwar,James Joshi,Joseph Tan, Anytime, anywhere access to secure privacy-aware healthcare services: Issues, approaches and challenges, Health Policy and technology ,(2015), pp. 299-311.

[5] José Luis Fernández-Alemán, Inmaculada Carrión Señor,Pedro Ángel Oliver Lozoya, Ambrosio Toval, Security and Privacy in electronic health records: A systematic literature review, Journal of Biomedical Informatics,(2013),pp. 541-562

[6] Sebastian Haas, Sven Wohlgemuth, Isao Echizen, Noboru Sonehara, Günter Müller, Aspects of privacy for electronic health records, International Journal of Medical Informatics,80,(2011),pp. e26-e31.

[7] ZHANG Li, WANG Qing , TIAN Bin, Security threats and measures for the cyber-physical systems, The Journal of China Universities of Posts and Telecommunications,(2013), pp. 25–29.

[8] Junbeom Hur, Kyungtae Kang, Dependable and Secure computing in medical information systems, Computer Communications,(2012),pp.20-28

[9] Khin Than Win,Willy Susilo, Yi Mu, Personal health record systems and their security protection, Journal of medical systems, (2006).

[10] Mamta and Shivaprakash, An overview of Healthcare Perspective based Security Issues in Wireless Sensor Networks, IEEE,(2016).

[11] Chunqiang Hu, Hongjuan Li, Yan Huo, Tao Xiang, Xiaofeng Liao, Secure and Efficient Data Communication Protocol for Wireless Body Area Networks, IEEE TRANSACTIONS ON MULTI-SCALE COMPUTING SYSTEMS, VOL. 2, NO. 2, (2016), pp.94-107

[12] Pallavi Meharia and Dharma P. Agrawal, A Hybrid Key Management Scheme for Healthcare Sensor Networks, IEEE, (2016).

[13] Hua-Pei Chiang , Chin-Feng Lai , Yueh-Min Huang, A green cloud-assisted health monitoring service on wireless body area networks, Information Sciences, 284 , (2014),pp.118–129

[14] Chandrani Ray Chowdhury, A Survey on Cloud Sensor Integration, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 8,(2014).

[15] Shah J. Miah, Jahidul Hasan, John G. Gammack, On cloud healthcare clinic: An e-health consultancy approach for remote communities in a developing country, Telematics and Informatics, 34, (2017), pp. 311-322.

[16] Kashfia Sailunaz, Musaed Alhussein , Md. Shahiduzzaman , Farzana Anowar , Khondaker Abdullah Al Mamun , CMED: Cloud based Medical system framework for rural health monitoring in developing countries, Computers and Electrical Engineering, 53,(2016),469-481.

[17] Charalampos Doukas, Ilias Maglogiannis, Managing Wearable Sensor Data through Cloud

Computing, IEEE, (2011)

[18] Charalampos Doukas, Ilias Maglogiannis, Bringing IoT and Cloud Computing towards Pervasive Healthcare,IEEE,(2012).

[19] Mona A. Alhumud, M. Anwar Hossain and Mehedi Masud, Perspective of Health Data Interoperability on Cloud-Based Medical Cyber-Physical Systems, IEEE.

[20] Sonith Raveendran Poyyeri, Vishnu Sivadasan, Byrav Ramamurthy,Janet Nieveen, MHealthInt: Healthcare Intervention Using Mobile App and Google Cloud Messaging,IEEE,(2016).