Journal of Advanced Zoology

ISSN: 0253-7214

Volume ***44*** *Issue* ***I-3 Year 2023*** *Page* ***381****:****385***

A solution to smart health and state of art

S.Mahimavathi M.E/CSE
Er. Perumal manimegalai college of engineering,Hosur
smahimavathi@gmail.com
Mr.P.Yogananth M.E
(Assistant Professor)/CSE
Er. Perumal manimegalai college of engineering,Hosur
yoganmse@gmail.com

Article History

Received: 08July2023
Revised: 20 Sept 2023
Accepted:03 Oct 2023

Abstract

A medical cyber–physical system (MCPS) is a unique cyber–physical system (CPS), which combines embedded software control devices, networking capabilities, and complex physiological dynamics of patients in the modern medical field. In the process of communication, device, and information system interaction of MCPS, medical cyber–physical data are generated digitally, stored electronically, and accessed remotely by medical staff or patients. With the advent of the era of medical big data, a large amount of medical cyber–physical data is collected, and its sharing provides great value for diagnosis, pathological analysis, epidemic tracking, pharmaceutical, insurance, and so on. This overview will present MCPS's architectures and frameworks from different perspectives, modeling and verification methods, identification and sign sensing technologies, key communications' technologies, data storage and analysis technologies, monitoring systems, data security and privacy protection technologies, and key research perspectives and directions. We can have a com- prehensive understanding of the important characteristics and technical route of MCPS, and grasp its research status and progress.

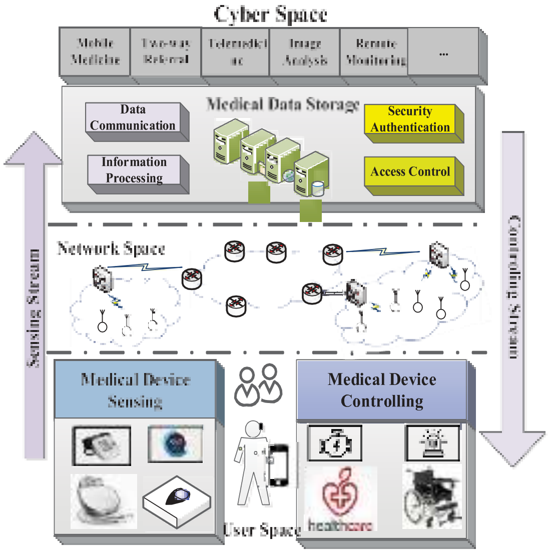
Index Terms— Architecture, medical cyber–physical systems (MCPSs), monitoring system, smart health.

Introduction

Medical cyber–physical systems (MCPSs) are a kind of cyber–physical systems (CPS) that are applied in the modern medical area and play an important role in the prevention and detection of COVID-19. Each MCPS has its embedded systems of control equipment and independent network systems [1]. The basic framework of MCPS includes the cyber space (including the network space) and the physical space (including the user space), as shown in

Fig. 1. The physical space is the physical foundation of MCPS. It includes all kinds of hard real-time health sensing devices, health diagnosis devices, and the user space composed of different users, provides sensing information to the cyber space through sensing devices, and receives the control information from the cyber space to control physical devices. The cyber space is the core component of MCPS, which is responsible for the processing, storage, and access security management of users, and health information. As the neural center of MCPS, the cyber space receives the sensing information from the physical space through the network transmission systems, identifies, stores, analyzes, and processes them, and generates the feedback control information that is sent to the physical space through the network transmission systems.

Compared with the Internet of Things (IoT), CPS empha- sizes the development and research of virtual application in the physical world [2], constructs a set of a closed-loop enabling system based on states sensing, real-time analysis, scientific decision-making, and precise execution between cyber space and physical space, solves the problems of complexity and uncertainty in the process of manufacturing and application services, improves the efficiency of resource allocation, and realizes resource optimization. It can be said that medical CPS is an important technical foreshadowing for the development of intelligent medical treatment and also one of the key supporting points for improving the medical system and the medical level.



Framework of MCPS

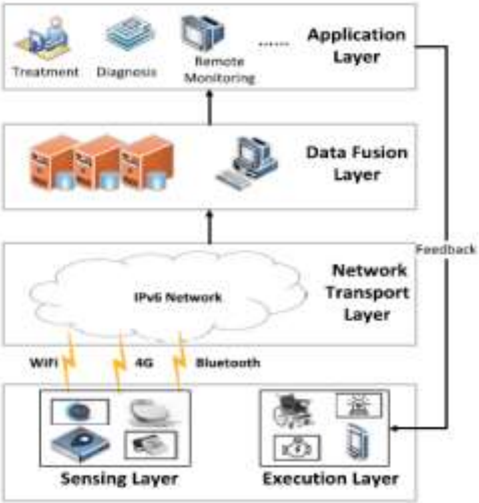
Cyber-Physical System Application

Cyber-physical systems are used in multiple areas, such as medicine, traffic management and security, automotive engineering, industrial and process control, energy saving, ecological monitoring and management, avionics and space equipment, industrial robots, technical infrastructure management, distributed robotic systems, protection target systems, nanotechnology and biological systems technology. A. Smart Technologies Modern construction technology enables the creation of intelligent building designed with minimum energy consumption or even without it. However, they need constant monitoring. Engineers must attach smart buildings to smart grids, and add control mechanism – cyber-physical systems [7]. Smart transport is equipped with various types of computerized embedded control systems. Cyber-physical solution use in this field makes it possible to create a fullfledged single system that will link the vehicles with other vehicles, environment and infrastructure [8]. An example of cyber-physical systems known to the general public is Google car, which does not require a driver. B. Internet of Things and Industry 4.0 In several sources [5], [9], [10] it is predicted that within ten years almost half of the electronic devices will be connected to the World Wide Web. This network is termed as the Internet of Things. It connects not only household appliances such as refrigerators, thermostats, but also sophisticated production equipment. Industry 4.0 concept aims at the comprehensive cyberphysical system use in manufacturing, customer relationship management and supply chain management processes, combining it all into one system. Smart manufacturing lines communicate with each other in order to optimize the production process. Comprehensive use of cyber-physical systems for commerce, industry and public health, military and civilian purposes, makes the protection of these systems a matter of national significance. That is why embedded system security systems, mainly anomaly detection system that allows resisting spoofing and service failure type attacks, are currently actively developed [11]. C. Healthcare Cyber-physical Systems There are hospitals, where robots already bring dishes to patients, sort mail, change bed linen and collect waste. Robotic beds transport patients to the surgery room. However, a fully automated healthcare system has not been implemented yet. Currently, a number of hospitals in the world remote operations are carried out with the help of a robotic hand and high-resolution cameras [12]; however, there is still a long way to autonomous surgery when a cyber-physical system itself, without human management, performs the operation.

Human-in-the-loop cyber-physical systems can greatly improve lives of people with special needs. Human-in-theloop cyber-physical systems formulate opinions about the user’s intentions based on his cognitive performance by analyzing data from sensors attached to the body or head. Embedded system converts these findings to robot control signals, which, thanks to robotic management mechanisms, allow users to interact with the surrounding natural environment. Example of human-in-the-loop CPS is robotic assistance systems and intelligent prosthesis [13]. From the examples above, it is clear that the cyber-physical systems are widely used all over the world in various industries, including medicine and healthcare. However, only one research was found [14], which summarizes the current situation related to the CPS application in healthcare, and it offers a detailed taxonomy.

Proposed system architecture

Energy Collection and Data Generation Layer: Different actions and gestures of the human body can produce different types of pressure areas. By installing piezoelectric devices in different pressure areas, electrical energy can be generated and provided to wearable health monitoring sensors implanted in the human body. With the assistance of a microcontroller and communication technology, the data collected by sensors are stored in the memory embedded in sensor nodes. Data Pre-processing Layer: It includes data aggregation, data transformation, and data filtering. Data Processing and Application Layer: It is responsible for the overall data processing and decision-making.



Conclusion

MCPS is a CPS applied in the modern medical field. Deepening the research and application of MCPS is of great significance to improve the national medical service system and improve the level of medical service. In recent years, artificial intelligence, blockchain, cloud computing, big data, wearable computing, and other technologies have provided new ideas for the construction of smart health but also put forward higher requirements for MCPS. In particular, how to design a secure, reliable, and efficient method of identity authentication and access control and how to realize the integration of heterogeneous networks and the secure sharing of medical big data are the key problems to be solved.

References

1)Y. Zhang, R. H. Deng, G. Han, and D. Zheng, "Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things," *J. Netw. Comput. Appl.*, vol. 123, no. 12, pp. 89–100, Dec. 2018.

2)S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay, and J. J. Rodrigues, "Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications," *IEEE Trans. Ind. Informat.*, vol. 15, no. 1, pp. 457–468, Jan. 2019.

3)G.-C. Li, C.-L. Chen, H.-C. Chen, F. Lin, and C. Gu, "Design of a secure and effective medical cyber-physical system for ubiquitous tele-monitoring pregnancy," *Concurrency Comput., Pract.*

4)Y. Zhang, J. Li, D. Zheng, X. Chen, and H. Li, "Towards privacy protection and malicious behavior traceability in smart health," *Pers. Ubiquitous Comput.*, vol. 21, no. 5, pp. 815–830, Jun. 2017.

5)L.-Y. Yeh, P.-Y. Chiang, Y.-L. Tsai, and J.-L. Huang, “Cloud-based fine grained health information access control framework for lightweight IoT devices with dynamic auditing andAttribute revocation,” *IEEE Trans. Cloud Comput.*, vol. 6, no. 2, pp. 532–544, Apr. 2018.
6)M. B. Tamboli and D. Dambawade, “Secure and efficient CoAP based authentication and access control for Internet of Things (IoT),” in*Proc. IEEE Int. Conf. Recent Trends Electron., Inf. Commun. Technol. (RTEICT)*, May 2016, pp. 1245–1250.
7)J. M. de Fuentes, L. Gonzalez-Manzano, A. Solanas, and F. Veseli,“Attribute-based credentials for privacy-aware smart health services inIoT-based smart cities,” *Computer*, vol. 51, no. 7, pp. 44–53, Jul. 2018.
8)F. Ullah, A. H. Abdullah, O. Kaiwartya, and Y. Cao, “TraPy-MAC:Traffic priority aware medium access control protocol for wireless bodyarea network,” *J. Med. Syst.*, vol. 41, no. 6, p. 93, Jun. 2017.
9)M. Luo, Y. Luo, Y. Wan, and Z. Wang, “Secure and efficient access control scheme for wireless sensor networks in the cross-domain context of the IoT,” *Secur. Commun. Netw.*, vol. 2018, pp. 1–10, Feb. 2018.
10)Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, “Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system,” *Inf. Sci.*, vol. 479, pp. 567–592, Apr. 2019.
11)T. Mikula and R. H. Jacobsen, “Identity and access management with blockchain in electronic healthcare records,” in *Proc. 21st Euromicro Conf. Digit. Syst. Design (DSD)*, Aug. 2018, pp. 699–706.
12)T. Mikula and R. H. Jacobsen, “Identity and access management with blockchain in electronic healthcare records,” in *Proc. 21st IEEE Euromicro Conf. Digit. Syst. Design (DSD)*, Oct. 2018, pp. 699–706, doi: 10.1109/DSD.2018.00008.
13)X. Zhang and S. Poslad, “Blockchain support for flexible queries with granular access control to electronic medical records (EMR),”in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6, doi: 10.1109/ICC.2018.8422883.
14)V. Malamas, P. Kotzanikolaou, T. K. Dasaklis, and M. Burmester,“A hierarchical multi blockchain for fine grained access to medical data,” *IEEE Access*, vol. 8, pp. 134393–134412, 2020.
15)Y. Ding and H. Sato, “Derepo: A distributed privacy-preserving data repository with decentralized access control for smart health,” in *Proc. 7th IEEE Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)/6th IEEE Int. Conf. Edge Comput. Scalable Cloud (EdgeCom)*, Aug. 2020, pp. 29–35, doi: 10.1109/CSCloud-EdgeCom49738.2020.00015.
16)K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
17)X. Cheng, F. Chen, D. Xie, H. Sun, and C. Huang, “Design of a secure medical data sharing scheme based on blockchain,” *J. Med. Syst.*, vol. 44, no. 2, pp. 1–11, Jan. 2020.