2022 3rd International Conference for Emerging Technology (INCET)
Belgaum, India. May 27-29, 2022

An adaptive Medical Cyber-Physical System for post diagnosis patient care using cloud computing and machine learning approach

M. Saef Ullah Miah
Faculty of Computing
Universiti Malaysia Pahang
Pekan, Malaysia
https://orcid.org/0000-0003-4587-4636

Talha Bin Sarwar
Faculty of Computing
Universiti Malaysia Pahang
Pekan, Malaysia
https://orcid.org/0000-0001-5974-1282

Saima Sharleen Islam
Department of Computer Science
American International University-Bangladesh (AIUB)
Dhaka, Bangladesh
saimasharleen0@gmail.com

Md. Samiul Haque
Institute of Information Technology
University of Dhaka
Dhaka, Bangladesh
s.h.shovon@gmail.com

Md. Masuduzzaman
Department of IT Convergence Engineering
Kumoh National Institute of Technology
Gumi, Republic of Korea
masud.prince@kumoh.ac.kr

Abhijit Bhowmik
Department of Computer Science
American International University-Bangladesh (AIUB)
Dhaka, Bangladesh
abhijit@aiub.edu

2022 3rd International Conference for Emerging Technology (INCET) | 978-1-6654-9499-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/INCET54531.2022.9824032

***Abstract*—Medical care is one of the most basic human needs. Due to the global shortage of doctors, nurses, and other healthcare personnel, medical cyber-physical systems are quickly becoming a viable option. Post-diagnosis surveillance is an essential application of these systems, which can be performed more successfully using various monitoring devices rather than active observation by nurses in their physical presence. However, most existing solutions for this application are rigid and do not consider current difficulties. Intelligent and adaptive systems can overcome the challenges because of the advances in relevant technology, especially healthcare 4.0. Therefore, this work presents an adaptive system based on cloud and edge computing architecture and machine learning approaches to perform post-diagnosis medical tasks on patients, thus reducing the need for nurses, especially in the post-diagnosis phase.**

***Index Terms*—cyber physical system, medical cyber physical system, healthcare 4.0**

I. Introduction

The term ”smart world” refers to a scenario in which the physical world is continuously connected to sensors, actuators, digital displays, and computing devices that are seamlessly integrated into everyday things and connected through an interconnected network [1]. The top five research areas dedicated to achieving this smart society are the Internet of Things, Wireless Sensor Networks, Mobile Computing, Pervasive Computing, and CPS [2]. The President's Council of Advisors on Science and Technology (PCAST) has identified CPS as a top priority for government research funding [3].

A Cyber-Physical System (CPS) combines computing, including the cyber world, and physical processes through computer networks. In addition, computers and networks integrated into physical processes are utilized to monitor and govern them via feedback loops [4]. One of the various fields in the field of CPS is Medical Cyber-Physical System (MCPS) [5]. MCPS is a networked, intelligent, safety-critical system for medical equipment. Previously, clinical settings might be considered closed-loop systems, with caregivers acting as controllers, medical equipment acting as sensors and actuators, and patients acting as ”plants”.

People's biggest concern these days is health care. Chronic diseases such as type 2 diabetes, kidney disease, and nutritional problems are common. These patients should be examined and treated at regular intervals to avoid major problems. In urgent cases, the patient also needs the presence of physicians and clinical assistants. Unfortunately, many patients do not receive adequate care. One of the most common reasons is the lack of physicians. In rural or remote areas, there are few doctors, and the hospitals may have unqualified nurses [6]. To provide adequate treatment, doctors must be present in the hospital almost all the time. Nurses must also be well trained and responsible for monitoring patients after diagnosis. Even then, mistreatment is possible. So modern technology needs to be improved. In this study, we examine a situation in which physicians are not always present in the hospital and patients are not always seen and treated by nurses. The proposed system would change treatment decisions and activities depending on sensor data. The goal is to design a system that can decide whether or not to treat a patient based on a collection of data. To achieve this goal, sensors and actions must be identified for various medical problems. It will also reduce post-diagnosis monitoring situations that rely on nurses.

This paper discusses various MCPS discussed in previous research articles and proposes a new model. This paper is divided into five sections. Section 1 is for the introduction, which discusses the rationale and objectives of the research. Section 2 summarizes other existing research. The third section

examines MCPS; the fourth section describes our proposed system. Section 5 discusses the future work and concludes the paper.

II. Background Study

A Cyber-Physical System (CPS) is a new generation of computer systems that combines computer and physical capabilities and can interact with humans in various ways. The ability to interact with and augment the capabilities of the physical environment is a critical enabler of future technological developments through computing, communication, and control. A Cyber-Physical System (CPS) is a system with embedded software (i.e., as a component of devices, structures, transportation devices, transportation directions, manufacturing systems, health processes, coordination processes, and management processes) that archives physical data directly via sensors and modifies physiological functions via actuators, analyses, stores, and interacts proactively or reactively with the physical and digital domains. [7].

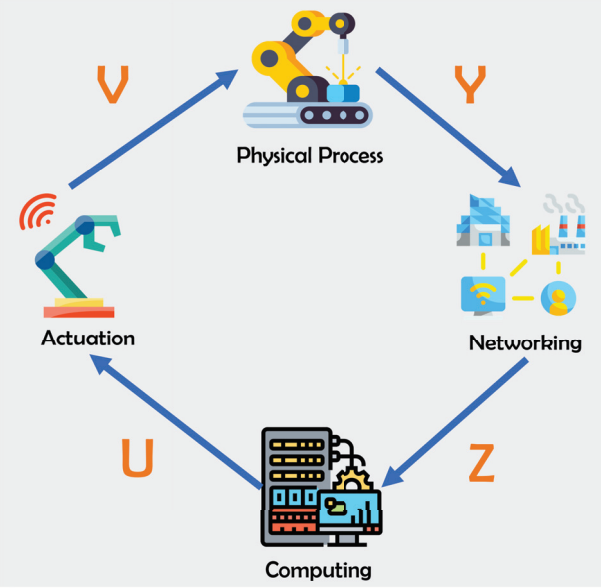

Fig. 1. CPS abstraction

The general workflow of CPS is shown in Figure 1. Y denotes the collection of sensor data, Z denotes the aggregation of the physical data in the network, U denotes the valid calculated result of the physical system states that could advise the controller to select proper instructions, and V denotes the control commands issued to the actuators [8].

A. Advantages of CPS

According to the Information Technology Laboratory (ITL), the capability to design and build successful cyber-physical systems will enable the government to address numerous national priorities in areas such as aerospace, automotive, energy, disaster response, healthcare, manufacturing, and urban governance in ways that traditional computing cannot [9]. In other words, one of the immeasurable benefits of cyber-physical systems is the acceleration of technological growth that will benefit a wide range of industries, businesses, and ultimately humanity. Figure 2 shows the capability of CPS technology to benefit various industries.

Fig. 2. Benefits of CPS

Intelligent traffic management, emergency response, and public safety technology are part of a smart city ecosystem. CPS helps cities replace infrastructure systems that have not been upgraded in a long time. CPS and the Internet of Things (IoT) can improve the safety of vehicle mobility. For example, all cars might be equipped with features like blind-spot monitoring, lane departure warning, and collision warning. Smart agriculture, often known as digital agriculture, is a term used to describe the use of technology to increase efficiency in the agricultural sector. Despite the apparent necessity for environmentally friendly business, health care, and other endeavors, the public still demands more answers. In many cases, CPS technology may be used to develop these solutions. Smart technology has improved security in several ways. Smart security has been made possible by modern CPS technology. A continuous smart gadget for people with diabetes communicates blood glucose readings to the wearer's smartphone, while a smart monitoring device for cancer patients tracks treatment response.

B. Related Study

Haque et al. [10] have provided an overview of cyber-physical systems in healthcare. Cyber-physical systems for healthcare applications are classified into eight categories: application, architecture, sensing, data management, computing, communication, security, and control/actuation. This categorization helps visualize trends, techniques and anticipated CPS solutions for specific applications. According to this article, security and privacy issues are among the least explored areas of CPS for healthcare applications. Although CPS can help anticipate incidents in healthcare, little research has been done. Lee et al. [5] have identified significant challenges in the

development of MCPS and have addressed promising areas of research. The field of MCPS is facing significant change due to increasing societal pressures and new technological opportunities. This would change the way these systems are developed and approved, expanding the functions and strengthening the safety assurances that MCPS provides to caregivers and patients. MCPS has difficulties that no other area of CPS has. They have identified significant challenges in the development of MCPS and have proposed promising research directions to overcome some of these challenges. Dey et al. [11] have concluded that physical failures are liberated and that immediate failures are unlikely. Cyber-physical systems reopen another thread, allowing cyberspace to attack physical systems via physical technologies. Personal and financial security requires privacy and security. According to Nair et al.'s [12] research, Medical Cyber-Physical Systems (MCPS) are a sector-specific use of CPS, similar to how CPS may be utilized in applications like smart grids smart cars, and industrial control systems (ICS). They discovered that MCPS offers unique challenges that set it apart from other CPS domains.

The CPS study addresses medical and biomedical engineering problems [13]. Smart operating rooms and hospitals, image-guided surgery, and physical and neural prosthesis are a few examples. So, medical equipment and systems that can connect with patients and caregivers in challenging circumstances are required. Many operating rooms include sedative infusion pumps, ventilators, oxygen delivery equipment, and sensors to monitor patient states. These devices are frequently combined to address specific patient or practitioner needs. The problem is to build systems and control mechanisms that are verifiable, safe, secure, and consistent. A series of workshops outlined the research problems in medical technology and health care. The authors have suggested a three-level processing architecture for sensor data, with level 1 being algorithmic [14]. However, they have not suggested a data processing mechanism or approach. Our purpose is to process data and forecast actions.

III. MEDICAL CYBER PHYSICAL SYSTEM

Due to the combination of embedded software that monitors the devices, networking capabilities, and the complicated physical changes exhibited by the patient's body, current medical device systems are classified as a unique class of cyber-physical systems termed medical CPS (MCPS) [15]. Due to the rising size and intricacy of MCPS, enhancing its security and effectiveness will require new design, authentication, and justification approaches [11]. In the design of MCPSs, model-based technology should take precedence. Models should incorporate devices and their associated communication, as well as patients and carers. MCPS enables the patient to communicate freely with the cyber world in order to receive the best possible care. MCPS deviates from the single system's computation and care. Numerous health system modules operate independently now, and some solutions are available that are only partially connected [16]. Building this type of MCPS requires overcoming several key challenges, [3], [5], [17], [18] which are identified in the following section.

A. MCPS Challenges

1) High Confidence Software: Certain hardware-dependent functions can also be implemented in software. As a result, trustworthy software development is critical to ensuring MCPS's security and efficacy.

2) Interoperability: Due to the fact that medical devices connect with one another and with a variety of different communication gateways, it is necessary to assure the safety, effectiveness, and security of all communicating devices or interfaces.

3) Context-Awareness: Any MCPS must be contextual, as it is capable of detecting early changes in patient health parameters.

4) Autonomy: The various modules of the MCPS should operate autonomously on the patients' present health status, which can be enhanced further by offering a wide number of health states and actions against this state data.

5) Security and Privacy: Data integrity violations can have catastrophic effects, as this information is directly tied to an individual's health status. As a result, every MCPS environment must maintain data security and privacy.

6) Certifiability: Due to the fact that MCPS is composed of numerous modules and interfaces, it is quite possible that there are multiple vendors. Thus, there must be an easier approach to integrate devices or software from disparate vendors, and certification is one such method.

IV. PROPOSED SYSTEM

The overview of the proposed system is shown in Figure 3. This system aims to monitor the patient after treatment using health monitoring sensors and perform the necessary post-treatment actions using healthcare actuators based on the patient's health status. The system consists of five different modules: health monitoring sensors, cloud control panel (CCP), edge-based dynamic machine learning model (EDMLM), healthcare actuators, and patient monitoring devices.

Data is sent from the monitoring sensors to the CCP and the CCP sends the data to the EDMLM for possible actuation. Then the CCP sends the actuation command to the actuators and the actuation is executed. This process is used to ensure possible actuation with high safety. If the data sent from the sensors is a low probability possible actuation or it is a new data set, the possible actuation must be approved by the caregiver and the notification alarm is sent to the caregivers through the monitoring devices. If approved by the caregiver, the actuation is performed and the data, actuation label, and confidence value are stored in the EDMLM and the model is trained to adjust for actuation reliability. If the actuation is rejected by the caregiver, the caregiver performs the necessary actions. The manual actuation value is collected along with the data generated by the sensors and also sent to the EDMLM for model adjustment. The communication

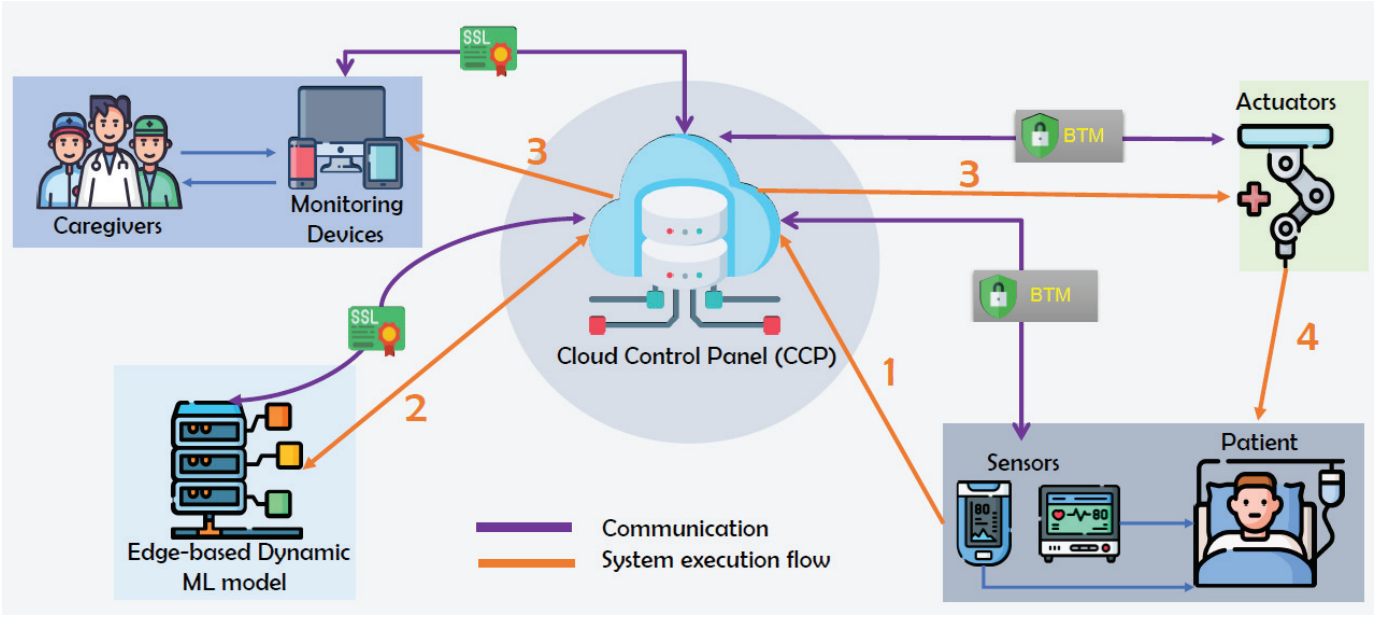

Fig. 3. Proposed System Architecture

between the monitoring devices, the EDMLM and the CCP is secured by the certification body. And the communication between the monitoring sensors, the actuators and the CCP is secured by a newly proposed Behavioral Trust Model (BTM). The data flow swim lane shown in Figure 4 shows the data flow between the different modules for both scenarios mentioned above.

The system collects sensor data only when all system components are functioning properly. This is a patient safety measure because safety is paramount. It is assumed that there is a risk to the patient if a component of the system fails at any stage of treatment. For example, if a sensor is defective, it will provide erroneous readings and the system will continue to operate with incorrect data. Another possibility is that the sensors are providing accurate readings, but the trigger system is not functioning properly for some reason. In this case, the system is unable to actuate a trigger. It is better if the system checks if the individual components are working properly and only then starts extracting values. Then the system determines whether the variables are connected or not and then collects all the data. Based on the results of the different sensors, the system continuously keeps the caregiver informed of the patient's health status. Based on the different thresholds of the different sensors, the system generates alarms and notifications about the patient's health status and transmits them to the caregiver.

A. Advantages of the proposed system

The security of the proposed system is ensured by implementing a secure communication framework and a novel trust management method. The communication between the monitoring devices, actuation providing model and the cloud control panel is secured by the certification authority. The proposed system leverages the cloud computing and edge computing infrastructure for system availability, integrity, and scalability. In addition to the infrastructure, the proposed system provides health monitoring through various interfaces, including mobile, web, and desktop applications. The proposed system also provides control and monitoring of single and multiple sensors. The proposed system dynamically adjusts actuation procedures based on new data and actuation values supported by caregivers with a dynamic machine learning model.

After a performance evaluation, our system takes appropriate actions in response to various health conditions, and our autonomous system evaluates whether the patient has recovered or not. Our proposed solution preserves data integrity because it is important to preserve patients' data. And compromising data integrity can end in a catastrophic event. In terms of each patient's health data, our proprietary behavioral trust management technique will ensure the privacy and security of our proposed system. CA will ensure that the multiple modules and interfaces we integrate through certification will simplify the process of connecting multiple providers.

B. Challenges of the proposed system

The main challenge for the proposed system is the dynamic training of the model that provides the actuation operations. The dynamic training of the model is performed for each new set of data acquired by the sensors, and human consent is required for each new set of data. Thus, the proposed system is dependent on humans to some extent and is not completely free from human intervention in the actuation phase.

V. CONCLUSION

This study has presented a system that can extract data from sensors and analyses the health status of patients. This system

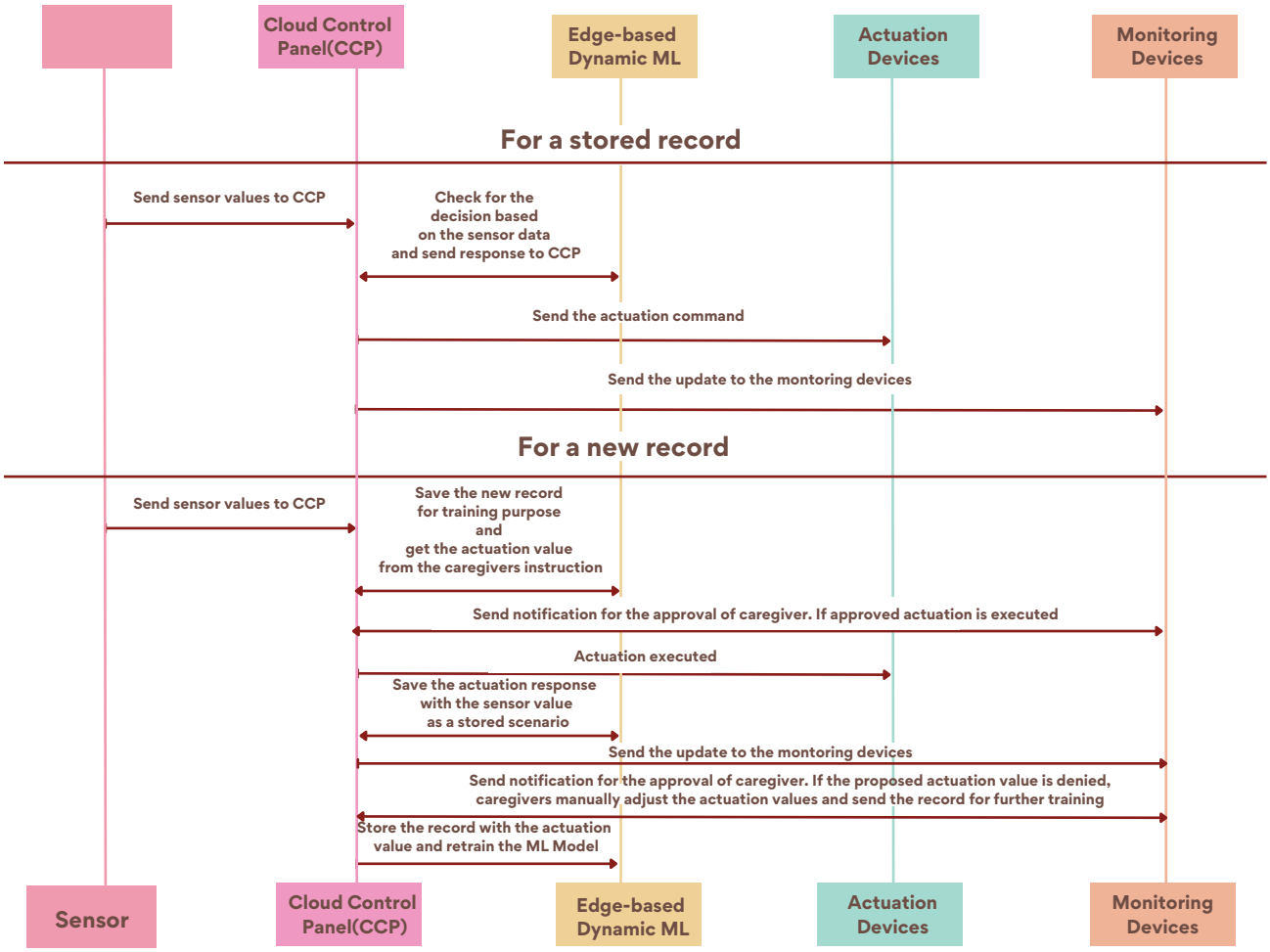

Fig. 4. Data flow of the Proposed System

can make decisions about activities to be performed on patients based on the data collected from these sensors. This system is based on cloud and edge computing architecture and can use a variety of machine learning algorithms to decide whether or not to perform an activity depending on the data. Since this system is still in the early stages of development, there is still much room for experimentation with alternative algorithms for the actuation process and accuracy of the system. In addition, various machine learning and deep neural networking approaches can be explored.

ACKNOWLEDGEMENT

This work has been partially supported by the Fundamental Research Grant Scheme (FRGS) project, under Grant No. RDU1901109 of Universiti Malaysia Pahang (UMP).

REFERENCES

[1] What is smart world. https://www.igi-global.com/dictionary/smart-world/70372.

[2] John A Stankovic. Research directions for the internet of things. *IEEE internet of things journal*, 1(1):3–9, 2014.

[3] Lui Sha, Sathish Gopalakrishnan, Xue Liu, and Qixin Wang. Cyber-physical systems: A new frontier. In *2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (sutc 2008)*, pages 1–9. IEEE, 2008.

[4] Harald Voit. *An arbitrated networked control systems approach to cyber-physical systems*. PhD thesis, Technische Universität München, 2013.

[5] Insup Lee, Oleg Sokolsky, Sanjian Chen, John Hatcliff, Eunkyoung Jee, BaekGyu Kim, Andrew King, Margaret Mullen-Fortino, Soojin Park, Alexander Roederer, et al. Challenges and research directions in medical cyber–physical systems. *Proceedings of the IEEE*, 100(1):75–90, 2011.

[6] Xiuxia Li, Lili Wei, Wenru Shang, Xin Xing, Min Yin, Juan Ling, Kuoray Mao, Yiliang Zhu, and Kehu Yang. Trace and evaluation systems for health services quality in rural and remote areas: a systematic review. *Journal of Public Health*, 26(2):127–135, 2018.

[7] Panos Antsaklis. Goals and challenges in cyber-physical systems research editorial of the editor in chief. *IEEE Transactions on Automatic Control*, 59(12):3117–3119, 2014.

[8] Eric Ke Wang, Yunming Ye, Xiaofei Xu, Siu-Ming Yiu, Lucas Chi Kwong Hui, and Kam-Pui Chow. Security issues and challenges for cyber physical system. In *2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing*, pages 733–738. IEEE, 2010.

[9] Thelma.allen@nist.gov. Cyber physical systems. https://www.nist.gov/itl/ssd/cyber-physical-systems, Aug 2016.

[10] Shah Ahsanul Haque, Syed Mahfuzul Aziz, and Mustafizur Rahman. Review of cyber-physical system in healthcare. *international journal of*

distributed sensor networks, 10(4):217415, 2014.

[11] Nilanjan Dey, Amira S Ashour, Fuqian Shi, Simon James Fong, and João Manuel RS Tavares. Medical cyber-physical systems: A survey. *Journal of medical systems*, 42(4):1–13, 2018.

[12] Meghna Manoj Nair, Amit Kumar Tyagi, and Richa Goyal. Medical cyber physical systems and its issues. *Procedia Computer Science*, 165:647–655, 2019.

[13] Hong Chen. Applications of cyber-physical system: a literature review. *Journal of Industrial Integration and Management*, 2(03):1750012, 2017.

[14] Shailesh Kumar Jha. Medical cyber physical system. *International Journal of Emerging Technology and Advanced Engineering*, 4(5):819–823, 2014.

[15] Han Qiu, Meikang Qiu, Meiqin Liu, and Gerard Memmi. Secure health data sharing for medical cyber-physical systems for the healthcare 4.0. *IEEE journal of biomedical and health informatics*, 24(9):2499–2505, 2020.

[16] Adib Mehedi, Abid Hassan Tokee, Surovi Islam, and Md Saef Ullah Miah. Iot based healthcare middleware. In *Proceedings of the International Conference on Computing Advancements*, pages 1–4, 2020.

[17] Jianhua Shi, Jiafu Wan, Hehua Yan, and Hui Suo. A survey of cyber-physical systems. In *2011 international conference on wireless communications and signal processing (WCSP)*, pages 1–6. IEEE, 2011.

[18] Alberto Huertas Celdrán, Manuel Gil Pérez, Félix J García Clemente, and Gregorio Martínez Pérez. Sustainable securing of medical cyber-physical systems for the healthcare of the future. *Sustainable Computing: Informatics and Systems*, 19:138–146, 2018.