# Medical Cyber–Physical Systems: A Solution to Smart Health and the State of the Art

Fulong Chen, *Member, IEEE*, Yuqing Tang, Canlin Wang, Jing Huang, Cheng Huang, Dong Xie, Taochun Wang, and Chuanxin Zhao

***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 comprehensive 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.**

## I. 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.

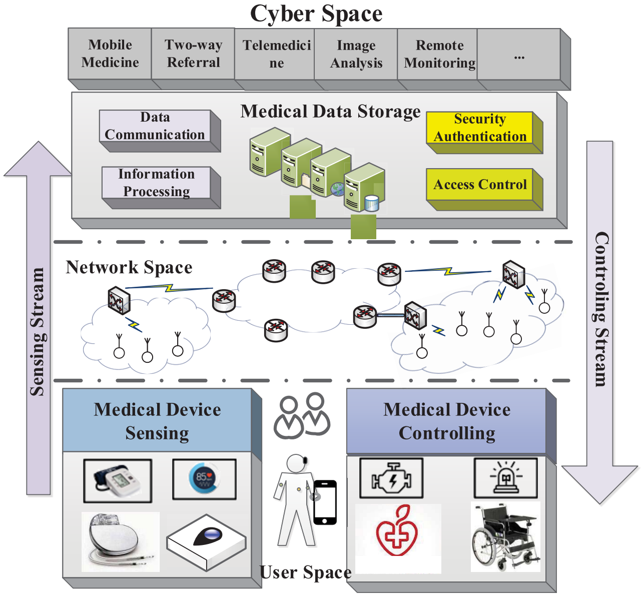

Fig. 1. Framework of MCPS.

Compared with the Internet of Things (IoT), CPS emphasizes 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.

Traditional MCPS architecture focuses on patient monitoring and data feedback. Some researchers pay attention to the

Manuscript received 16 March 2021; revised 9 October 2021; accepted 20 October 2021. Date of publication 4 November 2021; date of current version 30 September 2022. This work was supported in part by the National Natural Science Foundation of China under Grant 61972438 and in part by the Key Research and Development Projects in Anhui Province under Grant 202004a05020002. *(Corresponding author: Fulong Chen.)*

The authors are with the Anhui Provincial Key Laboratory of Network and Information Security, Anhui Normal University, Wuhu, Anhui 241002, China (e-mail: long005@ahnu.edu.cn; tangyuqing@ahnu.edu.cn; wangcanling@ahnu.edu.cn; huangjing@ahnu.edu.cn; chenghuang@ahnu.edu.cn; xiedong@ahnu.edu.cn; wangtc@ahnu.edu.cn; zhaocx@ahnu.edu.cn).

Digital Object Identifier 10.1109/TCSS.2021.3122807

interaction between cyber space and physical space, build the architecture based on the CPS, and combine big data and cloud computing to build a medical consortium. In addition, based on the architecture of the IoT, some researchers take the medical IoT as the typical application, wearable medical devices as data sensing devices, and patients, doctors, and managers as the main user nodes, which complete the communication of the network layer through the IPv4 or IPv6 gateway devices inside the hospital, and transmit the data of the IoT sensing layer to the application layer for analysis or visual presentation.

As the background of the application of CPS in the field of health care, MCPS provides flexible interaction between patients and the medical system to realize all-round 3-D medical treatment. MCPS can use the dynamic data of the sensor network and monitoring system to move the calculation and monitoring from the independent system to the remote monitoring center, builds the medical system into a medical union of cyber space and physical space, focuses on the interaction between the cyber system and the physical system in the medical environment, and updates the data and feedback data in time. MCPS has the characteristics of high integrity, limited physical resources, cross-domain transmission, multidomain networking, complex space domain, dynamic reorganization, high automation, high reliability, and security of CPS. The medical field includes national health information, electronic medical record (EMR), patient care information, operating room treatment information, and so on. Some of them are more and more controlled by computer systems with hardware and software components, and are high security and strong real-time systems. MCPS must be further researched and developed in control and fusion systems, sensor and mobile networks, security, reliability and stability, embedded systems and abstract computing, model development, security authentication, and data traceability.

The main work and contributions of this article are given as follows.

1) From different perspectives, we make a more comprehensive summary of the architecture and framework of MCPS and its modeling methods, and also classify and compare the existing MCPS architectures.
2) As the key component of MCPS, we analyze the monitoring system in detail from four aspects: system characteristics, architectures, technical requirements, and specific application scenarios.
3) Unlike previous related papers, such as [3], [4], [101], and [104], which only focus on one aspect, we make a broader summary from the underlying sensing and communication in MCPS to the storage and analysis of data, as well as data security and privacy protection.
4) We discuss the new ideas and challenges brought by the emergence of new technologies (such as big data, cloud computing, and blockchain) for the MCPS and provide a broader view of the development prospects and trends of new technologies in MCPS.

## II. Architecture and Framework

Architecture and framework can accurately describe the constituent elements of the whole system and the relationship between them [5], which provides consistent criteria for developers to build MCPS. Similarly, architecture or a framework is also the basis of MCPS research. Based on the literature research in recent ten years, we summarize and analyze the existing architectures and frameworks applied to MCPS from different perspectives.

### A. Functional and Behavioral Perspectives

The key task in the field of MCPS is to realize the collection, transmission, analysis, processing, storage, and access of patients' personal health data. According to different functions and tasks, it can be divided into the following two types of architecture.

1) *Transmission Architecture:* It focuses on the effective transmission of health data, especially how to ensure the effective transmission of cross-communication technology data, e.g., community medical IoT based on IPv6 [6] and smart medical systems based on edge computing [7]. Fig. 2 shows the layers of the IPv6-based community medical IoT in [6].
2) *Data Processing Architecture:* It focuses on the analysis and processing of health data, especially how to realize the effective aggregation, transformation, filtering, mining of massive medical perception big data, and provide decision-making basis, e.g., smart health monitoring management system architecture based on big data analysis [8] and MCPS architecture based on device AI [9].

   In the data processing architecture, the MCPS big data processing mainly includes data collection, data preprocessing, data storage, data analysis, and data application. As shown in Fig. 3, after the big data of MCPS are collected, the first step is data preprocessing, such as data cleaning, which includes error detection, error recovery, consistency and redundancy detection, and so on. After that, data compression is performed to reduce the size of the dataset to complete data storage. The last step is data analysis and mining to realize applications, such as information visualization. Data mining includes data characterization, frequency pattern analysis, classification, aggregation, correlation mining, and so on.

### B. Hierarchy and Structure Perspective

Din *et al.* [8] proposed a three-layer MCPS.

1) *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.
2) *Data Preprocessing Layer:* It includes data aggregation, data transformation, and data filtering.
3) *Data Processing and Application Layer:* It is responsible for the overall data processing and decision-making.

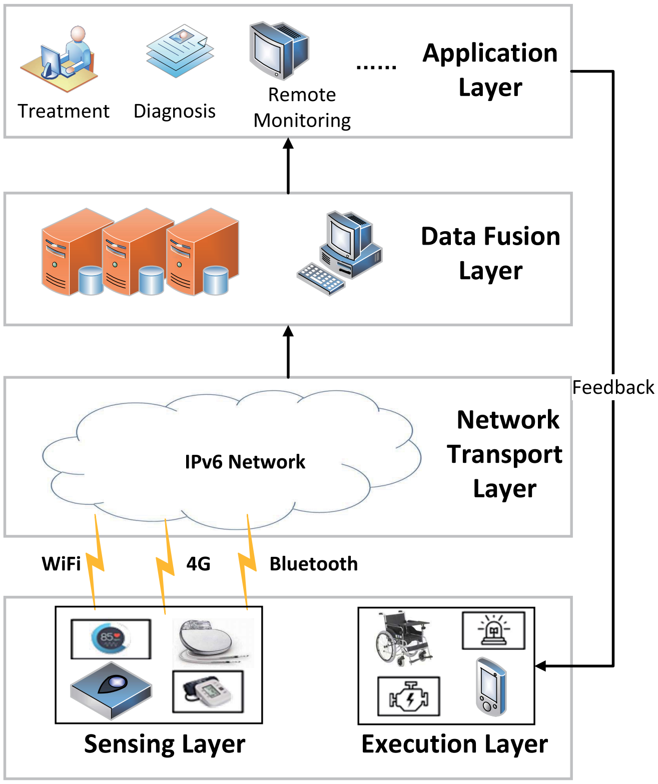

Fig. 2. Layers of CMIoT.

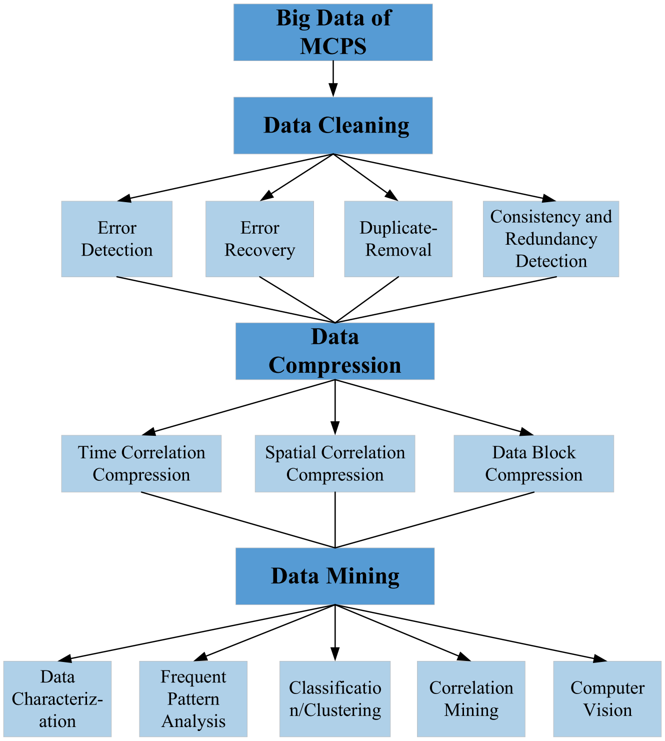

Fig. 3. Big data processing of MCPS.

This layer includes queue, Hadoop server, storage, rule engine, decision, and event management department.

Mowla *et al.* [10] presented a four-layer MCPS architecture. The acquisition layer collects human health data based on various sensor devices. The preprocessing layer temporarily stores and processes the data of the acquisition layer. The cloud layer provides large-scale data processing and computing services. The behavior layer provides health data visualization service for medical staff to realize analysis and decision-making. MCPS architecture based on device AI [9] is similar to it. The difference is that the preprocessing layer of the latter is not only used for temporary data storage and processing but also can perform cognitive decisions on devices.

The OmniPHI blockchain architecture model [11], [12] includes the client layer and the server layer. The former is installed in medical devices and wearable devices of patients. The latter is distributed among the super peers on the platform based on blockchain technology. This architecture is formed through a dedicated P2P network, in which health records are organized into data blocks, and link lists and distributed classified health data are formed. Another blockchain-based MCPS e-health [13] includes four layers, such as: 1) WSN layer that collects data based on WSN node and sends it to blockchain; 2) side chain layer that is mainly a WSN controller, that is, once all data enter the side chain, the smart contract will be verified, and then, the side chain will be added to the main chain (i.e., blockchain); 3) smart contract layer in which the smart contract is executed to create the side chain, verify the side chain, and, finally, insert the side chain into the blockchain after the smart contract is verified; and 4) blockchain layer that is the public blockchain with limited access.

Abdellatif's smart medical system [7] includes the following components.

1) *Hybrid Sensor:* The combination of sensing devices connected/close to the patient represents a set of data sources
2) *Patient Data Aggregator (PDA):* Generally, a wireless body area network is composed of multiple sensor nodes measuring different vital signs and a PDA. As a communication hub, PDA is deployed near patients and transmits the collected medical data to the infrastructure.
3) *Mobile/Infrastructure Edge Node (MEN):* MEN realizes the intermediate processing and storage function between data source and cloud, integrates medical and nonmedical data from different sources, processes, classifies, and notifies the collected data through the network, extracts interested information, and forwards the processed data or extracted information to the cloud.
4) *Edge Cloud:* It is used for data storage, pattern monitoring, and human health data analysis and management. Edge cloud can refer to a hospital, which monitors and records the status of patients, and provides medical assistance when needed.
5) *Monitoring and Service Providers:* They can be doctors, intelligent ambulances, or even relatives of patients to provide prevention, treatment, emergency, or rehabilitation medical services for patients.

Considering security needs, Alabdulatif *et al.* [14] proposed a smart medical framework based on completely homomorphic encryption. It depends on the interaction of different entities to achieve specific analysis tasks. Data aggregation, storage, and processing all include analysis tasks and are carried out in the way of privacy protection. It is composed of four components: 1) community members (CMs), including healthy people, elderly patients, and hospitalized patients in the smart community in which wired/wireless sensors are used to aggregate the biological signal data from CM, encrypt, and send it to the cloud for storage; 2) IoT gateway used for local analysis and processing of medical data in the community and local diagnostic feedback and then sending encrypted data to cloud storage for further analysis combined with other communication data; 3) cloud database (CD) storing CM's health data from the smart community in encrypted form with cloud storage technology; and 4) anomaly detection model (ADM) that is the system analysis engine for data analysis of encrypted data.

### C. Communication Perspectives

According to different communication modes, MCPS communication architecture models are generally divided into the following five types [11].

1) *Client/Server (CS) Mode:* The client process interacts with a single server process in a potentially independent host to access the shared resources which it manages.
2) *Point-to-Point (P2P) Mode:* All the processes involved play a similar role and interact as peers, regardless of client or server.
3) *Distributed Object (DO) Mode:* Each process contains a set of objects, some of which can receive both local and remote calls, while others can only receive local calls.
4) *Distributed Component (DC) Mode:* The application server provides a structure to support the separation between application logic and data storage.
5) *Distributed services Based on Event (DE) Mode:* The essence of indirect communication is to communicate through mediation so that there is no direct coupling between the sender and one or more receivers.

### D. Deployment Perspectives

From the perspective of deployment, MCPS functional architecture is divided into centralized architecture, distributed architecture, and hybrid architecture. In the centralized architecture, the computer performance needs to have a significant level of division, and most of the information processing and data service requests in the network are carried out on the centralized management of high-performance computer equipment. Distributed architecture does not require special high-performance computer equipment, but nodes in the same level of communication need to have the same or similar computing performance, and most of the network information processing tasks are carried out in the communication hub nodes (such as routers and gateways) in the process of network communication. Hybrid architecture has the characteristics of both of them, which requires the existence of high-performance communication nodes in the network. At the same time, the communication hub node also undertakes a considerable part of the data processing tasks.

### E. Requirement Perspectives

MCPS architecture based on different basic technologies has significant differences in application fields, network performance, and system security. The key technologies used in MCPS architecture include blockchain, routing coverage, the Chord algorithm, publish/subscribe service, IPv6, cloud computing, data encryption, and so on. In general, MCPS architecture contains a variety of basic technologies. According to different emphases on basic technologies, MCPS architecture can be divided into secure and reliable architecture and high-performance architecture. Security architecture emphasizes network communication security and system security. It has high data sensitivity and high requirements for privacy. However, its network communication efficiency and system real-time performance are relatively low. The high-performance architecture emphasizes more on network communication efficiency and system real time, and efficiency is the first priority of this kind of architecture.

### F. Comprehensive Classification and Comparison

In summary, the typical MCPS architectures are shown in Table I. The hierarchical distributed EHR model (HDEMR) [15] aims to maintain the patient data in the WHO and copy it to other hospitals in the region to ensure fault tolerance, but P2P distribution is the future proposal and does not include topics such as security, privacy, or interoperability. The ubiquitous medical service model in the cloud (m-health) [16] proposes a distributed event-based architecture (DE). Although it does not mention security or privacy, it has interoperability services that meet CCR standards. The ubiquitous PHR framework model (uPHR) [17] is also a DE model, which has interoperability services conforming to HL7, CCR, and CEN13606 standards, but it does not mention security and privacy. The conceptual framework (CF) model [18] is a wearable medical system framework based on a cloud server DO mechanism. It supports the security and privacy of CIA and HIPAA protocols but does not pay attention to interoperability. The healthticket model [19] is a design and implementation case for ubiquitous PHR. According to CCR and HL7 standards, the model is proposed as an architecture for mobile and healthcare providers to access patients through web applications. This is a client–server (CS) model, which uses a security mechanism called CP-ABE (ciphertext policy attribute encryption scheme) to ensure privacy. The distributed electronic patient record (DEPR) model [20] is a DC scheme based on the OpenEMR system, which meets multiple standards, but does not pay attention to security or privacy. SNOW project is a distributed medical data processing system. This model uses DO and has a privacy policy that follows the openEHR standard. One of the conceptual foundations of OmniPHR [12] is to divide the patient's health records into data blocks, which are the logical division of patient health datasets, such as laboratory data, drug-related datasets, X-ray datasets, and other datasets. OmniPHR focuses on the distribution and interoperability of PHR data. The purpose of this model is to allow a unified view of health records distributed in multiple health organizations and to solve the

TABLE I
ARCHITECTURES OF MCPS

| Architecture | Communication | Deployment | | | Requirement | | Function | | Hierarchy (Layers) |
|---|---|---|---|---|---|---|---|---|---|
| | | C | D | H | S | E | T | P | |
| CMIoT [6] | CS/DE | | | √ | ★ | ★★★ | √ | | -Sensing/execution<br>-Communication assistant<br>-Network transport<br>-Data fusion<br>-Application service |
| Edge Computing for SH [7] | DE | | √ | | ★ | ★★★ | √ | | -Hybrid sensor source<br>-Patient data aggregator<br>-Mobile/infrastructure edge node<br>-Edge cloud<br>-Monitoring and service provider |
| SHMM [8] | DO | | √ | | | ★★★ | | √ | -Energy collection and data generation<br>-Data preprocessing<br>-data processing and application |
| On-Device AI [9] | DE | | √ | | ★ | ★★ | | √ | -Acquisition<br>-Preprocessing<br>-Cloud-Behavior |
| OmniPHR [12] | CS/P2P | | | √ | ★★ | ★★ | | √ | -Client<br>-Server |
| Distributed e-health [13] | DO | | √ | | ★★ | ★ | | √ | -WSN<br>-Side chain<br>-Smart contract<br>-Blockchain |
| FHE-based [14] | CS/DO | | √ | √ | ★★★ | ★ | | | -Community member<br>-Internet of things gateway<br>-Cloud database<br>-Anomaly detection model |
| HDEHR [15] | DE/P2P | | √ | | | ★★ | | √ | -Community medical center and station<br>-Central hospital, specialized hospital, public health bureau<br>-Regional health center |
| m-Health [16] | DE | | √ | | | ★★★ | | √ | -Cloud storage<br>-Medical data mining<br>-Cloud engine-Session cache<br>-Service presentation<br>-Service interaction |
| uPHR [17] | DE | | √ | | | ★★ | √ | | -Medical equipment MD<br>-Concentrator CD<br>-Host system HS<br>-Third party host system |
| CF [18] | CS/DO | | | √ | ★★★ | ★ | | √ | Unkown |
| healthTicket [19] | CS | √ | | | ★★ | ★ | √ | | -Mobile devices<br>-Cloud storage<br>-Medical institutions |
| DEPR [20] | DC | | √ | | | ★★ | √ | | -Ontology<br>-Model driven event |

C:Centralized,D:Distributed,H:Hybrid,S:Security, E:Efficiency, T:Transmission, P:Processing; ★:Low,★★:Medium, ★★★:High; √:Yes

challenges of a scalable, resilient, and interoperable distributed architecture. The CMIoT [6] model is a heterogeneous component model used to study the community medical IoT. Taking the community as the application object, relying on the medical sensors of the medical IoT, and taking the IPv6 gateway device as the communication bridge, it constructs a communication model to provide community medical services in a ubiquitous environment.

## III. Modeling and Verification

### A. Traditional Modeling Methods of Embedded Systems

Embedded systems are the cores of CPS. Traditional modeling methods of embedded systems can be divided into formal methods and informal methods according to whether they support formalization or not. In formal methods, symbols and mathematical languages are used to describe system properties, such as algebraic languages, including OBJ, clear, ASL, ACT One/Two, and so on; process algebraic languages, including CSP, CCS, Π calculus, and so on; sequential logic languages, including PLTL, CTL, XYZ/E, UNITY, TLA, and so on; and network languages, including Petri nets [21]–[24], UML [25], FSM, and so on. The main limitation of Petri nets is that, with the increase in the system design scale and structure complexity, the difficulty of understanding the system increases sharply, resulting in poor readability. FSM is mainly composed of states and migration conditions. When the scale and structure of the design and development system become huge and complex, the number of states may explode, and the migration conditions may expand. In addition, FSM lacks explicit support for concurrent execution and hierarchy of computing systems. Informal methods, such as structured methods and object-oriented methods, can generally describe the functional attributes of the system, but the description of some nonfunctional attributes has certain limitations and is not conducive to strict verification through mathematical methods.

According to the elements of modeling objects, it can be divided into process-, task-, and component-based methods. The component-based approach includes object- (such as real-time UML), middleware- (such as COBRA, EJB, DCOM, SOM, and other business specifications), role-, domain-, and resource-oriented technologies.

According to the view classification of system description, it can be divided into state-oriented (such as FSM and Petri nets), activity-oriented (such as data flow diagram and control flow diagram), structure-oriented (such as component connection diagram), data-oriented (such as entity relationship diagram and the Jackson diagram), and heterogeneous models (such as control/data flow diagram).

According to the classification of development methods, there are two methods: top-down (such as Simulink, SDL, and statecharts) and bottom-up (such as HDL, UML, IDL, ADL, and Modelica). The former design method is suitable for requirement analysis, top-level architecture description, and system evaluation in the process of system development and design. The latter design method is suitable for the system that pays attention to the bottom function design, which is used to describe the specification, modeling, and verification of the bottom architecture of the system. These methods have played an important role in the traditional system design, but they face new problems and difficulties in the CPS collaborative design.

### *B. Modeling and Verification Methods of CPS*

CPS is different from the general pure software system and hardware system, but it is a complex system composed of software, hardware, sensing, control, communication, physics, and other complex factors [26]–[28]. Some functions can be realized by software, hardware, or physical devices. In addition, the CPS design and development process will involve computer nonfunctional properties, such as mechanical size, power consumption, and manufacturing cost. When it comes to the problem of computer functional attributes, that is, the problem of computational engineering, many CPSs have special standards and requirements for reliability, real time, multispeed, and other aspects. With the increasing demand for practical applications, CPS has powerful function changes, huge scale changes, and complex architecture changes so that the requirements for the system design and development process become more rigorous and harsh, and its standards naturally rise. The integration of information and physics in the embedded system involves the coordination of heterogeneous components so that the requirements for embedded systems design are very high. Objectively, the embedded systems in the CPS design should be remodeled, scalable, verifiable, efficient, and low cost, and support collaborative design and verification.

In order to support embedded system design in a heterogeneous environment, OMG proposes model-driven architecture (MDA) method. It is an open framework based on MOF, XMI, CWM, UML, and other standards. Its software design and model building have the characteristics of visualization. It uses XML to transfer and store data information, and separates platform technology and business application logic. It only models for software systems of embedded systems. Driven by MDA, there are various modeling and verification methods to support embedded system collaborative design. Lee [29] put forward a modeling and description language based on Ptolemy, which is structured, hierarchical, heterogeneous, and oriented to “role” and “director.” XML is used as the basic behavior and structure description language to realize the modeling environment for parallel and real-time embedded applications, and it is applied in the fields of science engineering, communication, and so on. At present, this method is mainly used for embedded system and CPS model verification, but it does not have the function of target system-oriented synthesis and compilation, and does not support the implantation of a new behavior model. The DEVS has a simple operation of semantics, but it lacks semantic descriptions of complex systems. Therefore, it has a poor description of system behavior attributes (computational model) and lacks certain openness of system model structure. However, the abstract formal mathematical description method still has a long way to go for specific system modeling. It also has some advantages, such as supporting the concept of time, communication mechanism, and system design structure, completing the automatic mapping from high-level modeling to bottom-level code implementation. In addition, with its rapid development, Modelica is highly concerned by the industry, and many enterprises begin to support this plan. With the support of Modelica, while completing the Acumen project, the research team of Zeng *et al.* [32] proposed the modeling and verification method of the hybrid system, using a continuous function to model a continuous system and carry out the discrete simulation. At present, the Taha team is committed to expanding its behavior description ability.

### *C. Modeling and Verification Methods of MCPS*

MCPS is more and more used in key occasions of the medical field, such as postoperative health care, drug delivery, diagnosis, and chemotherapy. As shown in Fig. 4, it includes some tasks and devices closely related to human life, e.g., every operation of the Da Vinci surgical robot may affect the lives of patients. Therefore, the system should be fully verified before it is put into use to meet the safety requirements. ISO 60601, a standard for medical devices, defines safety as avoiding unacceptable risk to the physical environment (i.e., patients) due to medical operation. The standard lists seven aspects of safety, including operation (error-free operation of medical equipment software), radiation (X-ray radiation safety), thermal (thermal safety of medical equipment operation), biocompatibility, and so on. The basic goal of all safety aspects is to avoid medical devices causing harm to patients.

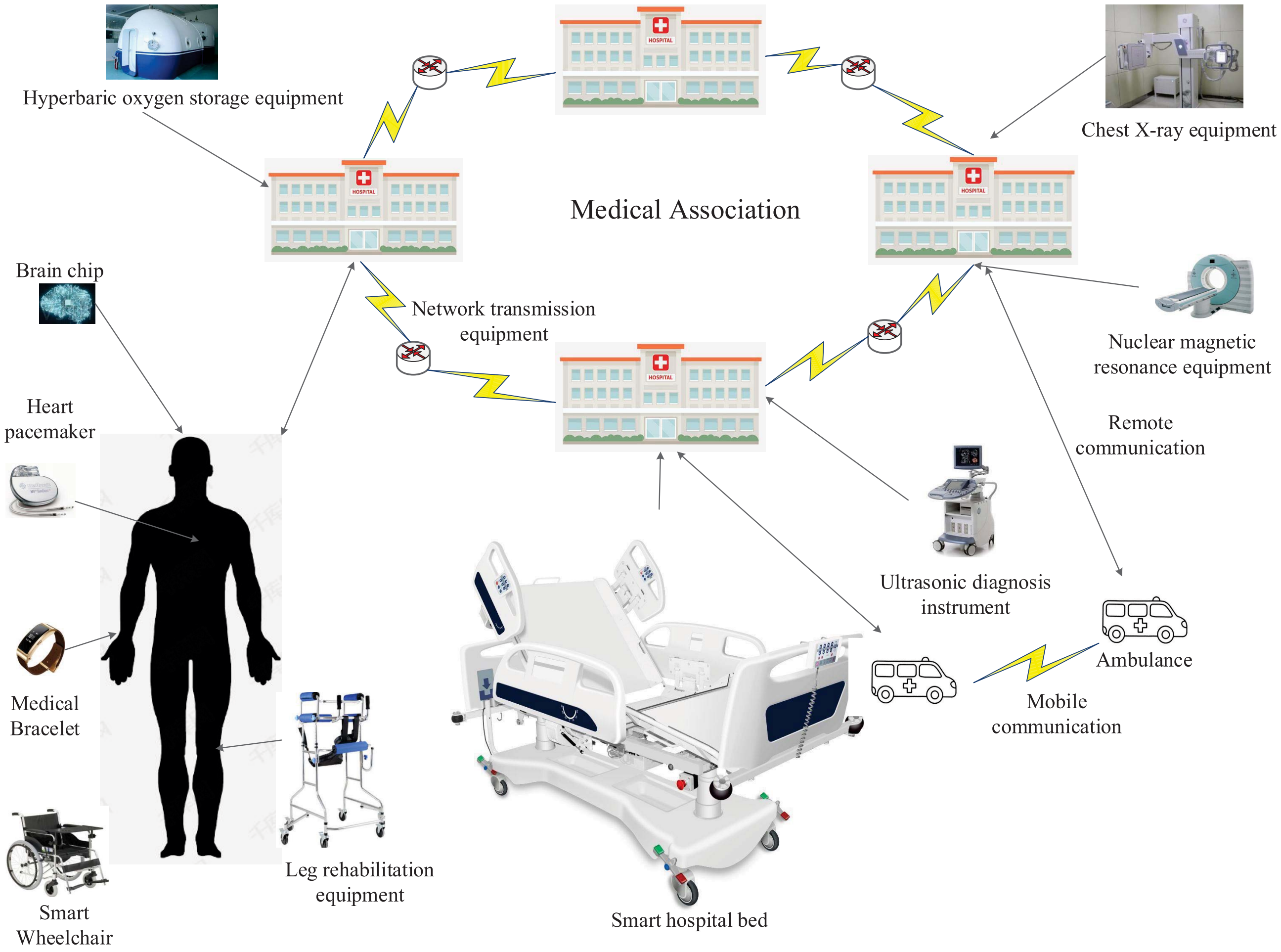

Fig. 4. MCPS.

Banerjee *et al.* [33] proposed an MCPS modeling and verification framework CPS-MAS for security verification. In this method, the operation of MCPS is regarded as a determining step in the algorithm and simulated as a state machine, and an abstract MCPS model is established. Then, the abstract models are analyzed under the given operating conditions, and the changes of system characteristics expressed by model parameters are obtained. The model parameters are compared with the security requirements expressed by constraints, and the security of MCPS is analyzed.

Murugesan *et al.* [34] proposed an end-to-end model-based method for medical device software development, which describes the proposed method through system model establishment, model verification, code generation, code execution, and so on. Taking the analgesia infusion pump as an example, the model is established through the MathWorks simulation tool to study the possible behavior of the system in the expected environment, so as to determine the accurate demand.

Lenardo *et al.* [35] also thought that patient safety is the main concern of MCPS, and the MCPS system needs to go through a strict verification process to ensure its correctness and standardization, and meet the needs of users. Silva *et al.* [35] proposed a model-based method that enables system developers to build an MCPS specification model based on patient and medical device model library and effectively simulate illegal behavior in the design phase.

According to the U.S. Food and Drug Administration (FDA) medical device recall database, at present, the medical device recall rate is at the highest level in history. One of the main reasons for the recall is the implicit assumptions about the physical or network components of the system, including the underlying agreements that are not clearly documented during the system development cycle. Taking Hamilton-T1 ventilator as an example, the internal oxygen consumption of pediatric patients during ventilation is seriously higher than expected, which will lead to the depletion of oxygen supply in the process of transportation and directly threaten the lives of patients. Fu *et al.* [36] pointed out that the constant in Hamilton-T1 ventilator internal oxygen consumption calculation formula was initially set for adult patients, and there is an implicit assumption that the internal oxygen consumption calculation formula is used for adult patients, while, for children, the constant will lead to very dangerous consequences. In order to avoid the threat caused by the implicit hypothesis, Fu *et al.* [36] proposed IAfinder (implicit assumption finder) that is used in the MCPS domain model verification. Based on data mining technology, IAfinder can extract implicit assumptions efficiently and automatically from the state diagram design model so that experts in related fields can verify them, and the verified implicit assumptions can be displayed.

*1) MCPS Modeling Based on ICE:* In MCPS, an integrated clinical environment (ICE) is a conceptual functional model and standard, which establishes the requirements for the safe integration of medical equipment and other equipment in medical systems [37]. Based on this conceptual model, researchers build a medical system model to assist the system design and improve the antierror ability. ICE can be regarded as a high-level framework for MCPS description.

Based on ICE, Jiang *et al.* [38] provide an environment for closed-loop testing, in which the patient model, especially the human heart model, is the control center of the pacemaker system, and its goal is to evaluate the safety and effectiveness of the device operation according to the patient's condition. Miller *et al.* [39] proposed a digital model-based method as an MCPS testing method. In this method, the model is used to test the medical device and evaluate its function by providing input and analyzing the output. The application scenarios of this method are, for example, mechanical ventilation devices connected to an artificial lung model. Murugesan *et al.* [41] considered component verification of medical system at multiple levels of abstraction and adopted different forms at different levels. It establishes a general, extensible, and practical method for hierarchical verification of attributes in complex MCPS.

However, the ICE-based model has some limitations. First, the ICE model is limited to the specific use of the system, and the patient and device models cannot support the new clinical environment so that the reusability of the model is low. Second, physical process simulation ignores important aspects of clinical scene dynamics, including external interference (such as user intervention) and the specific response of each patient to the same stimulus (such as drug supply). Third, the patient model either focuses on the relevant variables of specific clinical scenarios or ignores the relationship between the four vital signs (heart rate, respiratory rate, blood pressure, and body temperature).

*2) MCPS Modeling Based on Role:* For software system design, object-oriented methods are usually used. At present, the more popular object-oriented programming languages include Python, Java, C++, C#, and so on. The interface of an object is a method, which is a program used to modify and observe the state of an object. Using the object-oriented method, communication can only be realized by calling methods between objects. It is obvious that this method can only realize the sequence control transfer of programs, which is not conducive to the construction of the concurrence model. The role is a component in the system, which is different from the object. The interface of the role is port, which is mainly used for data transmission and reception. The system constructed by the role-oriented method separates the data transmission and transmission control, and emphasizes the causal relationship and concurrent behavior between the systems. Therefore, it is more suitable for CPS system modeling with mixed heterogeneous and dynamic concurrent characteristics.

Lenardo *et al.* [35] used role-based simulation model to carry out early verification of MCPS system. A reusable model library composed of patient model and device model is provided. The patient model is based on medical guidelines and a clinical database. The equipment model is built according to the technical specifications of sensing equipment and executive equipment. The model is built as a reusable component with the Ptolemy II modeling tool, which can be reused in different MCPS systems. It can also be adjusted and extended to meet the unpredictable MCPS design requirements.

*3) MCPS Modeling Based on Component:* Component technology is a new system development method. According to the system structure and function, the complex system is divided into independent modules. Each module can have a hierarchical structure, and there is a unified connection standard between the modules. For users, it is not necessary to know the details of each module's function implementation and just need to know the module's function and the provided connection standard, then the model can be constructed quickly, and the simulation and verification of the model can be realized. The component applied in the field of MCPS can be called the MCPS component. MCPS component refers to the basic elements of the MCPS system, which has independent attributes, composition structure, and behavior method. The interface of the component is the port, which is used for data transmission and reception. Components are connected and work together through ports. Combined with the idea of CPS hierarchical modeling, components can be divided into multiple levels. Therefore, components can be divided into atomic components and composite components. Atomic component refers to the component at the bottom, which cannot contain other components and has the most basic properties and methods. A composite component is at the top of the component hierarchy, which can contain multiple atomic components or other composite components, and has a relatively complex structure and function.

Based on component technology, Liu *et al.* [6] proposed a component collaborative modeling method XModel applied to MCPS, which constructs different types of components according to different functions of medical devices and designs a set of communication mechanisms between components according to the characteristics of MCPS network communication. At the same time, visual modeling is used to complete the connection between components and the construction of the model, so as to realize the dynamic simulation execution of the model. As shown in Fig. 5, the basic component library, including physical, sensing, control, computing, communication, transmission, and storage components, and MCPS component library, including user, sensor node, gateway, channel, router, and server components, are established. Based on the component library, a method for verifying the IPv6-based MCPS data path is constructed, and the verification of the 6LoWPAN scheme and the ConnID scheme is completed.

## IV. Identification and Sign Sensing

### A. Identification

The unique identification of nodes in MCPS is a necessary condition for secure access authentication and effective communication between nodes. There are essential differences between node identification and node network address. Node

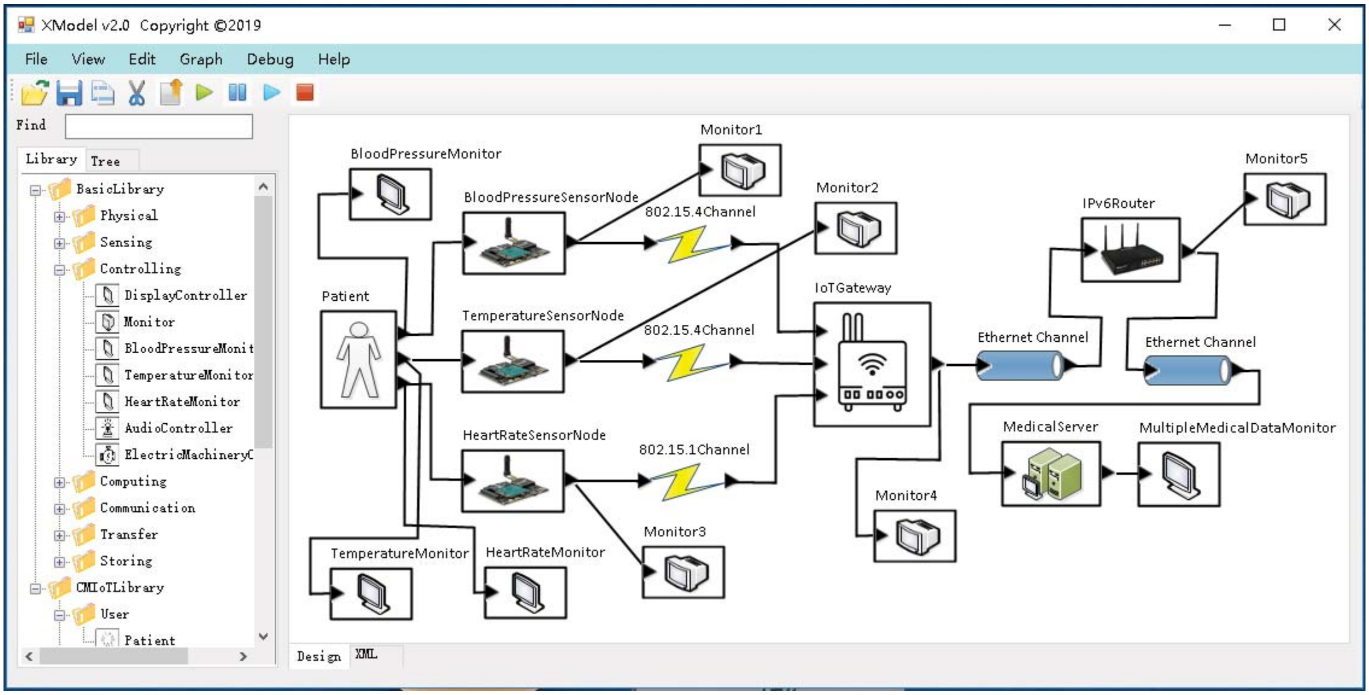

Fig. 5. XModel.

network address may change with the change of network address allocation strategy or network location, but node identification should always remain unchanged. How to ensure the unique identification of nodes in the global network of MCPS system, so as to realize the secure access authentication and effective communication between nodes, is an unavoidable problem in the field of MCPS research.

*1) Tag Identification:* In the field of traditional IoTs, there are many technologies that can be used for the unique identification of objects, such as bar code, electronic product code (EPC), quick response (QR) code, and radio frequency identification (RFID). These technologies can be summarized as tag identification technology.

In hospitals, if patients have serious medication errors, the incidence rate and mortality rate will be significantly improved. Combined with the scanner, computer software, and bar code-based unit dose drug packaging, the Bar Code Medication Administration (BCMA) technology is used in the hospital emergency room and effectively reduced the medication error rate and improved patient safety. BCMA [43] can reduce drug management errors by conducting five checks in drug management (correct patients, correct drugs, correct dosage, correct route, and correct time). Compared with the traditional bar code, QR can store more information and represent more data types. QR uses several geometric bodies corresponding to binary items to represent the text value information and realizes automatic information processing through automatic recognition by the input device or photoelectric scanning device. Kavitha *et al.* [45] proposed a QR-based medical image authentication mechanism, which uses a zero watermark scheme based on a support vector machine. A QR containing the HL7 information segment is used as a watermark, which contains the patient's ID information and detailed clinical data. At the same time, Kavitha *et al.* [45] further analyzed that the proposed scheme could effectively resist various network attacks, achieve effective identity authentication of medical images, effectively protect the patient's identity, and provide clinical data of patients to doctors remotely.

EPC and RFID are related. The RFID tag is the carrier of EPC. EPC can only be identified when stored in an RFID chip. Sanchez *et al.* [44] believes that, in the RFID system, the identification process is the most important. The traditional identification method based on one reader and a group of RFID tags is called the centralized method, and a distributed method applied in the identification process is introduced. This method separates the transmission and reception functions of the reader and replaces the reader with a new device called an illuminator. At the same time, another new device, the RFID listener, is introduced into the RFID network. Taking the large RFID system as the research object, the centralized method is compared with the distributed method. Through the analysis, it is concluded that the distributed or parallel implementation of the identification process not only reduces the delay but also greatly reduces the implementation cost.

Although tag identification technology has been very mature and widely used, these technologies require a corresponding reader within a specific distance from the object in order to read the object identification. Therefore, these technologies are still difficult to verify the unique identity of the nodes in the access network.

*2) Physical Identification:* In traditional computer networks and wireless sensor networks, the MAC address of a node is usually used as the global unique identification of the node in its specific network. For example, in Ethernet, the

MAC address of the Ethernet card can be used as the unique identification of the host within its network scope. In the ZigBee network, the MAC address of the ZigBee wireless module can be used as the unique identification of the ZigBee node within its network scope.

However, for MCPS with mixed heterogeneous characteristics, the MAC address is difficult to be used as the unique identification of global communication. In MCPS, there are various types of nodes and different types of communications, which leads to the widespread existence of the heterogeneous network, and the scenario of heterogeneous network communication is inevitable. Due to different communication technologies, different types of nodes have different MAC address formats. For example, ZigBee and WirelessHART nodes based on 802.15.4 standard adopt 64 bit MAC address, BLE nodes based on 802.15.1 standard, and Wi-Fi nodes based on the 802.11 standard adopt 48-bit MAC address. At the same time, the MAC address allocation method and the meaning of the address field are different. Therefore, it is difficult to ensure the unique identification of the node in the global network in MCPS, which integrates a variety of wireless communication technologies.

*3) Logical Identification:* As we all know, the IPv6 address belongs to the network layer address. Although it has 128 bits of length and massive address space, it  does not mean that the IPv6 address assigned to a node in the network must be fixed, that is, it does not mean that the IPv6 address can be directly used as the unique identification of all nodes in MCPS. However, the 64-bit interface identification field of the IPv6 address provides the system designers with the space to design the global unique identification of nodes. In MCPS, we can adopt a unified interface identification generation scheme. The generated interface identification can be used as a part of the IPv6 address and the unique identification of nodes in the global scope. Theoretically, the maximum number of nodes that can be identified is $2^{64}$, which is still a very large order of magnitude, enough to support the unique identification of MCPS nodes in the global scope. This scheme is called IPv6 address fusion identity.

IPv6 address fusion identification can not only effectively realize the global unique identification of MCPS nodes but also realize the data communication without increasing the network packet overhead due to the transmission of node identification. Because the node identification directly exists in the source and destination address fields of the network message, for the sender or receiver of the network, the node identification of the other party in the network communication can be verified by extracting the node identification from the source address or destination address of the network message.

### B. Sign Sensing

*1) Vital Signs' Data:* Breath, body temperature, pulse, and blood pressure are the four vital signs of the human body. They are the pillars to maintain the normal activities of the body. Any abnormality can lead to serious or even fatal diseases, and accordingly, some diseases may also lead to the change or deterioration of these four signs. The vital signs of normal people have internal relations with each other and are relatively stable in a certain range. When the human body suffers from disease or injury, abnormal changes of body temperature, pulse, and blood pressure will first appear in varying degrees, reflecting a dynamic process of disease from occurrence and development to recovery. Therefore, monitoring and recording of human vital signs provide an important basis for correct clinical diagnosis and timely treatment. At present, most medical institutions can only measure the vital signs of patients at a fixed time, which cannot obtain the vital signs' data of patients in real time, so that it is difficult to realize the real-time analysis and accurate treatment of the disease.

In the medical field, there is a more professional and strict division of human vital signs' data, and the specific measurement quantity is shown in Table II.

MCPS relies on all kinds of perceptible, interactive and controllable smart objects [46] to continuously and effectively monitor the changes of vital signs of patients [47]. At the same time, the computer equipment integrated with specific functions will feedback the analysis and processing results to the medical staff, patients, or their families in real time according to the monitored data information, so as to grasp the patients' physical conditions in time, and the medical staff can also formulate targeted medical plans in time, so as to promote the realization of the patient-centered medical pattern.

*2) Sign Sensor:* As the front-end antenna of MCPS, the sign sensor is used to collect the vital signs' data of the human body, which is the basis and starting point of MCPS operation. Its timeliness, accuracy, and convenience play a decisive role in the effective function of the whole MCPS.

According to the different classification bases, sign sensors can be divided into many categories. According to the different ways of contact with the human body, it can be divided into noncontact sensors, contact sensors, and intrusive sensors. The noncontact sensor can generate a signal without any contact with the human body, while the contact sensor must contact with the human body to generate a signal. Taking the human body temperature measurement as an example, the contact temperature sensor needs to be attached to the human body surface when measuring temperature and can only measure the temperature after the human body and the sensor reach the thermal balance, so its response time is long. The noncontact temperature sensor, such as infrared temperature sensor, whose temperature measurement is based on the infrared radiation energy of the measured object to determine the temperature of the object, does not contact with the measured object and has the characteristics of the high-temperature resolution, fast response speed, and good stability. An intrusive sensor is also called an implantable sensor. It can be directly implanted into the human body to collect vital signs' data, so as to obtain more accurate signs' data. Of course, implantable sensors are not only limited to data acquisition but also play an important role in the treatment and repair of human organs. For example, implantable bionic eyes can help blind patients regain their vision, and implantable medical robot arm can help patients with limb deformities regain their ability of action.

According to the different working principles, the physical sign sensor can be divided into strain sensor, capacitive sensor,

TABLE II
QUANTITIES TO BE MEASURED IN VITAL SIGNS' MEDICINE

| Type | Signs |
|---|---|
| Displacement | Skin thickness, subcutaneous fat thickness, cardiac displacement, etc |
| Vibration | Heart sound, sound, breath sound, blood vessel sound, etc |
| Force | Blood pressure, myocardial force, intraocular pressure, intragastric pressure, etc |
| Flow | Blood flow, respiratory gas flow, blood loss, etc |
| Temperature | Skin temperature, breathing temperature, blood temperature, etc |
| Chemical composition | Oxygen, carbon dioxide, carbon monoxide, blood glucose, blood lipid, triglyceride, water, etc |
| Biological components | Proteins, bacteria, viruses, etc |
| Radiation | X-ray, isotope dose, etc |
| Bioelectricity | ECG, EEG, EMG, electrooculogram, electrogastrogram, etc |

inductive sensor, piezoelectric sensor, magnetoelectric sensor, thermoelectric sensor, photoelectric sensor, and so on. According to the measured quantity, the sign sensor can be divided into vibration sensor (such as heart rate sensor), pressure sensor (such as blood pressure sensor), temperature sensor (such as body temperature sensor), and so on, which are used to measure different vital signs of the human body.

*3) Development and Challenges:* In MCPS, as a basic technology, physical sign sensing technology will develop along the direction of intelligence, miniaturization, multiparameter, remote control, and noninvasive detection in the future. At the same time, with the research and promotion of some new sensors (such as DNA sensors and bionic sensors), it provides an important driving force for the development of modern medicine, and the physical sign sensing equipment will eventually enter the implantable era from the portable era.

The development of sign sensing technology has brought rapid changes in the field of health care. However, at present, sign sensing technology is still facing many challenges.

1) *Accuracy:* Different from other fields, the physical sign sensor applied in the medical field has extremely high requirements for accuracy and sensitivity, which may cause inestimable consequences to human health due to subtle errors, which is a great challenge for the physical sign sensor technology.
2) *Size:* The size of the physical sign sensor is also a problem that cannot be ignored; especially for the implantable sensor, its size is strictly limited by the parts of human organs.
3) *Power:* Energy supply is an important obstacle to the development of a microsensor. In future research, human motion power generation will become the core solution of micro sensor charging.
4) *Biocompatibility:* Implantable sensors belong to foreign objects for the human body and are in the human body for a long time. How to avoid the rejection of the human body and how to ensure the safety of the human body and reduce the harm to the human body, that is, to effectively achieve the biocompatibility of implants, are problems that researchers must consider.

## V. COMMUNICATIONS' TECHNOLOGIES

The core concept of CPS can be summarized as computation, communication, control (3C), that is, CPS is a complex system deeply integrating computing, communication, and control equipment. Communication is the core hub to ensure the effective interaction between the discrete computing process in the network world and the continuous physical process in the real world [48]. As the expansion of CPS in the medical field, MCPS will inherit the 3C characteristics of CPS. Therefore, communication problems should be fully considered in MCPS.

### *A. Layer 1/2 Connection: Wireless Communication Technology for MCPS*

In the emerging field of MCPS, the number of medical sensing devices is increasing, and in order to meet the real-time needs, there will be a lot of network communication data in the network, as shown in Fig. 4. The single wireless communication technology of IoT limits the flexibility of MCPS, and the integration of multiple wireless communication technologies is the trend of MCPS development. Different communication technologies play their unique advantages in specific applications of MCPS, such as the transmission of human health data collected by medical sensors based on ZigBee technology, the identification and information processing of drugs based on RFID technology, and the information transmission of PDA and mobile phones based on low-power Bluetooth (BLE) technology. In addition, Z-Wave, 5G, Wi-Fi, ultranarrowband (UNB), and near field communications (NFCs) are also available wireless communication technologies in different scenes of MCPS.

### *B. Layer 3 Connectivity: IPv6 Technology for MCPS*

IPv6 has a huge address space, which can meet the needs of deploying large-scale and high-density sensor networks [49]. However, at the bottom of the MCPS system, all kinds of sensor execution nodes usually have the characteristics of low power consumption and limited resources. From the hardware level, they cannot directly run the huge IPv6 protocol stack. At the same time, there are a variety of wireless communication technologies in MCPS. Different wireless communication technologies have their own specific communication protocol stacks, and the frame load of the MAC layer of these protocol stacks is also extremely limited, which is basically difficult to carry IPv6 packets.

In 2004, IETF established 6LoWPAN [IPv6 over low-power wireless personal area network (WPAN)] working group to introduce IPv6 into the WPAN based on IEEE 802.15.4.

Two compression schemes of IPv6 header and upper header, including LoWPAN_HC1, LoWPAN_ HC2 [55], LoWPAN_IPHC, and LoWPAN_ NHC [56], have been proposed. In 2008, IETF established the Routing over Lossy and Low-power Networks (ROLL) working group, which focuses on the research and development of an IPv6 routing algorithm for low-power networks [57]. In September of the same year, Cisco, SAP, Sun, and other companies jointly established the IP for Smart Objects (IPSO) alliance to study how IoT nodes with limited resources can communicate through IP protocol. In 2010, the IETF Constrained Restful Environment (CoRE) working group established and proposed the application layer protocol CoAP [58] to meet the application layer protocol requirements of IoT devices with low computing power, small storage, and low power consumption. In 2011, the Framework Program 7 (FP7) established IoT6 [59] project working group to explore how IPv6 and related solutions (6LoWPAN, CoRE, and CoAP) can solve the current problems of the IoTs, and design and deploy IPv6 sensors based on the mobility, security, automatic configuration, and other characteristics of IPv6. In 2013, IETF further established 6lo (IPv6 over networks of resource-constrained nodes) working group [60] to study the adaptation layer supporting a variety of wireless communication technologies, including BLE, DECT ULE, MS/TP, G.9959, IEEE 1901.2, NFC, IEEE 802.11ah, and so on.

The GLoWBAL IPv6 solution proposed by Jara *et al.* [61] not only supports the combination of IEEE 802.15.4 devices and IPv6 technology but also supports the combination of other wireless communication technologies (such as BLE) and IPv6 technology. The access address identifier (AAID) is defined in the GLoWBAL IPv6 scheme, and the AAID-IPv6 conversion mechanism is applied to realize the combination of various wireless sensor network communication technologies and IPv6 technology. Jara *et al.* [62], [63] further proposed the IPv6 address proxy scheme, which mapped the data frame effective fields of EIB/KNX, X10, CAN, RFID, and other traditional communication technologies to the IPv6 address interface identifier field and realized the access of traditional communication technologies to IPv6 Internet through the multiprotocol network card.

Xiao *et al.* [64] proposed an IPv6 oriented TFAD model, in which the IoT subnet appears in the form of a hierarchical routing and forwarding tree. At the same time, each node in the IoT subnet can automatically configure the IPv6 address according to its hierarchical structure in the tree. In addition, the IPv6 addresses of nodes in the tree also achieve effective aggregation. On the basis of the TFAD model, Xiao *et al.* [65] further proposed the IPv6 hierarchical address compression mechanism (IACH), which uses the IPv6 address inheritance relationship of parent-child nodes in the hierarchy to ensure that the most concise address form is used in the forwarding process of IPv6 packets.

## VI. Data Storage and Analysis

According to the statistics of 158 papers related to MCPS from 2013 to 2019, some mentioned data storage and access control. In the change process of keywords, such as smart health/medicine, fog/edge/cloud computing, MCPS, medical IoTs, big data, blockchain, an data sharing, we can clearly feel the change of data storage technology applied in MCPS, and smart medicine is always running through it. The storage technology includes big data, fog computing, cloud computing, and other related discussions and has developed to today's blockchain technology. Before 2016, most of the data storage technology is not described and discussed in detail. In the literature after 2016, there are more descriptions of data storage technology, i.e., Health-CPS, MCPS assisted by cloud and big data, mining rare patterns in an intelligent medical environment based on data aggregation, and the analysis of the performance of the implementation of personal health record based on blockchain, which is closely related to the development of novel data storage technologies. The introduction of data mining and blockchain technology also has a huge impact on the data storage mode in MCPS, especially in data sharing, personal records management, EMRs, and other medical-related fields.

### A. Database

The database is the storage place of electronic documents or data. Users can add, query, update, and delete the data in the documents. It also refers to the dataset that is stored together in a certain way, can be shared with multiple users, has as little redundancy as possible, and is independent of the application. Common relational databases include MySQL, MariaDB, Percona Server, PostgreSQL, Microsoft Access, Microsoft SQL Server, Oracle, OceanBase, and so on.

The database is widely used in the field of medical data storage. Gillies *et al.* [66] proposed to store the EMR in the database, analyzed some defects in the existing database query technology, and proposed a more efficient query method and web service architecture, which can be extended to multiple databases. Xu *et al.* [67] proposed to develop a comprehensive medical supply information system, in which a data network is established to link patient data, inventory data, service information, supplier information, and doctor information from various sources and store them in the database. Through the link and integration of information in the database, the relationship between the use and management of medical supply can be analyzed and studied by using the decision support model. Wu *et al.* [68] found that the community health care center is mainly composed of the database server, nursing center workstation, and medical staff, in which personal information, monitoring data, and doctor information are stored in the database.

Some groups have jointly established databases to store public medical data for open source and research, such as the Cochrane collaboration. It is composed of researchers, medical professionals, patients, and nurses from all over the world. It aims to improve the efficiency of health care interventions by producing, preserving, disseminating, and updating systematic reviews. Cochrane has established six databases, including the systematic review database, the central registration control experiment database, the methodology database, the systematic review summary database, the health technology assessment database, and the economic assessment database. The database keeps dynamic updates, which is conducive to the learning and research of various scholars.

### *B. Big Data*

With the development of information technology and IoTs, information is growing explosively. Big data refer to complex datasets that are difficult to be effectively and economically stored, managed, and processed by traditional data management systems. Big data bring challenges in data storage, management, and processing, as well as opportunities to explore new values in data.

Because complex data are difficult to be processed by traditional database management and data analysis tools, the management and analysis of medical big data involve many different problems, such as the structure, storage, and analysis of medical big data. Azar *et al.* [69] proposed using a new classifier to deal with medical big datasets. The introduction of big data processing technology has brought new opportunities and efficiency improvement to medical big data processing. Suitable big data processing technology saves a lot of computing time.

Big data processing technology includes association rule learning, classification, cluster analysis, data fusion, machine learning, natural language processing, regression, signal processing, and so on using big data processing, and the analysis technology can improve diagnostic accuracy, improve the curative effect, and reduce cost and waste. Din and Paul [8] proposed big data processing and decision management of healthcare, including energy collection and data generation, data preprocessing, and data processing and applications. In order to protect the privacy of Covid-19-related medical big data in the cloud, Ma *et al.* [70] proposed a privacy-preserving word embody-based text classification method for mining COVID-19 medical documents. Big data processing technology has brought new solutions to the data processing of MCPS [71].

### *C. Cloud Computing*

Cloud computing as an effective computing model can be applied to the regional medical data center to provide storage and computing solutions for a large number of medical data. The regional medical data center is the service of cloud computing platform [72].

Cloud computing can not only play a huge role in medical big data storage but also can be applied in other medical-related fields. For example, in the medical image information system, cloud services and cloud computing environment can be used, which can not only reduce the number of high delay image transmissions but also reduce the response time [73]. The edge computing function in cloud computing and the next-generation wireless network technology realize intelligent medical treatment, including the concept of local edge cloud, which can enable complex data analysis methods for data storage, pattern detection, trend discovery, and population health management. It can be used in hospitals to monitor and record the status of patients while providing necessary help [7].

### *D. Blockchain*

Medical data have some unique characteristics, which needs to both share in real time and protect the privacy of patients. The verification, storage, and synchronization of medical data have always been difficult. Traditional medical data access needs to spend a lot of resources and time for permission review and data verification, which has great risks and permissions. Therefore, some scholars apply blockchain technology to the sharing of medical data. The essence of blockchain is a decentralized database, which is characterized by decentralization, openness, tamper-proof, anonymity, and traceability. In order to improve the response speed, prevent data tampering, and better realize data sharing, Xue *et al.* [74] proposed to use blockchain technology to solve the problem of medical data sharing and ensure the security of medical data storage.

In order to solve the problem that personal health records and electronic health records (EHRs) are usually scattered in multiple places and not integrated, Roehrs *et al.* [11] proposed the Omniphr architecture model, which describes the infrastructure supporting distributed and interoperable phr. The implementation of the model was evaluated using datasets of more than 40 000 anonymous adult patients in two hospital databases, and the distribution and reintegration of the data were tested to form a single view of health records, achieving 98% availability. Huang *et al.* [75] proposed a secure data sharing scheme for the smart medical system, which combines blockchain, smart contract, and zero-knowledge proof to reduce the contradiction between patient privacy and health data research or business needs.

At the same time, many enterprises also realize that blockchain technology can be closely combined with medical data and applied in the direction of medical data sharing. Medilot is a decentralized medical platform based on blockchain, artificial intelligence, and database management system technology, which is aimed at patients, healthcare providers, researchers, and commercial companies. The MCPS project is implemented to allow medical practitioners to securely access patients' health records and use the collected data for predictive health reports. A private blockchain framework BlockBench [76] and an efficient storage engine ForkBase [77] for blockchain and bifurcation applications are proposed, which are supported by the National University of Singapore and a number of medical institutions. Gem Company has developed a medical and supply chain management blockchain application Gem medical network, which is based on the development of Ethereum, and the security will be increased through the permission chain so that patients can control access, and any changes will be recorded in a shared accounting system.

### *E. Problems and Challenges*

With the rapid development of IT and IoT technology, the amount of medical data is growing exponentially, and the storage and processing of a large number of medical data have become a new challenge. The traditional database for the storage and processing of a large number of medical data has some defects, such as slow transmission speed, high computational resource consumption, and low processing efficiency. Big data, cloud computing, and blockchain technology have brought new solutions for the storage and processing of medical data. At the same time, these technologies have the advantages of saving computing time, improving processing efficiency, and high security when dealing with a large number of medical data storage and processing problems. Also, it will bring new problems and challenges, such as storage security, resource consumption, and so on.

## VII. Monitoring System

Monitoring is very practical in MCPS, and it is a very important and necessary part of the hospital information system (HIS). It is responsible for the data collection and monitoring of each part of MCPS, providing traceability queries for the accidents and conditions in the medical system, and providing real-time queries for the patients' conditions and conditions. The monitoring system, including remote monitoring system and mobile monitoring system, is a medical system that monitors various vital signs' parameters. The remote monitoring system is applied in the scene of security monitoring of outpatient and inpatient buildings, supporting 24-h monitoring of patients in ward and intensive care unit (ICU), operation observation and learning in the operating room, and consultation of doctors. The mobile monitoring system is mainly composed of wearable medical sensing instruments and implantable medical devices (IMDs) (cardiac pacemaker, insulin pump, and so on) to collect patients' data and condition in real time. The most direct application of the medical monitoring system is the critical emergency ward and operating room, which can record the diagnosis and operation process, and provide comprehensive and reliable treatment processes for patients. The monitoring system is conducive to the standardized management of the hospital and improves the diagnosis and treatment of patients and nursing levels. At the same time, it can save the video of the operation process, help to solve medical disputes, and distinguish responsibility. Considering the convenience of users' use and maintenance in the future, the monitoring system of MCPS must be based on the requirements of the hospital, in line with high standards and high quality, improve the performance price ratio of products, and fully reflect the current digital trend in design.

With the development of artificial intelligence, big data, and cloud computing technology, the monitoring system in the medical environment is constantly improved combined with new technologies to provide patients and medical staff with a more intelligent, traceable, private, and real-time monitoring system. Baig *et al.* [78] selected and classified more than 50 different health monitoring systems (HMSs), investigated and analyzed the efficiency and clinical acceptability of HMSs, and gave a strategic critical analysis. Chiuchisan *et al.* [79] introduced the development of Parkinson's disease intelligent system and the application of a family monitoring system in assisting and supporting doctors in the diagnosis of Parkinson's disease. Liu *et al.* [80] proposed a new type of ECG automatic diagnosis system, which can carry out real-time ECG diagnosis and timely medical assistance for people in need. The system consists of three parts: data acquisition subsystem, deep learning analysis subsystem, and background management subsystem. Saha *et al.* [81] proposed to use some sensors and microcontrollers to provide an intelligent health system, which can sense the physical condition and send the data to the website of the cooperative hospital. If the condition is serious, the ambulance will be assigned to the specific location of the patient. In order to solve the phenomenon of scattered and isolated patient data, Costa *et al.* [82] investigated different methods of collecting and combining hospital vital signs' data, and proposed to combine the patient data in hospital wards to improve the efficiency of information processing. Mardini *et al.* [83] emphasized the dependence of chronic diseases and the elderly on the medical monitoring system and found that, in recent years, patients' requirements for medical monitoring have become higher and higher. Tuli *et al.* [84] proposed a novel framework named HealthFog, which is used to integrate integrated deep learning into edge computing devices and deploy it to the practical application of automatic heart disease analysis. HealthFog uses IoT devices to provide medical services as fog services and effectively manages the data of patients with heart disease according to the requirements of users.

### A. Key Characteristics

*1) Safety:* In MCPS, safety means that the auxiliary medical system will not threaten people's safety and can alarm in time to meet the high requirements of medical staff and the national information department for early warning. Safety in MCPS is embodied in personal safety, operation safety, physical safety, and the ability to resist attacks. More scholars consider information security and data leakage in the process of medical system informatization. However, as MCPS is closely related to life, we should consider personal safety and possible accidents, so as to avoid accidents caused by decision-making mistakes, which will cause life harm to patients or operators. From the perspective of CPS, it is to protect the physical components and ensure the credibility of the device so that the physical environment and its application determine the safety of MCPS.

MCPS controls the embedded medical equipment through the wireless network and the RF signal, which has the functions of perceiving the life symptoms of patients, and constantly monitoring and collecting the medical data of human body. Once the patient's body has problems, the equipment must be able to give early warning in time, inform the medical institution of the disease in time, and upload the emergency medical data to the server. In MCPS, a large number of MCPS safety cases are given [85], and the physical attacks and information attacks that MCPS is vulnerable to are compared. The safety of MCPS is guaranteed from the perspective of engineering and structure. Wu *et al.* [86] proposed a workflow adaptation and validation protocol to help doctors safely adjust the workflow according to the pathophysiological model to respond to patients' adverse events. AlTawy [87] classified and compared different proposals for the concept of emergency authentication and attempted to balance the tradeoff between the safety measures of IMDs in emergency and the safety of patients. Chen *et al.* [88] designed a safety monitoring technology using the maximum model and online training of computing virtual subject (CVS) set, and the safety of the technology was verified in the case study of surgical blood glucose control. Based on the IEEE 11073 interoperable medical device communication standard, the monitoring service is provided in the operating room of MCPS through authentication technology [89]. The interconnection case of ultrasound dissector and microscope is used to prove that the cost of this monitoring is lower than that of the practical monitor. By identifying the potential security threats of Internet-of-Medical-Things (IoMT) devices, Anandarajan *et al.* [90] used situational crime prevention theory to propose control mechanisms in order to reduce the possibility and impact of such threats.

*2) Reliability:* There is no doubt that wireless communication technology, mobile platform, and biosensor technology have provided effective technical support for people in the field of health care. With the development of mobile communication technology, people are more and more inclined to use wireless devices in medical monitoring systems. However, wireless communication is more vulnerable to interference than wired communication. Considering the security and confidentiality of patient information, the main standards of the patient monitoring system should include reliability, efficiency, and environmental awareness. To ensure that the information system and the physical system of MCPS will not fail, and to ensure the accuracy of the information provided, is the goal of a reliable medical monitoring system. It is very important to comply with medical standards and provide high-quality data transmission in MCPS. Realizing the reliability of medical monitoring system is the most basic guarantee for medical work.

Reliability is very important in embedded medical devices, especially the application of wearable devices in MCPS. Wearable devices are used as intelligent medical monitoring devices to provide real-time feedback to patients. Patients can wear the devices in their normal daily activities. At the same time, medical staff can better know the patient's condition than the short-term monitoring of the hospital or doctor's office. In order to prevent the devices from being abnormal, their reliability in MCPS is required. Once the medical devices are abnormal, the life of patients will be threatened, which will have a great impact. The difference between wearable devices and medical perception devices is that the former is worn by patients and the latter is placed and used by medical staff. For all medical devices, working time is a very important factor, and the data collected by medical devices before the battery runs out unexpectedly must be recovered. For wearable devices that can warn of serious conditions in advance, if they fail or run out of power, they may be life-threatening. Santos *et al.* [91] focus on providing timely and reliable health data through mobile health monitoring programs and fuzzy logic health assessment. Shangguan *et al.* [92] proposed an independent HMS, which not only detects the actual violation of constraints but also calculates the possibility of violation of constraints. This mechanism can quickly and accurately estimate the health status of the monitored system and help to prevent accidents or disasters.

### *B. Architectures*

*1) Independent Private Cloud:* The traditional HIS is based on the central server architecture, which stores the medical data in the server cluster of the data center and manages it through database technology, cloud computing, and other technologies. The trusted third party authenticates and controls the identity of each user, and the key center distributes the key to ensure the security of the real system. The structure of an independent private cloud requires the hospital to have a data center with high computing power, and a safe and trusted third party; the whole system relies too much on the data center. At present, many scholars improve this kind of structure by combining artificial intelligence and mobile computing.

Mohammed *et al.* [93] provide the visualization of electronic ECG and background data records through Android App, upload them to the user's private centralized cloud or specific medical cloud, and save the records of all monitoring data for medical personnel to retrieve and analyze. Li *et al.* [153] carried out all-around safety monitoring and early warning for pregnant women through data transmission between cloud computing centers and mobile devices, doctors, and guardians. Wang *et al.* [95] completed the processing and analysis of medical data through the data interaction between cloud medical service center and the hospital's artificial intelligence system and control system, so as to generate the patient's medical report and provide it to doctors for diagnosis. MCPS with independent private cloud hands over the main data analysis load to the high-performance cloud computing center for processing. Other devices only need to complete the data collection and transmission to meet the lightweight requirements of medical devices, but the computing power and security requirements of cloud computing data centers are very high.

*2) Distributed System:* With the development of distributed computing and blockchain, more and more scholars try to distribute MCPS, add more trusted nodes, make the system have higher security and reliability, make medical sensors analyze and record transaction metadata in real time, backup and store on multiple devices, and enhance the nonrepudiation of medical data. A distributed medical monitoring system can realize the sharing of medical data, improve the continuity of medical data time dimension, maintain the integrity of medical data, and provide protection for the privacy of patients' personal medical data. MCPS combined with all kinds of wearable devices needs more distributed architecture to ensure the smooth operation of the whole system.

Ahnn *et al.* [96] proposed a distributed energy-saving mobile health monitoring platform named mHealthMo, which considers sensor information collection and energy-saving processing. Griggs *et al.* [97] used the smart contract system in Ethereum to support real-time patient monitoring and medical intervention by sending notifications to patients and medical professionals. At the same time, it can also record all kinds of medical behaviors. The smart device calls the smart contract to write records of all events on the blockchain to ensure the traceability of medical events. In the e-health system based on blockchain proposed by Casado-Vara *et al.* [13], a smart contract is used to realize the transaction between blockchain and wireless sensor network, and distributed architecture is used to provide the medical system with no third-party verification. MCPS of the distributed system will gradually be patient-centered, which can promote the development of personal health management and precision medicine, ensure the integrity of medical data, save multiple data checks, and reduce medical costs.

### C. Technology Requirements

*1) Lightweight:* MCPS requires low energy consumption and lightweight algorithms. Healthcare applications also need small lightweight devices with low computing power and low communication function. These devices need to be installed in inconspicuous and comfortable positions on the body, such as waistband, watch, or vest. Most sensors are used to deploy fixed nodes that transmit data at low rates. Because many patients are not willing to disclose their illness information, in order to protect the privacy of patients, the monitoring equipment must be smaller; the larger the device is, the more cumbersome it is, and the device around the patients is easier to be observed. Therefore, proper power and performance balance is a necessary condition, which requires that the device does not have high computing power and storage power.

Based on the low-power BLE sensor, a solution for monitoring personal vital signs' data was designed to help diabetic patients better manage their chronic diseases [98]. Meanwhile, the classification method based on machine learning was tested on the diabetes dataset, and the results show that the multilayer perceptron can provide early diabetes with the user's sensor data as input to the prognosis of the disease. Lopez-Iturri *et al.* [99] adopted a lightweight communication protocol to minimize energy and bandwidth utilization and provide access control and data tracking functions for ICU. Schalk *et al.* [100] investigated the context-aware wearable HMS and the application prospect of a low-power wireless sensor network in it.

*2) Data Security:* For the medical monitoring system, security is the most important challenge. Patient data communication is generated continuously and transmitted through remote devices. The main security issues include preventing the disclosure of patient data, authentication of legal users, and access authorization of patient medical data and records. Because users often want to keep their data encrypted, they should encrypt the data and ensure their physical security. Although combining different security strategies can better ensure the security of the system, these solutions cannot well adapt to the resource-constrained monitoring system [101]. Thus, in the monitoring system of MCPS, the balance of encryption strength and computing power must be considered. It is not advisable to use a slightly more secure encryption mechanism with higher computing power and storage capacity at the same time. Therefore, in order to achieve security, the bearing capacity of devices in MCPS to computing resources must also be considered.

Mitchell *et al.* [102] proposed an intrusion detection technology based on behavior rules embedded in medical devices in MCPS and took vital signs monitoring medical devices as an example to prove that intrusion detection technology can effectively detect false positives to deal with more complex and hidden attackers in the medical environment. You *et al.* [103] proposed a lightweight specification-based illegal behavior detection technology to detect the illegal behavior of embedded MCPS devices through automatic model checking and formal verification. Medical monitoring technology in MCPS is the basic guarantee of sensing data. If it cannot meet the technical requirements of security, the data will be tampered or leaked, which will have a serious impact on medical diagnosis and treatment.

### D. Application Scenarios

*1) Personal Health Monitoring:* Personal health monitoring is mainly reflected in the family monitoring of the elderly, children, pregnant women and disabled patients, emergency warnings, and so on. According to a report released by the United Nations, the proportion of people aged 60 and above to the total population is expected to double between 2007 and 2050, reaching two billion by 2050. The monitoring of the personal health environment will promote the development of smart homes. The term "smart home" refers to a special type of home or residence, equipped with sensors and actuators, integrated into the residential infrastructure, which aims to monitor the environment of residents and improve the personal experience at home. The monitoring system is an indispensable part. Privacy is the main problem that hinders the adoption and use of home monitoring technology, for example, the possible privacy violation caused by the use of cameras. In personal healthcare [153], monitoring the needs of the elderly or pregnant women in the family is a hot topic. It establishes a cloud computing platform for each pregnant woman user. Based on a secure medical data exchange protocol, it can remotely monitor the pregnancy situation and ensure the privacy of pregnant women when transmitting data. Pregnant women do not need to worry about the illegal acquisition of medical information in the medical environment.

Although the personal monitoring system in the home environment has promoted the development of health care, due to the limited resources of sensors and the dependence of intelligent development on mobile data, further research and development are needed. If the monitored person goes beyond the monitoring range, avoids the perception of the sensor, or shows behavior that cannot be recognized by the sensor, then, even if the monitored person is carrying out normal behavior activities, the monitoring will produce false positives. In addition, the delay of the network connection will also lead to the delay of real-time monitoring data.

*2) Hospital Monitoring System:* The hospital monitoring system is the focus of managers of laboratory, testing and radiation departments, doctors' consulting rooms, wards, nurse's offices, and emergency departments. The demand of a hospital for a monitoring system is very large, and almost all medical occasions need monitoring equipment to collect data, so as to record the medical information and facilitate the hospital's macrounderstanding of patients, people flow, department needs, and other aspects. Lopez-Iturri *et al.* [99] implemented and analyzed the context-aware ICU. The deterministic simulation of the wireless channel analysis was carried out by transmitting hybrid optimized 3-D ray to evaluate the potential interference impact and provide the required capacity threshold for the adopted transceivers. A new design method was provided for the health care construction of the hospital through the case of ICU.

In the MCPS environment, medical staff not only needs to understand the patient's physical condition, medical equipment, and perception of the medical environment but also can monitor the medical staff's own situation through the HMS. Wang *et al.* [95] refer to doctors' past health data from the cloud server and provide appropriate suggestions and predictions about doctors' health status. The proposed doc-care monitoring system can provide doctors with their own health information so that doctors can better diagnose patients.

*3) Smart Medical System:* Medical management departments have a great demand for timely prevention and detection of epidemic situations, prevention of epidemic situations, and supervision of disease. The health management department can call the remote monitoring system to understand the real-time situation of each hospital and analyze the monitoring medical data to understand the latest disease situation. For drug management departments, monitoring data can not only provide the data of the disease and patients but also extract the price data of drugs, the use of medical devices, the detection results of hospital disinfection, and the current situation of infectious disease control and prevention. Without MCPS, medical institutions belong to the information island, with massive medical data resources, but cannot establish effective contact with the outside world. Insurance, pharmaceutical enterprises, scientific research institutions, and other peripheral institutions in urgent need of data support are unable to obtain medical data conveniently and quickly. It is very difficult and costly for enterprises participating in medical insurance to obtain data, which restricts the development of the industry. Breaking through the isolated island of medical information is a very urgent problem at present. Avoiding repeated examination of patients and realizing the sharing of medical data under the condition of ensuring safety can improve the convenience for patients, hospitals, and management departments.

In the process of smart city construction, smart healthcare has always been regarded as an equally important module with smart government, smart grid, intelligent transportation, and other urban information construction projects. The medical monitoring system provides the support of medical data collection and transmission for the construction of smart healthcare. Because of the sensitivity of medical data, the security and reliability of medical monitoring systems are very important, which is directly related to the patient's privacy and the doctor's diagnostic records. The development of medical monitoring technology is very important to improve the medical level of the whole country and build smart healthcare.

## VIII. Data Security and Privacy Protection

### *A. Threats and Requirements*

As shown in Table III, we summarize the possible threats in the MCPS from three security aspects of integrity, confidentiality, and availability. The possible threats in three layers of MCPS are given as follows.

1) *Sensing/Execution Layer:* The sensing/execution layer contains various sensing devices and diagnostic devices. Therefore, it is most vulnerable to physical attacks at this layer. The common threats are node capture, illegal substitution, exhaustion attack, insider leak, and so on.
2) *Network Layer:* For the network layer, attackers may launch attacks during the data transmission phase to capture and tamper with data or break the transmission channel. The attacks that an attacker may launch are selective forwarding attacks, sinkholes, wormholes, flooding, jamming, and so on.
3) *Application Layer:* The application layer of MCPS will process a large amount of sensitive medical data. Therefore, the attacks in this layer will threaten data security and privacy. The possible attacks on the application layer are buffer overflow, identity theft, and so on.

The security and privacy of patient-related data cannot be ignored. Data security means the complete storage and transmission of medical data to ensure its integrity, effectiveness, and authenticity. Data privacy protection means that only legitimate users can access the medical data of patients. The requirements for data security and privacy protection are given as follows.

1) *Data Integrity:* It means that all data values stored in the database are in the correct state. It includes four categories, such as entity integrity, domain integrity, referential integrity, and user-defined integrity. The database uses many methods to ensure data integrity, including foreign keys, constraints, rules, and triggers. The system well deals with the relationship between the four, uses different methods according to different specific situations, and complements each other.
2) *Data Availability:* It is to ensure that authorized users can use data or data systems. Medical big data not only bring huge benefits but also face huge challenges, such as unreliable or inaccurate data. In addition, unauthorized access leading to data loss or destruction will affect the availability of data.
3) *Data Audit:* It is the compliance management of fine-grained audit of database operation, warning the risk behavior of database, and blocking the attack behavior. It is an effective means to monitor the use of medical resources. In addition, cloud service providers who store medical data have a great responsibility and need reasonable audit methods. Audit content usually includes users, cloud service providers, access, and operation process.
4) *Information Privacy:* Patient information records can be divided into two categories. One is general records, which refers to records that can be publicly accessed. The other is sensitive records, including the patient's personal identity information and some medical diagnosis

TABLE III
THREATS IN MCPS

| Security properties | Sensing/Execution layer | Network layer | Application layer |
|---|---|---|---|
| Integrity | -Data inject<br>-Node capture<br>-Illegal substitution<br>-Insider tampering<br>-Replay attack | -Selective forwarding attack<br>-Sinkhole | -Buffer overflow<br>-False terminal trigger |
| Confidentiality | -Node capture<br>-Insider leak<br>-Hardware hacking | -Wormholes<br>-Eavesdropping | -Buffer overflow |
| Availability | -Dos<br>-Exhaustion attack<br>-Physical attack | -Jamming<br>-Flooding<br>-Sinkhole | -Buffer overflow<br>-Identity theft |

information. The access of sensitive records needs reasonable access control policies.

### B. Technologies

Security and privacy protection in MCPS is very necessary. Kaspersky's security announcement pointed out: the healthcare industry is in the top ten industries attacked by blackmail software. In 2017, the extortion virus WannaCry paralyzed nearly 80 national health services in the U.K., including hospitals and general clinics. As a result, 20 000 medical appointments were canceled, five hospitals refused to accept ambulances, and 600 general practitioners had to use pens and paper to record the medical process. In the black market, the value of personal medical information is 50 times higher than that of the credit card information.

*1) Security System and Architecture:* In order to improve adaptive health services based on patient scenarios, build medical device integration and interoperable infrastructure, protect the security and privacy of verifiable identity and services, and control the secure access of health data and devices, MCPS monitors/controls the physiological dynamics of patients through embedded systems, distributed computing, and network. MCPS has the characteristics closely related to life, which requires the system to be efficient and reliable, resist malicious attacks, and run safely [104]. MCPS contains a large number of devices with different functions and users with different roles, including illegal devices and illegal users. Therefore, a good architecture design can not only help MCPS achieve distributed storage and data sharing but also solve some data security and privacy problems.

Kocabas *et al.* [105] describe the general architecture of MCPS composed of four layers: data collection, data aggregation, cloud processing, and operation. Due to the different hardware and communication ability of each layer, they proposed a new encryption scheme to ensure data privacy in the layer. Fu *et al.* [106] developed a mathematical hypothesis model and composition rules, and developed an algorithm combining mathematical hypothesis model with system model so that the security of the system can be verified not only by medical and engineering professionals but also by existing formal verification tools. Aiming at the existing MCPS models, Almohri *et al.* [107] deeply studied the threats modeled in MCPS and constructed an abstract architecture of MCPS to demonstrate various threat modeling options. They also discussed possible security technologies and their applicability and practicability in the design of secure MCPS. Researchers focus on the interaction and feedback between physical space and cyber space, build an architecture based on CPS, and construct a related framework combined with blockchain technology to ensure the safety and reliability of the medical field. Ghoneim *et al.* [109] proposed a new medical image forgery detection system for healthcare framework. The system works on the noise image of the image, applies a multiresolution regression filter to the noise image, and feeds the output back to the support vector machine and extreme learning classifier to verify whether the healthcare-related image is changed. Al-Turjman *et al.* [110] proposed a context-sensitive seamless identity provision (CSIP) framework for IIoT. Medical smart phone is one of the widely used facilities in the medical industry, which aims to improve the service quality of patients and medical staff. These devices build a new CPS network architecture, called medical smart phone network (MSN). Meng *et al.* [111] focused on the detection of malicious devices in MSN and designed an intrusion detection method based on trust behavior analysis. Schneble *et al.* [112] explored the concept of joint learning, and designed and implemented a large-scale distributed intrusion detection solution based on machine learning for MCPS, so as minimize the communication and computing costs involved in traditional machine learning-based solutions. Choudhary *et al.* [113] proposed a specification-based lightweight bad behavior detection management technology to efficiently detect the bad behavior of IoT devices embedded in MCPS through automatic model checking and formal verification and verified the specification-based bad behavior detection technology by using patient-controlled analgesia (PCA) devices embedded in MCPS.

As the core technology of bitcoin, Ethereum, and other digital cryptocurrencies, blockchain technology has the characteristics of decentralization, distrust, time-series data, data encryption, smart contract, and so on. The combination of MCPS and blockchain can allow us to promote the sharing of resources [114] so that it can be well applied in the medical field. Based on the smart contract of blockchain, Griggs *et al.* [97] promoted the security analysis and management of medical sensors. Using the private blockchain based on the Ethereum protocol, they created a system in which the sensor communicates with an intelligent device, which calls the intelligent contract and writes the records of all events on the blockchain. The smart contract system will support real-time patient monitoring and medical intervention by sending notifications to patients. Krotofil *et al.* [115] proposed a blockchain-based EMR architecture, called granular access authorization supporting flexible query (GAA-FQ), which can authorize different levels of authorization granularity, while maintaining compatibility with the underlying blockchain data structure. Cao *et al.* [116] introduced the architecture of eHealth system based on cloud, analyzed the requirements of EHR security and patient privacy, and proposed an eHealth framework based on blockchain. However, the existing EMR system lacks standard data management and sharing strategy. In order to solve the above problems, Fan *et al.* [117] and others proposed an information management system medblock based on blockchain to process patients' information.

*2) Secure Authentication:* Security authentication technology is a method to confirm the identity of users and device nodes and multisource services in MCPS, so as to ensure that the participants and services in the system are legal. The technology of identity authentication has changed from software authentication to hardware authentication, from single-factor authentication to multifactor authentication, from static authentication to dynamic authentication. Traditional identity authentication technology is based on trusted third-party service centers, using PKI, biometrics, combination factor authentication, password, and other methods for authentication. The traditional authentication methods maintain security based on the difficulty problem, and the protocol is not universal. Therefore, it is difficult to apply to the MCPS with complex structure, high redundancy, and multidomain interaction [105]. Ameyv *et al.* [118] gave the security objectives of CPS, including perception security, storage security, communication security, execution security, and feedback security. To ensure the integrity and accuracy of the data sensed by the physical sensor, the data stored in MCPS will not be tampered with by unauthorized users, the security of internal and external communication channels of the system will not be attacked, the execution device of MCPS is authorized before the operation, and the feedback loop of the control system is protected, so as to make accurate decisions.

Based on the wide application of RFID in a medical environment, He *et al.* [119] analyzed the security requirements of the RFID authentication scheme and summarized the performance and security of the RFID authentication scheme based on elliptic curve cryptography (ECC). They found that, although most of the authentication schemes cannot meet all the security requirements and have satisfactory performance, some ECC-based authentication schemes are suitable for the medical environment in terms of performance and security. The biological mode is an ideal choice for user authentication in MCPS, but, with the development of various deception methods, the traditional biological mode detection system may not be able to achieve. Mowla *et al.* [120] proposed a fog-based MCPS cognitive security application and cognitive detection security algorithm (BM-CD) to detect biometric morphological deception of face, iris, and fingerprint supported by selective set enhancement learner. Alhayajneh *et al.* [121] analyzed and evaluated the accuracy, cost, and implementation feasibility of the most prominent biometric authentication technology and proposed to adopt a variety of biometric authentication schemes to ensure the confidentiality, integrity, and reliability of wireless body LAN (WBAN). WBAN plays an indispensable role in MCPS. It is a network composed of multiple wearable devices or implantable devices, which uses wireless technology to communicate. Therefore, a secure and reliable authentication scheme is essential. Xu *et al.* [122] proposed a secure lightweight authentication scheme for WBAN. With this scheme, forward secrecy can be guaranteed without using asymmetric encryption, and the security of the scheme can be verified and analyzed by using the automatic security verification tool proverif. Moosavi *et al.* [123] proposed an end-to-end security scheme for mobile medical IoT. The scheme includes three parts: first, a secure and efficient end-user authentication and authorization architecture based on certificate-based DTLS handshake, then a secure end-to-end communication based on session recovery, and, finally, powerful mobility based on internet intelligent gateway. In order to prevent unauthorized users from accessing general devices, Amin *et al.* [124] proposed a mutual authentication and key agreement protocol to protect the confidential information in devices. Based on ECC, Mohsen *et al.* [125] proposed a new lightweight mutual authentication and key agreement protocol for real-time wireless medical sensor networks between doctors/nurses, trusted servers, sensors, and patients. Aiming at the challenges brought by the electronic health information management system using IoTs, including the communication security of wireless channel, the protocol between authentication key and entity, the access control scheme, and other defects, Aghili *et al.* [126] proposed a new lightweight, secure, and efficient authentication protocol, which is also suitable for access control. Cao *et al.* [116] proposed a password-based authentication system for appointments between patients and hospitals in order to realize the friendliness of patients with low-power devices and resistance to impersonation attacks.

The security authentication solution based on the blockchain can mitigate or completely negate all kinds of attacks, which is beneficial to the security of such systems. The ledger implemented by Alexopoulos *et al.* [127] using blockchain technology is used to protect the authentication of trust management (TM) system and model its system. Aiming at the problem of data source security authentication in a smart contract, Zhang *et al.* [128] realized the data source authentication through the front-end blockchain and the back-end trusted hardware SGX. AI-Bassam *et al.* [129] aimed at the problem that the current X.509 certificate standard can only issue certificates for user's identity but cannot sign certificates for fine-grained identity attribute information, improved it based on smart contract, and add authentication for attribute information, so that, if the user's identity information is authenticated, the attributes corresponding to the identity are also trustworthy, which realizes the transfer of trust between the user's identity and the user's attributes.

*3) Secure Transmission and Storage:* In the data generation, transmission, and receiving end, the corresponding cryptography knowledge can be used to ensure the safety and reliability

TABLE IV

DATA ENCRYPTION SCHEMES FOR MCPS

| Scheme | Technologies | Characteristics |
|---|---|---|
| Elhoseny [130] | RSA | Safety protection of diagnostic text data in medical Images |
| Srisakthi [131] | Discrete transformation | Save space/computing cost |
| Tian [132] | Cloud storage and dynamic hash table | Reducing computing/communication cost |
| Zhang [133] | Cloud computing and ECC | Effective retrieval of medical data |
| Zheng [134] | ABE | Solve the privacy issues in users data sharing |
| Wang [139] | ABE and Block-chain | Digital signature for easy management |
| Ma [135] | Certificateless public key encryption | Efficient keyword search without key management |
| Chen [136] | Verifiable keyword search | Fine-grained authorization control |
| Li [145] | Certificate-free signature | Anonymous access control |
| Zhang [138] | Identity-based authorized searchable encryption | Enable the encrypted diagnostic data sharing efficiently |

TABLE V

COMPARISON OF SEVERAL SEARCHABLE ENCRYPTION SCHEMES FOR MCPS

| Algorithm | Ma [135] | | Chen [136] | | Zhang [138] | |
|---|---|---|---|---|---|---|
| | Storage costs | Computatin costs | Storage costs | Computatin costs | Storage costs | Computatin costs |
| Encryption | $3\lvert G_1\rvert$ | $P+5E+H$ | $(n+\lvert N\rvert)\lvert G_1\rvert+\lvert G_2\rvert$ | $(n+\lvert N\rvert)E_1+E_2$ | $2\lvert G_1\rvert$ | $3M+H+A$ |
| Trapdoor | $\lvert G_1\rvert$ | $E+H$ | $l\lvert G_1\rvert+\lvert G_2\rvert$ | $lE_1+E_2$ | $\lvert G_2\rvert$ | $H+P+M$ |
| Search | - | $2P+3E$ | $l\lvert G_2\rvert$ | $lP$ | - | $2P+M$ |

$P$:a bilinear pairing from $G_1$ to $G_2$, $E$:a general modular exponentiation, $E_1$:modular exponentiation in $G_1$, $E_2$:modular exponentiation in $G_2$, $H$:a hash function in $G_1$, $M$:multiplication, $A$:a point addition, $|G_1|$:the element lengths in $G_1$, $|G_2|$:the element lengths in $G_2$, $|N|$:the number of leaf nodes in the access structure, $n$:the number of keywords, $l$:the number of queried keywords

of data. Some researchers have combined cloud storage and other related technologies to propose corresponding encryption models or schemes for medical scenarios. Table IV shows several data encryption schemes on MCPS. Table V shows the comparison of the computational costs and storage costs of several searchable encryption schemes in MCPS.

Elhoseny *et al.* [130] proposed a hybrid security model for the security protection of diagnostic text data in medical images. The model is based on the combination of the 2-D discrete wavelet transform level 1 (2d-dwt-1l) or the 2-D discrete wavelet transform Level 2 (2d-dwt-2l) steganography with the proposed hybrid encryption scheme. The hybrid encryption mode is constructed by using the combination of advanced encryption standards and RSA algorithms. Srisakthi *et al.* [131] proposed a secure encryption model based on discrete transformation, which can save space and reduce the calculation cost to protect user data. Combined with cloud storage technology, Tian *et al.* [132] proposed a new public audit scheme for secure cloud storage based on a dynamic hash table (DHT). Similarly, Chandrasekhar *et al.* [147] proposed a proxy signature scheme based on trapdoor hash for health information exchange (HIE). Zhang *et al.* [133] proposed an identity-based ECC-based agent outsourcing scheme for public audit in MCPS based on cloud computing. This scheme allows the patient authorized agent to generate the signature of medical data and upload the corresponding encrypted medical data to the cloud-based MCPS. Any third-party auditor (TPA) can audit medical data effectively without retrieving the whole medical dataset. Zheng *et al.* [134] used attribute-based encryption (ABE) technology to realize data sharing, and proposed an efficient medical data sharing scheme, which removes the attribute matching function and hides all the attributes in the access control structure by using the attribute bloom filter. Aiming at the keyword search problem in the mobile medical system (MHS) based on the cloud, Ma *et al.* [135] designed a certificateless public key encryption scheme with keyword search. Their scheme avoids the key management and custody problems. Later, for the same problem of keyword search in MHS, Chen *et al.* [136] proposed a verifiable keyword search encryption scheme for MHS that can realize fine-grained authorization control in MHS based on big data. In order to solve the problem of how to search the medical data in the cloud without decryption, Li *et al.* [137] proposed two secure and effective dynamic searchable symmetric encryption (SEDSSE) schemes, in which using secure k-nearest neighbor (KNN) and ABE technology to construct dynamic searchable symmetric encryption scheme, forward privacy, and backward privacy can be realized simultaneously. An enhanced scheme is also proposed to solve the key sharing problem in the KNN-based searchable encryption scheme. Zhang *et al.* [138] proposed an identity-based authorized searchable encryption scheme (IBASE). By using identity-based encryption (IBE) and keyword search functions, doctors can authorize assistants to process encrypted diagnostic data shared with patients in the cloud-assisted electronic medical information system, thus greatly reducing the work intensity of doctors. In order to achieve the confidentiality, authentication, and integrity of medical data and support fine-grained access control (FGAC), Wang *et al.* [139] proposed a secure EHR system based on attribute cryptography and blockchain technology. They used ABE and IBE to encrypt medical data and used identity-based signature (IBS) to realize digital signature, which greatly facilitates the management of the system.

Alguliyev *et al.* [140] described the challenges of CPS in a “tree” structure and summarized them as attacks on sensor devices [115], actuators [141], computing components [142],

TABLE VI
ACCESS CONTROL SCHEMES FOR MCPS

| Scheme | Technologies | Characteristics |
|---|---|---|
| Zhang [151] | Anonymous ABE | Fine-grained access control and privacy protection |
| Roy [152] | FGAC | provably secure mobile user authentication |
| Li [153] | Cloud characteristics and signature cryptosystem | Ensure the security and privacy of healthcare data in the cloud |
| Yeh [155] | ABAC and ECC | Cloud-based personal health systems |
| Tamboli [156] | FGAC | Improve privacy of the system |
| Yang [160] | Two-fold access control mechanism | Save the storage overhead in the big data storage system |
| Ding [165] | Decentralized access control and fully homomorphic encryption | Security and privacy issues of medical data persistence |

and communication and feedback [107]. Many wireless devices may be connected in the CPS network, which has different QoS requirements and priorities [108]. The sensors and actuators of MCPS are related to the life safety of patients, the interactive data are related to the privacy of patients, and the feedback information is related to the doctor's control of patients' physical condition. Therefore, MCPS should give priority to ensure the reliable transmission and data security of emergency health care information. For the security and privacy of streaming medical data of heterogeneous network devices, Omala *et al.* [143] proposed a heterogeneous signature encryption scheme, in which the sender is in the certificateless encryption (CLC) environment and the receiver is in the identity-based environment. Qiu *et al.* [144] proposed a secure data storage and sharing method, which is composed of selective encryption algorithm, and fragmentation and decentralization. Even when the transmission medium (such as cloud server) and key are damaged, it can also protect data security and privacy. Li *et al.* [145] also proposed a new certificateless signature encryption scheme for WBAN. O'Connor *et al.* [146] believe that the first stage of the universal availability of the IoTs in the field of smart health is to ensure that digital health citizens (i.e., technology users) fully understand what they agree to when they register their accounts, which is further strengthened by the proposed "design privacy" requirements related to the upcoming general data protection regulation (GDPR). They put forward some practical methods that should be considered when designing and developing the IoTs for data collection and data sharing in the field of health.

Although the above encryption schemes based on cryptography can ensure secure data storage and transmission, the computation and storage costs of the encryption scheme are large. Therefore, some noncryptographic schemes are proposed to protect data security and privacy. Xiao *et al.* [149] proposed a new trajectory privacy protection design, called query logic separate storage (QLDS). QLDS introduces fine-grained anonymity in order to extract query logic to retrieve personal trajectories and prevent the actual trajectories tuples from gathering to any routing ID or user ID on the server side. Zhang *et al.* [150] proposed a new anonymization technology based on streaming classification information, which provides strong privacy protection to prevent privacy leakage and information tampering. Their technology adopts an innovative two-phase anonymity method, which is very easy to implement and efficient in terms of speed and communication. These noncryptographic schemes can also be used in MCPS.

*4) Access Control:* Access control is to strictly control the access rights of users and devices in MCPS, to ensure that each legal access is accurate and effective, and to prevent unauthorized access and illegal services. Because the data in MCPS are related to patient privacy and physician prescription data security, MCPS emphasizes the importance of security on the basis of feedback and control [105]. Table VI shows some access control schemes.

In order to solve the problem of privacy in user data sharing, Zhang *et al.* [151] implemented the aggregation authorization and access control of privacy in the IoTs by introducing a secure smart health system SSH and solved the problems of aggregation authentication, FGAC, and privacy protection. Roy *et al.* [152] proposed a combination method of FGAC for multiserver data based on cloud, as well as a provably secure mobile user authentication mechanism for medical industry 4.0, which is the first scheme of FGAC for multiple cloud servers in the mobile cloud computing environment. Then, Li *et al.* [145] used the cloud features and high efficiency of MCPS to achieve the required medical monitoring and effectively protect the privacy related to pregnant women. They established a cloud computing platform for all users, which can access cloud information at any time according to the needs of users. Zhang *et al.* [154] proposed a secure S-Health system, which realized FGAC of S-Health cloud data, thus ensuring the privacy protection of users. Yeh *et al.* [155] designed PHI cloud storage, batch processing, and FGAC mechanism in the framework of community medical IoT by combining ECC algorithm and attributed-based access control (ABAC) model. Tamboli and Dambawade [156] designed a lightweight COAP protocol access control mechanism based on IFTF, which reduces the encryption and decryption time of ECC and improves the efficiency of access control based on access credentials. Jose *et al.* [157] proposed attribute-based credentials (ABCs) to deal with the S-Health privacy problem and laid the foundation for the further adoption of other privacy-aware smart city services based on IoTs. Ullah *et al.* [158] designed an effective media access control strategy, Ming *et al.* [159] proposed a secure and effective cross-domain access control scheme for wireless sensor networks, and Yang *et al.* [160] proposed a smart IoT medical big data storage system with adaptive dual access control mechanism based on privacy protection. Its purpose is to ensure the safety of patients' health care data, realize access control in normal and emergency situations, support smart data deduplication, and save the storage space of big data storage systems. Mikula and Jacobsen [162] demonstrated the application of blockchain in identity and access management by using the hyperledger fabric framework and provided the proof of concept of e-health record use case based on healthcare field. Zhang *et al.* [163] proposed a blockchain-based EMR architecture, called GAA-FQ, which can authorize different levels of authorization granularity, while maintaining compatibility with the underlying blockchain data structure. In order to achieve FGAC and data privacy for health data, Malamas *et al.* [164] proposed a novel hierarchical blockchain architecture. In order to solve the security and privacy problems of medical data persistence in smart medicine, Ding *et al.* [165] proposed a new database called Derepo, which uses distributed ledger technology to make the access control mechanism have reliable attributes. In addition, the complete homomorphic encryption scheme is used to protect data privacy while maintaining computability. The design of Derepo is user-centered. Only the data owner can make access control policies and decrypt its data, while the authorized third party can perform data processing on its encrypted data without knowing the original values.

### C. Challenges

When developing the security and privacy system of MCPS, any developer will consider the influence of various factors in order to achieve a better balance between them. In order to achieve a better security environment, special attention needs to be paid to several challenges.

1) *Insecure Network:* WLAN has been widely used in various fields. Due to its convenience, in the field of MCPS, more devices and software services rely heavily on wireless networks, such as Wi-Fi. It is known that Wi-Fi is vulnerable to all kinds of intrusion, including unauthorized router access, man-in-the-middle attack, deception, denial-of-service attack, violent attack, and so on. In addition, most of the free wireless networks in public places are not authenticated and trusted so that the network security factor is the primary consideration of MCPS.
2) *Lightweight Protocol for Devices:* Due to the limited storage space of medical devices, low-cost devices and software applications based on medical sensors should follow specific strategies to provide services. At present, if we want to provide advanced security protection for medical sensors, we must design different levels of security protocols according to the application scenarios, especially lightweight security protocols to ensure the communication security of sensors.
3) *Data Security Sharing:* In MCPS, the patient's medical records (outpatient medical records, hospitalization records, body temperature list, medical order list, laboratory test list, medical image examination data, special examination consent, operation consent, operation and anesthesia record list, pathological data, nursing records, and other medical records) are important data. If these medical records can be shared with patients, hospitals, and researchers, it will promote great progress in the medical field. Therefore, how to realize data sharing of heterogeneous and diverse massive medical data is also a hot topic in today's research.

## IX. Key Research Perspectives and Directions of MCPS

In the era of rapid development of science and technology, the research of MCPS aims to build a closed-loop enabling system based on data automatic flow between cyber space and physical space in the medical and health environments, including state perception, real-time analysis, scientific decision-making, and accurate execution, so as to solve the complexity and uncertainty problems in the process of medical service, improve the efficiency of resource allocation, and realize resource optimization. MCPS is an important technical cornerstone for the development of smart medicine, and it is also one of the key supporting points to improve the national medical service system and improve the level of medical service. Therefore, the development of complex heterogeneous MCPS will make great progress.

### A. Heterogeneous Network

The heterogeneous network is composed of computers, network devices, and systems produced by different manufacturers. In most cases, it can support different functions or applications by running different protocols. In MCPS, there are many kinds of heterogeneous devices, including medical sensor devices, execution devices, terminal devices, and so on. In order to solve the problems of state perception, real-time analysis, scientific decision-making, and accurate execution based on the automatic flow of data between cyber space and physical space in the medical and health environment, we need to focus on the heterogeneous network architecture of the integrated system for the access of heterogeneous devices. Although these networks provide users with a variety of communication methods and access services anytime and anywhere, in order to truly realize self-organization, self-adaptive, and end-to-end high-quality service communication, we need to fully study the complementary characteristics of different networks and realize the integration of heterogeneous network technologies.

### B. Information Sharing and Utilization

With the upgrading of hardware and algorithms in the medical field, information islands are gradually adjacent to each other. Computers can not only recognize text information but also image information. The internal exchange of information is no longer a problem technically, and it is rapidly applied in the grassroots. However, in order to build a close medical association, we need to realize the close integration of information of communities, hospitals, medical institutions, and other departments, realize the interconnection of big data in the medical field, and establish a regional medical information sharing platform to provide convenient services for the comprehensive sharing of medical information. In MCPS, medical data have the characteristics of heterogeneous, multisource, multitype, timeliness, mass, confidentiality, user-related, and so on. It integrates the information unit, network unit, sensor unit, control unit, physical unit, the user unit, and other elements. To realize the distributed storage and secure sharing of medical data, it is necessary to break through the traditional information system architecture and design reliable security system authentication and access control methods.

### *C. Information Security and Privacy*

Medical big data are of great help to medical information resources, medical diagnosis technology, drug research and development, assisting medical staff in accurate diagnosis, timely predicting treatment, reducing medical costs, and eliminating information barriers of urban and rural medical services. However, in the context of the development of medical big data, medical data security and personal privacy protection are increasingly prominent. The sources of medical data are diverse, including medical records, health logs, medical experiments, genetic data, scientific research data, and so on. It is noteworthy that, with the rapid development of science and technology, all kinds of health APP operators and third-party industry research institutions engaged in medical big data analysis have been involved in the collection of medical data. Therefore, not only the technical level of security and privacy but also the management level is more important. Medical institutions and their medical staff should follow the relevant regulations and strictly keep patient privacy. Except for medical, teaching, and research purposes, patients' medical records should not be leaked, so as to ensure the security and privacy of medical data.

### *D. System Integration*

MCPS is the necessary technical support and cornerstone of modern information hospital operation and has made great contributions to the realization of more advanced, scientific, and standardized hospital management. In the face of complex MCPS, including HIS, LIS, CIS, OA, EMR, RIS, PACS, and so on, it is necessary to establish a standardized and integrated information platform to support the smooth operation of HIS and achieve wide internal information resource sharing, business collaboration, and external interconnection. First, the unification of standardization needs data standards, information system interaction specifications, and platform technical specifications. Then, according to the requirements of inheritance, the interface with the original business system and information system should be provided, and the existing resources and services should be inherited. Finally, the standardization of integration requirements is necessary, so as to achieve the integration of clinical information systems, hospital management information systems, and other systems.

### *E. Decision-Making Analysis*

Medical decision-making analysis is an emerging field derived from health economics, applied health policy and insurance design, and business intelligence. In the current era of "big data" with the explosive growth of information, the amount of information in the medical field database is expanding, and at the same time, it is also facing the challenge of massive and heterogeneous data. In the face of the urgent need to improve the digital medical field and how to integrate various types of data generated by multiple systems or sensors and tap the value behind the massive data, so as to make effective use of them, analyze medical decision-making problems, assist judgment, and improve the management and decision-making ability of relevant medical personnel, it is of great significance to optimize the industry structure and improve service ability and management level in clinical business, pharmaceutical product research and development, public health, and other fields.

### *F. Derived Topics*

With the emergence of mobile Internet, IoT, cloud computing, big data, machine learning, blockchain, virtual reality (VR), and augmented reality (AR), these technologies have made great contributions to medical informatization.

In recent years, new forms of medical services have sprung up. "Internet + medicine" has been a major exploration in many aspects, such as registration settlement, remote diagnosis and treatment, and consulting services. Some regions have implemented the landing project of Internet hospitals, but there are still some problems. In terms of standards, because the Internet hospital is in the embryonic stage of development, the relevant standard system has not been established; in terms of infrastructure construction, the interconnection of information resources has not been difficult to achieve, and the phenomenon of isolated medical information is very serious.

At present, cloud computing is widely used in the medical field, which injects new vitality into the whole medical industry. However, many public cloud networks are configured as closed systems and lack unified technical standards. Different manufacturers do their own things in the process of product and service development, resulting in the lack of integration between these networks, making it difficult for medical institutions to unite it systems in cloud computing, which brings challenges to medical institutions who want to merge a series of IT systems in the cloud. Therefore, we should explore the challenges and opportunities for medical institutions to go up to the cloud at present, so as to clear up doubts for medical institutions to go up to the cloud, develop ideas for the industrial cloud, and comprehensively accelerate the vigorous development of medical health cloud ecology.

Big data have become a recognized resource. The rapid development of the big data industry has brought unlimited room for enterprises to rise and also promoted the development of basic people's livelihood medical industry. As a new engine, health care big data will promote the implementation of new demands. However, at present, it is difficult to integrate medical big data and provide users with access to a complete data decision support system.

The integration of machine learning makes the diagnosis accuracy of the medical system greatly improved. It can not only customize the treatment plan for patients but also replace the work of some doctors, making medical care more intelligent, safe, and efficient. However, in the process of clinical decision-making, machine learning does not have a mature perception, reasoning, and interpretation abilities. Even the most advanced machine learning algorithms cannot provide the sensitivity, specificity, and accuracy required by clinical decision-making and cannot meet the requirements of clinicians.

"MCPS + blockchain" allows us to promote the sharing of services and resources, so as to create services between devices, and also allows us to simplify several time-consuming workflows in the encryption verification process in an automated way [166]. The decentralized feature of blockchain helps MCPS to realize distributed storage and data sharing, but its high requirements for computing, transmission, and storage capacity cannot be met by the current MCPS. The traditional workload proof algorithm is not suitable and not only needs to improve the accounting method of medical interactive data but also needs to redesign the identity authentication and service authentication protocol, and access control strategy [167].

## X. 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.

## Acknowledgment

The authors would like to thank their colleagues and students at the Anhui Provincial Key Laboratory of Network and Information Security.

## References

[1] I. Lee and O. Sokolsky, "Medical cyber physical systems," in *Proc. IEEE Int. Conf. Workshops Eng. Comput. Based Syst.*, Jun. 2010, pp. 743–748.

[2] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Proc. IEEE Design Automat. Conf.*, Jun. 2010, pp. 731–736.

[3] N. Dey, A. S. Ashour, F. Shi, S. J. Fong, and J. M. R. Tavares, "Medical cyber-physical systems: A survey," *J. Med. Syst.*, vol. 42, no. 4, p. 74, 2018.

[4] R. Chaari *et al.*, "Cyber-physical systems clouds: A survey," *Comput. Netw.*, vol. 108, pp. 260–278, Oct. 2016.

[5] H. M. Chen, L. Cui, and K.-B. Xie, "A comparative study on architectures and implementation methodologies of Internet of Things," *Chin. J. Comput.*, vol. 36, no. 1, pp. 168–188, Jan. 2013.

[6] C. Liu, C. Zhang, F. Chen, and C. Zhao, "Towards IPv6-based architecture for big data processing of community medical Internet of Things," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2018, pp. 1333–1338.

[7] A. A. Abdellatif, A. Mohamed, C. F. Chiasserini, M. Tlili, and A. Erbad, "Edge computing for smart health: Context-aware approaches, opportunities, and challenges," *IEEE Netw.*, vol. 33, no. 3, pp. 196–203, May 2019.

[8] S. Din and A. Paul, "Smart health monitoring and management system: Toward autonomous wearable sensing for Internet of Things using big data analytics," *Future Gener. Comput. Syst.*, vol. 91, pp. 611–619, Feb. 2019.

[9] N. I. Mowla, I. Doh, and K. Chae, "On-device AI-based cognitive detection of bio-modality spoofing in medical cyber physical system," *IEEE Access*, vol. 7, pp. 2126–2137, 2019.

[10] N. Mowla, I. Doh, and K. Chae, "Selective fuzzy ensemble learner for cognitive detection of bio-identifiable modality spoofing in MCPS," in *Proc. 20th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2018, pp. 63–67.

[11] A. Roehrs, C. A. da Costa, R. da Rosa Righi, V. F. da Silva, J. R. Goldim, and D. C. Schmidt, "Analyzing the performance of a blockchain-based personal health record implementation," *J. Biomed. Informat.*, vol. 92, Apr. 2019, Art. no. 103140.

[12] A. Roehrs, C. Costa, and R. Rosa, "OmniPHR: A blockchain based interoperable architecture for personal health records," *J. Biomed. Informat.*, vol. 71, pp. 70–81, Jul. 2017.

[13] R. Casado-Vara and J. Corchado, "Distributed e-health wide-world accounting ledger via blockchain," *J. Intell. Fuzzy Syst.*, vol. 36, no. 3, pp. 2381–2386, Mar. 2019.

[14] A. Alabdulatif, I. Khalil, X. Yi, and M. Guizani, "Secure edge of things for smart healthcare surveillance framework," *IEEE Access*, vol. 7, pp. 31010–31021, 2019.

[15] C. Xia and S. Song, "Resource allocation in hierarchical distributed EHR system based on improved poly-particle swarm," in *Proc. 5th Int. Conf. Biomed. Eng. Informat.*, Oct. 2012, pp. 1112–1116.

[16] C. He, X. Fan, and Y. Li, "Toward ubiquitous healthcare services with a novel efficient cloud platform," *IEEE Trans. Biomed. Eng.*, vol. 60, no. 1, pp. 230–234, Jan. 2013.

[17] K. Simon, M. M. Sonai, and S. Lee, "A ubiquitous personal healthrecord (uPHR) framework," in *Proc. Int. Conf. Adv. Comput. Sci. Electron. Inf. (ICACSEI)*, Aug. 2013, pp. 423–427.

[18] S. Safavi and Z. Shukur, "Conceptual privacy framework for health information on wearable device," *PLoS ONE*, vol. 9, no. 12, Dec. 2014, Art. no. e114306.

[19] M. Kyazze, J. Wesson, and K. Naude, "The design and implementation of aubiquitous personal health record system for south Africa," *Stud. Health Technol. Informat.*, vol. 206, pp. 29–41, Nov. 2014.

[20] O. Kemkar and P. Kalode, "Formulation of distributed electronic patient record (DEPR) system using openemr concept," *Int. J. Eng. Innov. Res.*, vol. 4, no. 1, pp. 85–89, Jan. 2015.

[21] S. Pasandideh, L. Gomes, and M. Pedro, "Modelling cyber physical social systems using dynamic time Petri nets," in *Proc. Doctoral Conf. Comput., Elect. Ind. Syst.*, 2018, pp. 81–89.

[22] Y. Tong, Z. Li, C. Seatzu, and A. Giua, "Verification of state-based opacity using Petri nets," *IEEE Trans. Autom. Control*, vol. 62, no. 6, pp. 2823–2837, Jun. 2017.

[23] F. Salinas *et al.*, "Modeling and control design based on Petri nets for serial multicellular choppers," *IEEE Trans. Control Syst. Technol.*, vol. 23, no. 1, pp. 91–100, Jan. 2015.

[24] J. Wang, J. Yan, and L. Li, "Microscopic modeling of a signalized traffic intersection using timed Petri nets," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 2, pp. 305–312, Feb. 2016.

[25] K. Thramboulidis and F. Christoulakis, "UML4IoT—A UML-based approach to exploit IoT in cyber-physical manufacturing systems," *Comput. Ind.*, vol. 82, pp. 259–272, Oct. 2016.

[26] C. W. Tsai, C. F. Lai, and A. V. Vasilakos, "Future Internet of Things: Open issues and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2201–2217, May 2014.

[27] T. Adegbija, A. Rogacs, C. Patel, and A. Gordon-Ross, "Microprocessor optimizations for the Internet of Things: A survey," *IEEE Trans. CAD Integr. Circuits Syst.*, vol. 37, no. 1, pp. 7–20, May 2018.

[28] A. Engel and A. Koch, "Heterogeneous wireless sensor nodes that target the Internet of Things," *IEEE Micro*, vol. 36, no. 6, pp. 8–15, Nov. 2016.

[29] E. A. Lee, "The past, present and future of cyber-physical systems: A focus on models," *Sensors*, vol. 15, no. 3, pp. 4837–4869, Feb. 2015.

[30] M. Lohstroh, H. Kim, J. C. Eidson, C. Jerad, B. Osyk, and E. A. Lee, "On enabling technologies for the Internet of important things," *IEEE Access*, vol. 7, pp. 27244–27256, 2019.

[31] E. Lee, "Modeling in engineering and science," *Commun. ACM*, vol. 62, no. 1, pp. 35–36, Dec. 2018.

[32] Y. Zeng *et al.*, "Modeling electromechanical aspects of cyber-physical systems," *J. Softw. Eng. Robot.*, vol. 7, no. 1, pp. 100–119, 2016.

[33] A. Banerjee, S. K. S. Gupta, G. Fainekos, and G. Varsamopoulos, "Towards modeling and analysis of cyber-physical medical systems," in *Proc. 4th Int. Symp. Appl. Sci. Biomed. Commun. Technol. (ISABEL)*, 2011, pp. 1–5.

[34] A. Murugesan *et al.*, "From requirements to code: Model based development of a medical cyber physical system," in *Proc. Int. Workshop Softw. Eng. Health Care*, 2014, pp. 96–112.

[35] L. Silva, H. Almeida, A. Perkusich, and M. Perkusich, "A model-based approach to support validation of medical cyber-physical systems," *Sensors*, vol. 15, no. 11, pp. 27625–27670, Oct. 2015.

[36] Z. Fu, Z. Wang, C. Guo, Z. Zhang, S. Ren, and L. Sha, "IAFinder: Identifying potential implicit assumptions to facilitate validation in medical cyber-physical system," in *Proc. 55th ACM/ESDA/IEEE Design Autom. Conf. (DAC)*, Jun. 2018, pp. 1–6.

[37] *Medical Devices and Medical Systems Essential Safety Requirements for Equipment Comprising the Patient-Centric Integrated Clinical Environment (ICE), Part 1: General Requirements and Conceptual Model*. Standard ASTM F2761-09, 2013. [Online]. Available: https://www.astm.org/Standards/F2761.htm

[38] Z. Jiang, M. Pajic, and R. Mangharam, "Cyber–physical modeling of implantable cardiac medical devices," *Proc. IEEE*, vol. 100, no. 1, pp. 122–137, Jan. 2012.

[39] B. Miller, F. Vahid, and T. Givargis, "Digital mockups for the testing of a medical ventilator," in *Proc. 2nd ACM SIGHIT Symp. Int. Health Informat. (IHI)*, 2012, pp. 859–862.

[40] K. van Heusden, E. Dassau, H. C. Zisser, D. E. Seborg, and F. J. Doyle, "Control-relevant models for glucose control using a priori patient characteristics," *IEEE Trans. Biomed. Eng.*, vol. 59, no. 7, pp. 1839–1849, Jul. 2012.

[41] A. Murugesan, O. Sokolsky, S. Rayadurgam, M. Whalen, M. Heimdahl, and I. Lee, "Linking abstract analysis to concrete design: A hierarchical approach to verify medical CPS safety," in *Proc. ACM/IEEE Int. Conf. Cyber-Physical Syst. (ICCPS)*, Apr. 2014, pp. 139–150.

[42] C. Liu *et al.*, "Characteristic, architecture, technology and design methodology of cyber-physical systems," in *Proc. EAI Int. Conf. Ind. IoT Technol. Appl.*, vol. 202, nos. 230–246, 2017, pp. 230–246.

[43] M. Van Ornum, "Improving bar code medication administration compliance in a community hospital through a nursing leadership initiative," *J. Nursing Care Qual.*, vol. 33, no. 4, pp. 341–347, Oct. 2018.

[44] L. Sanchez and V. Ramos, "Towards an efficient identification process for large-scale RFID systems," *Sensors*, vol. 18, no. 7, p. 2350, Jul. 2018.

[45] C. Kavitha and S. Sakthivel, "An effective mechanism for medical images authentication using quick response code," *Cluster Comput.*, vol. 22, no. S2, pp. 4375–4382, Mar. 2019.

[46] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[47] Z. Pang, J. Tian, and Q. Chen, "Intelligent packaging and intelligent medicine box for medication management towards the Internet-of-Things," in *Proc. 16th Int. Conf. Adv. Commun. Technol.*, vol. 2, no. 6, Feb. 2014, pp. 352–360.

[48] R. Li *et al.*, "Survey of modeling methods in cyber-physical system," *J. Commun.*, vol. 37, no. 5, pp. 165–175, Jul. 2016.

[49] Y. Cui and J. Wu, *Next Generation Internet and IPv6 Transition*. Beijing, China: Tsinghua Univ. Press, 2014.

[50] T. Narten, G. Huston, and L. Roberts, "IPv6 address assignment to end sites," IETF, Tech. Rep. RFC 6177, Mar. 2011, doi: 10.17487/RFC6177.

[51] F. Gont *et al.*, "Recommendation on stable IPv6 interface identifiers," IETF, Tech. Rep. RFC 8064, Feb. 2017, doi: 10.17487/RFC8064.

[52] M. Bagnulo and J. Arkko, "Support for multiple hash algorithms in cryptographically generated addresses (CGAs)," IETF, Tech. Rep. RFC 4982, Jul. 2007, doi: 10.17487/RFC4982.

[53] T. Narten, R. Draves, and S. Krishnan, "Privacy extensions for stateless address autoconfiguration in IPv6," IETF, Tech. Rep. RFC 4941, Sep. 2007, doi: 10.17487/RFC4941.

[54] O. Troan, B. Volz, and M. Siodelski, "Issues and recommendations with multiple stateful DHCPv6 options," IETF, Tech. Rep. RFC 7550, May 2015, doi: 10.17487/RFC7550.

[55] G. Montenegro *et al.*, "Transmission of IPv6 packets over IEEE 802.15.4 networks," IETF, Tech. Rep. RFC 4944, Sep. 2007, doi: 10.17487/RFC4944.

[56] J. Hui and P. Thubert, "Compression format for IPv6 datagrams over IEEE 802.15.4-based networks," IETF, Tech. Rep. RFC 6282, Sep. 2011, doi: 10.17487/RFC6282.

[57] T. Winter *et al.*, "RPL: IPv6 routing protocol for low-power and lossy networks," IETF, Tech. Rep. RFC 6550, Mar. 2012, doi: 10.17487/RFC6550.

[58] Z. Shelby, "Constrained RESTful environments (CoRE) link format," IETF, Tech. Rep. RFC 6690, Aug. 2012, doi: 10.17487/RFC6690.

[59] S. Ziegler *et al.*, "IoT6-moving to an IPv6-based future IoT," in *Proc. Future Internet Assem.*, vol. 7858, 2013, pp. 161–172.

[60] C. Gomez, J. Paradells, C. Bormann, and J. Crowcroft, "From 6LoWPAN to 6Lo: Expanding the universe of IPv6-supported technologies for the Internet of Things," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 148–155, Dec. 2017.

[61] A. J. Jara, M. A. Zamora, and A. Skarmeta, "Glowbal IP: An adaptive and transparent IPv6 integration in the Internet of Things," *Mobile Inf. Syst.*, vol. 8, no. 3, pp. 177–197, 2012.

[62] A. Jara, P. Moreno-Sanchez, A. Skarmeta, S. Varakliotis, and P. Kirstein, "IPv6 addressing proxy: Mapping native addressing from legacy technologies and devices to the Internet of Things (IPv6)," *Sensors*, vol. 13, no. 5, pp. 6687–6712, May 2013.

[63] A. J. Jara, S. Varakliotis, A. F. Skarmeta, and P. Kirstein, "Extending the Internet of Things to the future internet through IPv6 support," *Mobile Inf. Syst.*, vol. 10, no. 1, pp. 3–17, 2014.

[64] R. Xiao, W. Chen, and B. Sun, "Light weight and tree-based forwarding model in IPv6 IoT subnet," *J. Softw.*, vol. 25, no. 8, pp. 1729–1742, Sep. 2014.

[65] R. Xiao *et al.*, "Address compression in IPv6 Internet of Things hierarchical forwarding system," *J. Comput. Res. Develop.*, vol. 53, no. 4, pp. 834–844, Jun. 2016.

[66] C. Gillies *et al.*, "Minimum Steiner tree for automatic SQL query generation applied on a medical record database," in *Proc. IEEE World Congr. Services*, Jul. 2011, pp. 443–450.

[67] E. Xu, M. Wermus, and D. B. Bauman, "Development of an integrated medical supply information system," *Enterprise Inf. Syst.*, vol. 5, no. 3, pp. 385–399, Aug. 2011.

[68] Z. Wu *et al.*, "A community health service architecture based on the Internet of Things on health-care," *Chin. J. Biomed. Eng.*, vol. 25, no. 3, pp. 114–120, Mar. 2016.

[69] A. T. Azar and A. E. Hassanien, "Dimensionality reduction of medical big data using neural-fuzzy classifier," *Soft Comput.*, vol. 19, no. 4, pp. 1115–1127, Mar. 2015.

[70] B. Ma *et al.*, "Assuring privacy-preservation in mining medical text materials for COVID-19 cases—A natural language processing perspective," in *Proc. VLDB Int. Workshop Very Large Internet Things (VLIoT)*, Aug. 2020, pp. 6–13.

[71] D. V. Dimitrov, "Medical Internet of Things and big data in healthcare," *Healthcare Inform. Res.*, vol. 22, no. 3, pp. 156–163, Jul. 2016.

[72] Z. Jiemin and L. Jinsheng, "The district medical data center based on cloud computing," in *Proc. 5th Int. Conf. Comput. Sci. Educ.*, Aug. 2010, pp. 1424–1427.

[73] C.-W. Jeong, W.-H. Kim, S. Lypengleang, Y.-S. Jeong, S.-C. Joo, and K.-H. Yoon, "The development of a medical image information system environment using data synchronization based on cloud computing," *Multimedia Tools Appl.*, vol. 75, no. 23, pp. 15479–15492, Dec. 2016.

[74] T. Xue *et al.*, "Research on medical data sharing model based on blockchain," *Acta Automatica Sinica*, vol. 43, no. 9, pp. 1555–1562, Dec. 2017.

[75] H. Huang, P. Zhu, F. Xiao, X. Sun, and Q. Huang, "A blockchain-based scheme for privacy-preserving and secure sharing of medical data," *Comput. Secur.*, vol. 99, Dec. 2020, Art. no. 102010.

[76] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "BLOCKBENCH: A framework for analyzing private blockchains," in *Proc. ACM Int. Conf. Manage. Data*, May 2017, pp. 1085–1100.

[77] S. Wang *et al.*, "Forkbase: An efficient storage engine for blockchain and forkable applications," *Proc. VLDB Endowment*, vol. 11, no. 10, pp. 1137–1150, Feb. 2018.

[78] M. M. Baig and H. Gholamhosseini, "Smart health monitoring systems: An overview of design and modeling," *J. Med. Syst.*, vol. 37, no. 2, pp. 1–14, Jan. 2013.

[79] I. Chiuchisan and O. Geman, "An approach of a decision support and home monitoring system for patients with neurological disorders using Internet of Things concepts," *WSEAS Trans. Syst.*, vol. 13, no. 1, pp. 460–469, Jan. 2014.

[80] C. Liu, G. Chen, X. Yuan, Y. Zhang, and Z. Xiao, "Real-time health monitoring system based on wearable devices," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2020, pp. 2002–2004, doi: 10.1109/IWCMC48107.2020.9148180.

[81] H. N. Saha, N. F. Raun, and M. Saha, “Monitoring patient’s health with smart ambulance system using Internet of Things (IOTs),” in *Proc. 8th Annu. Ind. Automat. Electromech. Eng. Conf. (IEMECON)*, Aug. 2017, pp. 91–95.

[82] C. A. da Costa, C. F. Pasluosta, B. Eskofier, D. B. da Silva, and R. da Rosa Righi, “Internet of Health Things: Toward intelligent vital signs monitoring in hospital wards,” *Artif. Intell. Med.*, vol. 89, pp. 61–69, Jul. 2018.

[83] M. T. Mardini, Y. Iraqi, and N. Agoulmine, “A survey of healthcare monitoring systems for chronically ill patients and elderly,” *J. Med. Syst.*, vol. 43, no. 3, p. 50, Jan. 2019.

[84] S. Tuli *et al.*, “HealthFog: An ensemble deep learning based smart healthcare system for automatic diagnosis of heart diseases in integrated IoT and fog computing environments,” *Future Gener. Comput. Syst.*, vol. 104, pp. 187–200, Mar. 2020.

[85] A. Ray and R. Cleaveland, “Security assurance cases for medical cyber-physical systems,” *IEEE Des. Test. Comput.*, vol. 32, no. 5, pp. 56–65, Oct. 2015.

[86] P.-L. Wu, L. Sha, R. B. Berlin, and J. M. Goldman, “Safe workflow adaptation and validation protocol for medical cyber-physical systems,” in *Proc. 41st Euromicro Conf. Softw. Eng. Adv. Appl.*, Aug. 2015, pp. 464–471.

[87] R. Altawy and A. M. Youssef, “Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices,” *IEEE Access*, vol. 4, pp. 959–979, 2016.

[88] S. Chen, O. Sokolsky, J. Weimer, and I. Lee, “Data-driven adaptive safety monitoring using virtual subjects in medical cyber-physical systems: A glucose control case study,” *J. Comput. Sci. Eng.*, vol. 10, no. 3, pp. 75–84, Sep. 2016.

[89] F. Kuhn, D. Thoma, D. Labitzke, and S. Fischer, “Monitoring as a service for networked medical cyber-physical systems,” in *Proc. 43rd Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Oct. 2017, pp. 8648–8653.

[90] M. Anandarajan and S. Malik, “Protecting the internet of medical things: A situational crime-prevention approach,” *Cogent Med.*, vol. 5, no. 1, Sep. 2018, Art. no. 1513349.

[91] F. A. O. Santos, G. S. de Jesus, G. A. Botelho, and H. T. Macedo, “Smart health: Using fuzzy logic in the monitoring of health-related indicators,” in *Proc. 8th Euro Amer. Conf. Telematics Inf. Syst. (EATIS)*, Apr. 2016, pp. 1–4.

[92] L. Shangguan and S. Gopalswamy, “Health monitoring for cyber physical systems,” *IEEE Syst. J.*, vol. 14, no. 1, pp. 1457–1467, Mar. 2020.

[93] J. Mohammed, C.-H. Lung, A. Ocneanu, A. Thakral, C. Jones, and A. Adler, “Internet of Things: Remote patient monitoring using web services and cloud computing,” in *Proc. IEEE Int. Conf. Internet Things(iThings), IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom)*, Sep. 2014, pp. 256–263.

[94] 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 telemonitoring pregnancy,” *Concurrency Comput., Pract. Exper.*, vol. 30, no. 2, p. e4236, Jul. 2017.

[95] S. Wang *et al.*, “Construction of medical equipment-based doctor health monitoring system,” *J. Med. Syst.*, vol. 43, no. 5, pp. 1–7, Apr. 2019.

[96] J. H. Ahnn and M. Potkonjak, “MHealthMon: Toward energy-efficient and distributed mobile health monitoring using parallel offloading,” *J. Med. Syst.*, vol. 37, no. 5, pp. 1–11, Jul. 2013.

[97] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, “Healthcare blockchain system using smart contracts for secure automated remote patient monitoring,” *J. Med. Syst.*, vol. 42, no. 7, pp. 1–7, Jul. 2018.

[98] G. Alfian, M. Syafrudin, M. Ijaz, M. Syaekhoni, N. Fitriyani, and J. Rhee, “A personalized healthcare monitoring system for diabetic patients by utilizing BLE-based sensors and real-time data processing,” *Sensors*, vol. 18, no. 7, p. 2183, Jul. 2018.

[99] P. Lopez-Iturri *et al.*, “Implementation and operational analysis of an interactive intensive care unit within a smart health context,” *Sensors*, vol. 18, no. 2, p. 389, Jan. 2018.

[100] P. S. Wilhelm and M. Reza, “Survey on a smart health monitoring system based on context awareness sensing,” *Commun. CCISA*, vol. 25, pp. 1–13, Feb. 2019.

[101] R. Atat, L. Liu, J. Wu, G. Li, C. Ye, and Y. Yang, “Big data meet cyber-physical systems: A panoramic survey,” *IEEE Access*, vol. 6, pp. 73603–73636, 2018.

[102] R. Mitchell and R. Chen, “Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems,” *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 1, pp. 16–30, Jan. 2015.

[103] I. You, K. Yim, V. Sharma, G. Choudhary, I.-R. Chen, and J.-H. Cho, “Misbehavior detection of embedded IoT devices in medical cyber physical systems,” in *Proc. IEEE/ACM Int. Conf. Connected Health, Appl., Syst. Eng. Technol.*, Sep. 2018, pp. 88–93.

[104] M. R. Kanjee and H. Liu, “Authentication and key relay in medical cyber-physical systems,” *Secur. Commun. Netw.*, vol. 9, no. 9, pp. 874–885, May 2014.

[105] O. Kocabas, T. Soyata, and M. K. Aktas, “Emerging security mechanisms for medical cyber physical systems,” *IEEE/ACM Trans. Comput. Biol. Bioinf.*, vol. 13, no. 3, pp. 401–416, May 2016.

[106] Z. Fu, C. Guo, S. Ren, Y. Ou, and L. Sha, “Modeling and integrating human interaction assumptions in medical cyber-physical system design,” in *Proc. IEEE 30th Int. Symp. Comput.-Based Med. Syst. (CBMS)*, Jun. 2017, pp. 1615–1618.

[107] H. Almohri, L. Cheng, D. Yao, and H. Alemzadeh, “On threat modeling and mitigation of medical cyber-physical systems,” in *Proc. IEEE/ACM Int. Conf. Connected Health, Appl., Syst. Eng. Technol. (CHASE)*, Jul. 2017, pp. 114–119.

[108] H. Song, J. Bai, Y. Yi, J. Wu, and L. Liu, “Artificial intelligence enabled Internet of Things: Network architecture and spectrum access,” *IEEE Comput. Intell. Mag.*, vol. 15, no. 1, pp. 44–51, Feb. 2020.

[109] A. Ghoneim *et al.*, “Medical image forgery detection for smart healthcare,” *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 33–37, Apr. 2018.

[110] F. A. Turjman and S. Alturjman, “Context-sensitive access in industrial Internet of Things (IIoT) healthcare applications,” *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2736–2744, Feb. 2018.

[111] W. Meng, W. Li, Y. Wang, and M. H. Au, “Detecting insider attacks in medical cyber–physical networks based on behavioral profiling,” *Future Gener. Comput. Syst.*, vol. 108, pp. 1258–1266, Jul. 2020.

[112] W. Schneble and G. Thamilarasu, “Attack detection using federated learning in medical cyber-physical systems,” in *Proc. 28th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Aug. 2019, pp. 1–8.

[113] G. Choudhary, P. V. Astillo, I. You, K. Yim, I.-R. Chen, and J.-H. Cho, “Lightweight misbehavior detection management of embedded IoT devices in medical cyber physical systems,” *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 4, pp. 2496–2510, Dec. 2020.

[114] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, “Blockchain-based medical records secure storage and medical service framework,” *J. Med. Syst.*, vol. 43, no. 1, pp. 1–9, Nov. 2018.

[115] M. Krotofil, J. Larsen, and D. Gollmann, “The process matters: Ensuring data veracity in cyber-physical systems,” in *Proc. 10th ACM Symp. Inf., Comput. Commun. Secur.*, Apr. 2015, pp. 133–144.

[116] S. Cao, X. Zhang, and R. Xu, “Toward secure storage in cloud-based eHealth systems: A blockchain-assisted approach,” *IEEE Netw.*, vol. 34, no. 2, pp. 64–70, Mar. 2020.

[117] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, “MedBlock: Efficient and secure medical data sharing via blockchain,” *J. Med. Syst.*, vol. 42, no. 8, pp. 1–11, Jun. 2018.

[118] M. Ameyv, “Security for cyber-physical systems,” *Int. J. Comput. Technol.*, vol. 1, no. 6, pp. 257–261, Jul. 2014.

[119] D. He and S. Zeadally, “An analysis of RFID authentication schemes for Internet of Things in healthcare environment using elliptic curve cryptography,” *IEEE Internet Things J.*, vol. 2, no. 1, pp. 72–83, Feb. 2015.

[120] N. I. Mowla, I. Doh, and K. Chae, “Binarized multi-factor cognitive detection of bio-modality spoofing in fog based medical cyber-physical system,” in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2019, pp. 43–48, doi: 10.1109/ICOIN.2019.8718118.

[121] A. Alhayajneh, A. Baccarini, G. Weiss, T. Hayajneh, and A. Farajidavar, “Biometric authentication and verification for medical cyber physical systems,” *Electronics*, vol. 7, no. 12, p. 436, Dec. 2018.

[122] Z. Xu, C. Xu, W. Liang, J. Xu, and H. Chen, “A lightweight mutual authentication and key agreement scheme for medical Internet of Things,” *IEEE Access*, vol. 7, pp. 53922–53931, 2019.

[123] S. R. Moosavi *et al.*, “End-to-end security scheme for mobility enabled healthcare Internet of Things,” *Future Gener. Comput. Syst.*, vol. 64, pp. 108–124, Mar. 2016.

[124] R. Amin, R. S. Sherratt, D. Giri, S. H. Islam, and M. K. Khan, “A software agent enabled biometric security algorithm for secure file access in consumer storage devices,” *IEEE Trans. Consum. Electron.*, vol. 63, no. 1, pp. 53–61, Feb. 2017.

[125] N. R. Mohsen, B. Ying, and A. Nayak, "Authentication protocol for real-time wearable medical sensor networks using biometrics and continuous monitoring," in *Proc. Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2019, pp. 1199–1206, doi: 10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00201.

[126] S. F. Aghili, H. Mala, M. Shojafar, and P. Peris-Lopez, "LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT," *Future Gener. Comput. Syst.*, vol. 96, pp. 410–424, Jul. 2019.

[127] N. Alexopoulos, J. Daubert, M. Muhlhauser, and S. M. Habib, "Beyond the hype: On using blockchains in trust management for authentication," in *Proc. IEEE Trustcom/BigDataSE/ICESS*, Aug. 2017, pp. 546–553.

[128] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town crier: An authenticated data feed for smart contracts," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 270–282.

[129] M. Al-Bassam, "SCPKI: A smart contract-based PKI and identity system," in *Proc. ACM Workshop Blockchain, Cryptocurrencies Contracts*, Apr. 2017, pp. 35–40.

[130] M. Elhoseny, G. Ramirez-Gonzalez, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure medical data transmission model for IoT-based healthcare systems," *IEEE Access*, vol. 6, pp. 20596–20608, 2018.

[131] S. Srisakthi and A. P. Shanthi, "Design of a secure encryption model (SEM) for cloud data storage using Hadamard transforms," *Wireless Pers. Commun.*, vol. 100, no. 4, pp. 1727–1741, Apr. 2018.

[132] H. Tian *et al.*, "Dynamic-hash-table based public auditing for secure cloud storage," *IEEE Trans. Services Comput.*, vol. 10, no. 5, pp. 701–714, Sep. 2017.

[133] X. Zhang, J. Zhao, L. Mu, Y. Tang, and C. Xu, "Identity-based proxy-oriented outsourcing with public auditing in cloud-based medical cyber–physical systems," *Pervas. Mobile Comput.*, vol. 56, pp. 18–28, May 2019.

[134] D. Zheng, A. Wu, Y. Zhang, and Q. Zhao, "Efficient and privacy-preserving medical data sharing in Internet of Things with limited computing power," *IEEE Access*, vol. 6, pp. 28019–28027, 2018.

[135] M. Ma *et al.*, "Certificateless searchable public key encryption scheme for mobile healthcare system," *Comput. Elect. Eng.*, vol. 65, pp. 413–424, May 2018.

[136] Z. Chen *et al.*, "Verifiable keyword search for secure big data-based mobile healthcare networks with fine-grained authorization control," *Future Gener. Comput. Syst.*, vol. 87, pp. 712–724, Oct. 2018.

[137] H. Li, Y. Yang, Y. Dai, S. Yu, and Y. Xiang, "Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data," *IEEE Trans. Cloud Comput.*, vol. 8, no. 2, pp. 484–494, Apr. 2020.

[138] X. Zhang, Y. Tang, S. Cao, C. Huang, and S. Zheng, "Enabling identity-based authorized encrypted diagnostic data sharing for cloud-assisted E-health information systems," *J. Inf. Secur. Appl.*, vol. 54, Oct. 2020, Art. no. 102568.

[139] H. Wang and Y. Song, "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain," *J. Med. Syst.*, vol. 42, no. 8, pp. 152–160, Jul. 2018.

[140] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," *Comput. Ind.*, vol. 100, pp. 212–223, Sep. 2018.

[141] S. M. Djouadi, A. M. Melin, E. M. Ferragut, J. A. Laska, J. Dong, and A. Drira, "Finite energy and bounded actuator attacks on cyber-physical systems," in *Proc. Eur. Control Conf. (ECC)*, Jul. 2015, pp. 3659–3664.

[142] A. L. King, L. Feng, O. Sokolsky, and I. Lee, "Assuring the safety of on-demand medical cyber-physical systems," in *Proc. IEEE 1st Int. Conf. Cyber-Physical Syst., Netw., Appl. (CPSNA)*, Aug. 2013, pp. 1–6.

[143] A. A. Omala, A. S. Mbandu, K. D. Mutiria, C. Jin, and F. Li, "Provably secure heterogeneous access control scheme for wireless body area network," *J. Med. Syst.*, vol. 42, no. 6, pp. 1–14, Apr. 2018.

[144] H. Qiu, M. Qiu, M. Liu, and G. Memmi, "Privacy-preserving health data sharing for medical cyber-physical systems," 2019, *arXiv:1904.08270*.

[145] F. Li, Y. Han, and C. Jin, "Cost-effective and anonymous access control for wireless body area networks," *IEEE Syst. J.*, vol. 12, no. 1, pp. 747–758, Mar. 2018.

[146] Y. O'Connor *et al.*, "Privacy by design: Informed consent and Internet of Things for smart health," in *Proc. 7th Int. Conf. Current Future Trends Inf. Commun. Technol. Healthcare*, vol. 113, Dec. 2017, pp. 653–658.

[147] S. Chandrasekhar, A. Ibrahim, and M. Singhal, "A novel access control protocol using proxy signatures for cloud-based health information exchange," *Comput. Secur.*, vol. 67, pp. 73–88, Jun. 2017.

[148] Z. Xiao, J.-J. Yang, M. Huang, L. Ponnambalam, X. Fu, and R. S. M. Goh, "QLDS: A novel design scheme for trajectory privacy protection with utility guarantee in participatory sensing," *IEEE Trans. Mobile Comput.*, vol. 17, no. 6, pp. 1397–1410, Jun. 2018.

[149] S. Xiao, H. Yu, Y. Wu, Z. Peng, and Y. Zhang, "Self-evolving trading strategy integrating Internet of Things and big data," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2518–2525, Oct. 2017.

[150] J. Zhang *et al.*, "On efficient and robust anonymization for privacy protection on massive streaming categorical information," *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 5, pp. 507–520, Sep. 2017.

[151] 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.

[152] 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.

[153] 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 telemonitoring pregnancy," *Concurrency Comput., Pract. Exper.*, vol. 30, no. 2, p. e4236, Jan. 2018.

[154] 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.

[155] 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.

[156] 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.

[157] J. M. de Fuentes, L. Gonzalez-Manzano, A. Solanas, and F. Veseli, "Attribute-based credentials for privacy-aware smart health services in IoT-based smart cities," *Computer*, vol. 51, no. 7, pp. 44–53, Jul. 2018.

[158] F. Ullah, A. H. Abdullah, O. Kaiwartya, and Y. Cao, "TraPy-MAC: Traffic priority aware medium access control protocol for wireless body area network," *J. Med. Syst.*, vol. 41, no. 6, p. 93, Jun. 2017.

[159] 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.

[160] 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.

[161] 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.

[162] 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.

[163] 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.

[164] 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.

[165] 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.

[166] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[167] 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.

**Fulong Chen** (Member, IEEE) received the B.S. degree from Anhui Normal University, Wuhu, China, in 2000, the M.S. degree from China West University, Nanchong, China, in 2005, and the Ph.D. degree from Northwestern Polytechnical University, Xi'an, China, in 2011.

He is currently a Professor with the School of Computer and Information, Anhui Normal University. His research interests are embedded and pervasive computing, cyber–physical systems, high-performance computer architecture, and security of the Internet of Things.

**Yuqing Tang** received the B.S. degree from Anhui Normal University, Wuhu, China, in 2019, where she is currently pursuing the master's degree with the School of Computer and Information.

Her research interests are blockchain and cyber–physical systems.

**Canlin Wang** received the B.S. degree from Anhui Normal University, Wuhu, China, in 2019, where she is currently pursuing the master's degree with the School of Computer and Information.

Her research interests are blockchain and cyber–physical systems.

**Jing Huang** received the B.S. degree from Anhui Normal University, Wuhu, China, in 2019, where she is currently pursuing the master's degree with the School of Computer and Information.

Her research interests are blockchain and cyber–physical systems.

**Cheng Huang** received the B.S. degree from the Anhui University of Science and Technology, Huainan, China, in 2017, and the M.S. degree from Anhui Normal University, Wuhu, China, in 2020.

His research interests are blockchain and cyber–physical systems.

**Dong Xie** received the Ph.D. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2017.

He is currently with the School of Computer and Information, Anhui Normal University, Wuhu, China. His research interests include cryptography, information security, and compressed sensing.

**Taochun Wang** received the B.S. and M.S. degrees from Yunnan University, Kunming, China, in 2002 and 2005, respectively, and the Ph.D. degree from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2016.

He is currently a Professor with the School of Computer and Information, Anhui Normal University, Wuhu, China. His research interests are privacy preservation and the Internet of Things.

**Chuanxin Zhao** received the Ph.D. degree from Soochow University, Suzhou, China, in 2011.

He is currently a Professor with Anhui Normal University, Wuhu, China. His current research interests are in the areas of rechargeable sensor networks, fog computing, and Internet-of-Things (IoT) resource optimization.