Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.030958
Article

MEC-IoT-Healthcare: Analysis and Prospects

Hongyuan Wang[1], Mohammed Dauwed[2], Imran Khan[3], Nor Samsiah Sani[4,*], Hasmila Amirah Omar[4], Hirofumi Amano[5] and Samih M. Mostafa[6]

[1]College of Computer Science, Guangdong University of Science and Technology, DongGuan, 523083, China
[2]Department of Medical Instrumentation Techniques Engineering, Dijlah University College, Baghdad, Iraq
[3]Department of Electrical Engineering, University of Engineering & Technology, Peshawar, 814, Pakistan
[4]Center for Artificial Intelligence Technology, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600, Bangi, Selangor, Malaysia
[5]Research Institute for Information Technology, Kyushu University, Fukuoka, 819-0395, Japan
[6]Computer Science-Mathematics Department, Faculty of Science, South Valley University, Qena, 83523, Egypt
*Corresponding Author: Nor Samsiah Sani. Email: norsamsiahsani@ukm.edu.my
Received: 07 April 2022; Accepted: 11 May 2022

Abstract: Physical sensors, intelligent sensors, and output recommendations are all examples of smart health technology that can be used to monitor patients' health and change their behavior. Smart health is an Internet-of-Things (IoT)-aware network and sensing infrastructure that provides real-time, intelligent, and ubiquitous healthcare services. Because of the rapid development of cloud computing, as well as related technologies such as fog computing, smart health research is progressively moving in the right direction. Cloud, fog computing, IoT sensors, blockchain, privacy and security, and other related technologies have been the focus of smart health research in recent years. At the moment, the focus in cloud and smart health research is on how to use the cloud to solve the problem of enormous health data and enhance service performance, including cloud storage, retrieval, and calculation of health big data. This article reviews state-of-the-art edge computing methods that has shifted to the collection, transmission, and calculation of health data, which includes various sensors and wearable devices used to collect health data, various wireless sensor technologies, and how to process health data and improve edge performance, among other things. Finally, the typical smart health application cases, blockchain's application in smart health, and related privacy and security issues were reviewed, as well as future difficulties and potential for smart health services. The comparative analysis provides a reference for the the mobile edge computing in healthcare systems.

Keywords: IoT; mobile-edge computing; cloud computing; e-health

1 Introduction

With the acceleration of population aging, the prevalence of chronic diseases and the outbreak of epidemics, more and more attention is focused on the quality of life and health issues of residents, and people are paying more and more attention to health issues. However, the average age of the population increases and the epidemic of chronic diseases has led to the rapid growth of people's demand for medical resources, especially in urban areas with high population concentration. The medical resources of hospitals and clinics at all levels are very precious, and it is difficult to provide real-time medical protection for patients. It is conceivable that in the near future, medical and health services will gradually transform from centralized medical services provided by hospitals to ubiquitous and real-time smart health services. There are three reasons for this evolution. First, people's interest in more comprehensive, smarter and more proactive medical and health services demand for smart health services continues to grow. The key part of the service is to provide personal health data that can be used for smart health services through real-time, unobtrusive health monitoring. Secondly, the common and shared characteristics of smart health service infrastructure will be reduced and increasing cost of medical and health services at this stage. Finally, with the rapid development of cloud computing, fog computing and Internet-of-Things (IoT) sensors and other related technologies, a solid foundation has been laid for the transformation of medical services.

This change in the form of medical services has gradually given birth to the concept of smart health. In a nutshell, smart health is the use of the environment-aware network and sensing infrastructure of the IoTs to provide real-time, smart and ubiquitous health care services. Smart health services first need to be real-time. For example, the monitoring of some key physiological indexes does not accept large delays to avoid delays in timing. This real-time performance needs to be achieved through the cooperation of cloud computing, fog computing and edge devices. Using some smart programs on the fog side or smart sensors on the edge, smart health services can provide smarter medical services. Finally, smart health services are ubiquitous, no matter where the person is, use the surroundings IoT sensors and wearable sensor devices can realize ubiquitous smart health services.

As shown in Fig. 1, the requirements for performance, energy efficiency, security, and privacy protection of smart health services nowadays lead the system to set up diversified computing layers in the cloud, terminal equipment and between the two, and provide high-quality through cross-layer design and management. It can be seen that after the terminal sensor collects the relevant human physiological index, there are usually many options for data processing. For the massive data processing that does not require high real-time and mobile computing, we can use the cloud proxy directly upload data to the cloud. For smart health services that require high real-time and mobile computing, the data is first uploaded to the fog computing layer (such as a smart gateway) through a fog proxy, in the fog computing layer. The fog will reasonably decide how to process the data according to the current load situation, cloud operation status and task attributes. Fig. 1 describes three upload schedulers that are cloud, cloud-side assisted, and fog-side computing.

Next, this article will discuss in detail the related research and development of smart health from the cloud to the edge and list typical smart health applications. Moreover, since the blockchain has a wide range of application scenarios, the application of the chain in smart health is discussed. Finally, the privacy and security of smart health is discussed, as well as some opportunities and challenges are encountered in the future.

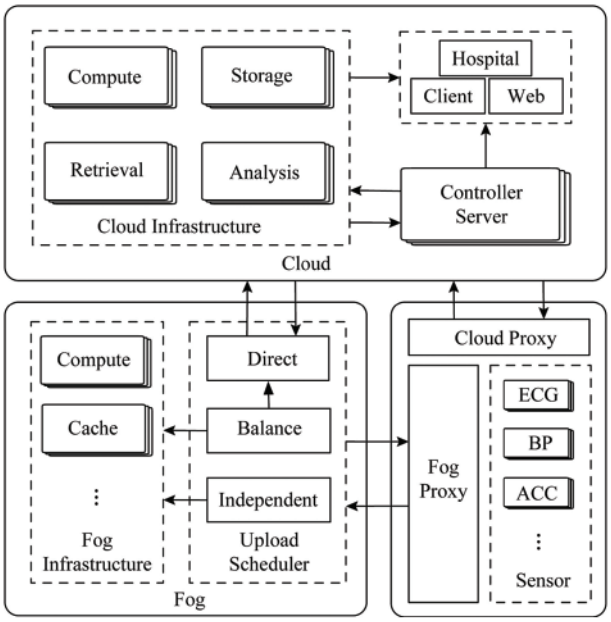

Figure 1: Proposed model

2 Smart Health in the Cloud

Thanks to the rapid development of the IoTs and mobile networks, most of the researches are focusing on smart health and various types of biosensors and other related portable medical devices [1]. These medical gadgets can capture a wide range of real-time health data, including blood pressure, body temperature, and heart rate, among other things. The health data are massive, and storing, analyzing, and processing them on mobile devices is tough. How to quickly and effectively process health big data has become a challenge. Big data usually refers to exabyte (EB) and a larger range of data. It has the characteristics of large capacity, diversification, speed, and complexity [2]. Health big data not only has all the characteristics of big data, but also the value and significance of health big data to people is also not available. The typical stand-alone systems and portable mobile devices do not have the storage and processing capacity for smart health big data, however the cloud computing platform has powerful computing storage capabilities. Currently, it is stored and analyzed in the cloud and processing health big data is the most suitable and cost-effective method.

Cloud computing is an abstraction of computing resources. It provides users with dynamically scalable and virtualized computing resources as services. It has basic features such as on-demand service provision, extensive access methods, aggregated resource pools, and rapid and flexible allocation [3–6]. Thanks to these basic characteristics of cloud computing, smart health service providers can build real-time, smart and ubiquitous smart health applications on the cloud-based system framework, and can satisfy the requirements of big data in smart health. It can be said that the rapid development of cloud computing has laid a solid foundation for the actual implementation of smart health services. Based on this, most researches have begun to pay attention to cloud computing and smart health services, how to use them to achieve real-time smart health services and how to meet the requirements of health big data has become the focus of research. This article analyzes and summarizes the relevant research on cloud and smart health in recent years. Next, we start from smart health big data with

three aspects of storage, retrieval and data processing are introduced to the research and development of smart health big data in the cloud.

2.1 Storage of Health Big Data in the Cloud

With the continuous development of medical informatization and the rapid development of various medical sensor technologies, most health big data are generated in real time, and it becomes much difficult to store data in stand-alone systems or portable mobile devices [7]. Most sensor health data are generated in real time, especially some health monitoring data generated by wearable devices, which must be uploaded and processed in time to avoid missing the best opportunity. As shown in Table 1, for health big data in the cloud to different research focus, this article will discuss from three aspects that are storage for heterogeneous data, storage with high reliability and high fault tolerance, storage based on privacy and security.

Table 1: Database analysis for MEC-IoT-health

Parameter	Reference [8]	Reference [9]	Reference [10]	Reference [11]	Reference [12]	Reference [13]
Data	Health	Health	HER & image	Clinic file	HER	Health
Focus	Optimizing complexity	Optimizing complexity	Fault tolerance & reliability	Fault tolerance & reliability	Security & privacy	Security & privacy
Method	NoSQL	NoSQL/SQL	Hadoop distributed file system	Distributed file system	RAID-3	Encryption
Pros	Resolve pattern difference	Different structure data	Large fault tolerance	Mass storage	Data security	Personal privacy

2.1.1 Storage Optimized for Data Complexity

Different from traditional Internet big data, various types of medical and health equipment will generate a large amount of complex heterogeneous health data. It is difficult for these medical and health data with different structures to be standardized and defined in a unified model. Traditional relational databases will It is difficult to meet the storage requirements of the heterogeneity and complexity of medical and health data [14]. How to store health big data has become a key challenge for smart health research. At present, thanks to the emergence and rapid development of non-relational databases, commercial and open source solutions are beginning to use non-relational databases to replace traditional relational databases to process healthy big data. Compared with traditional relational database systems, non-relational databases break the limitation of schema fields and provide schemalessness. The data storage is more flexible. Some common non-relational databases are shown in Table 2 that are Key-value database, document database, column database, graph database and time series database.

Table 2: Application scenarios of non-relational database

	Database						
	HBase	Memcached	Neo4J	Redis	InfluxDB	MongoDB	CouchDB
Type	Column	Key value	Graph	Key value	Time series	File	File
Utilization	Large medical data	Cache of health data	Medical data lookup	Cache of health data	Electronic health information	Heterogeneous health information	Heterogeneous health information

Since non-relational databases do not require a fixed table mode, it is a common practice to use non-relational databases for the storage of heterogeneous health big data. Reference [8] proposed a fast non-relational database based comprehensive method for processing, storing, retrieving and analyzing medical and health big data. This method is based on a non-relational database and uses a patient-centric data architecture to achieve rapid data storage and flexible expansion. The time series mode can be used for a visual representation of patient records, which can be used as a reference for doctors to provide consultations to patients. The method proposed by [8] can overcome the model differences of various types of medical and health big data, and ensure flexibility and large-scale storage.

Medical and health big data generally comes from multiple different sources, such as various types of medical sensors with different functions, large medical equipment, and portable medical equipment. The data forms and structures are not the same. Therefore, the database must adopt a series of different models to store and process different forms of medical and health big data. Reference [9] proposed a framework for managing health big data, which combines relational databases and non-relational databases (graphic and document databases) to adapt to the different cloud forms of medical and health big data in China. In summary, smart health services based on non-relational databases can effectively deal with the storage problem of heterogeneous health big data.

2.1.2 High Reliability and High Fault Tolerance Storage

Due to the particularity of health big data, health big data not only has a huge amount of data, but also requires very high security, and has zero tolerance for data loss. For this reason, we are designing storage and file management for medical and health big data. A series of work has been carried out on the system. The file and storage system must not only meet the needs of storing massive medical and health data, but also need to ensure high reliability and high fault tolerance to provide reliable medical information services. The distributed file system is composed of a large number of storage nodes are connected to a large file system through a network, which can store massive amounts of data, and the data is usually protected by methods such as keeping copies to ensure high reliability of services [15]. At present, many studies have adopted distributed file systems. It solves the storage problem of massive medical and health data, and ensure the high reliability and fault tolerance of medical services.

Hadoop distributed file system (HDFS) is a distributed file system of Hadoop that can store massive amounts of big data. Reference [10] tried to solve the problem of storing and sharing medical images and electronic medical records in the cloud, and developed a HDFS-based medical imaging file accessing system (MIFAS). The system is a medical imaging system with a distributed file system, which can realize high-reliability medical data storage and high fault tolerance.

To address some of the shortcomings of existing hospital management systems, reference [11] presented a cloud computing-based smart hospital file management system. Some stand-alone hardware devices have storage capacity constraints, and resource sharing between platforms is one of these limitations. The performance of the hardware has been lowered. A core server and numerous

server blocks make up this system. Large files are broken down into fixed-size blocks, with three backup blocks for each block. The file system metadata is managed by the main server, which includes the physical address of the namespace, access control, file block mapping, and other associated information. This approach makes use of a large number of low-cost server clusters that may flexibly allow applications to overcome physical barriers and make the most use of system resources based on their requirements.

2.1.3 Storage Based on Privacy and Security Protection

Compared with traditional Internet big data, the privacy and security of medical and health big data are more important. Personal privacy is a very sensitive topic. If you simply store medical and health data in the cloud, it may cause many privacy and security issues. Especially with the rapid growth of Internet data and the acceleration of medical informatization, people are paying significant attention to the issues of privacy and security. How to store health big data safely in the cloud has become a major challenge.

The redundant array of inexpensive disk (RAID-3) is a traditional disk storage array strategy, which can guarantee the security of disk data. Reference [12] developed a new technique for storing electronic medical records spread across two clouds and local sites using the RAID-3 algorithm. It renders the segmented data stored in each cloud useless and unusable on its own. This strategy maintains patient data on the cloud in order to address the growing need for EHR storage space as well as the data security requirements are essential.

To address the security, integrity, confidentiality, and integration challenges of diverse medical and health services, reference [13] developed a data capture and auto identification reference (DACAR) platform. For data storage, the DACAR platform uses a private cloud, while hosting services are provided via a hybrid cloud. To maintain the security of medical and health data as well as personal privacy, the platform employs database-level encryption, digital signature verification, hashing, and integrity verification technologies.

2.2 Retrieval of Health Big Data in the Cloud

The medical and health data stored in the cloud comes from various types of medical equipment, medical sensors, and heterogeneous embedded devices. These massive amounts of data often have different patterns and structures. For these different forms of medical and health big data stored in the cloud efficient retrieval has become a very challenging issue. Reference [16] analyzed the functions of the medical information retrieval system from the historical retrieval records based on the electronic health record search system and what specific requirements need to be met. Reference [17] analyzed the query log records of medical search engines to promote the efficiency of information retrieval in electronic health records. The analysis results show that the information needs of the medical field are much more complex than those of general Internet search engines. Query accuracy and time efficiency are two important indicators for evaluating the performance of medical retrieval systems.

2.2.1 Medical Information Retrieval

Retrieving large-scale medical information in the cloud is a very time-consuming operation, and due to the privacy of medical information, most of the medical information in the cloud is encrypted, which makes the retrieval more difficult. How to effectively improve the retrieval efficiency of medical information has become a research focus. In trials, reference [18] looked into the impact of query complexity and expansion tactics on genetic information retrieval. They discovered that query

expansion tactics did not significantly boost efficiency. The study also demonstrates that string index expansion outperforms word index expansion, and that queries with fewer terms perform better than queries with more terms. According to these findings, genetic information retrieval systems should allow variable query expansion methodologies and be able to respond to questions of varying levels of complexity.

Because sensitive medical data must be encrypted before being stored in the cloud, data recovery from encrypted documents is a vital technique in cloud storage. Many of the searchable encryption solutions currently available are intended for single-user applications. Reference [19] is a flexible encrypted document search solution that focuses on the application scenarios with many senders and various consumers. Attribute-based encryption (ABE) is employed in this system to offer fine-grained access control and synonym keyword search. Reference [20] proposed a retrieval scheme for encrypted electronic medical records. The scheme uses a hierarchical attribute vector representation method to achieve flexible and complex multi-domain keyword join queries, such as subset queries and range query etc.

2.2.2 Medical Image Retrieval

Medical image retrieval is different from information query. Information query only needs to match similar keywords or strings to find relevant content, but this is problematic for medical image retrieval. The goal of medical image retrieval is to help relevant medical personnel make decisions. In these scenarios, given the medical images that need to be retrieved, the goal is to retrieve similar images or related medical information from the cloud database. The queried content can help relevant medical personnel understand the reference medical interpretation of the queried image. If the image or information given by the retrieval system does not match the semantics of the queried image, this will lead to distrust of the user. On the other hand, if the result given by the retrieval system is similar to the queried medical image, but it is wrong result, then this will lead to misjudgment by relevant medical personnel.

Reference [21] proposed an enhanced framework for medical image retrieval, aiming to maintain image visual and semantic similarity. They designed an enhanced algorithm to effectively learn the distance function, which can maintain the semantic similarity of retrieval results and images, and has a very low computational cost. Reference [22] proposed a content-based image retrieval framework suitable for medical images of different imaging modalities. This framework includes image pre-filtering machine learning methods, similarity matching using statistical distance measurement, and related feedback schemes. This image retrieval framework can effectively narrow the semantic gap and improve retrieval efficiency.

Medical information and image retrieval are two important directions for the retrieval of health data in the cloud. In addition to studying how to retrieve data in the cloud, it is also necessary to focus on how to integrate and retrieve various distributed and heterogeneous medical information systems. Reference [23] describes a retrieval framework that retrieves biomedical information from various distributed and heterogeneous sources, manages it to improve the results obtained and shortens response time, and finally integrates it to make it useful to relevant medical personnel, providing all available information about the patient. Reference [24] proposed a client-server proxy framework that allows portals to access different hospital information systems through the intranet and the Internet. It can remotely access the hospital usually a closed information system and server that indexes all medical data and allows complex data retrieval.

2.3 Computing of Health Big Data in the Cloud

Medical sensors and portable mobile devices have limited computing power, which does not allow real-time processing of medical and health data on-site. The collected data needs to be transmitted to nodes with more powerful computing power for processing. The cloud computing platform is a platform with powerful computing power and it can be accessed anytime and anywhere, which can help edge medical devices and portable mobile devices to calculate and process data. Using cloud computing can not only do medical and health big data processing in the cloud, but also help relieve the load pressure of edge medical devices and significantly improve mobile devices efficiency in healthcare.

2.3.1 Cloud Processing

The scale of cloud computing platforms is very large. Large commercial cloud computing platforms even have tens of thousands of servers to provide services. Thanks to the powerful computing power of cloud computing, various types of medical big data can be analyzed and processed in the cloud. Such tasks usually require strong computing power, not real-time.

Bio-signal analysis is a time-consuming and labor-intensive thing and usually requires the support of cloud computing. Reference [25] proposed a bio-signal analyzing cloud computing architecture (BACCA). The system is based on the concept of service-oriented architecture and integrates heterogeneous platforms, protocols, and applications in the cloud. In this biosignal analysis framework, for different data sets, the overall accuracy of brainwave biosignal analysis has been improved to 98%.

It is a common practice to use data mining to discover in-depth information on massive medical big data in the cloud. Reference [26] developed a cloud-based personal health care system. The system uses portable mobile devices to organize personal health data according to time. The sequence is stored in the cloud. When the data is sufficient, the data mining method is used in the cloud to automatically extract useful health information, such as personal health information hidden in big data.

The analysis and processing of electronic health information in the cloud has become the norm due to the heterogeneous character and huge scale of electronic health records. Methods including Bayesian networks, neural networks, pattern recognition, and logistic regression have been widely used in recent years. It is used to collect patient information from electronic health records and predict linked diseases. Reference [27] compared the performance of three different classification methods in predicting coronary artery disease, and found that the neural network based on the multilayer perceptron network method shows the best performance in the prediction. In summary, by migrating the health big data to the cloud data center for processing, it can help smart health applications to dig out more in-depth medical information hidden in the health data.

2.3.2 Offloading Medical Edge Device

Edge devices often do not have sufficient computing power, which limits the performance and efficiency of mobile medical services. At the same time, since mobile medical services require high real-time performance, if all data is processed in the cloud, it will cause a large amount of data due to network transmission delay. How to combine edge medical equipment and cloud computing to provide efficient and real-time mobile medical services has become a challenge.

Using the cloud to help edge devices alleviate some of the pressure on high-performance computing is a way to effectively improve the service performance. Reference [28] proposed a cloud computing framework to relieve mobile devices from performing multimedia when providing mobile health services. The framework demonstrates that multimedia and security algorithm-related activities

may be done in the cloud, allowing mobile medical service providers to enhance the capability of their mobile health apps beyond the restrictions of current mobile devices.

The collaborative work of cloud and edge devices can effectively improve the quality of mobile medical services. To achieve more effective individualized medical monitoring, reference [29] presented a new hybrid mobile cloud computing approach. The case of ECG monitoring and analysis has been studied, and a mobile cloud prototype has been developed. This hybrid mobile cloud solution can be significantly stronger than traditional mobile-based medical monitoring in terms of diagnostic accuracy, execution and energy efficiency, and has a personalized solution potential of large-scale data analysis in healthcare.

Limited by the performance of edge medical devices, it is difficult to provide fast and accurate medical diagnosis through edge devices. Cloud computing can help smart health applications meet this requirement. Reference [30] developed a cloud-based 12-lead ECG service. In order to achieve universal remote 12-lead ECG diagnosis. The service employs cloud computing to improve the quality and efficiency of medical services by enhancing the capabilities of edge medical devices.

3 MEC-Smart Health

At present, research on cloud smart health mainly focuses on the storage, analysis and calculation of health big data. The combination of cloud and smart health can help smart health services solve big data and performance problems. With the aid of cloud, smart health services can store and process massive health big data, and dig out useful information from big data. But cloud alone is not enough. As mentioned in the introduction, smart health services are real-time, intelligent and ubiquitous. For Meeting such requirements of smart health services requires a lot of work at the edge of the network. This article summarizes, analyzes and highlights relevant research in recent years, and divides the research on smart health at the edge into health data. There are three main aspects of acquisition, calculation and wireless transmission technology.

3.1 Data Collection

Smart health big data has experienced a rapid growth process, and a large amount of health data comes from unobtrusive sensors and wearable devices. Sensors and wearable technologies are regarded as the cornerstones of smart health and are the data source of the entire smart health system. Tiny sensors can be woven or integrated into any inconspicuous corners of clothing, accessories and living environments, so that medical and health information can be obtained continuously and in real time in daily life. In order to provide long-term health monitoring, the sensors can even be built to paste electronic tattoos and directly print on human skin. Heart rate, respiration rate, blood pressure, blood oxygen saturation, and muscle activity are all physiological indicators of personal wellness. Data derived from physiological data can be used to offer health status indicators and has a high diagnostic value.

3.1.1 Sensor Technology

Sensors are the cornerstone of the entire smart health system and the basic element of the monitoring system. It requires long-term preparation and real-time measurement of related physiological indexes. The development of micro-biological sensing equipment, smart technology, microelectronics, and wireless communication has made various types of sensors can sense and measure data more effectively and faster, and at the same time have lower energy consumption and fewer processing

resources. As shown in Table 3, common sensor technologies for monitoring various physiological indexes are listed.

Table 3: Edge sensor main physiological indices

	Data type					
	Respiratory rate	Heart rate	Body temperature	ECG	Blood pressure	Accelerometer
Method	Impedance plethysmography, piezoelectric	Photoplethysmography	Thermistance, IR, Hg	Coupling capacitot	Pulse wave propagation	Piezoresistive, capacitance, piezoelectric
Sensor type	Piezoelectric	Skin electrodes	Probe, skin patch	Skin electrodes	Cuff-based	Accelerometer
Size	Small	Tiny	Tiny	Tiny	Medium	Tiny
Physical contact	No	Direct/ indirect	N/A	Indirect	Direct	No

One of the most popular physiological indicators recorded by wearable sensors for human activity monitoring is body temperature (BT). The temperature fluctuations detected on the skin can show what is going on with the human body's temperature and can be used to detect a variety of health problems. Medical symptoms, including stroke, shock and heart disease, etc. In smart health services, in addition to the most common applications such as the use of body temperature to determine the patient's physical condition, it can also be used to determine the person's activity status [31], and even some wearable devices can collect energy from the waste heat emitted by the human body surface [32], etc. Temperature sensors are very common in human life. Common sensor methods for measuring temperature include mercury, infrared, thermistor, and thermocouple.

One of the most often measured indicators in physical examinations is blood pressure (BP). Heart function and peripheral vascular resistance can both be determined by BP. It's also useful for detecting disorders, tracking changes in the condition, and evaluating therapy outcomes. A potential BP measurement technology is the pulse wave propagation method [33]. The relationship between pulse wave velocity and arterial pressure is used to calculate the BP. This method does not require the use of a sphygmomanometer cuff for additional measurement.

One of the most commonly observed physiological measures is heart rate (HR). It is essential for human health and disease surveillance. For heart rate monitoring, there are a variety of sensor options. Photoplethysmography (PPG) [34] is a common method for measuring HR. It tracks the change in blood vessel volume during the cardiac cycle using a photoelectric sensor that detects the difference in intensity of reflected light after absorption by human blood and tissues. Calculate the HR in the middle based on the pulse waveform. To accomplish discreet measurement, the PPG sensor can be integrated into everyday items (such as watches, earrings, and gloves). Reference [35] proposed a controllable indirect contact sensor for PPG measurement. The circuit changes the intensity of the light to accommodate different types of clothes. Reference [36], on the other hand, demonstrated that a digital camera may be used to remotely capture the PPG from the subject's face and quantify the HR and respiration rate.

Electrocardiography (ECG) is a technique that can offer physiological information regarding heart rate and regularity and is frequently employed in the diagnosis of cardiac disorders. Wearable ECG sensors, based on this, can be utilized for short-term assessment of cardiovascular disorders, particularly in individuals with chronic heart disease. The capacitive coupling sensing method is a sensor method for measuring biological points, which can be used to measure electrocardiogram and electroencephalogram [37], etc. The skin and the electrode form a two-layer capacitor in this manner. Some difficulties produced by the adhesive electrode during long-term monitoring, such as skin infection and signal deterioration, can be prevented by avoiding direct contact with the body.

Respiratory rate (RR) is an important physiological parameter for monitoring the health of patients. Respiration is a necessary process for gas exchange between the human body and the external environment. The human body inhales oxygen and exhales carbon dioxide through the breathing process, thereby maintaining normal physiological functions. For respiratory rate monitoring, piezoelectric sensors with a piezoelectric polymer sensing element can be utilized [38]. Impedance plethysmography [39], which is placed on the ribs and belly, is another extensively used method of respiration measurement. A current source that generates a high-frequency sinusoidal current drives the sinusoidal coil. The inductance of the coil changes as the chest moves during breathing, changing the amplitude of the sinusoidal current and therefore demodulating the breathing signal.

The accelerometer (ACC) is a sensor that tracks human movement. It is mostly used to measure acceleration in a certain frequency band along a specific axis. They are useful for a variety of things, including fall detection [40] and motion analysis [41]. There are numerous ways for measuring acceleration that are based on piezoelectric, piezoresistive, or variable capacitance. They all work on the same idea of stretching a spring or comparable equivalent part to gauge acceleration.

3.1.2 Smart Wearable Device

Smart health systems usually integrate sensor technology with the IoTs to enable healthcare systems to monitor patients. At present, there are already many smart wearable devices in the industry that can help monitor physiological parameters. Generally, smart wearable devices It has these characteristics: miniaturization, low energy consumption, intelligence and personalization.

FuelBand is an activity tracker that can be worn on the wrist. FuelBand can track the exercise and calories burned over a period of time, and share the readings of the wristband to the online community. As a smart watch, Apple watch is not only supports step recording, sleep monitoring and energy consumption recording, as well as professional medical data such as heart rate monitoring and electrocardiogram drawing. The Fitbit bracelet can not only record steps and calculate activity consumption, but also intelligently judge whether you are exercising and what kind of exercise. With the continuous development and breakthroughs of related technologies and algorithms, such as more accurate new step counting algorithms [42], these smart wearable devices have become more and more important and have become an important part of the smart health system, as smart health key components of the data source in the system, they undertake a large number of health data collection work, provide rich and diverse health data for the back-end system, and use these data to conduct detailed analysis of human health.

3.2 Data Computing

Storing, retrieving and processing medical and health data on a cloud computing platform is a very efficient architecture that can help smart health applications quickly land and function. The cloud can help smart health services deal with big data and performance challenges, but it is difficult

to meet real-time requirements of smart health. Thanks to the research and development of the IoTs and sensor technology, most medical health data is generated at the edge of the network. A large amount of medical health data needs to be processed in real time. This this type of medical health data is intolerable network delays and lags have very high requirements for real-time performance, which puts a lot of pressure on cloud computing platforms. Therefore, there are many studies that have not placed the calculation and processing of medical and health data in the cloud computing center, but have migrated to the cloud computing center. The fog computing platform closer to the edge node can effectively improve the real-time performance of the service through the fog computing platform, and meet the high real-time demand of smart health services.

3.2.1 Fog Computing in e-Health

Cisco took the lead in proposing the concept of fog computing, which is an extension of the concept of cloud computing [43]. Fog computing moves services and computing closer to the user end, satisfies low-latency, real-time applications, and can reduce the burden on the network at the same time. Fog computing refers to a micro cloud computing structure close to the edge. Unlike traditional cloud computing structures, data and application resources in fog computing are placed in a logical position between edge nodes and the cloud, which is also called a fog network. Reference [44] gave a comprehensive introduction to the system architecture and resource management in the edge computing environment, but did not specifically introduce the smart health application.

In the development of smart health services, explosive health data are generated at edge nodes, such as the use of medical sensors to monitor patient physiological indexes, etc. Due to the limited power and performance of edge devices, it is difficult to process the collected health data in real time, and if all such data is transmitted to the cloud computing center for processing, it will cause a large delay and affect the user experience. Moreover, the large-scale implementation of the IoT is expected to introduce billions of edge devices connected to the Internet, given the large number of connected devices as well as the large amount of data, there will be a lot of delays in connecting to the cloud. Based on this, fog computing has become an intermediate processing station for smart health applications. This type of health data is migrated from large-scale data centers to micro-scale data centers close to edge nodes. Data centers can not only reduce latency and improve the efficiency of edge devices, but also reduce the network pressure imposed by a large number of data requests on the back-end cloud computing platform [45]. For example, the data processing of some small embedded medical devices does not require each piece of data is transferred to the cloud computing center for processing, but some tasks with high real-time requirements are handed over to the smart gateway for processing, which will save a lot of network costs and improve real-time performance. In summary, in the cloud and setting up a fog computing layer between edge nodes can effectively improve the real-time performance of services. Fog computing is an important example of shifting to a layered system architecture and a more responsive design.

3.2.2 Using Fog to Improve Smart Health Services

The continuous development of the IoT and sensor technology enables us to develop smarter healthcare solutions that are not only suitable for use in hospitals, but also in daily life to protect medical health. A bridging point between the sensor infrastructure network and the back-end Internet, generally referred to as a gateway, is required in most IoT-based healthcare systems, particularly in smart homes and smart hospitals. Gateways at the network's edge typically only perform basic services, such as converting and transmitting real-time data between protocols, as seen on the Internet and in sensor networks. The sensor network and the data transferred are effectively controlled by these

gateways. Using the strategic position of these gateways at the edge of the network, more services can be provided, such as local storage and local real-time data processing, thereby presenting a smart electronic health gateway. Through this type of smart electronic health gateway, a geographically distributed intermediate intelligent computing layer can be formed between the sensor node and the cloud computing platform to realize the concept of fog computing in the smart health IoT system. The smart electronic health gateways are responsible for handling some of the burdens of sensor networks and remote cloud computing centers. The fog computing architecture can cope with many challenges in the ubiquitous healthcare system, such as mobility, energy efficiency, and scalability.

The IoTs technology can be applied to smart health and other related fields. As a bridge between wireless sensor networks and the traditional Internet, IoT gateways play an important role in smart health applications. Reference [46] proposes an IoT gateway system based on ZigBee and packet protocol, as well as data transmission between wireless sensor networks and mobile communication networks, based on typical IoT application scenarios and telecom operator needs. The control function of a wireless sensor network as well as the conversion of multiple sensor network protocols are discussed. The prototype system was completed, and the system was verified.

Reference [47] presented a broad framework for wireless sensor networks and Internet connections based on smart gateways. This framework supports Internet-based query functionalities for data-centric sensor networks and allows access to diverse sensor nodes. It also allows transparent access from one network to another without altering each network's protocol. Furthermore, the framework can be expanded to include a multi-gateway design for fault tolerance and load balancing.

Reference [48] demonstrated a general-purpose sensor network platform SwissGate, which provides a high-level interface for sensor network programming and a multi-layer architecture that can effectively process and optimize the operation of sensor networks.

Reference [49] proposed the design of smart gateway middleware, which allows application code to be executed on the gateway by providing a simplified interface for the sensor network and the Internet. Since the gateway fully understands and controls the sensor network and the Internet, the smart gateway can act as a performance enhancement agent and smart cache to protect the limited resources of the sensor network.

A revolutionary adjustable smart IoT gateway was proposed in reference [50], which has three major advantages. The gateway for starters has a plug-in design which allows different communication protocols to be adapted for different networks. Second, it provides a consistent external interface that makes software development more versatile. Finally, it provides a versatile protocol for converting various sensor data into a single format. The gateway provides superior scalability and flexibility, as well as a reduced cost, as compared to similar studies.

Reference [51] proposed a three-tier architecture of smart medical health infrastructure, and provided an example use case as a template for smart sensor-based medical infrastructure. The architecture is based on a service-oriented architecture, and the architecture integrates role models and points. Layer cloud computing architecture and fog computing notification paradigm in order to provide a feasible intermediate computing layer architecture for medical and health applications.

Cloudlet is a highly mobile micro data center located at the edge of the cellular network. It is a cloud computing center extension that moves cloud computing resources to the cellular network's edge to fulfil low-latency and real-time tasks. It can help smart health applications reduce latency to achieve faster response and improve application interactivity. Reference [52] introduced a Cloudlet-based large-scale medical body area network system. The goal is to dynamically select and collect data

by using the cloudlet system. Therefore, minimizing the end-to-end data packet cost, and at the same time trying to minimize the end-to-end data packet delay by dynamically selecting the neighboring clouds, thereby minimizing the overall delay, and finally realizing real-time monitoring of medical and health data. The services can also use the Cloudlet platform to help offload tasks. Reference [53] proposed a Cloudlet-based mobile medical model. The model first looks for services from the Cloudlet only when the service is not available and then the user will connect to the medical cloud. In addition, Reference [54] established a novel medical data sharing system based on Cloudlet, which can prevent malicious attacks while reducing the communication energy consumption. Reference [55] proposed a new architecture of Cloudlet and SDN can smooth the heterogeneity of devices and access networks, and realize the rapid access to medical data collection and analysis through the cloud environment. In short, as the middle layer of cloud and edge sensor networks, it can help reduce latency, assist in computing, and reduce the energy consumption.

With the research and development of fog computing, smart health applications have benefited a lot from it. Among them, smart gateways and micro data centers can greatly improve the real-time performance of smart health applications and provide more auxiliary functions for smart health applications.

3.3 Technology Deployment in Health

In the smart health system, in order to achieve comprehensive health services, many physiological sensors are often arranged on the human body. These sensors work together to collect the required physiological indexes in real time and continuously, and send them to the central node. The node performs data aggregation and other processing before transmitting it to the corresponding back-end system. In order to realize the collaborative work of these physiological sensors and the central node, the researchers proposed the concept of body sensor network (BSN). Body area network is attachment The small network on the human body is composed of various small physiological sensors and central nodes. Through the body area network, various sensor devices can transmit monitoring data to the central node for data processing, and the central node performs data filtering and cleaning on the physiological data after operations such as aggregation and aggregation, the data is sent to the back-end system.

3.3.1 Standards

Sensor networks are usually divided into two types: wired and wireless. For the former, the use of conventional network cables will increase the failure rate of the system and will affect the user experience and comfort. Therefore, more wireless technologies are used in body area network systems. As shown in Table 4, there are a variety of wireless technologies that can be used in body area networks, such as Bluetooth, WiFi, ZigBee, WiMAX, MICS, etc.

Table 4: Various networks deployment in health

Parameter	Network type				
	WiFi	MICS	Bluetooth	ZigBee	WiMAX
Bit rate	54 Mbps	0.4 Mbps	1∼3 Mbps	0.25 Mbps	128 Mbps
Range	200 m	2 m	10∼100 m	1075 m	15000 m
Bandwidth	2.4, 5 GHz	0.402∼0.405 GHz	2.4∼2.48 GHz	0.868/0.915, 2.4 GHz	2.3∼3.5 GHz

ZigBee [56] is a wireless network technology that allows for low-speed, short-distance communication. The IEEE 802.15.4 standard is used for the media access layer and the physical layer. The ZigBee protocol is typically used for minimal data transmissions due to its ultra-low power consumption. In smart health applications, speed and long battery life are important [57,58]. These applications have low data rate requirements and usually have a battery life of months or even years.

Bluetooth (originally IEEE 802.15.1) is a common short-range wireless communication technology, usually used to exchange data between mobile devices. It is a low-cost radio frequency standard that works in the 2.4 to 2.48 GHz frequency band [59]. Compared with ZigBee, Bluetooth has a faster data transmission rate. Bluetooth has been increasingly used in smart health applications that require high bandwidth [60–62].

WiFi is a wireless local area network technology based on IEEE 802.11. It works at 2.4 and 5 GHz. It is one of the most common wireless network technologies in daily life. WiMAX is a high-speed wireless network standard based on IEEE 802.16. Used in metropolitan area networks, the transmission distance can reach tens of kilometers. Compared with ZigBee and Bluetooth, WiFi has higher power consumption and has some privacy protection issues, which is not suitable for mobile computing scenarios. But indoor monitoring and activities in the identified smart health scenarios, due to the universality of indoor WiFi today, WiFi is gradually developing as the main solution [63,64].

The medical implant communications service (MICS) is an ultra-low-power communication protocol specially used for medical equipment and medical experiments. It uses the 402∼405 MHz frequency band, which is generally used to transmit low-rate data. It is generally used for low power consumption and the scenario of low data transmission rate [65].

3.3.2 Body Area Networks

The body area network technology is one of the core technologies for the development of the Internet of Things in smart health services. It is responsible for connecting various physiological sensors together to form a small network system for collecting, processing and transmitting physiological indexes on the human body. The network system is responsible for the data source and preprocessing in the smart health service. Its performance directly affects the quality of the smart health service. As a small network system, the body area network has very high requirements for energy consumption, security and privacy, but also lacks advanced software abstraction support. Based on this, the researchers focused on security, energy consumption, development framework, etc.

In terms of energy consumption, reference [66] proposed an energy-efficient dual-frequency transceiver for body area networks. The transceiver provides 30–70 MHz channel communication and 402–405 MHz medical implant communication services. It can achieve up to 30% energy saving effect. Reference [67] introduced a self-configurable wearable BSN system with a high-efficiency wireless power supply sensor that can continuously monitor electrocardiogram (ECG) at selected positions of the body with low power consumption.

In terms of security, reference [68] proposed a healthcare system based on the IoT using body area networks, called body sensor network (BSN)-Care, which uses a lightweight anonymous authentication protocol and an encryption scheme offset codebook to ensure User information security. In body area networks, due to the strict resource limitations of the network, only lightweight mechanisms can be deployed to meet security requirements. Reference [69] proposed using human heartbeat pulse interval information from another perspective. To generate physical identifiers that identify sensor nodes to ensure safety. The inherent ability of the human body to transmit information is a unique and resource-saving method to protect wireless communications in the body area network.

In terms of development framework, reference [70] is based on the emerging domain-based programming paradigm launched an open source programming framework SPINE for body area network, which aims to support the rapid and flexible prototyping and management of body area network applications. Reference [71] proposed a body area network hardware development platform with low power consumption, flexible and compact design, providing a versatile environment for research and development body area network.

4 Cloud-Edge Analysis in e-Health

A large number of researches have also focused on smart health-related applications. Significant research applications on smart health have been developed, as shown in Table 5. Next, some of the application cases will be introduced, including health monitoring systems, disease prediction prevention, smart health hardware, etc.

Table 5: Summary of various deployment networks in health monitoring

Ref.	Data type	Application	Shortcomings	Mobility
[72]	ECG	Cloud-based	Requires large storage space	×
[73]	Audio	Audible pathology	Small real-time analysis	×
[74]	Body temperature, blood pressure & heart rate	Wireless	Inapplicable in huge traffic	×
[75]	Health	Wearable	Requires high processing capability	✓
[76]	Blood pressure	Fall event prediction & hypertension	Lower accuracy	×
[77]	ECG	Heart disease analysis	Lower power efficiency	✓
[78]	ECG, heart rate & blood pressure	Bio-signal	Limited hardware support	✓
[79]	Respiratory rate & ECG	Mobility & HR	Lower power efficiency	✓
[80]	Health	Wearable	Lower energy efficiency	✓
[81]	Health	Analysis & visualization of data	Lower accuracy	×
[82]	Health	HetMed	Inapplicable in huge traffic	×

4.1 Health Monitoring

Health monitoring is currently one of the most widely used applications in smart health. Real-time physiological index monitoring can effectively help diagnose and improve health. Reference [72] described a smart health monitoring system in which ECG and other medical data are collected by mobile devices and sensors and securely uploaded to the cloud for medical practitioners to view. At the same time, the framework employs signal amplification, watermarking, and other associated analysis techniques to protect medical practitioners against identity theft and clinical errors. Reference [73] uses

the cloud things people voice pathology for monitoring the feasibility and proposed solutions. More specifically, in the monitoring framework based on local binary pattern on the spectral representation of the speech signal and for detecting pathologies study, the machine classifier proposes a speech pathology detection system. The proposed monitoring framework can achieve high-precision detection and is easy to use. Reference [74] developed a real-time wireless physiological monitoring system whose function is to pass wireless communication channels and wired local area network monitors the physiological status of elderly patients. The system collects body temperature, blood pressure and heart rate data through a customized medical examination module. Medical staff can monitor the patient's physiological status in real time through the computer and analyze the patient's physiological changes. In addition, considering the real-time monitoring of patients, some studies have designed a physiological monitoring system based on wearable personal devices [75], which can realize real-time and uninterrupted physiological index monitoring.

4.2 Disease Prediction and Prevention

Disease prediction and prevention is a type of smart health application that can help discover patients' conditions in advance. Unlike traditional medical services, disease prediction and prevention can remind patients before problems occur and help patients avoid problems. The design and preliminary verification of a platform for collecting and automatically analyzing biological signals for risk assessment of vascular events and falls in patients with hypertension are described in reference [76]. This cloud-based mobile health platform is built to be highly scalable and versatile. It also provides active remote monitoring through data mining. The system can predict vascular events in the next 12 months with an accuracy rate of 84%, and the accuracy rate for monitoring fall events is 72%.

Centralized medical service resources are becoming more and more scarce, and it is more important to provide patients with self-test health services. Reference [77] developed a heart attack self-test application that allows potential victims to quickly assess whether you have a heart disease without the intervention of medical experts. Based on technologies such as mobile phones and ECG sensors, the system analyzes the user's symptoms and detects whether there is a heart disease by analyzing the collected ECG records. If there is a risk, the user will be immediately urged call emergency services.

4.3 Medical Hardware

Based on the needs of mobile and portability, many smart health hardware with novel functions have been developed. This smart health hardware has opened up a new development path for smart health services. Reference [78] developed a smart vest, the vest series of sensor arrays are used to collect the wearer's physiological indexes and generate the overall health status of the wearer. The physiological indexes monitored by the vest include blood pressure, heart rate, electrocardiogram and body temperature. Reference [79] developed a washable sensor vest for recording heart rate and exercise signals. The vest is composed of a sensor for monitoring ECG and respiration rate and an electronic board for exercise detection, signal processing and wireless data transmission. The sensor vest can not only obtain very high quality data can also detect arrhythmia events. In addition to functionality, it is also necessary to consider the trade-off between smart health hardware performance and energy consumption. Reference [80] designed a new type of cross-end analysis for wearable devices engine architecture, which implements the universal classification design of wearable sensors and energy-efficient data aggregators, which extends battery life and reduces system latency.

4.4 Other Applications

Health data visualization and analysis are also common smart health applications. Through the visual display and analysis of the collected real-time data, it can help medical personnel find the problems more accurately. Reference [81] built a foundation for the medical field mobile application on the Android platform, which uses the concepts of the IoT and cloud computing. It provides end users with visualization of electronic electrocardiogram and background health data. The collected data can be uploaded to the user's private cloud or specific medical cloud, the program saves all health data records and can be retrieved by medical personnel for medical analysis.

Various remote and heterogeneous medical and health information systems have created the situation of medical information islands. The smart health management platform needs to integrate various information islands and add unified management to promote information sharing. The CardioNet is a distributed medical system that connects different medical entities and systems, such as hospitals, emergency rooms, and laboratories. Reference [82] proposed and verified CardioNet, which is a distributed medical system that connects different medical entities and systems, such as hospitals, emergency rooms, and laboratories. Through the network, the distributed system can provide various services, such as remote monitoring, online consultation, and hospital event management, among others.

The application cases of smart health are very diverse. They help people improve their health in all aspects and relieve the pressure on resources under the existing medical system [83].

5 Blockchain in e-Health

In recent years, blockchain technology has attracted increasing attention. As an emerging technology, the decentralized, transparent and secure characteristics of blockchain make it have many applications in medical treatment. Blockchain is essentially a distributed database technology. It uses technologies such as proof of work, distributed timestamp protocol, longest chain algorithm, and related encryption algorithms (such as SHA256) to achieve a distributed consensus mechanism and user anonymity, which are also two important features of blockchain [84].

As shown in Fig. 2, each block contains the version number, the hash value of the previous block, the Merkle root node, the timestamp, the random number, and the transaction data. The block header is made up of the first five items, and each block must contain the SHA256 hash value of the preceding block header, ensuring that the file cannot be tampered with. If a block is tampered with, the hash value of all subsequent blocks must be modified, and each block carries the creation timestamp, ensuring that the blocks are chained in a chronologically orderly fashion. At the same time, the blockchain uses a proof-of-work process to reach consensus, which uses random integers in the block to achieve proof of work. The blockchain realizes a decentralized, transparent and secure distributed database.

Most of the current medical forms are centralized management models. Patient data is stored in third-party institutions, and the data of each institution is not interoperable, forming islands of information. When patients change from one institution to another, all previous medical and health data cannot be shared. This is a loss for patients, and it also increases the burden on medical service providers. The decentralized management of blockchain can just solve this problem of smart health services. It is suitable for applications that want to cooperate with each other without transferring control to the central administrator. At the same time, the non-tamperable and data encryption characteristics of the blockchain can also ensure the correctness of health data and protect patients. Not only that, thanks to the decentralized, transparent and safe characteristics of blockchain, smart

health services can also use to promote the accuracy of clinical trials, solve the drug supply chain, and build a smart health management platform. For example, as shown in Table 6, blockchain has many applications in smart health services. Next, this article will introduce the research and development of blockchain in smart health services.

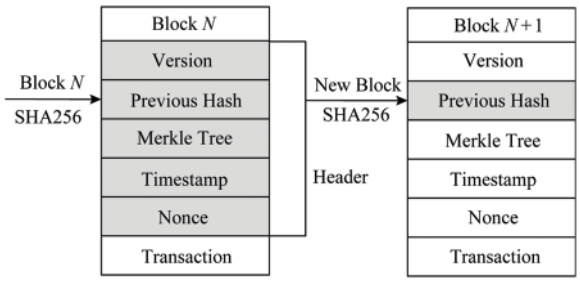

Figure 2: Layered blockchain architecture

Table 6: Summary of blockchain based applications for e-Health

Ref.	Method	Main idea	Emphasis	Advantages
[85]	Ehtereum	Smart contact	HER	Decentralized
[86]	Hyperledge fabric	Channel formation	Health data	Security & privacy
[87]	Health	Asymmetric encryption	Medical image	Security & privacy
[88]	Ethereum	Smart contract	Data utilization	Transparent
[89]	Health	Machine learning	Training model	Decentralized
[90]	Health	Timestamp	Trials	Immutable
[91]	Health	Timestamp	Counterfeit medicine	Transparent/immutable
[92]	Health	Smart contract	Supply chain	Transparent/immutable
[93]	Ethereum	Share infrastructure	Platform management	Decentralized
[94]	Health	Identity	Platform management	Decentralized
[95]	Health	Work proof	Transaction process	Autonomy

5.1 Data Sharing

Through sensors and wearable technology, personal health data provides huge and ever-increasing value for medical and health services, benefiting patients and medical service providers, but subject to privacy protection and security, it cannot fully exert its value. Personal health data is usually extremely sensitive personal privacy data, but different from conventional personal privacy data (such as home address, credit card, etc.), the sharing of health data within a certain range is of great benefit to patients and medical service providers. This type of health data sharing can help patients, medical service providers, and third-party vendors to obtain useful information and break information silos.

At the same time, decentralized health data sharing can also prevent data from being controlled and tampered by central managers.

Blockchain technology exactly meets the needs of such scenarios. Through blockchain, a delicate balance of privacy and accessibility can be achieved. Based on this, many studies and projects have begun to focus on using blockchain to share health data to improve medical record management. Reference [85] proposed a blockchain-based framework called Ancile, which can enable patients, medical service providers and third parties to efficiently and securely access electronic health records and realize the sharing of medical records. At the same time, the privacy of sensitive patient information can be protected. Reference [86] proposed a user-centric health data sharing solution based on blockchain, using channel mechanisms to protect the privacy and enhance the identity management, and ultimately achieve the goal of safe sharing of health data. Not only on medical records, reference [87] developed a cross-domain image sharing framework that uses blockchain as a distributed database to establish ledger of radiology research, while the access rights are defined by the patient. The framework is proven to eliminate the security problems of third-party access to medical images, and meets the standards of interoperable health systems, and can be easily extended to other medical fields.

5.2 Blockchain Vitality in Medical Research

Thanks to the decentralized, transparent and safe characteristics of blockchain, many studies have begun to focus on the application of blockchain technology in the field of medical research. The combination of blockchain and medical research has also broadened the application scenarios of smart health services. The centralized management of the blockchain is different. The decentralized management of the blockchain allows traditional medical research to be carried out in the form of decentralized cooperation, which greatly improves the utilization of medical data, and the non-tamperable and time-based characteristics of the blockchain can improve medical research credibility of data ensures the traceability of data. Blockchain, as a distributed database technology, brings new vitality to medical research.

Medical researchers recommend using blockchain to promote the use of clinical data. Reference [88] proposed MedRec, a novel decentralized record management system that uses blockchain technology to process electronic medical records and data in the system, medical stakeholders participate in the network as blockchain miners. They maintain the network through a proof-of-work protocol in exchange for mining rewards for access to anonymous data. MedRec can provide a large amount of anonymous medical data to enhance the capabilities of researchers. At the same time, it can also attract patients and related institutions to release metadata. In addition to promoting the utilization of medical clinical data, the emergence of blockchain technology enables decentralized cross-institutional medical research. Reference [89] described a new framework ModelChain that makes blockchain technology suitable for decentralized research of medical predictive models. Unlike traditional centralized architectures, each participating node contributes to model parameter estimation without revealing any patient information, and can be used from multiple institutions predictive model learning based on the data. In clinical trials, reproducibility and correctness are major challenges in medical research. Blockchain has become a key point to deal with these challenges. Reference [90] discussed blockchain in clinical trials, the inviolability of a large amount of historical data in the entire document process can be guaranteed. The traceability of data and the prevention of posterior reconstruction can be ensured, and clinical trials can be safely automated through smart contracts. Blockchain technology ensures clinical trials fine-grained control of data security. Thanks to the promotion of medical research by blockchain, smart health services can obtain safer and more accurate medical support.

5.3 Blockchain Support in Drugs Industry Safety

Drug safety issues have always been one of the important reasons for the tension between doctors and patients. Medical accidents caused by drug safety issues frequently occur, but for non-medical practitioners, it is difficult to distinguish the authenticity of drugs, and even cost for counterfeit products. Although in the current smart health service, the authenticity of medicines can be obtained from the central administrator, it is really difficult to avoid the tampering and fraud of the central administrator. Due to the high benefits and huge market value of the counterfeit medicine market, it is difficult to completely eliminate the phenomenon of counterfeit drugs from the perspective of management and law. The emergence of blockchain allows researchers to see an opportunity to solve this problem from another angle. Using the non-tamperable and completely transparent characteristics of blockchain, researchers try to expose the entire process of medicines from raw materials to production to distribution in everyone's eyes.

The Hyperledger working group proposed a project that uses blockchain technology to improve the security of the pharmaceutical supply chain [91]. Companies such as Accenture, Cisco, Intel, IBM, Block Stream, Bloomberg, etc., are all involved in this project. The project envisages the use of timestamp and sequence of the blockchain to facilitate the verification of the production time and location of the drug, which can help solve the problem of counterfeit drugs and substandard drugs, and accurately indicate the manufacturing location of the product. In addition, reference [92] also proposed a blockchain-based solution to improve the supply chain security of the pharmaceutical industry. Each drug is attached with a clear identification label, allowing drug ownership to pass through the block trusted network of smart contract verification on the chain is transferred from upstream suppliers to downstream consumers. In short, blockchain as a supply chain infrastructure can bring integrity, traceability and transparency to the global drug supply chain, which can be very good solution to the problem of counterfeit medicines.

5.4 Blockchain Cross-Layer Feature

At present, a large number of researchers are concerned about the combination of blockchain and smart health, and have put forward many innovative research results. At the same time, the industry is not to be outdone. Different from the smart health application of cloud and fog cross-layer design, the industry proposed a transparent and safe smart health support platform for blockchain decentralized management.

Reference [93] is a blockchain network based on Ethereum. It solves the trade-offs between patient-centered medical services and operational efficiency by establishing a healthcare ecosystem connected to a general data infrastructure. Shared data infrastructure for identity solutions, data storage and smart contract applications. Gem Health Network is a continuum that covers the entire smart health service, from health and prevention to billing and claims and a series of processes. One of the healthcare giants Philips Healthcare has announced that it has joined the Gem Health Network.

Guardtime, a data security company located in the Netherlands, has cooperated with the Estonian government to create a blockchain-based smart health management platform that can be used to verify the identity of patients [94]. Currently, all Estonian citizens and medical service providers can use it. Guardtime platform to obtain relevant medical information, Guardtime platform already operates more than one million health records.

In summary, blockchain has a wide range of applications in health data sharing, promotion of medical research, standardization of the pharmaceutical industry and support platforms, and the influence of blockchain is still expanding, and related applications continue to emerge, such as

medicine fraud monitoring [95] etc. A smart health platform based on blockchain-based decentralized management can help operate a complete public health infrastructure, and provide more complete, safe and intelligent services on top of this.

6 Security and Privacy

6.1 e-Health Record

The personal health record (PHR) service allows people to create, manage, and control personal health data over the internet, making it easier to store, retrieve, and share medical data. Each patient has complete control over his or her own medical records, which can be shared freely with other users, such as medical service providers, family members, or friends. Many PHR services are outsourced to specialized third-party service providers due to the high expense of creating and maintaining specialized data centers. For example, Google Health, Microsoft HealthVault, Inter Component Ware (ICW) LifeSensor, etc. Literature [96,97] proposed the design of the information storage architecture for PHR in the cloud.

Because of its service-centric storage method, PHR provides convenient services for most people, but there are still many security and privacy risks that may hinder its widespread use. For example:

1) Whether patients can truly control the sharing of their sensitive personal health information (PHI), especially when the data is stored on a third-party server, and the service provider may not be completely credible;
2) Sensitive personal health records are of high value. Third-party storage servers are usually important targets for various malicious attacks, which may lead to exposure of sensitive personal health records. Therefore, for patients, a sufficiently fine-grained data access control mechanism is essential. A feasible and guaranteed method is to encrypt personal health record data before outsourcing. Basically, the PHR owner should decide how to encrypt the file and which set of users is allowed to obtain access to each file, only the user who has obtained the decryption key has the right to access the corresponding file. When necessary, the patient should also have the ability to revoke the corresponding access [98].

Different from PHR managed by patients, electronic health record (EHR) is only managed by professional health managers. In most countries, according to the law, PHR and EHR have clear boundaries and different requirements. Therefore, EHR is involved infrastructure that is usually completely different than the simple PHR-based cloud model.

The basic requirements of the EHR model are still functional storage and basic data operations in the EHR. It is developed, maintained, and managed by healthcare practitioners, and can be shared with other health professionals through an EHR server in the cloud. However, the EHR storage and processing aren't the only services that can be delegated to third-party cloud service providers. Third-party billing services are commonly used by healthcare providers to manage their billing fees and patient health insurance. This is a common circumstance in practice that many doctors delegate invoicing to third-party suppliers. These billing systems collect bills from a variety of medical insurance and service providers for a single patient. As a result, privacy becomes more important in this model, because health insurance or billing services should not access the private details of EHR. Therefore, the privacy and security design of EHR becomes extremely important, as shown in Table 7, which summarizes the privacy and security design solutions based on different technologies.

Table 7: Summary of privacy and security for different technologies

Ref.	Technique	Cryptographic correctness/Revocable	Shortcoming
[96]	HPE	Yes	Single trustee
[99,100–103]	ABE	Yes	Slow bilinear calculation
[104]	PUD	Yes	Low search performance
[104–106]	ABE	Yes	Complex domain
[107]	IBE	Yes	Large power consumption
[108,109]	OC	Yes	Lack of emergency feature
[97,110,111]	TVD	Yes/No	

6.2 Attribute Encryption Based Access Control

Attribute-based encryption, also known as fuzzy identity-based encryption, is a promising encryption primitive that supports fine-grained access. It does not need to be the same as identity encryption. We must know the recipient's identity information for each encryption. In ABE, it regards the identity as a series of attributes. When the attributes owned by the user exceed the preset threshold described by the encryptor, the user can decrypt it.

Literature [99,100,107] uses the ABE methods to control fine-grained access to electronic health record data. Thanks to the support for fine-grained access, the privacy and privacy of EHR security issues, ABE has been widely used.

However, the above schemes have common shortcomings. First, they usually assume that a trusted institution in a single system is used. This will cause a load bottleneck, and it will also encounter the problem of the trust of the key custodian. Because the trusted institution can access all encrypting files, which poses the risk of privacy exposure. In addition, it is impractical to delegate all attribute management tasks (confirm the attributes or roles of all users and generate keys) to a trusted organization. Normally, in different organizations, a set of authorization certification methods are applied to one's own organization. For example, professional associations will be responsible for certifying medical professional qualifications, while health service providers will be responsible for certifying the work levels of their employees. Secondly, there is still a lack of effective and on-demand ABE withdrawal mechanisms. This is an important part of ensuring the security of PHR. Based on this, reference [112] proposed an attribute-based access control scheme for trackable multi-authorization agencies in a smart health environment. This scheme not only supports multiple authorized agencies, but also supports malicious user tracking mechanism.

In the current ABE-based privacy security control, most methods do not distinguish between personal and public domains (PUDs), which have different attribute definitions, key management requirements, and scalability issues. Reference [104] made corresponding research based on the PUDs problem, and proposed an architecture that uses different authentication management methods in multiple fields.

6.3 Revocable ABE

Effective and on-demand revoking of users or attributes in ABE is a well-known challenging problem. In traditional methods, this is usually done by the authority frequently broadcasting key

updates to users who have not been revoked [101], which cannot be guaranteed for complete backward and forward process safety, and low efficiency.

Reference [105] proposed a basic architecture based on attribute encryption on the EHR system. Each patient's EHR file is encrypted using the ABE variant ciphertext protocol attribute encryption (CP-ABE), which is characterized by Allows to directly revoke access rights. Similarly, reference [102] also used CP-ABE to manage shared PHR, and introduced the concept of social or professional fields. Literature [103,106] proposed two types of CP-ABE schemes with direct attribute revocation capabilities have been introduced, instead of periodic revocation.

The communication overhead of a revocable ABE in key revocation is still high, because it requires the data owner to send the updated ciphertext component to each user who has not been revoked.

6.4 Client Security

At present, most of the existing distributed storage frameworks above take into account the access security and control issues of the server, and few involve the security of the client platform.

The trusted virtual domain (TVD) [110,111] is a widely used distributed security framework in a multi-domain environment. Reference [97] designed a security framework based on TVD to ensure the data security of the client and external data storage. In mobile wearable devices, the EHR data update frequency is very fast, and it usually takes five minutes to transmit once [113]. Reference [108] proposed a safe and privacy-protected opportunity calculation based on opportunity calculation [109,114] framework to ensure the security of client data transmission of mobile wearable devices.

7 Challenges and Opportunities

On the basis of in-depth research on the aspects of smart health in the cloud, fog end, edge, and privacy and security, it pointed out the six major challenges that smart health may face and proposed technical opportunities that can solve these problems.

7.1 Trade-Off Between Performance and Energy Efficiency at the Object End

In the scenario of smart health services, there will be a large number of medical sensors distributed around living places. These sensors are the source of smart health data. They will continuously generate personal health data and send these data to the cloud and fog. The energy consumption of sensors has become the key point of the entire system. If the energy consumption is too high, real-time and continuous services cannot be provided. If the performance is too low, sufficient data cannot be collected and processed, which will also affect the smart health service quality. How to weigh the energy consumption and performance of the sensor has become a key point of subsequent research. Low-power wireless transmission technology and sensor technology will become an important method to solve the compromise between energy consumption and performance design at the end, and there will be more in the future. Many researches have focused on low-power wireless transmission technology and sensor technology to minimize the data calculation at sensor nodes (such as data cleaning, filtering and aggregation, etc.), and achieve high quality and fast speed while maintaining low power consumption. Responsive smart health services, for example, deploy IoT smart gateways and micro data center cloud-assisted sensor nodes for data processing.

7.2 Heterogeneous Data and Diversified Applications

At present, various types of health data come from various systems and sensors of different forms. The structure and form of these data are not the same. This will cause the service to do a lot of preprocessing of the data, which not only affects the performance of the service, but also increases the probability of error. Therefore, the standardization and structuring of data is an indispensable part of the formation of smart health big data. The formulation of a unified data format standard for various types of health data is the most fundamental and direct solution to this problem. However, due to the existence of various independent medical systems for a long time, and the existence of different data forms for different types of medical data, it is difficult to achieve uniform standards for heterogeneous medical data in the short term. In this case, how to make the smart health back-end system adapt to heterogeneous data with high performance has become the key to the problem, which includes using NoSQL database to break the limitation of format, structured or semi-structured processing of heterogeneous data, and use distribution technology to speed up the pretreatment process, etc.

7.3 Medical Big Data Perception

In the construction of smart health, health data is generated all the time, and such health data is also different from general Internet big data as it has very high requirements for real-time performance. The data needs to be generated in real time and processed in real time, and due to individual mobility characteristics of different network environments need to realize the mobile perception of health services. At present, the use of cloud computing can effectively process big data, but with the development of the IoT, the amount of data is increasing, and the cloud cannot process health data in real time. At this time, fog and edge computing can better meet the real-time requirements of health data and improve the performance of services. Fog computing, edge computing and the IoT technology are one of the best solutions to solve the real-time and mobile perception of smart health applications. By setting up a diversified computing layer between the cloud and sensor nodes, it can meet the requirements of real-time and mobile perception of smart health services. Especially in the upcoming 5G era, the scale of health data has become larger, fog computing, cross-layer computing layer composed of edge computing and IoT technology is critical to the improvement of the quality of smart health services.

7.4 Security and Privacy of Personal Data

Data security is an eternal topic. Although smart health big data may help alleviate many health-related problems, its ability to collect personal health information may endanger the privacy of citizens. The protection of privacy and infrastructure security is still in the research community. From the collected personal data, it is possible to determine personal living habits, family member status and even religious beliefs and other private information. This information is very sensitive, especially closely related to health. Design a complete protection of citizen's mechanism of privacy security has become a major challenge. At present, attribute-based encryption methods and revocable ABE can effectively control fine-grained access to health data and ensure privacy and security. Blockchain is considered to solve the privacy and security of smart health data. The breakthrough point of security, the management of smart health data through the blockchain can not only realize the sharing of health data, but also because of the encryption characteristics of the blockchain, it also guarantees privacy and security.

7.5 Adaptive Edge Resource Integration

Edge devices face the problem of not being a single tree. In order to support the increasingly complex field intelligent applications, the coordination of complex edge devices is first required. It is necessary to build a software platform to realize independent discovery and adaptive management of edge computing resources, especially with the help of blockchain technology provides an incentive mechanism to promote the integration of edge device computing resources.

7.6 Highly Reliable and Available System Design

Medical and health scenarios have high requirements for high reliability and high availability. It is necessary to study efficient communication technologies to deal with various sudden data congestion. It is necessary to study intelligent task scheduling technology to allocate key tasks to backup hardware on demand operation. Real-time system status monitoring is required to reduce the occurrence of downtime risks. Distributed technology is required to ensure the availability of health services through a copy mechanism.

8 Conclusion

Thanks to the rapid development of cloud computing, fog computing and the IoT technology, research on smart health is increasing. After investigating a large number of researches in the field of smart health in recent years, this article first starts from the cloud and introduces the benefits of smart health big data storage, retrieval and processing in the cloud. Then, from the perspective of fog computing, various researches on enhancing smart health services through fog computing are introduced. Then, starting from the edge, the research introduces various sensors and wearables of smart health services, they are the source of data generation. Finally, this article discusses many emerging applications of blockchain in smart health services and the privacy and security issues of smart health data. Compromise of consumption and performance design, heterogeneous data and diversified applications, medical big data-aware systems, adaptive edge resource integration, high-reliability and high-availability system design, and other hot research directions in the future, especially the fusion design that spans the cloud and the edge, will be promising.

Acknowledgement: This project was supported financially by the Academy of Scientific Research and Technology (ASRT), Egypt, Grant No. (6475), (ASRT) is the 2nd affiliation of this research. Samih M. Mostafa is the corresponding author.

Funding Statement: This publication was supported by the Ministry of Education, Malaysia (Grant Code: FRGS/1/2018/ICT02/UKM/02/6).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. Tareq, E. A. Sundarajan, M. Mohd and N. S. Sani, "Online clustering of evolving data streams using a density grid-based method," *IEEE Access*, vol. 8, pp. 166472–166490, 2020.

[2] A. Nasif, Z. A. Othman and N. S. Sani, "The deep learning solutions on lossless compression methods for alleviating data load on iot nodes in smart cities," *Sensors Journal*, vol. 21, no. 12, pp. 1–23, 2021.

[3] M. A. Rahman, N. S. Sani, R. Hamdan, Z. A. Othman and A. A. Bakar, "A clustering approach to identify multidimensional poverty indicators for the bottom 40 percent group," *PloS One Journal*, vol. 16, no. 8, pp. 1–12, 2021.
[4] A. B. Abdulkareem, N. S. Sani, S. Sahran, Z. A. A. Alyessari, A. Adam *et al.,* "Predicting COVID-19 based on environmental factors with machine learning," *Intelligent Automation & Soft Computing*, vol. 28, no. 2, pp. 305–320, 2021.
[5] Z. A. Othman, A. A. Bakar, N. S. Sani and J. Sallim, "Household overspending model amongst B40, M40 and T20 using classification algorithm," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 7, pp. 392–399, 2020.
[6] Q. Alsafasfeh, O. A. Saraereh, A. Ali, L. A. Tarawneh, I. Khan *et al.,* "Efficient power control framework for small-cell heterogeneous networks," *Sensors*, vol. 20, no. 5, pp. 1–14, 2020.
[7] K. M. Awan, M. Nadeem, A. S. Sadiq, A. Alghushami, I. Khan *et al.,* "Smart handoff technique for internet of vehicles communication using dynamic edge-backup node," *Electronics*, vol. 9, no. 3, pp. 1–17, 2020.
[8] X. R. Zhang, X. Sun, T. Xu and P. P. Wang, "Deformation expression of soft tissue based on BP neural network," *Intelligent Automation & Soft Computing*, vol. 32, no. 2, pp. 1041–1053, 2022.
[9] X. Zhang, J. Zhou, W. Sun and S. K. Jha, "A lightweigh CNN based on transfer learning for COVID-19 diagnosis," *Computers, Materials & Continua*, vol. 72, no. 1, pp. 1123–1137, 2022.
[10] C. Yang, S. Wenchung and L. Chen, "Accessing medical image file with co-allocation HDFS in cloud," *Future Generation Computer Systems*, vol. 43, no. 8, pp. 61–73, 2015.
[11] S. Chang, M. Lu, T. Pan and C. Chen, "Evaluating the e-health cloud computing systems adoption in Taiwan's healthcare industry," *Life Journal*, vol. 11, no. 4, pp. 1–18, 2021.
[12] M. Kim, S. Yu, J. Lee, Y. Park and P. Youngho, "Design of secure protocol for cloud-assisted electronic health record system using blockchain," *Sensors Journal*, vol. 20, no. 10, pp. 1–24, 2020.
[13] B. Yin and X. T. Wei, "Communication-efficient data aggregation tree construction for complex queries in IoT applications," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3352–3363, 2018.
[14] S. M. He, K. Xie, K. X. Xie, C. Xu and J. Wang, "Interference-aware multisource transmission in multiradio and multichannel wireless network," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2507–2518, 2019.
[15] Y. S. Luo, K. Yang, Q. Tang, J. Zhang and B. Xiong, "A multi-criteria network-aware service promotion composition algorithm in wireless environments," *Computer Communications*, vol. 35, no. 15, pp. 1882–1892, 2012.
[16] Z. F. Liao, J. B. Liang and C. C. Feng, "Mobile relay deployment in multihop relay networks," *Computer Communications*, vol. 112, no. 1, pp. 14–21, 2017.
[17] B. Yin and J. Liu, "A Cost-efficient framework for crowdsourced data collection in vehicular networks," *IEEE Internet of Things Journal*, vol. 8, no. 17, pp. 13567–13581, 2021.
[18] D. Cao, B. Zheng, B. Ji, Z. Lei and C. Feng, "A robust distance-based relay selection for message dissemination in vehicular network," *Wireless Networks*, vol. 26, no. 3, pp. 1755–1771, 2020.
[19] Z. Xu, W. Liang, K. C. Li, J. Xu and H. Jin, "A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles," *Journal of Parallel and Distributed Computing*, vol. 149, no. 4, pp. 29–39, 2021.
[20] Z. Xu, X. Li, J. Xu, W. Liang and K. K. R. Choo, "A secure and computationally efficient authentication and key agreement scheme for internet of vehicles," *Computers & Electrical Engineering*, vol. 95, no. 3, pp. 1759–1788, 2021.
[21] J. Wang, W. Wu, Z. Liao, Y. W. Jung and J. U. Kim, "An enhanced PROMOT algorithm with D2D and robust for mobile edge computing," *Journal of Internet Technology*, vol. 21, no. 5, pp. 1437–1445, 2020.
[22] K. Gu, N. Wu, B. Yin and W. Jia, "Secure data query framework for cloud and fog computing," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 332–345, 2019.
[23] K. Gu, N. Wu, B. Yin and W. Jia, "Secure data sequence query framework based on multiple fogs," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 4, pp. 1883–1900, 2019.

[24] Q. Tang, K. Wang, Y. Song, F. Li and J. H. Park, "Waiting time minimized charging and discharghing strategy based on multiple mobile edge computing supported by software-defined network," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6088–6101, 2019.
[25] W. J. Li, Z. Y. Chen, X. Y. Gao, W. Liu and J. Wang, "Multimodal framework for indoor localization under mobile edge computing environment," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4844–4853, 2018.
[26] H. Takeuchi and N. Kodama, "Validity of association rules extracted by healthcare-data-mining," in *IEEE 36th Annual Int. Conf. in Medicine and Biology Society*, Chicago, USA, pp. 4960–4963, 2014.
[27] Z. Liao, J. Peng, B. Xiong and J. Huang, "Adaptive offloading in mobile-edge computing for ultra-dense cellular networks based on genetic algorithm," *Journal of Cloud Computing*, vol. 10, no. 1, pp. 1–16, 2021.
[28] M. Nkosi and F. Mekuria, "Cloud computing for enhanced mobile health applications," in *IEEE 2nd Int. Conf. on Cloud Computing Technology and Science*, Las Vegas, USA, pp. 629–633, 2010.
[29] X. Wang, Q. Gui and B. Liu, "Enabling smart personalized healthcare: A hybrid mobile-cloud approach for ECG telemonitoring," *IEEE Jounal of Biomedical and Health Informatics*, vol. 18, no. 3, pp. 739–745, 2014.
[30] J. Hsieh and M. Hsu, "A cloud computing based 12-lead ECG telemedicine service," *BMC Medical Informatics and Decision Making*, vol. 12, no. 1, pp. 77–88, 2012.
[31] Z. Laio, J. Peng, J. Huang, W. Jie *et al.,* "Distributed probabilistic offloading in edge computing for 6G-enabled massive internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5298–5308, 2020.
[32] V. Leonov, "Thermoelectric energy harvesting of human body heat for wearable sensors," *IEEE Sensors Journal*, vol. 13, no. 6, pp. 2284–2291, 2013.
[33] Y. Poon and Y. Zhang, "Cuff-less and noninvasive measurements of aerterial blood pressure by pulse transit time," in *IEEE 27th Annual Conf. in Medicine and Biology*, Shanghai, China, pp. 5877–5880, 2006.
[34] T. Tamura, Y. Maeda and M. Sekine, "Wearable photoplethysmographic sensor–past and present," *Electronics*, vol. 3, no. 2, pp. 282–302, 2014.
[35] Z. Liao, Y. Ma, J. Huang, J. Wang and J. Wang, "HOTSPOT: A UAV-assisted dynamic mobility-aware offloading for mobile-edge computing in 3-D space," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10940–10952, 2021.
[36] Z. Poh, J. McDuff and R. Picard, "Advancements in noncontact, multiparameter physiological measurements using a webcam," *IEEE Transactions on Biomedical Engineering*, vol. 58, no. 1, pp. 7–11, 2011.
[37] J. Baek, G. Chung and K. Kim, "A smart health monitoring chair for nonintrusive measurement of biological signals," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 1, pp. 150–158, 2012.
[38] A. Lanard, E. Scilingo and E. Nardani, "Comparative evaluation of susceptibility to motion artifact in different wearable systems for monitoring respiratory rate," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 2, pp. 378–386, 2010.
[39] Z. Zhang, Y. Shen, W. Wang and B. Wang, "Design and implementation of sensing shirt for ambulatory cardiopulmonary monitoring," *Journal of Medical and Biological Engineering*, vol. 31, no. 3, pp. 207–215, 2011.
[40] T. Shany, S. Redmond and M. Narayanan, "Sensors-based wearable systems for monitoring of human movement and falls," *IEEE Sensors Journal*, vol. 12, no. 3, pp. 658–670, 2012.
[41] Y. Kan and C. Chen, "A wearable inertial sensor node for body motion analysis," *IEEE Sensors Journal*, vol. 12, no. 3, pp. 651–657, 2012.
[42] T. Song, X. Huo and X. Wu, "A two-stage method for target searching in the path planning for mobile robots," *Sensors*, vol. 20, no. 23, pp. 1–24, 2020.
[43] F. Bonomi, R. Milito and J. Zhu and A. Sateesh, "Fog computing and its role in the internet of things," in *IEEE 1st MCC Workshop on Mobile Cloud Computing*, New York, USA, pp. 13–16, 2012.
[44] C. Li, Y. Xue and J. Wang, "Edge-oriented computing paradigms: A survey on architecture design and system management," *ACM Computing Surveys*, vol. 51, no. 2, pp. 39–73, 2018.
[45] J. Batalla and F. Gonciarz, "Deployement of smart home management system at the edge: Mechanisms and protocols," *Neural Computing and Applications*, vol. 31, pp. 1301–1315, 2019.

[46] Q. Zhu, R. Wang and Q. Chen, "IoT gateway: Bridging wireless sensor networks into internet of things," in *IEEE/IFIP Int. Conf. on Embedded and Ubiquitous Computing*, New York, USA, pp. 347–352, 2010.
[47] K. Emara, M. Abdeen and M. Hashem, "A Gateway-based framework for transparent interconnection between wsn and ip network," in *IEEE Int. Conf. on Smart Technologies*, Sr. Petersburg, Russia, pp. 1775–1780, 2009.
[48] R. Mueller, J. Rellermeyer, M. Duller and G. Alonso, "Demo: Generic platform for sensor network applications," in *IEEE Int. Conf. on Mobile Adhoc and Sensor Systems*, Pisa, Italy, pp. 1–3, 2007.
[49] D. Bimschas, H. Hellbruck and R. Mietz, "Middleware for smart gateways connecting sensornets to the internet," in *IEEE 5th Int. Workshop on Middleware Tools, Services and Run-Time Support for Sensor Networks*, New York, USA, pp. 8–14, 2010.
[50] G. Shang, Y. Chen, C. Zuo and Z. Yanxu, "Design and implementation of a smart iot gateway," in *IEEE Int. Conf. on Green Computing and Communications*, Beijing, China, pp. 720–723, 2013.
[51] V. Stantchev, A. Barnawi, G. Ghulam, J. Schubert and G. Tamm, "Smart items, fog and cloud computing as enablers of servitization in healthcare," *Sensors & Transducers*, vol. 185, no. 2, pp. 121–128, 2015.
[52] M. Quwaider and J. Jaraweh, "Cloudlet-based for big data collection in body area networks," in *IEEE 8th Int. Conf. for Internet Technology and Secured Transmissions*, London, UK, pp. 137–141, 2013.
[53] A. Loai, W. Bakhader, R. Mehmood and H. Song, "Cloudlet-based mobile cloud computing for healthcare applications," in *IEEE Global Communications Conf.*, Washington DC, USA, pp. 1–6, 2016.
[54] M. Chen, Y. Qian and J. Chen, "Privacy protection and intrusion avoidance for cloudlet-based medical data sharing," *IEEE Transactions on Cloud Computing*, vol. 2, no. 4, pp. 2529–2533, 2016.
[55] A. Amraoui and K. Sethom, "Cloudlet softwarization for pervasive healthcare," in *IEEE 30th Int. Conf. on Advanced Information Networking and Applications Workshops*, Crans-Montana, Switzerland, pp. 628–632, 2016.
[56] S. Lee, Y. Su and C. Shen, "A comparative study of wireless protocols: Bluetooth, uwb, zigbee, and wifi," *Industrial Electronics Society Journal*, vol. 5, no. 8, pp. 46–51, 2007.
[57] K. Navya and M. Murthy, "Zigbee based patient health monitoring system," *Journal of Engineering Research and Applications*, vol. 3, no. 5, pp. 483–486, 2013.
[58] Y. Kim, S. Lee and K. Lee, "Coexistence of zigbee-based wban and wifi for health telemonitoring systems," *IEEE Journal of Biomedical and Health Informatics*, vol. 20, no. 1, pp. 222–230, 2016.
[59] B. Isyaku, M. Zahid, M. Kamat, K. Bakar and F. Ghleb, "Software defined networking flow table management of openflow switches performance and security challenges: A survey," *Future Internet*, vol. 12, no. 9, pp. 1–13, 2020.
[60] A. More and S. Keeping, "Bluetooth low energy: Wireless connectivity for medical monitoring," *Journal of Diabetes Science and Technology*, vol. 4, no. 2, pp. 457–463, 2010.
[61] T. Laine, C. Lee and H. Suk, "Mobile gateway for ubiquitous healthcare system using zigbee and bluetooth," in *IEEE 8th Int. Conf. on Innovative Mobile and Internet Services in Ubiquitous Computing*, Birmingham, UK, pp. 139–143, 2014.
[62] M. Taee, N. Jaradat and A. Ali, "Mobile phone-based health data acquisition system using bluetooth technology," in *IEEE Jordan Conf. on Applied Electrical Engineering and Computing Technologies (AEECT)*, Amman, Jordan, pp. 1–6, 2011.
[63] M. Khan, Z. Kabir and S. Hassan, "Wireless health monitoring using passive wifi sensing," in *IEEE 13th Int. Wireless Communications and Mobile Computing Conf.*, Valencia, Spain, pp. 1771–1776, 2017.
[64] B. Tan, Q. Chen, K. Chetty, K. Woodbridger, W. Li *et al.,* "Exploiting wifi channel state information for residential healthcare informatics," *IEEE Communications Magazine*, vol. 56, no. 5, pp. 130–137, 2018.
[65] F. Zhang, Y. Zhang and J. Silver, "A batteryless 19 μW MICS/ISM-band energy harvesting body area sensor node soc," in *IEEE Int. Solid-State Circuits Conf.*, San Francisco, USA, pp. 298–300, 2012.
[66] N. Cho, J. Bae and J. Yoo, "A 10.8 mw body channel communication/mics dual-band transceiver for a unified body sensor network controller," *IEEE Journal of Solid-State Circuits*, vol. 44, no. 12, pp. 3459–3468, 2009.

[67] J. Yoo, L. Yan, S. Lee, Y. Kim and H. Yoo, "A 5.2 mw self-configured wearable body sensor network controller and a 12 μw 54.9% efficiency wirelessly powered sensor for continuous health monitoring system," *IEEE Journal of Solid-State Circuits*, vol. 45, no. 1, pp. 178–188, 2010.

[68] P. Gope and T. Hwang, "BSN-care: A secure iot-based modern healthcare system using body sensor network," *IEEE Sensors Journal*, vol. 16, no. 5, pp. 1368–1376, 2016.

[69] S. Bao, Y. Poon, Y. Zhang and L. Shen, "Using the timing information of heartbeats as an entity identifier to secure body sensor network," *IEEE Transactions on Information Technology in Biomedicine*, vol. 12, no. 6, pp. 772–779, 2008.

[70] G. Fortino, R. Giannantonio, R. Gravina, P. Kuryloski and R. Jafari, "Enabling effective programming and flexible management of efficient body sensor network applications," *IEEE Transactions on Human-Machine Systems*, vol. 43, no. 1, pp. 115–133, 2013.

[71] L. Lo, S. Thiemjarus, R. King and G. Yang, "Body sensor network–a wireless sensor platform for pervasive healthcare monitoring," in *IEEE 3rd Int. Conf. on Pervasive Computing*, Berlin, Germany, pp. 70–88, 2005.

[72] M. Hossain and G. Mohammad, "Cloud-assisted industrial internet of things (IIoT)–enabled framework for health monitoring," *Computer Networks*, vol. 101, no. 7, pp. 192–202, 2016.

[73] G. Muhammad, M. Rahman and A. Alelaiwi, "Smart health solution integrating iot and cloud: A case study of voice pathology monitoring," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 69–73, 2017.

[74] B. Lin, N. Chou, F. Chong and S. Chen, "RTWPMS: A real-time wireless physiological monitoring system," *IEEE Transactions on Information Technology in Biomedicine*, vol. 10, no. 4, pp. 647–656, 2006.

[75] M. Sun, L. Burke, Z. Mao and Y. Chen, "eButton: A wearable computer for health monitoring and personal assistance," in *IEEE 51st Annual Design Automation Conf.*, New York, USA, pp. 1–6, 2014.

[76] P. Melillo, A. Orrico, P. Scala, F. Crispino and L. Pecchia, "Cloud-based smart health monitoring system for automatic cardiovascular and fall risk assessment in hypertensive patients," *Journal of Medical Systems*, vol. 39, no. 1, pp. 109–115, 2015.

[77] P. Leijdekkers and V. Gae, "A Self-test to detect a heart attack using a mobile phone and wearable sensors," in *IEEE 21st Int. Symp. on Computer-Based Medical Systems*, Jyvaskyla, Finland, pp. 93–98, 2008.

[78] P. Pandin, K. Mohanavelu, K. Safeer, T. Kotresh, D. Shakunthala *et al.,* "Smart vest: Wearable multi-parameter remote physiological monitoring system," *Medical Engineering & Physics*, vol. 30, no. 4, pp. 466–477, 2008.

[79] M. Rienzo, F. Rizzo, G. Parati, G. Brambilla, M. Ferratini *et al.,* "MagIC system: A new textile-based wearable device for biological signal monitoring, applicability in daily life and clinical setting," in *IEEE 27th Annual Int. Conf. in Medicine and Biology*, Shanghai, China, pp. 7167–7169, 2005.

[80] A. Wang, L. Chen and W. Xu, "XPro: A cross-end processing architecture for data analytics in wearables," in *IEEE 44th Annual Int. Symp. on Computer Architecture*, New York, USA, pp. 69–80, 2017.

[81] J. Mohammed, C. Lung, A. Ocneanu, A. Thakral, C. Jones *et al.,* "Internet of things: Remote patient monitoring using web services and cloud computing," in *IEEE Int. Conf. on Internet of Things*, Taipei, Taiwan, pp. 256–263, 2014.

[82] G. Sebestyen, A. Hangan, S. Oniga and Z. Gal, "eHealth solutions in the context of internet of things," in *IEEE Int. Conf. on Automation, Quality and Testing, Robotics*, Cluj-Napoca, Romania, pp. 1–6, 2014.

[83] J. Kang, H. Chung, J. Lee and J. Park, "The design and analysis of a secure personal healthcare system based on certificates," *Symmetry Journal*, vol. 8, no. 11, pp. 1–17, 2016.

[84] R. Bohme, N. Christin, B. Edelman and T. Moore, "Bitcoin: Economics, technology, and governance," *Journal of Economic Perspective*, vol. 29, no. 2, pp. 213–238, 2015.

[85] G. Dagher, J. Mohler, M. Milokkovic and P. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable Cities and Society*, vol. 39, pp. 283–297, 2018.

[86] X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *IEEE 28th Annual Int. Symp. on Personal, Indoor, and Mobile Radio Communication*, Montreal, Canada, pp. 1–5, 2017.

[87] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health Informatics Journal*, vol. 25, no. 4, pp. 1398–1411, 2018.
[88] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *IEEE 2nd Int. Conf. on Open and Big Data*, Vienna, Austria, pp. 25–30, 2016.
[89] Q. Tran, B. Tumbull, H. Wu, A. Silva, K. Kormusheva *et al.,* "A survey on privacy-preserving blockchain systems (PPBS) and a novel PPBS-based framework for smart agriculture," *IEEE Open Journal of the Computer Society*, vol. 2, pp. 72–84, 2021.
[90] M. Benchoufi and P. Ravaud, "Blockchain technology for improving clinical research quality," *Trials Journal*, vol. 18, no. 1, pp. 335–340, 2017.
[91] A. Haleem, M. Javed, R. Singh, R. Suman and S. Rab, "Blockchain technology applications in healthcare: A overview," *International Journal of Intelligent Networks*, vol. 2, pp. 130–139, 2021.
[92] M. Uddin, K. Salah, R. Jayaraman, S. Pesic and S. Ellahham, "Blockchain for drug traceability: Architectures and open challenges," *Health Informatics Journal*, vol. 27, no. 2, pp. 576–583, 2021.
[93] A. Khatoon, "A blockchain-based smart contract system for healthcare management," *Electronics*, vol. 9, no. 1, pp. 1–23, 2020.
[94] G. Capece and F. Lorenzi, "Blockchain and healthcare: Opportunities and prospects for the ehr," *Sustainability*, vol. 12, no. 22, pp. 1–18, 2020.
[95] E. Chukwu and L. Garg, "A systematic review of blockchain in healthcare: Framework, prototypes, and implementations," *IEEE Access*, vol. 8, pp. 21196–21214, 2020.
[96] L. Ming, S. Yu, N. Cao and W. Lou, "Authorized private keyword search over encrypted data in cloud computing," in *IEEE 31st Int. Conf. on Distributed Computing Systems*, Minneapolis, USA, pp. 383–392, 2011.
[97] H. Lohr, A. Sadeghi and M. Winandy, "Securing the e-health cloud," in *Proc. of the 1st ACM Int. Health Informatics Symp.*, New York, USA, pp. 220–229, 2010.
[98] K. Mandi, P. Szolovits and I. Kohane, "Public standards and patients' control: How to keep electronic medical records accessible but private," *British Medical Journal*, vol. 322, no. 7281, pp. 283–287, 2001.
[99] Y. Shucheng, C. Wang, K. Ren and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *IEEE Int. Conf. on Computer Communications*, San Diego, USA, pp. 534–542, 2010.
[100] R. Dahhan, Q. Shi, G. Lee and K. Kifayat, "Survey on revocation in ciphertext-policy attribute-based encryption," *Sensors Journal*, vol. 19, no. 7, pp. 1–18, 2019.
[101] H. Li, L. Deng and C. Yang, "An enhanced media ciphertext-policy attribute-based encryption algorithm on media cloud," *International Journal of Distributed Sensor Networks*, vol. 16, no. 2, pp. 3318–3329, 2020.
[102] L. Ibraimi, M. Asim and M. Petkovi, "Secure management of personal health records by applying attribute-based encryption," in *IEEE 6th Int. Workshop on Wearable, Micro, and Nano Technologies for Personalized Health*, Oslo, Norway, pp. 71–74, 2009.
[103] J. Hur and D. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1214–1221, 2011.
[104] M. Li, S. Yu and Y. Zheng, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013.
[105] N. Narayan, M. Gagne and R. Safavi, "Privacy preserving ehr system using attribute-based infrastructure," in *Proc. of the ACM Workshop on Cloud Computing Security*, New York, USA, pp. 47–52, 2010.
[106] S. Jahid, P. Mittal and N. Borisov, "EASiER: Encryption-based access control in social networks with efficient revocation," in *Proc. of the 6th ACM Symp. on Information, Computer and Communication Security*, Hong Kong, China, pp. 411–415, 2011.
[107] Z. Xia, X. Mao, K. Gu and W. Jia, "Two-dimensional behavior marker-based data forwarding incentive scheme for fog computing-based SIoVs," *IEEE Transactions on Computational Social Systems*, vol. 9, no. 3, pp. 1–13, 2021.

[108] R. Lu, X. Lin and X. Shen, "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 3, pp. 614–624, 2013.
[109] Z. Xia, Z. Fang, K. Gu, J. Wang, J. Tan *et al.,* "Effective charging identity authentication scheme based on fog computing in V2G networks," *Journal of Information Security and Applications*, vol. 58, no. 3, pp. 1026–1037, 2021.
[110] Y. Abdsulsalam and M. Hedabou, "Security and privacy in cloud computing: Technical review," *Future Internet*, vol. 14, no. 1, pp. 1–18, 2022.
[111] S. Cabuk, C. Dalton and K. Eriksson, "Towards automated security policy enforcement in multi-tenant virtual data centers," *Journal of Computer Security*, vol. 18, no. 1, pp. 89–121, 2010.
[112] S. M. Idrees, M. Nowostawski, R. Jameel and A. Mourya, "Security aspects of blockchain technology intended for industrial applications," *Electronics*, vol. 10, no. 8, pp. 1–14, 2021.
[113] M. Yuce, S. Ng, N. Myo, J. Khan and W. Liu, "Wireless body sensor network using medical implant band," *Journal of Medical Systems*, vol. 31, no. 6, pp. 467–474, 2007.
[114] A. Passarella, M. Conti, E. Borgia and M. Kumar, "Performance evaluation of service execution in opportunistic computing," in *Proc. of the 13th ACM Int. Conf. on Modeling, Analysis, and Simulation of Wireless and Mobile Systems*, Bodrum Turkey, pp. 291–298, 2010.