Information Sciences 645 (2023) 119329

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Distributed power storage and converter system health monitoring Internet of Things under blockchain

Zuozhi Liu

School of Mathematics and Statistics, Guizhou University of Finance and Economics, Guiyang 550025, China

ARTICLE INFO

Keywords:
Blockchain
Medical Internet of Things
Microgrid
Health status monitoring
Deep learning
Information storage

ABSTRACT

This study to solve the information storage problem in the current medical system analyzes the privacy and security effects of the blockchain (BC) in the Internet of Medical Things (IoMT) and accurately predicts the health status of IoMT users. First, a microgrid is designed to supply power to BC, and then BC is applied to IoMT so that medical data can be stored safely and secure information can be shared. Then, deep learning is used to predict and analyze the characteristics of users' health data. Besides, the IoMT model under BC and improved AlexNet are constructed. Finally, the model is evaluated based on an example. According to the results, the calculation overhead of the model keeps stable at 0.13 s, and the usage of central processing unit is always lower than 17.62%. Regarding data transmission security, the average delay of the model reported keeps stable at 350 ms, and the area under the characteristic curve of receiver operating is 0.9217. This algorithm can accurately predict the user's physiological health. In this study, a system with high model efficiency and superior performance is created. This work is of significance for the intelligent development and secure information storage in the medical field and contribute to the development of the medical industry.

1. Introduction

1.1. Research background

At present, China is trapped in a shortage of medical resources, and the medical resources are unevenly distributed between urban and rural areas. Patients in China will visit different medical institutions and seek good medical resources after considering their health conditions. After being diagnosed, patients may not receive the treatment from the same medical institution. As patients do not seek treatment and care at the same medical institution, the electronic medical records of patients become fragmented [1]. From the perspective of medical institutions, repeated inspections have also caused a waste of medical resources. Usually, patient medical records are stored in the information systems of medical institutions at all levels and patients can only get copies of their medical or handwritten outpatient records. Medical and handwritten outpatient records can wear and tear easily, so medical histories are incomplete [2] and doctors fail to treat patients accurately. Due to the inconsistency of system interfaces and conflicts of interest, medical institutions at all levels have neither the will nor the motivation to share patients' medical information with other medical institutions. With the advancement of information technology in recent years, electronic medical records may gradually replace traditional hadwritten medical records. Although electronic medical records can reduce the wear and tear of paper medical records,

E-mail address: lzz_gufe@163.com.

https://doi.org/10.1016/j.ins.2023.119329
Received 5 January 2022; Received in revised form 7 June 2023; Accepted 10 June 2023
Available online 21 June 2023

the problem of incomplete medical records cannot be fixed. Moreover, the electronic medical records are patients' private information. As a result, a large number of patient medical records can be accessed to or obtained by medical workers [3]. If the hospital illegally uses medical record resources, it will go against the patients' privacy. In addition, it is tough to find medical records with a commercial and medical value in a large amount of medical record data, many of which are medical records without retail and medical value [4].

Blockchain (BC) technology has now been widely applied in many fields. For example, Luo et al. (2023) found that applying BC technology in electric vehicle charging scenarios could improve the charging efficiency [5]. With the advent of BC technology, the distributed data charactieristics makes it possible for BC technology to solve the problem of incomplete medical history records [6]. All participants on the BC can access the attributes of all descriptions, which improves the sharing of some medical record resources in medical institutions at all levels and reduce the waste of some medical resources. At the same time, BC cannot be changed once it is created. This feature effectively prevents electronic medical record from being tampered. Revision: BC technology provides a more secure way of storing medical information, enabling the tracking of patient records after diagnosis and treatment [7]. By utilizing BC technology, patients' medical information can be stored, patients can have a complete control of their medical history from birth to the present, and doctors can obtain comprehensive medical data of patients. This can significantly enhance the accuracy of patient diagnosis and treatment. Currently, the BC-based electronic medical record storage system has garnered significant attention and many experts shift their eyes to the relevant researches [8]. Electronic medical records serve as a complete medical history of a patient. A sound BC-based electronic medical record system is beneficial to the diagnosis of patients by medical institutions, as well as the study of medical records by research institutions and the data collection by pharmaceutical companies. However, electronic medical records contain patient privacy, which would cause negative implications if compromised. Therefore, the BC used to store electronic medical records requires specific access control mechanisms to prevent data leakage. In addition to security factors, the efficiency of BC access to stored electronic medical records significantly impacts the system's performance, so the blocks for holding patient electronic medical records should be added or queried easily.

In addition to BC technology, many scholars have proposed using the Internet of Things (IoT) in the medical field to solve the problems of complicated and expensive medical treatment caused by the imperfect medical system in urban development. For example, the return prediction of medical waste generated by reverse logistics and the intelligent monitoring and management of unique patient physiological health have been studied in an in-depth manner. However, user privacy security issues should also be taken into account in today's transparent network information. With its wide application in electronic data, intelligent transportation, smart homes, environmental protection, and other fields, the IoT has been listed as an emerging industry with national critical strategic significance. The Internet of Medical Things (IoMT) is defined as application of IoT to the medical field and can realize the intelligent acquisition of human physiological parameters, drug management information, and patient status and establish a complete and efficient disease monitoring and prediction system through advanced computer technology. Although numerous medical data are collected, the potential of IoMT system has not been fully tapped. It seriously wastes a large amount of data resources in healthcare networks and affects public or private hospitals and other healthcare institutions [9]. User information leakage is also a pressing issue. Therefore, an effective psychological protection system through technology will play a crucial role in the development of the future public healthcare system. Many scholars have conducted studies on this issue. For example, Wang et al. (2022) studied a wearable remote rehabilitation medical data security system using IoT technology [10].

The security of private data is reflected in the storage and this is an essential problem in the system during the operation of the IoT. The stable operation of BC and IoMT cannot be achieved without the use of electrical energy. In the traditional power supply model, there is a strong coupling and dependency between the system units that cannot be widely distributed due to the different locations of power points and load centers [11]. A microgrid is an independent power supply system that integrates distributed power supply, energy storage, and control equipment. The system can flexibly deploy and control IoT and BC according to requirements and reduce device coupling [12]. IoT monitors the health status of users. As an unsupervised algorithm, deep learning autonomously learns multi-level features of data from massive raw medical data. It can abstract the relevant physiological information of users and provide support for accurate and rapid analysis of their health status. Physiological health and health prediction play a crucial role in the intellectual development of the medical field. In this study, an innovative approach in combination of BC and IoT technologies has been adopted to design a distributed IoT model for monitoring the health of a power storage and converter system. The proposed model addresses the current challenges associated with information storage in healthcare systems. This model enables the accurate prediction on the health status of IoT medical devices' users and ensures the security of medical data storage and information sharing. Furthermore, it makes a significant contribution to the security of IoT systems by using BC technology to securely store and share medical data and protecting the privacy of medical information. Additionally, the proposed model leverages deep learning technology to analyze and predict user health data characteristics, which improves the accuracy and efficiency of medical diagnoses. Although IoT and deep learning technologies have been used in other solutions to predict and analyze medical data, very few have incorporated BC technology to securely store and share medical data. Therefore, the proposed model has a significant advantage over medical data security, while also improving the efficiency and accuracy of medical data processing.

1.2. Research problem statement and contributions

As discussed above, the gap between this work and previous studies lies in the application of microgrid technology in medical data research. The key here is to improve the information storage capacity of the medical system by combining BC technology, IoT technology, and deep learning technology. This study aims to develop a model for information security storage and data prediction. The theoretical significance of this study is as follows: it can accurately predict the user's health status and protect the user's privacy and security, which has significant social value in the medical field. The innovative aspect of this study lies in using microgrids to

power the BC and combining BC technology and IoT technology to provide secure storage of medical information and data information sharing. In IoMT, deep learning is adopted to accurately predict and analyze the characteristics of user health data, and the IoMT model is constructed via BC and enhanced AlexNet. The model is then evaluated based on case analysis. The practical contribution of this study is to provide a reference for subsequent intelligence and privacy security protection in healthcare.

1.3. Research structure

This study explores the data storage of the medical system through BC technology and IoT technology. Section 1 is the introduction, which mainly expounds on the research background, purpose, gap, significance, and innovation points. Section 2 clarifies the research status, and application principle of business continuity technology. Section 3 demonstrates the methods used to analyze the application of BC, share background information about the distributed BC, and build the IoT model based on the BC technology and improved AlexNet. Section 4 discusses the application effect of business continuity in the medical system, evaluates the performance of the constructed model, and analyze the experimental results. Section 5 is the conclusion part and summarizes the main findings, research significance, research limitations, and prospects.

2. Recent related works

2.1. BC's application status in IoT

As it plays an imperative role in developing current information technology, BC has been widely used in IoT systems. During its rapid growth, the IoT has been widely applied to various fields, and security-related research has also attracted the attention of many scholars. Ismail et al. (2021) performed a comparative analysis on BCs, explained the classification and architecture of BCs, compared different consensus mechanisms, and discussed scalability, privacy, interoperability, energy consumption, and regulatory issues [13]. To meet the security requirements of the IoT, Chen et al. (2022) proposed an IoT consistency protocol based on reputation. This protocol resizes stronger attacks using improved BCs and provides opportunities for a few users with less computing power to participate in the consensus [14]. Suler et al. (2021) proposed an automated online reliability assessment method under physical network systems. An evaluation framework under machine learning knowledge is established, and an online sorting algorithm is designed to realize online real-time analysis and evaluation [15]. Qiao and Lv (2023) proposed a decentralized collaborative learning model based on BC, and realized a reliable energy digital twins model [16]. Douiba et al. (2023) proposed an IoT security classification system to better understand the different threats and defense mechanisms in the field of IoT security, and pointed out the challenges and future research directions of BC in IoT security [17]. Zubaydi et al. (2023) discussed the application of BC technology in IoT security and privacy protection using smart homes as an example. In that literature, a BC-based smart home system architecture was proposed and the key technologies and application scenarios of BC technology for security and privacy protection in smart homes were analyzed. It also identified the problems and challenges in current applications and proposed future research directions [18].

Woźniak et al. (2020) proposed a Recurrent Neural Networks (RNN) model for threat detection in IoT and network malware. The model comprises three main components: data collection, data processing, and RNN model training. The data collection stage involves collecting data from IoT devices and network traffic, while the data processing stage includes data preprocessing, feature extraction, and data cleaning. The RNN model training stage involves training and optimizing the RNN model using training data. The research results showed that the RNN model effectively detects and identifies malware threats in IoT devices and network traffic, with high detection accuracy and robustness. This research provides a new approach and method for IoT security research [19]. Woźniak et al. (2020) also proposed a fuzzy rule-based 6G IoT home environment control system comprising sensors, actuators, controllers, and user interfaces. The system provides intelligent and adaptive control of the home environment with high performance and reliability. This study proposes a new approach and method for 6G IoT research and application [20]. Kundu et al. (2021) proposed an IoT failure prediction framework based on interpretable machine learning. They collected environmental and soil data during the growth period of pearl millet using IoT hardware sensors and predicted pearl millet growth using interpretable deep learning models. The researchers proposed an interpretable deep learning framework using multiple deep learning models and visualized the model's working process to help farmers better understand pearl millet growth. This research indicated that interpretable machine learning frameworks can help improve farmers' decision-making abilities and provide more accurate predictions of pearl millet growth [21].

In summary, the development of BC technology provides fundamental capabilities for the evolution of IoT systems and necessary security guarantees for the advancement of information technology. Therefore, BC technology will continue to play an increasingly important role in the technological developments in the future. However, the infrastructure of BC technology is not yet complete. In other words, the optimization measures for the application of BC technology are not mature enough. Therefore, more efforts should be made to provide references and technical support for the promotion of BC technology.

2.2. The trend of deep learning in the medical field

Currently, there are many studies on deep learning applications in the medical field, such as segmentation and recognition of medical images and tumor staging prediction. Still, there are few references for its adoption in IoMT. Given that IoMT has a natural and close continuity with medical informatization and the IoT, the research on IoMT has much in common with that of the IoT, and many scholars have conducted research on it. Liu et al. (2021) focused on improving IoMT by using formal approaches based on reliability, security, and healthcare provided by the network physical system community [22]. Piccialli et al. (2022) proposed a dynamic adaptive

Table 1
Summary of previous studies.

Year	Authors	Solution methods	Databases	Types of BCs or IoT	Study objectives	Novelties	Factors/features
2020	Woźniak M, Siłka J, et al.	Based on a recurrent neural network model.	Open data set	Industrial internet of things	Enhance network traffic security	This work combines deep learning models with the IoT.	Number of network features
2020	Woźniak M, Zielonka A, et al.	A 6G IoT home environment control system based on fuzzy rules.	Open data set	Infrastructure internet of things	Improve information transmission speed	This work is based on the 6G network communication standard for developing the next level of IoT.	Water flow management, windbreak control, safety aspects, and limiting CO_2 through adaptive ventilation
2021	Kundu et al.	Using interpretable machine learning algorithms to predict the growth of Echinococcosis granulosus.	Automatic intelligent data collector collection	Integrated internet of things	Intelligent identification of crop diseases	This work proposes a deep learning and IoT-based solution for plant disease detection and classification.	Bacterial blight and rust diseases in Pearl millet
2021	Ismail et al.	They compared and contrasted BC technology	Collected in this work	Private BC	Help design and develop data management systems in the healthcare industry for better patient care	A new BC cloud integration paradigm has emerged in the healthcare field.	Classification, advantages, and disadvantages
2021	Suler et al.	They proposed an automated on-line reliability evaluation method based on network physical system	Data collected from McKinsey and Ovum	Industrial internet of things	Enhance factory intelligence	This work investigates the latest research findings on IoT sensor networks, digital mass production, and sustainable organizational performance based on the networked physical systems of smart factories.	Descriptive statistics
2021	Liu et al.	They described the practical adoption of the democratization of medical devices by patients and healthcare providers	Open data set	–	Improve image segmentation accuracy	This work summarizes the three main methods of medical image segmentation and their limitations, and expands future directions for development.	Quantity, resolution
2021	Budd et al.	They proposed an IoMT device authentication scheme based on the physically unclonable function to prevent attackers from using various vulnerabilities to attack the whole network	–	–	Enhance accuracy of medical image analysis	This work examines the role that humans can play in the development and deployment of deep learning diagnostic applications, with a focus on techniques that preserve important inputs from end-users.	Active learning, interaction with model outputs, real-world considerations, future prospects, and unanswered questions
2022	Chen et al.	They proposed a reputation-based IoT consistency protocol	Open data set	Private BC	Consider user privacy issues using BC technology	This work reviews proposed solutions for providing different vehicle services using BC technology, while overcoming inherent privacy leakage issues in BC and vehicle services.	Privacy and data confidentiality
2022	Piccialli et al.	They proposed a dynamic adaptive network fuzzy inference system	–	–	Outline and analyze current challenges and future research directions	This work proposes a comprehensive and in-depth study on the deep learning methods and their applications in medicine.	Health data, clinical images, genomic sequences, and prescription therapy data

(*continued on next page*)

Table 1 (*continued*)

Year	Authors	Solution methods	Databases	Types of BCs or IoT	Study objectives	Novelties	Factors/features
2023	Cerchione et al.	Creating a distributed electronic health record ecosystem using BC technology.	Open data set	Private BC	Definition of BC network framework, design of BC platforms, and assessment of potential added value	This work provides a new approach to manage medical records and better share patient health data between healthcare institutions.	Clinical and nursing assessment information, physical examinations, comprehensive clinical diaries, medical reports, outpatient services, and other diagnostic expert tests
2023	Douiba et al.	An improved intrusion detection system using gradient boosting and decision trees.	Optimized nsl-kdd, IoT-23, BoT-IoT and Edge IIoT	Infrastructure internet of things	Enhance IoT security	This work uses the open-source IoT security tool Catboost.	Accuracy, recall, and precision
2023	Zubaydi et al.	A systematic review of the latest methods for integrating BC and IoT has been conducted	–	Public BC	Enhance data security	This work describes different works that integrate BC technology and IoT to solve various aspects of privacy and security issues.	Types of BCs and platforms, consensus algorithms, evaluation environments and metrics, future work or unresolved issues

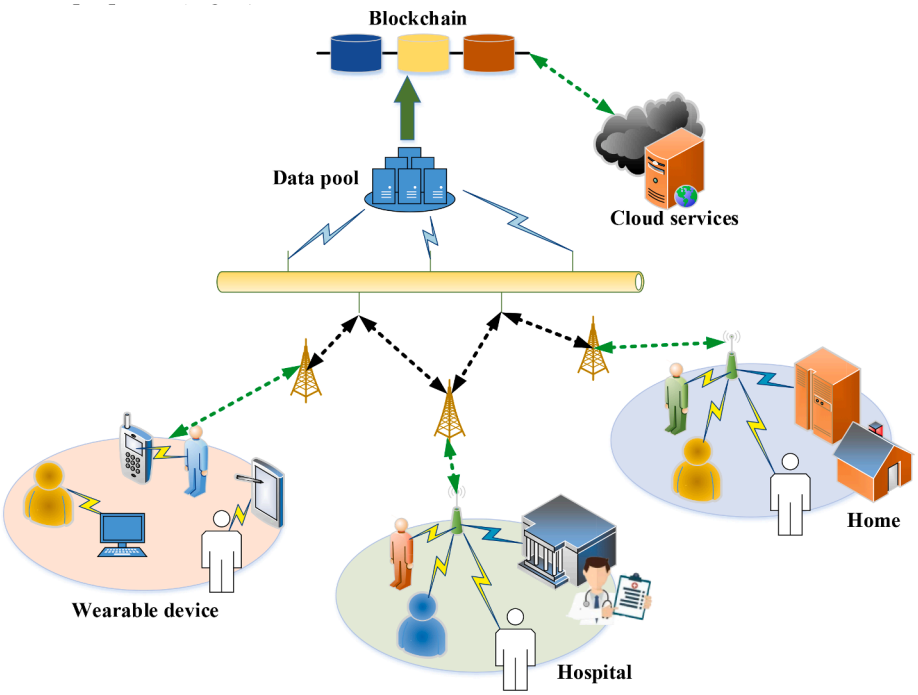

Fig. 1. BC-based IoMT data information sharing structure.

network fuzzy reasoning system. Missing values were interpolated simply and accurately, and the missing values populated the entire data set. The genetic algorithm and particle swarm optimization algorithm were employed to evaluate the final performance of IoMT [23]. Budd et al. (2021) proposed an IoMT device authentication scheme based on the physical non cloning function to prevent attackers from using various vulnerabilities to attack the entire network [24]. Cerchione et al. (2023) provided an overview of the application of deep learning in the field of electronic health record processing, including research progress on automatic classification, annotation, and prediction of medical data [25].

In summary, many scholars have studied the security issues of the IoT, as it is increasingly widely applied today. However, there are few studies on the adoption of BC in IoMT in the medical field, so more in-depth research is needed for realizing the intellectual development in the medical field. Therefore, deep learning algorithms are used to predict and monitor patient health status in IoMT. Moreover, BC is adopted to ensure the security of private information in IoMT. By doing so, this study hopes to provide an experimental

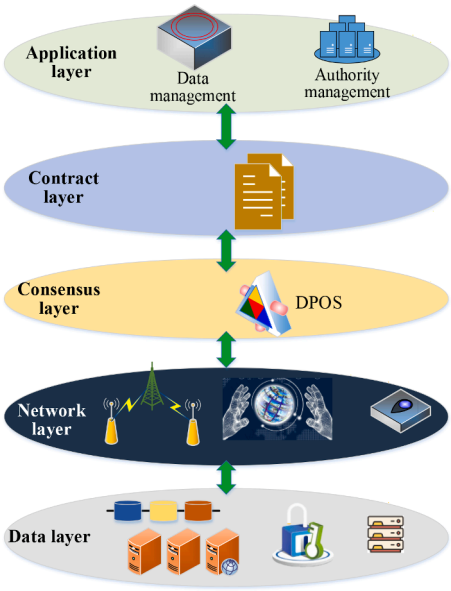

Fig. 2. Distributed BC system structure.

reference for IoT health monitoring and information security in the medical field. In summary, the concluding table is shown in Table 1.

3. Methodology

3.1. Feasibility analysis of BC applied to IoMT

With the rapid progression of information technology, cloud computing, BC, and other intelligent technologies, IoT in the medical field has further increased requirements for data security performance. Although cloud computing has solved the issue of medical data storage, data sharing remains a challenge. When traditional authentication theory and technology are applied to establish a third-party trust mechanism in IoMT, its third-party credibility is questioned. Security authentication is complex in the IoMT environment, which includes multiple heterogeneous networks, multiple types of nodes, and different user nodes and device nodes. There are few studies on various authentication technologies, yet data sharing has not been realized [26,27]. Huang et al. (2023) studied the consensus mechanism of software-defined BC in the IoT and proposed a practical Byzantine fault-tolerant supervised consensus scheme based on improved proof of delegation rights. In the context of the development of IoT technology, decentralized distributed computing paradigm was utilized to improve BC smart contract technology [28]. The introduction of BC provides a solution to the high dependence on third-party trust centers in security authentication and implements secure data transmission, thanks to its decentralized feature. Therefore, a BC-based IoMT data-sharing scheme is proposed (Fig. 1).

In Fig. 1, the data in the IoMT database will be encrypted after BC is applied in IoMT. During information use, the information is first encrypted through blocks, and then the information can be acquired through block decoding after being transmitted to the using organization [29]. Therefore, by incorporating BC into the IoMT model, the data can be ensured to be tamper-proof and traceable. Furthermore, security threats in the authentication of medical data providers and users can be addressed by utilizing bilinear mapping and mathematical problems in the security authentication stage. This also enables the avoidance of relying on the reliability of third-party service centers, and facilitates the realization of two-way authentication between hospitals and BC nodes [30]. The patient's medical records, such as outpatient medical records, inpatient medical records, medical image data, medical orders, laboratory records, and other important data, can be safely stored in this system. The system can also share data with patients, hospitals, researchers, and others to advance medicine.

3.2. BC distributed energy storage and energy consumption analysis

The BC model is a decentralized distributed system, in which each participant has identical copies and data synchronization and verification are achieved through information exchange. During BC progression, it has gone from the BC 1.0 phase of decentralized money and payments to the current industry development BC 2.0 phase. In this stage, Ethereum, as a distributed BC system, provides the concept of smart contracts, and the scripting language of smart contracts can run on the Ethereum virtual machine [31]. Ethereum comprises an adoption layer, smart contract layer, incentive layer, consensus layer, network layer, and data layer (Fig. 2).

When distributed BC is applied to the IoT, mobile terminal devices distributed everywhere will generate massive interactive data

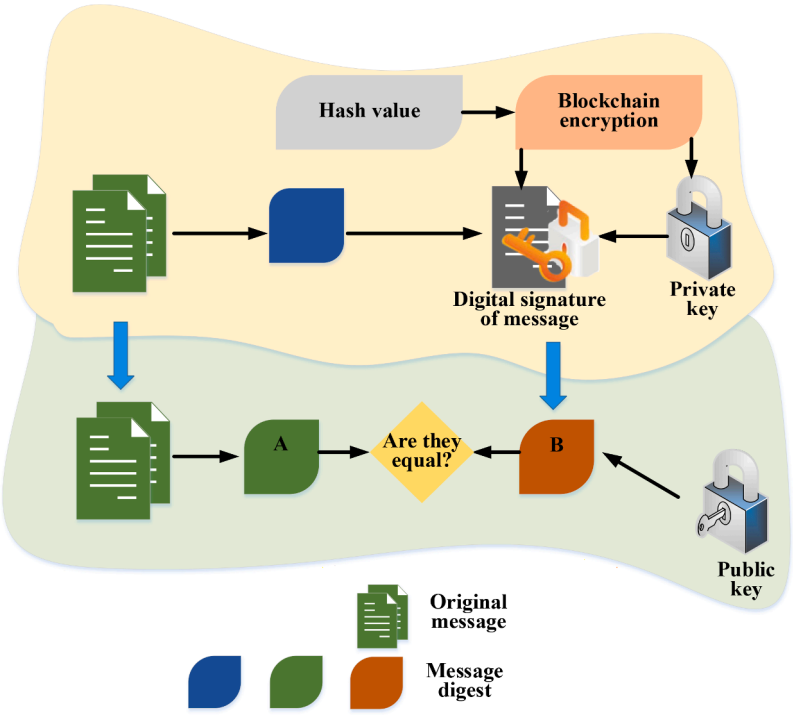

Fig. 3. Transaction signature and verification process.

every day. The cost of interactive data collection and privacy protection of sensitive data are undoubtedly challenges for developing IoT systems [32]. The data layer is the foundation of the Ethereum data structure, which contains encryption algorithms such as hash values, asymmetric encryption, and digital labels. It ensures the security of Ethereum accounts. During digital signature transactions, each transaction is digitally marked with a private key to ensure that the transaction can't be tampered with by others and the transaction is initiated by the sender [33,34]. When a transaction is initiated by the initiator, it is displayed in the IoT system and made visible to all users. The most commonly used hash algorithm in BC is Secure Hash Algorithm-256, which is a secure hash function with high computational efficiency and is almost unbreakable. Using this algorithm ensures that the transaction is transparent and fair. Furthermore, the specific transaction content is encrypted using the hash value, making it impossible for anyone other than the two parties involved to access it. As a result, the hash value serves as protection for the original data. When data are stolen or tampered with, BC encrypts the information to prevent information leakage. The hash value is composed of 256-bit binary numbers. The hash value varies regarding the original content, so it has high-strength encryption performance. It is assumed that d is the private key and g is the element point (x, y).

Buffers are set to prevent data loss in the system. Each buffer comprises two parts: a storage area that actually stores data and a buffer header that identifies the buffer. When the core needs a free buffer, it takes a free buffer from the header of the corresponding free buffer list according to the type of data to be loaded, and loads a disk data block. The hashno value is calculated based on the device number and block number data pair corresponding to the data block, and the hashno value is put into the head of the corresponding hash chain table.

According to the elliptic curve algorithm, the public key is represented as follows.

$$q = d \times g \tag{1}$$

The process of transaction signature and verification in the digital signature algorithm is shown in Fig. 3.

In this process, the transaction is encrypted using the sender's private key during the signing process. Encryption algorithms can be classified into two types: symmetric algorithms and asymmetric algorithms. Asymmetric algorithms are considered more secure than symmetric algorithms. However, in practical applications, symmetric encryption algorithms are typically used to encrypt data, while asymmetric encryption algorithms are used to encrypt a key of the symmetric encryption algorithm. This work adopts an asymmetric algorithm. Commonly used asymmetric algorithms include Ron Rivest; Adi Shamir; Leonard Adleman (RSA), Elgamal, the knapsack algorithm, Rabin, and Ellipse Curve Cryptography (ECC). Since the security strength is often linearly related to the critical length, the key size has to be increased to improve the encryption security. In this case, the ECC algorithm has a slight increase in the crucial length, so it has certain advantages.

Here, a simple data example can illustrate the advantages of ECC algorithm. It is assumed that a message with a length of 128 bits needs to be encrypted while ensuring a security level of 128 bits. Comparing the key lengths and encryption/decryption speeds of ECC and RSA algorithms, it is found that ECC requires a 256-bit key at the 128-bit security level, while RSA requires a 3072-bit key.

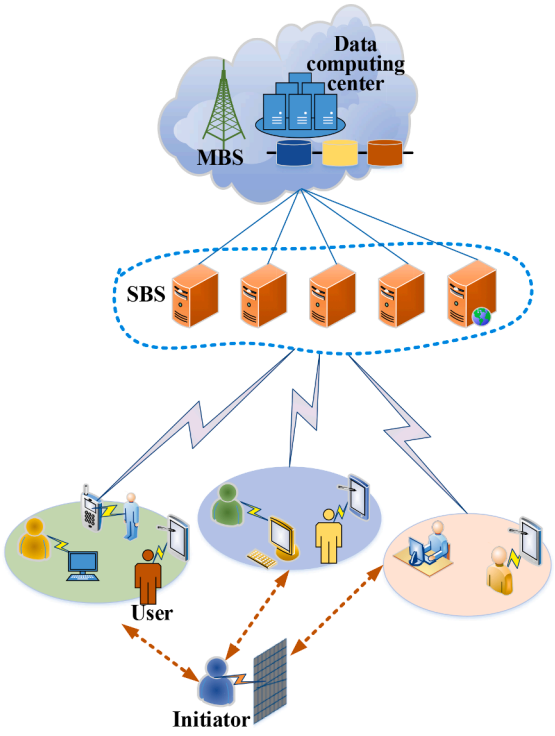

Fig. 4. Mobile distributed computing system model formed by distributed nodes or base stations and health monitoring users.

Therefore, using ECC can save storage space and improve computational efficiency. In terms of encryption/decryption speed, ECC is also faster than RSA. For instance, an ECC encryption implementation based on Nvidia Tesla K20 GPU (graphics processing unit) can achieve a speed of over 600 MB per second, while RSA can only reach a speed of 100 MB per second. Additionally, due to the lower computational requirements of ECC, it is more suitable for mobile devices and embedded systems with limited computing and storage resources.

The State Cryptography Administration of China released the national secret sm2 algorithm at the end of 2010. It has made optimization and improvement on the theoretical basis of the ECC algorithm and is better than the RSA algorithm in terms of algorithm efficiency and security strength. The critical length it uses is shorter than that of the RSA algorithm, but it can achieve faster, safer, and more reliable data encryption. Therefore, this work chooses the ECC algorithm as the encryption algorithm [35].

The first step is selecting a random number $k \in [1, n-1]$ and calculating point (x_1, y_1) according to Equation (2).

$$(x\_1, y\_1) = k \times g \tag{2}$$

In the second step, r is calculated using Equation (3). If $r = 0$, it should return to the first step to reselect the random number k.

$$r = x_1 mod n \tag{3}$$

In the third step, if r $\neq 0$, the hash value $h(m)$ of message digest m is calculated using Equation (4).

$$h(m) = HASH(m) \tag{4}$$

The fourth step is calculating S_v according to the random number k, the hash value $h(m)$ of the message digest, the private key SKv, and formula (5). If$S_v = 0$, it should return to the first step to reselect the random number k.

$$S_v = \left[(h(m) + SKv^{*} r)^{*} k^{-1}\right] mod n \tag{5}$$

In the fifth step, if$S_v \neq 0$, the signature of the hash value $h(m)$ is $\{r, S_v\}$.

The original information is further verified. Step 1: If $\{r, S_v\}$ is an integer between [1, n-1], the following equation is calculated.

$$\omega = {S_v}^{-1} mod n \tag{6}$$

In the second step, message digest A and message digest B are calculated as follows.

$$\mu_1 = (HASH(m) \cdot \omega) mod n \tag{7}$$

$$\mu_2 = (r \cdot \omega) mod n \tag{8}$$

The third step is calculating a point on the elliptic curve as follows.

$$(x_1, y_1) = \mu_1 g + \mu_2 q \tag{9}$$

$$r = x_1 mod n \tag{10}$$

In the fourth step, if the above equation exists and r is 0 or∞, it should refuse to sign; otherwise, it should pass the inspection [36]. Furthermore, the data acquisition process is analyzed. The mobile distributed computing system formed by a distributed node or base station and users is shown in Fig. 4.

In this distributed system, a macro base station (MBS) covers many small base stations (SBSs), which jointly serve U users, denoted as $\mu = \{1,2,\cdots,U\}$. Each user is connected to a small base station. However, multiple base stations sharing the same spectrum will cause interference and influence each other. Then, it is set that $P_u^k(t)$ refers to the propagation power of base station k serving user u, and $\sigma_u(t)$ refers to the additive white Gaussian noise of the user [37]. Therefore, the signal-to-interference plus noise ratio (SINR) of the wireless channel connecting user u and the base station is marked as follows.

$$\gamma_u^k(t) = \frac{g_u^k(t) P_u^k(t)}{\sum_{i \neq k} \sum_{u \in \mu}^{i} g_u^i(t) P^i(t) + \sigma_u^i(t)} \tag{11}$$

$g_u^k(t)$ refers to the channel loss of user u and base station k, and $g_u^i(t)$ refers to the channel loss of user u in the other base station i. It is assumed that all spectrum resource bandwidth W in all base stations is divided into B subchannels, and the channel bandwidth of participant u is $b_u = \{1, 2, \cdots, W/B\}$. Then, the transmission rate of uploading and downloading connecting participant u and base station k is calculated as shown in Equation (12).

$$r_u^k(t) = b_u \log\left(1 + \gamma_u^k(t)\right) \tag{12}$$

The energy consumption of a single segment should consider the total energy consumption, including the energy consumed by the SBS when downloading the segment, as well as the energy consumed by the user to execute the segment and return the model results. It is assumed that the downlink transmission power of the SBS is P_u^k; then, the transmission power of user u is also P_u^k, so the energy consumed by user u to complete the unit segment is calculated as follows.

$$e_u = P_u^k(t) \frac{N^D}{r_u^k(t)} + \kappa (h_u)^3 t_u^{\text{self}} + P_u(t) \frac{N^R}{r_u(t)} \tag{13}$$

κ refers to the energy efficiency coefficient of the processor. N^D and N^R refer to the content (data set and default model) that needs to be downloaded and uploaded for each small segment (part of the task), respectively. $\frac{N^D}{r_u}$ and $\frac{N^R}{r_u}$ refer to the time consumption of downloading input data and returning result data from IPFS, respectively. h_u refers to the number of computing resources provided by the user. The first part is the energy consumed by the base station when downloading a small segment from the IPFS, and the second is the energy consumed by the user to execute the small segment. The third is the energy consumed by the user to return the results after performing the task [38].

The optimization of task allocation selects users and uses resource allocation to minimize energy consumption, allowing the network to learn by itself. In addition, the delay of all users should be less than the QoS to obtain revenue, and the optimization goal is as follows.

$$\begin{aligned} & minE_u = \sum_{u \in u} \left[P_u^k(t) \frac{N^D}{r_u^k(t)} + n_u \kappa (h_u)^3 t_u + P_u(t) \frac{N^R}{r_u(t)} \right]. \\ & st. \sum_{u \in \mu} \left[\frac{N_u^D}{r_u^k(t)} + n_u \frac{\alpha \left(N_u^D + N_u^{\text{self}} \right)}{h_u} + \frac{N^R}{r_u(t)} \right] \leq \tau \end{aligned} \tag{14}$$

n_u refers to the sum of the number of small segments executed by the user being selected, $\sum_{u \in \mu} n_u = n$. The workload of n is the entire task, and E_u refers to the total energy consumption. Therefore, the goal of task allocation is minimizing energy consumption and propagation delay.

In terms of energy consumption, the BC mechanism in the IoT is supplied with energy in the form of a microgrid. It is assumed that there are t different types of microgrid i, and each type corresponds to a production cost function. They are independent of each other. Therefore, when the cost function type of microgrid i is C_i^k and λ_i^l is selected as the fluctuation factor λ_i, the probability of the cost function of this type is as follows.

$$p\left(C_i = C_i^k; \lambda_i = \lambda_i^l\right) = p\left(C_i = C_i^k\right)\left(\lambda_i = \lambda_i^l\right) = p_i^k \eta_i^l \tag{15}$$

p_i^k refers to the production cost probability of microgrid i. refers to the fluctuation factor probability of microgrid i, $k = 1,2\ldots,t$; $l = 1,2,\ldots,n$. Thus, the cost expectation of microgrid i is obtained as follows.

$$E(C_i) = \sum_{l=1}^{t} \sum_{k=1}^{t} p_i^k \eta_i^l \left(1 + \lambda_i^l\right) C_i^k \tag{16}$$

At this time, the game model is converted from an incomplete information game to a complete information and imperfect information game model. Nash equilibrium is used to solve this game problem.

Taking microgrid 0 as the entry point and assuming the selected cost function is type 1, the cost function is as follows.

$$C(p_0) = a_0 p_0^2 + b_0 p_0 + c_0 \tag{17}$$

Then, the cost expectation of microgrid i is calculated as follows.

$$EC_i = \sum_{l=1}^{t} \sum_{k=1}^{t} p_i^k p_i C_i^k = \overline{a}_i p_i^2 + \overline{b}_i p_i + \overline{c}_i, i = 1, 2, \cdots, N-1 \tag{18}$$

The above equation calculates the profit function of microgrid i as follows.

$$\pi(p_i) = \rho p_i - \left(\overline{a}_i p_i^2 + \overline{b}_i p_i + \overline{c}_i\right) \tag{19}$$

ρ refers to the electricity price at this moment. At this time, the abovementioned complete information game can be solved through Nash equilibrium [39]. From the equilibrium conditions of the Cournot model, there are the following equations.

$$\frac{\partial \pi(p_0)}{\partial p_0} = \rho - (2a_0 p_0 + b_0) = 0 \tag{20}$$

$$\frac{\partial \pi(p_i)}{\partial p_i} = \rho - (2\overline{a}_i p_i + \overline{b}_i) = 0 \tag{21}$$

The total output power p of all microgrids is determined according to the load prediction given by the supply–demand balance hypothesis.

$$p = p_0 + \sum_{i=1}^{N-1} p_i \tag{22}$$

According to Equations (20), (21), and (22), the optimal bidding power of microgrid 0 after estimating the situation of other power plants is obtained.

$$p_0 = \frac{p + \sum_{i=1}^{N-1} \frac{\overline{b}_i}{2\overline{a}_i} - \sum_{i=1}^{N-1} \frac{b_0}{2\overline{a}_i}}{1 + \sum_{i=1}^{N-1} \frac{a_0}{\overline{a}_i}} \tag{23}$$

The expected value of the 0 marginal cost price of the microgrid is calculated as follows by taking the derivative of the cost function.

$$\rho_0 = \rho = \frac{\partial C(p_0)}{\partial p_0} = 2a_0 p_0 + b_0 \tag{24}$$

MurmurHash is a high-performance and low-collision hash function that is suitable for use in large-scale data processing. Its computation speed is much faster than commonly used hash functions such as MD5 (Message-Digest Algorithm) and SHA (Secure Hash Algorithm)-1. MurmurHash also has a relatively uniform hash value distribution, reducing the occurrence of hash collisions. In the case of large data processing, the use of MurmurHash can improve system efficiency, reduce the occurrence of hash collisions, and thereby enhance system reliability. Moreover, due to MurmurHash's high computational efficiency, it can reduce the consumption of computing resources, and consequently lower system costs. Therefore, MurmurHash is selected as the hash function for this research.

In system design, it is important to consider using a buffer to store queued data for better data flow control. If data packets are lost, various methods can be used for recovery, for example, retransmission, in which if a data packet is lost, the sender can resend the packet. If the receiver does not receive the packet within a certain time, it can send a retransmission request to the sender. Upon receiving the request, the sender will resend the data packet. This approach is suitable for applications that do not require real-time performance. Error checking and retransmission involve attaching error checking codes to each data packet to ensure that it is not damaged during transmission. If the receiver detects errors in the data packet, it can request the sender to retransmit the packet. This approach is suitable for applications with high real-time performance requirements. Forward error correction involves adding redundant information to data packets, allowing the receiver to recover lost data packets in case of packet loss. This approach is suitable for situations with low packet loss rates. Fast retransmit is a method used in the transmission control protocol (TCP), where the receiver sends duplicate acknowledgement messages to inform the sender which data packets have been received. When the sender receives three identical ACK messages, it assumes that the packet has been lost and immediately retransmits it. This method allows for faster recovery of lost data packets and is suitable for situations with high packet loss rates.

3.3. Privacy and security analysis of the IoMT model based on the combination of BC and deep learning

Akter et al. (2022) applied BC technology in the IoMT to ensure authenticity and protect the data privacy of all entities (i.e. data owners and data analysts), and ultimately achieved excellent results [40]. According to the above analysis, the BC-based mobile distributed computing process is realized based on Ethereum, and the architectural design is shown in Fig. 5. In this architecture, the physical layer (data acquisition), deep learning layer, network transmission layer, and intelligent contract layer are successively from

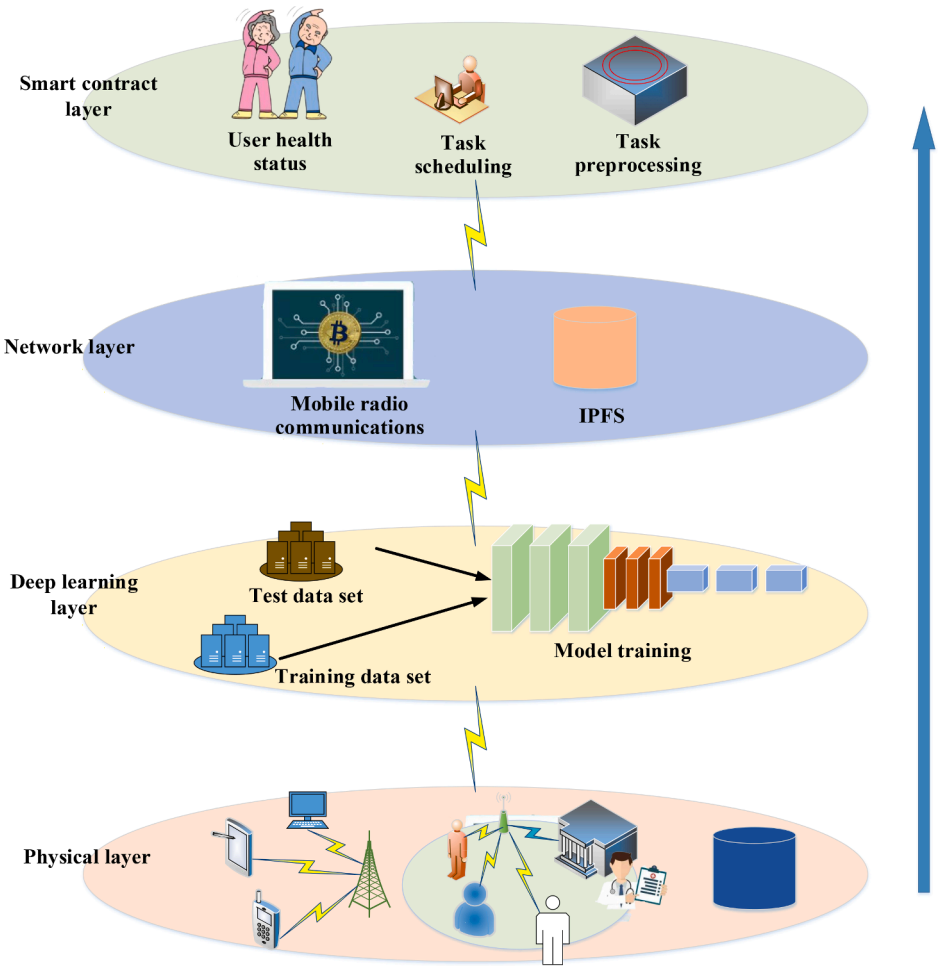

Fig. 5. Structure of the IoMT model based on the combination of BC and improved AlexNet.

the bottom up. Mobile devices, microgrids, base stations, BC data storage, and IPFS file storage services are at the lowest physical level. The BC data cache space is responsible for storing the metadata of the task, while the IPFS file storage service stores the complete data of the job. Above these layers is the deep learning layer, which utilizes AlexNet, a neural network with more layers and stronger learning ability, to analyze the collected data, including the training data set, test data set, and the neural network-improved AlexNet model training. The relevant data and parameters of deep learning are acquired through the data interface to train the model, which is then returned to the smart contract. The next layer above is the network transport layer, which mainly includes the BC network transport protocol and the IPFS peer-to-peer network transport protocol. BC's network transport protocol transmits mission metadata, and IPFS's transport protocol sends complete mission data. The top layer is the smart contract, which runs on the Ethereum virtual machine (EVM) [41]. It consists of three parts: user health monitoring, distributed training scheduling, and system preprocessing when starting tasks.

During the running of the Ethereum virtual machine, the first part monitors the health status of the user. It is responsible for receiving the physical health status and data of the user from the mobile terminal. The second part is the distributed training scheduling layer, which is responsible for coordinating the collaboration between participants, aggregating their models, and distributing new models. The third part is the preprocessing stage, which is initiated when the system receives a task. This stage is responsible for receiving and preprocessing the task request sent by the initiator, selecting the participants, and sending the task metadata to the participants. Finally, it returns the training results to the initiator. In summary, the model can generate certain intelligent computing means for the data calculation process by using deep learning technology to train the model and learning through deep learning technology, which provides a certain basis for the model to predict the user's condition and provide support for optimizing the designed medical system. Deep learning can not only accurately and quickly calculate input data results through forward computation but also calculate the specific errors of data processing through backpropagation, providing a basis for model optimization. Therefore, deep learning can effectively improve the efficiency and accuracy of the designed medical system, which is innovative research [42].

The AlexNet model is a kind of convolutional neural network (CNN). Data enhancement is conducted to solve the problem of

insufficient data in this model. Besides, the Relu6 activation function is used to enhance the stability of the model. Local Response Normalization (LRN) is used in the original AlexNet to normalize the first and second layers to enhance the generalization performance of the model. However, the LRN algorithm has limited practical improvement on the model while significantly increasing the training time of the model [43]. This work uses the batch normalization (BN) algorithm to reduce the data offset caused by the activation function and effectively solve the problem of uneven data distribution during the training process. The BN algorithm achieves feature normalization. In this work, the AlexNet model part uses the Adam optimizer, with 0.0002 as the initial learning rate; cross-entropy is selected as the loss function to avoid the problem of the gradual decrease in the learning rate caused by the mean square error. Since a large number of parameters are introduced in the fully connected layer of the AlexNet network, Dropout is added after the fully connected layer. This technology reduces the complex co-adaptation of neurons and makes the model effective for fusion. The improved AlexNet model mainly deals with image information in medical information.

In this model, users interact with each other in the BC network through peer-to-peer communication to complete resource allocation. The smart contract serves as the management module of the system and is responsible for collecting and monitoring users' physiological health status and other data in real-time. Once the smart contract receives the task, it performs operations such as locking tokens, selecting users, allocating resources, and sending back training results.

The time delay of service and energy consumption during data transmission are analyzed. In business service delay, task travel time, which is the time it takes for participants to discover and retrieve tasks, is calculated according to Equation (25).

$$t_{m,n}^{bt} = \frac{ds_m}{r_n(t)} + t_m^{aw} \tag{25}$$

$r_n(t)$ is the download transfer rate. The user training time, that is, the time used by participants to train the model, is calculated via Equation (25).

$$t_{m,n}^{dl} = \sigma_i \times c_{n,i} \times ds_m \tag{26}$$

σ_i is the number of CPU cycles required to execute the i-type unit-quantity tasks. The user return time, that is, the time it takes for the participant to return the model, is calculated as shown in Equation (27).

$$t_{m,n}^{re} = \frac{\lambda}{r_n^{'}(t)} \tag{27}$$

λ refers to the space occupied by the model parameters, and $r_n^{'}(t)$ refers to the upload transmission rate.

Furthermore, its energy consumption is calculated, mainly including the user opportunity cost and waiting time for allocation. User opportunity cost refers to the cost consumed by users to download, execute, and return tasks, calculated as follows.

$$em_{m,n} = P_k \frac{ds_m}{r_n(t)} + \kappa c_{n,t}^3 \times t_{m,n}^{bt} + p_n \frac{\lambda}{r_n^{'}(t)} \tag{28}$$

The waiting time for allocation refers to the difference between the time o_m when the task is released and the time T_a when the task is allocated, as shown in Equation (29).

$$t_m^{aw} = T_a - o_m \tag{29}$$

It is assumed that the amount of local interactive data that each device can provide is ds_n^{self} , and the comprehensive benefit of the matching pair is calculated as follows.

$$\begin{aligned} CI &= \alpha(Q_m \times pc_n) + \beta ds_n^{\text{self}} \\ &+ \frac{\gamma}{t_{m,n}^{bt\,'} + t_{m,n}^{dl\,'} + t_{m,n}^{re\,'}} - \rho em_{m,n}^{\ '} + \theta t_m^{aw} \end{aligned} \tag{30}$$

α, β,γ, ρ refer to the weight coefficients, and $t_{m,n}^{bt\,'}, t_{m,n}^{dl\,'}, t_{m,n}^{re\,'}, em_{m,n}^{\ '}$ are the values after normalization processing. The processing method is shown in Equation (31).

$$x_i^{'} = \frac{x_i - min(X)}{max(X) - min(X)}, x_i \in X \tag{31}$$

X refers to the set consisting of x_i, min(X) is the element with the smallest value in set x, and max(X) is the element with the most considerable value.

Furthermore, the neural network of the deep learning layer in the IoMT is analyzed to improve the training process of the AlexNet model. First, the t-th feature data $y_t^l(i,j)$ of the lth convolutional layer is sampled according to the overlapping pooling method.

$$\begin{aligned} a_t^l(i,j) = max\{&y_t^l(i,j), i_s \le i \le i_s + w_c - 1 \\ &j_s \le j \le j_s + w_c - 1\} \end{aligned} \tag{32}$$

s is the pooling movement step length, w_c refers to the width of the pooling area, and $w_c > s$.

After the first and second pooling layers of the AlexNet model, a local normalization layer is supplemented to standardize the

start
Input: Selection random number , Initialization policy parameter , mapping parameter , experience pool *D,* initialization target network parameter $\theta_{t\ \mathrm{arg}} \leftarrow \theta; \varphi_{\mathrm{targ}} \leftarrow \varphi$
Output: User health status
If $k \in [1, n-1]$ do
  Calculate point (x_1, y_1), as shown in equation (6)
  Calculate r, the formula is $r \leftarrow x_1 mod n$
  If r=0 do
    Calculate hash value $h(m) \leftarrow HASH(m)$
    Calculate S_v

$$S_v \leftarrow \left[(h(m) + SKv * r) * k^{-1}\right] mod n$$

  End if
End if
If Update network **then**
    Random and uniform sampling from experience pool D, size batch_ size

$$B = (s, a, r, s', d)$$

  Calculate target value y ‘

$$y' \leftarrow r + \gamma(1-d)\theta_{\mathrm{targ}}\left(s', \lambda_{\theta_{tz_g}}(s')\right)$$

  Update map network functions with gradient rise

$$\varphi \leftarrow \sum_{(s,a,r',d) \in B} \left(\phi_{\varphi}(s,a) - y'(r,s',d)\right)^2$$

  end if
Until convergence/maximum steps reached
end

Fig. 6. Model algorithm flow chart based on the combination of BC and improved AlexNet.

medical data, denoted as $c_t^l(i,j)$.

$$c_t^l(i,j) = a_t^l(i,j) \Big/ \left(k + \phi \sum_{max(0,t-m/2)}^{min(N-1,t+m/2)} \left(a_t^l(i,j)\right)^2 \right)^{\delta} \tag{33}$$

k, ϕ, δ, and m are all hyperparameters, which can be successively set to values of 2, 0.78, 10^4, and 7, and N is the total number of convolution kernels of the l-th convolutional layer. The ReLU function is used as the activation function to activate the convolution output $S_t^l(i,j)$ to prevent gradient dispersion in the network model [44].

$$y_t^l(i,j) = f\left(S_t^l(i,j)\right) = max\left\{0, S_t^l(i,j)\right\} \tag{34}$$

$f(\cdot)$ refers to the ReLU activation function. The parameter of the dropout operation is set to 0.5 to prevent overfitting in the fully connected layer. All the feature maps when l is 5 in Equation (32) are reconstructed into a high-dimensional single-layer neuron structure C^5; then, the input Z_i^6 of the i-th neuron in the sixth fully connected layer is calculated as follows.

$$Z_i^6 = W_i^6 C^5 + b_i^6 \tag{35}$$

W_i^6 and b_i^6 refer to the weight and bias of the i-th neuron in the 6th fully connected layer, respectively. In the process of improving the generalization ability, the neuron C^l of the 6th and 7th fully connected layers are discarded and output, $r_j^l \sim$ bernoulli $(dp), \widetilde{C}^l = r^l C^l$; then, the input Z_i^{l+1} of the i-th neuron of the 7th and 8th fully connected layers is $W_i^{l+1}\widetilde{C}^l + b_i^{l+1}$. The output C_i^l of the i-th neuron in the 6th and 7th fully connected layers is $f\left(Z_i^l\right)$, that is, $max\left\{0, Z_i^l\right\}$. Equation (36) indicates the input q^i of the first neuron of the 8th fully connected layer.

$$q^i = soft\max(Z\_i\Lambda 8) = e\Lambda(Z\_i\Lambda 8) / (\sum\_(j=1)\Lambda 12 e\Lambda(Z\_i\Lambda 8)) \tag{36}$$

Meanwhile, the cross-entropy loss function suitable for the classification task is taken as the error function of the model, which can be expressed as:

Table 2
Simulation tools.

		Edition
Software	Operating system	Linux 64bit
	Python	Python 3.6.1
	Simulation platform	MATLAB 2018b
	Development platform	PyCharm
Hardware	CPU	Intel core i7-7700@4. 2 GHz 8
	RAM	Kingston ddr4 2400 MHz 16G
	GPU	Nvidia GeForce 1060 8G
Parameters	Number of participants	5
	Number of subsections	[200, 400, 600, 800, 1000]
	Number of subchannels available	[0, 2, 3, 4, 5]
	Type	[0, 1, 2, 3]
	Size of the subsection	1 Mb
	Block return G	50
	Number of system nodes	500

$$\text{Loss} = \sum_{i=1}^{N} q_i \cdot \log(p_i) \tag{37}$$

$$p_i = \frac{\exp\left(\widetilde{y}_i\right)}{\sum_{i=1}^{K} \exp\left(\widetilde{y}_j\right)} \tag{38}$$

N denotes the number of categories; q_i signifies the true category distribution of the sample; $\widetilde{y}_i$ refers to the output result of the neural network; p_i stands for the classification result after the Softmax classifier. The input of the Softmax function is an $M-$dimensional real number vector, set as s, which can be written as Equation (39).

$$\xi(s)_i = \frac{e^{s_i}}{\sum_{m=1}^{M} e^{s_i}}, i = 1, 2, \cdots, M \tag{39}$$

In essence, the Softmax function can map an $M-$dimensional arbitrary real number vector to an $M-$dimensional vector whose values are all in the range of (0,1) to realize the normalization of the vector. To reduce the computational complexity of the model system, the output data volume is reduced to 2^8 through μ-companding conversion, that is, $\mu = 255$, thereby improving the prediction efficiency of the model. Equation (40) describes normalization.

$$f(s_t) = \text{sign}(s_t) \frac{\ln(1 + \mu|s_t|)}{\ln(1 + \mu)}, |s_t| < 1 \tag{40}$$

Model algorithm training includes the learning rate update strategy using the polynomial decay "poly" learning rate adjustment method [45].

$$\text{init} \setminus \_\text{lr} \times \left(1 - \frac{\text{epoch}}{\max \setminus \_\text{epoch}}\right)^{\text{power}} \tag{41}$$

The algorithm constructed in the IoMT model is shown in Fig. 6.

3.4. Case analysis

For the convolutional neural network model constructed in this work, it is designed for medical information classification and diagnosis. The model utilizes convolutional neural networks for image classification tasks. The key advantage of CNN is its ability to automatically learn features, making it highly suitable for processing high-dimensional data such as images. A standard CNN model consists of convolutional layers, pooling layers, and fully connected layers. The convolutional and pooling layers are primarily used for feature extraction, while the fully connected layers are used for classification. In the neural network configuration presented in this work, multiple convolutional and pooling layers are used for feature extraction, and the extracted features are connected to the fully connected layers, which ultimately output classification results using the softmax function.

The performance of the IoMT model based on BC and improved AlexNet is evaluated. The model is simulated in MATLAB, and the improved AlexNet neural network framework is implemented by TensorFlow 1.13.0. In the simulation experiment, an IoMT is designed by taking the medical data of each top-three hospital in Guizhou city as an example. The case analysis of the model ensures anonymity to ensure patient privacy, and the medical data of each hospital are encrypted so that the attacker can't assess patient privacy. The chain-task data generated in the entire IoMT are distributed into data sets, which are divided into training data sets and test data sets by 7:3, and the proportion of each type of data in the two data sets is kept consistent. The settings of the system hardware, software, and parameters are shown in Table 2.

Table 3
Computational costs of the models under different algorithms in a single terminal scenario.

Number of iterations	The algorithm reported here	AlexNet	DenseNet	IGCNet	VGGNet	CNN
0	0.12	0.15	0.20	0.26	0.33	0.48
5	0.13	0.13	0.19	0.27	0.32	0.48
10	0.11	0.14	0.19	0.26	0.34	0.46
15	0.11	0.14	0.21	0.27	0.32	0.45
20	0.13	0.15	0.20	0.26	0.33	0.46
25	0.11	0.15	0.20	0.27	0.32	0.47
30	0.13	0.14	0.21	0.26	0.31	0.47
35	0.12	0.14	0.20	0.27	0.33	0.46
40	0.12	0.15	0.20	0.28	0.31	0.46
45	0.11	0.13	0.21	0.27	0.32	0.48

Table 4
Computational cost of models under different algorithms in multi-terminal scenarios.

Number of iterations	The algorithm reported here	AlexNet	DenseNet	IGCNet	VGGNet	CNN
1	0.010	0.010	0.015	0.018	0.020	0.025
3	0.015	0.013	0.020	0.023	0.025	0.050
5	0.018	0.020	0.026	0.035	0.040	0.070
7	0.024	0.026	0.033	0.055	0.060	0.080
9	0.026	0.033	0.049	0.068	0.070	0.090
11	0.033	0.048	0.064	0.078	0.080	0.110
13	0.048	0.048	0.075	0.093	0.095	0.125
15	0.068	0.070	0.080	0.112	0.115	0.150
17	0.074	0.075	0.098	0.134	0.135	0.175
19	0.087	0.090	0.125	0.174	0.175	0.220

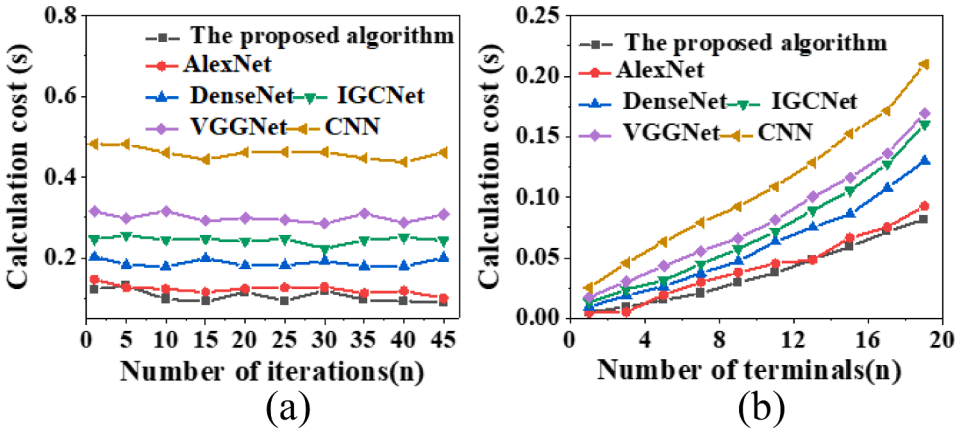

Fig. 7. Computational costs of models under different algorithms (a. Single-terminal scenario; b. Multi-terminal scenario).

First, the neural network of the improved AlexNet algorithm model is compared with AlexNet [46], DenseNet [47], Visual Geometry Group Network (VGGNet) [48], Interleaved Group Convolutions for Deep Neural Networks (IGCNet), and Convolutional Neural network (CNN) regarding the computation cost, data transmission delay, data security, and physiological health status prediction accuracy (Table 1). Secondly, the encryption properties of BC technology are comprehensively evaluated to determine the overall encryption status of the medical system after implementing BC technology. The application of BC technology is also assessed under different scenarios to provide a reference for the future formal application of BC technology in the medical system. Lastly, the encryption capabilities of BC technology are compared with other technologies to demonstrate its advantages and promote the comprehensive adoption and advancement of BC technology.

4. Results and discussion

4.1. Comparison of system performance of models under each algorithm

Table 3 and Table 4 summarizes the results of calculation cost, comprehensive income, and system operation efficiency.

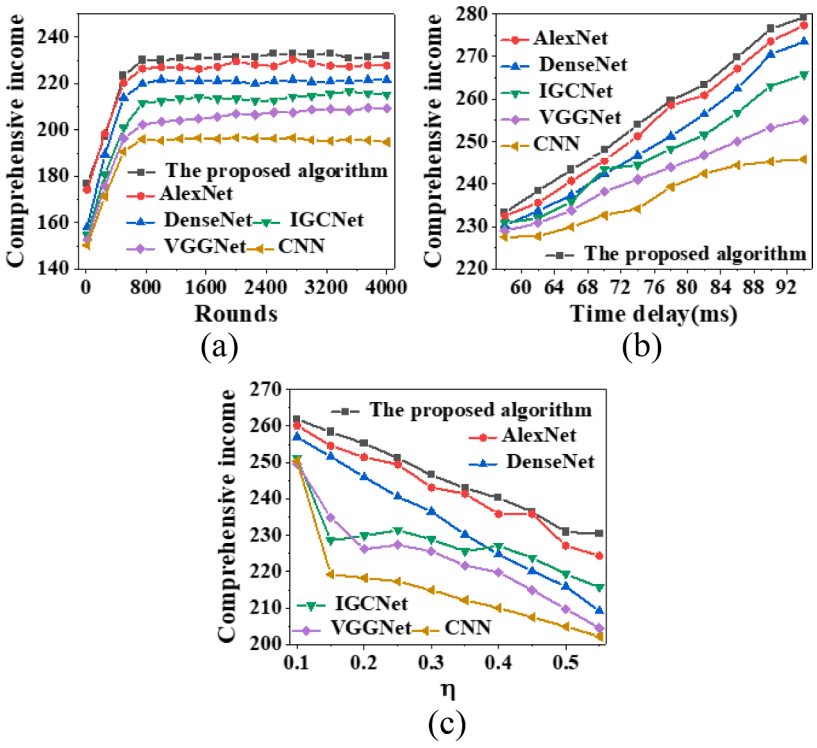

Fig. 8. Comparison curves of the comprehensive income of each algorithm under different indicators (a. different round numbers; b. different time delays; c. different energy consumption coefficients).

Fig. 7 illustrates the data in Table 3 and Table 4.

The computational overhead in Fig. 7a suggests that the computational overhead of each algorithm does not change significantly as the number of iterations increases in a single terminal scenario. The constructed algorithm has the lowest computational cost, which is stable at 0.13 s. In contrast, the computational cost of the other algorithms is significantly higher than that of the constructed algorithm. The analysis of the calculation cost of each algorithm in a multi-terminal scenario indicates that the calculation cost shows an increasing trend with the increase in the number of terminals. However, the calculation cost of the constructed model algorithm is dramatically lower than that of other algorithms. Therefore, the IoMT model based on BC and improved AlexNet has the optimal computational overhead, no matter for a single terminal or multiple terminals, which is conducive to the system's operation.

Fig. 8 and Fig. 9 are obtained in the same way.

Fig. 8 shows the comprehensive income of each algorithm under different indicators. According to the convergence shown in Fig. 8a, with the increase in rounds, all model algorithms show a trend of increasing first and then stabilizing, reaching the state of convergence. In addition, the framework reported here has a relatively higher equipment utilization rate, so the final convergence of the comprehensive profit value is higher. From the perspective of delay in Fig. 8b, the number of tasks to be completed increases with the increase in delay regardless of which framework is adopted, the throughput increases, and the comprehensive income of the system becomes greater. Additionally, the task slicing-based allocation framework proposed in this chapter utilizes the different computational efficiencies of various types of tasks. As a result, more tasks can be completed per unit of time, and the overall benefits are slightly superior to those of other algorithms. The analysis of different energy consumptions shown in Fig. 8c indicates that each algorithm shows a decreasing trend with increasing energy consumption. When spectrum resource allocation and user selection are not considered, the model exhibits an accelerated decline followed by a slow decline. The reason is that the random selection of users and the task-free fragmentation framework ignore the impact of task return and data volume on the combined gain when the energy consumption factor is excessively small.

The system operating efficiency of each algorithm under different numbers of system nodes is shown in Fig. 9. The analysis of block propagation time in Fig. 9a shows that the overall block propagation time increases with the increase in system node data. However, the block propagation time of the framework model is significantly shorter than that of other model algorithms, which means that the constructed framework can form consensus more quickly, and the system runs more efficiently. For the throughput analysis shown in Fig. 9b, the system throughput using the constructed framework mechanism is significantly superior to other model algorithms. As the number of nodes increases, the consensus throughput of the proposed framework mechanism does not decrease dramatically, indicating that the system's running efficiency is higher and the amount of data that can be processed simultaneously is larger. The analysis of transmission throughput shown in Fig. 9c suggests that all advanced neural networks have almost the same transmission throughput, close to 1, and the algorithm constructed is closest to 1 (1 packet per frame per household). As the number of system nodes

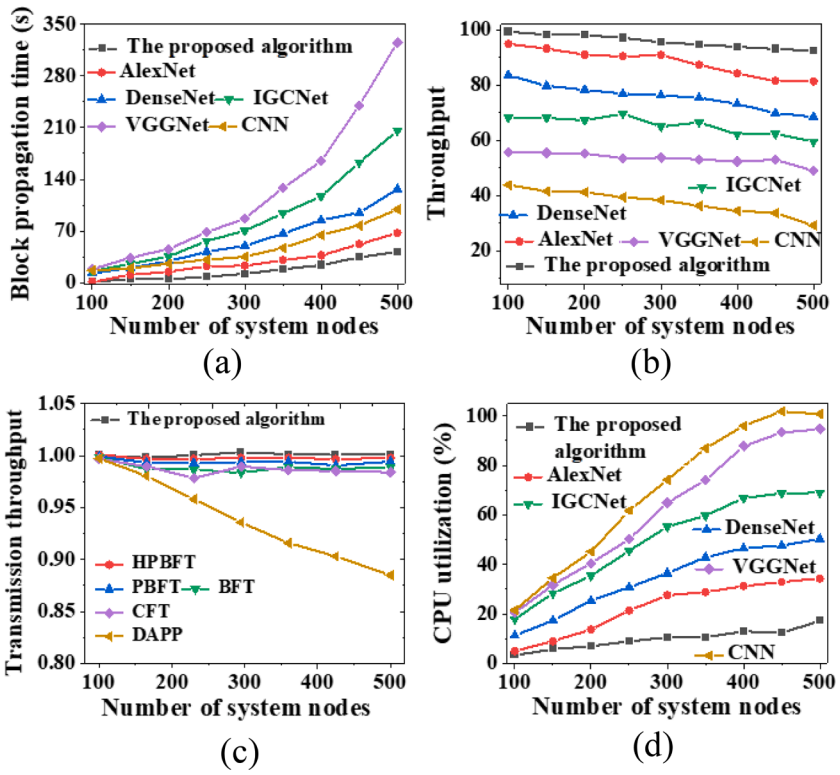

Fig. 9. System operating efficiency comparison curve of each algorithm under different numbers of system nodes (a. block propagation time; b. consensus throughput; c. sending throughput; d. CPU occupancy rate).

increases, the throughput of the CNN decreases. This directly causes some end users to fail to obtain time slots, which can't meet the stringent requirements of security adoptions. The CPU usage analysis shown in Fig. 9d suggests that the CPU usage of the main control board of other algorithms reaches 100% when the number of system nodes increases, which means that the terminal will crash and can't work normally. However, the CPU usage of the main control board by using the framework consensus mechanism is always below 17.62% and does not increase significantly with the increase in the number of nodes. This is because the trusted chips mainly perform the computing functions in this consensus mechanism, and the CPU usage of the main control board is negligible. Therefore, the IoMT framework reported here has superior operational efficiency.

4.2. Comparative analysis of data transmission security under various algorithms

The model algorithm is compared with AlexNet, DenseNet, VGGNet, IGCNet, and CNN from different data volumes to verify the data transmission security and privacy protection performance of the constructed algorithm, as presented in Fig. 10. The prediction accuracy of each algorithm is analyzed in Fig. 11.

Fig. 10 compares various model algorithms' data security transmission performance under different data volumes. With the increase in data, the average delivery rate of network data shows an upward trend. The delivery rate of constructed health monitoring user data messages is no less than 80% (Fig. 10a). The average leakage rate of network data changes slightly, and the leakage rate of health monitoring user data messages does not exceed 10% (Fig. 10b). In addition, the average delay decreases with the increase in the number of autonomous vehicles. The average delay of health monitoring user data transmission of the model algorithm basically stabilizes at approximately 350 ms (Fig. 10c). Therefore, from the perspective of the data volume of different health monitoring users, the constructed model algorithm shows a higher average delivery rate and the lowest average leakage rate compared to the others. Moreover, it has low latency and robust network data security transmission and privacy protection performance.

The comparison results of the ROC and AUC of each model algorithm are shown in Fig. 11. According to the ROC of each algorithm in Fig. 11a, the area under the ROC curve of the constructed algorithm is the largest, which is 0.9217. The ROC values of AlexNet, DenseNet, VGGNet, IGCNet, and CNN are 0.9115, 0.8806, 0.8951, 0.8514, and 0.807, respectively. According to the ROC, the combination of BC and the improved AlexNet algorithm has a higher classification probability than the others. From Fig. 11b, the convergence rate of the constructed algorithm is obviously faster compared with the convergence speed of various algorithms in the training process, reaching the convergence state when the number of iterations is approximately 20. The convergence rate of the other algorithms is slower, and the order is AlexNet > DenseNet > IGCNet > VGGNet > CNN. Therefore, the constructed IoMT model based on the combination of BC and improved AlexNet has the highest probability of prediction accuracy and the fastest training

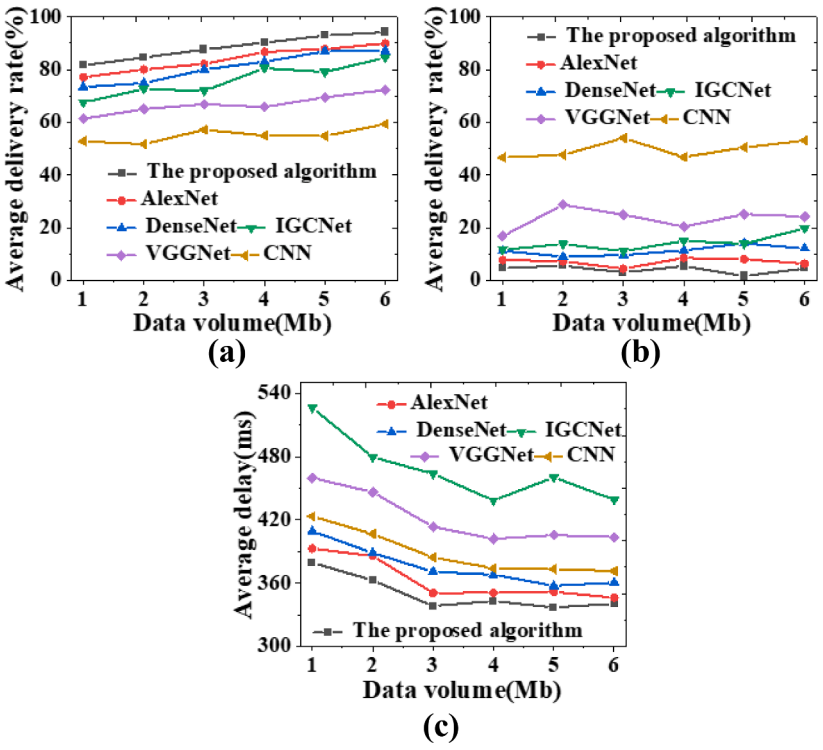

Fig. 10. Curves of network data security transmission of each mechanism algorithm under different health monitoring user data volumes (a. average delivery rate; b. average leakage rate; c. average delay).

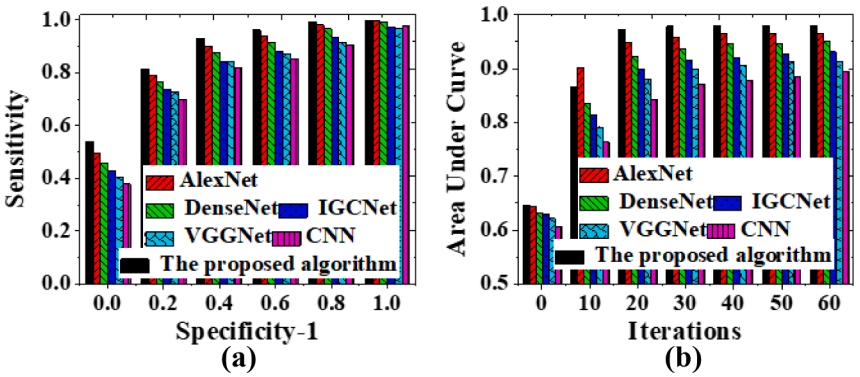

Fig. 11. ROC and AUC change curves under different algorithms (a. ROC; b. AUC).

Table 5
The summarized results of Fig. 7 and Fig. 11.

Image catagory	Results
Fig. 7	Regardless of whether it is a single terminal or multiple terminals, the IoMT model based on BC and the improved AlexNet has the best computational cost, which is beneficial for the system operation.
Fig. 8	The task slicing-based allocation framework proposed in this chapter further utilizes the different computational efficiency of different types of tasks, which completes more tasks per unit time and has slightly better overall benefits than other algorithms.
Fig. 9	The algorithm proposed in this work performs well in block propagation time, consensus throughput, send throughput, and CPU utilization rate.
Fig. 10	From the perspective of the data volume of different health monitoring users, the model algorithm constructed in this work has higher average delivery rate and the lowest average leakage rate than other algorithms.
Fig. 11	The IoMT model constructed by combining BC and improved AlexNet has the highest probability prediction accuracy and the fastest training convergence speed.

convergence speed.

The results of Fig. 7 and Fig. 11 are summarized in Table 5.

5. Conclusions

The medical services should draw more and more attentions from the whole society. This study aims to establish a model for medical information storage and prediction. BC technology is used to apply to the IoT and research is conducted on data storage in the medical field from the perspective of sage storage and transmission of medical information. Deep learning is used to accurately predict and analyze user health data characteristics in IoT and an IoT model is built based on BC technology and improved AlexNet. The model achieves excellent performance in safe medical information storage and data prediction. It is worth noting that this model can provide an experimental basis for intelligence and privacy security protection in the medical field. The practical significance lies in the fact that it can be applied to the medical system and improve the overall efficiency of the medical system in the future. However, there are some deficiencies in this study. First, there is still room for improving BC expansion and BC consensus speed. In the future, BC performance will be further studied. Second, this study only focuses on the privacy protection and security of data in IoT. The subsequent study should make more efforts to increase user anonymity through the research and adoption of zero-knowledge proof and secure multi-party computing. In addition, the encryption algorithm reported here was not compared with other research results and was not verified with sufficient data. Therefore, future research needs to explore BC expansion and BC consensus speed, compare the method with other encryption algorithms, and add more model data to enhance the integrated optimization of healthcare systems, improve the overall performance of healthcare systems, and strengthen healthcare services.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The authors are unable or have chosen not to specify which data has been used.

Acknowledgement

This work was supported by the Science and Technology Foundation of Guizhou Province (QKHJC[2020]1Y253, QKHJC-ZK[2022] YB024) and the Innovative exploration and academic emerging Foundation of Guizhou University of Finance and Economics (No. 2022XSXMB09).

References

[1] H. Estiri, Z.H. Strasser, J.G. Klann, P. Naseri, K.B. Wagholikar, S.N. Murphy, Predicting COVID-19 mortality with electronic medical records, NPJ Digital Med. 4 (1) (2021) 1–10.
[2] I. Keshta, A. Odeh, Security and privacy of electronic health records: Concerns and challenges, Egypt. Inf. J. 22 (2) (2021) 177–183.
[3] M.B. Maas, M. Kim, R.G. Malkani, S.M. Abbott, P.C. Zee, Obstructive sleep apnea and risk of COVID-19 infection, hospitalization and respiratory failure, Sleep Breath. 25 (2) (2021) 1155–1157.
[4] R. Wood, C. Sinnott, I. Goldfarb, M. Clapp, T. McElrath, S. Little, Preterm birth during the coronavirus disease 2019 (COVID-19) pandemic in a large hospital system in the United States, Obstet. Gynecol. 137 (3) (2021) 403.
[5] H. Luo, H. Yu, J. Luo, PRAFT and RPBFT: A class of blockchain consensus algorithm and their applications in electric vehicles charging scenarios for V2G networks, Internet of Things Cyber-Phys. Syst. 3 (2023) 61–70.
[6] Z. Qu, Z. Zhang, M. Zheng, A quantum blockchain-enabled framework for secure private electronic medical records in Internet of Medical Things, Inf. Sci. 612 (2022) 942–958.
[7] L. Ouyang, Y. Yuan, Y. Cao, F.Y. Wang, A novel framework of collaborative early warning for COVID-19 based on blockchain and smart contracts, Inf. Sci. 570 (2021) 124–143.
[8] Y. Wang, Z. Wang, M. Zhao, X. Han, H. Zhou, X. Wang, A.S.V. Koe, BSM-ether: Bribery selfish mining in blockchain-based healthcare systems, Inf. Sci. 601 (2022) 1–17.
[9] Y. Kazançoğlu, M. Sağnak, Ç. Lafcı, S. Luthra, A. Kumar, C. Taçoğlu, Big data-enabled solutions framework to overcoming the barriers to circular economy initiatives in healthcare sector, Int. J. Environ. Res. Public Health 18 (14) (2021) 7513.
[10] K. Wang, S. Xie, J. Rodrigues, Medical data security of wearable tele-rehabilitation under internet of things, Internet of Things Cyber-Phys. Syst. 2 (2022) 1–11.
[11] Q. Zhou, J. Pan, S. Deng, F. Xia, T. Kim, Triboelectric nanogenerator-based sensor systems for chemical or biological detection, Adv. Mater. 33 (35) (2021) 2008276.
[12] F.S. Al-Ismail, DC microgrid planning, operation, and control: a comprehensive review, IEEE Access 9 (2021) 36154–36172.
[13] L. Ismail, H. Materwala, A. Hennebelle, A scoping review of integrated blockchain-cloud (BcC) architecture for healthcare: applications, challenges and solutions, Sensors 21 (11) (2021) 3753.
[14] W. Chen, H. Wu, X. Chen, J. Chen, A Review of Research on Privacy Protection of Internet of Vehicles Based on Blockchain, J. Sens. Actuator Netw. 11 (4) (2022) 86.
[15] P. Suler, L. Palmer, S. Bilan, Internet of Things sensing networks, digitized mass production, and sustainable organizational performance in cyber-physical system-based smart factories, J. Self-Governance Manage. Econ. 9 (2) (2021) 42–51.
[16] L. Qiao, Z. Lv, A blockchain-based decentralized collaborative learning model for reliable energy digital twins, Internet of Things Cyber-Phys. Syst. 3 (2023) 45–51.
[17] M. Douiba, S. Benkirane, A. Guezzaz, M. Azrour, An improved anomaly detection model for IoT security using decision tree and gradient boosting, J. Supercomput. 79 (3) (2023) 3392–3411.

[18] H.D. Zubaydi, P. Varga, S. Molnár, Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review, Sensors 23 (2) (2023) 788.
[19] M. Woźniak, J. Siłka, M. Wieczorek, M. Alrashoud, Recurrent neural network model for IoT and networking malware threat detection, IEEE Trans. Ind. Inf. 17 (8) (2020) 5583–5594.
[20] M. Woźniak, A. Zielonka, A. Sikora, M.J. Piran, A. Alamri, 6G-enabled IoT home environment control using fuzzy rules, IEEE Internet Things J. 8 (7) (2020) 5442–5452.
[21] N. Kundu, G. Rani, V.S. Dhaka, K. Gupta, S.C. Nayak, S. Verma, et al., IoT and interpretable machine learning based framework for disease prediction in pearl millet, Sensors 21 (16) (2021) 5386.
[22] X. Liu, L. Song, S. Liu, Y. Zhang, A review of deep-learning-based medical image segmentation methods, Sustainability 13 (3) (2021) 1224.
[23] F. Piccialli, V. Di Somma, F. Giampaolo, S. Cuomo, G. Fortino, A survey on deep learning in medicine: Why, how and when? Information Fusion 66 (2021) 111–137.
[24] S. Budd, E.C. Robinson, B. Kainz, A survey on active learning and human-in-the-loop deep learning for medical image analysis, Med. Image Anal. 71 (2021), 102062.
[25] R. Cerchione, P. Centobelli, E. Riccio, S. Abbate, E. Oropallo, Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem, Technovation 120 (2023), 102480.
[26] S. Alam, M. Shuaib, S. Ahmad, D.N.K. Jayakody, A. Muthanna, S. Bharany, I.A. Elgendy, Blockchain-Based Solutions Supporting Reliable Healthcare for Fog Computing and Internet of Medical Things (IoMT) Integration, Sustainability 14 (22) (2022) 15312.
[27] M. Kumar, S. Verma, A. Kumar, M.F. Ijaz, D.B. Rawat, ANAF-IoMT: A Novel Architectural Framework for IoMT-Enabled Smart Healthcare System by Enhancing Security Based on RECC-VC, IEEE Trans. Ind. Inf. 18 (12) (2022) 8936–8943.
[28] R. Huang, X. Yang, P. Ajay, Consensus mechanism for software-defined blockchain in internet of things, Internet of Things Cyber-Phys. Syst. 3 (2023) 52–60.
[29] Q. Wang, J. Hu, Y. Wu, Y. Zhao, Output synchronization of wide-area heterogeneous multi-agent systems over intermittent clustered networks, Inf. Sci. 619 (2023) 263–275, https://doi.org/10.1016/j.ins.2022.11.035.
[30] K.K. Jena, S.K. Bhoi, D. Mohapatra, C. Mallick, K.S. Sahoo, A. Nayyar, A fuzzy rule based machine intelligence model for cherry red spot disease detection of human eyes in IoMT, Wirel. Netw (2022) 1–19.
[31] D. Połap, G. Srivastava, K. Yu, Agent architecture of an intelligent medical system based on federated learning and blockchain technology, J. Inf. Secur. Appl. 58 (2021), 102748.
[32] B. Li, X. Zhou, Z. Ning, X. Guan, K.C. Yiu, Dynamic event-triggered security control for networked control systems with cyber-attacks: A model predictive control approach, Inf. Sci. 612 (2022) 384–398, https://doi.org/10.1016/j.ins.2022.08.093.
[33] T.M. Ghazal, Positioning of UAV base stations using 5G and beyond networks for IOMT applications, Arab. J. Sci. Eng. 1 (2021).
[34] M.R. Khosravi, S. Samadi, BL-ALM: A blind scalable edge-guided reconstruction filter for smart environmental monitoring through green IoMT-UAV networks, IEEE Trans. Green Commun. Networking 5 (2) (2021) 727–736.
[35] Y. Yang, T. Lin, P. Liu, P. Zeng, S. Xiao, UCBIS: An improved consortium blockchain information system based on UBCCSP, Blockchain: Res. Appl. 3 (2) (2022), 100064.
[36] N.R. Mosteanu, A. Faccia, Fintech frontiers in quantum computing, fractals, and blockchain distributed ledger: Paradigm shifts and open innovation, J. Open Innov.: Technol. Market Complexity 7 (1) (2021) 19.
[37] Y. Sun, X. Li, F. Lv, B. Hu, Research on Logistics Information Blockchain Data Query Algorithm based on Searchable Encryption, IEEE Access (2021) 1.
[38] T. Sadad, A.R. Khan, A. Hussain, U. Tariq, S.M. Fati, S.A. Bahaj, A. Munir, Internet of medical things embedding deep learning with data augmentation for mammogram density classification, Microsc. Res. Tech. 84 (9) (2021) 2186–2194.
[39] V. Prasannakumari, S. Usha, R.S. Nisha, Aid of Blockchain Technology to Healthcare Systems and a BC Framework for Capsule Endoscopy Diagnosis, Ann. Roman. Soc. Cell Biol. (2021) 8064–8068.
[40] S. Akter, F. Reza, M. Ahmed, Convergence of Blockchain, k-medoids and homomorphic encryption for privacy preserving biomedical data classification, Internet of Things and Cyber-Phys. Syst. 2 (2022) 99–110.
[41] Z. Qu, Z. Zhang, B. Liu, P. Tiwari, X. Ning, K. Muhammad, Quantum detectable Byzantine agreement for distributed data trust management in blockchain, Inf. Sci. 637 (2023), 118909, https://doi.org/10.1016/j.ins.2023.03.134.
[42] A. Rehman, S. Abbas, M.A. Khan, T.M. Ghazal, K.M. Adnan, A. Mosavi, A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique, Comput. Biol. Med. 150 (2022), 106019.
[43] Kumar M, A., & Chakrapani, A. (2022). Classification of ECG signal using FFT based improved Alexnet classifier. Plos one, 17(9), e0274225.
[44] M.A. Almaiah, A. Ali, F. Hajjej, M.F. Pasha, M.A. Alohali, A Lightweight Hybrid Deep Learning Privacy Preserving Model for FC-Based Industrial Internet of Medical Things, Sensors 22 (6) (2022) 2112.
[45] A. Ali, M.F. Pasha, J. Ali, O.H. Fang, M. Masud, A.D. Jurcut, M.A. Alzain, Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography, Sensors 22 (2) (2022) 528.
[46] N. Muhammad Hussain, A.U. Rehman, M.T.B. Othman, J. Zafar, H. Zafar, H. Hamam, Accessing artificial intelligence for fetus health status using hybrid deep learning algorithm (AlexNet-SVM) on cardiotocographic data, Sensors 22 (14) (2022) 5103.
[47] Y. Perugachi-Diaz, J. Tomczak, S. Bhulai, Invertible densenets with concatenated lipswish, Adv. Neural Inf. Proces. Syst. 34 (2021) 17246–17257.
[48] J. Raja, P. Shanmugam, R. Pitchai, An automated early detection of glaucoma using support vector machine based visual geometry group 19 (vgg-19) convolutional neural network, Wirel. Pers. Commun. 118 (1) (2021) 523–534.