Journal of Database Management
Volume 34 • Issue 3

Overview of Internet of Medical Things Security Based on Blockchain Access Control

Yikai Liu, College of Science, North China University of Science and Technology, Tangshan, China & Hebei Key Laboratory of Data Science and Application, Tangshan, China & The Key Laboratory of Engineering Computing in Tangshan City, Tangshan, China

Fenglan Ju, Financial Department, North China University of Science and Technology, Tangshan, China

Qunwei Zhang, College of Science, North China University of Science and Technology, Tangshan, China & Hebei Key Laboratory of Data Science and Application, Tangshan, China & The Key Laboratory of Engineering Computing in Tangshan City, Tangshan, China

Meng Zhang, College of Science, North China University of Science and Technology, Tangshan, China & Hebei Key Laboratory of Data Science and Application, Tangshan, China & The Key Laboratory of Engineering Computing in Tangshan City, Tangshan, China

Zezhong Ma, College of Science, North China University of Science and Technology, Tangshan, China & Hebei Key Laboratory of Data Science and Application, Tangshan, China & The Key Laboratory of Engineering Computing in Tangshan City, Tangshan, China

Mingduo Li, State Key Laboratory of Process Automation in Mining and Metallurgy, Beijing, China & Beijing Key Laboratory of Process Automation in Mining and Metallurgy, Beijing, China

Aimin Yang, College of Science, North China University of Science and Technology, Tangshan, China & Hebei Key Laboratory of Data Science and Application, Tangshan, China & The Key Laboratory of Engineering Computing in Tangshan City, Tangshan, China*

Fengchun Liu, College of Science, North China University of Science and Technology, Tangshan, China & Hebei Key Laboratory of Data Science and Application, Tangshan, China & The Key Laboratory of Engineering Computing in Tangshan City, Tangshan, China

ABSTRACT

The Internet of Things provides convenience to health systems, especially for remote monitoring of patient physical indicators. While providing convenience, there may be more security vulnerabilities in protecting patient and doctor information and storing health data effectively. As an important research branch in the field of the Internet of Things, the Internet of Medical Things is important for the overall improvement of public health in terms of how to safely conduct technology development and application research and to effectively implement healthcare needs. Blockchain technology is decentralized and untrusted as well as prevents tampering with data and reduces the cost of trust. Its good performance has a strong developmental nature in the healthcare field. This paper analyses how to solve security problems through access control under the Internet of Medical Things, and optimizes three access control methods. The Internet of Medical Things accesses control approach that introduces blockchain technology enhances computational and storage capabilities and is a good solution to the problem of third-party trustworthiness. Even in the face of the rapid growth of end devices, blockchain technology can solve some of the problems arising from access control of massive devices through three directions: hierarchical management, compressed storage and performance optimization. Finally, it provides directions for future research on the security aspects of blockchain technology under the Internet of Medical Things.

KEYWORDS

Access Control, Blockchain, Computational Capabilities, Health Systems, Internet of Medical Things, Network Security, Remote Monitoring, Storage Capabilities

DOI: 10.4018/JDM.321545

*Corresponding Author

1. INTRODUCTION

In 2005, the International Telecommunication Union (ITU) officially proposed the concept of the Internet of Things (IoT) (Gupta & Quamara, 2020). The application technology of sensors and other IoT devices has been developing and maturing, and the Internet of Medical Things (IoMT) industry has been rapidly emerging. IoMT is the application of IoT technology in the medical field. The earliest European IoT research project group proposed a blueprint for the development of IoMT in the "Strategic Research Roadmap for the Internet of Things" in 2009. Through the Internet and other network methods, it will interconnect massive sensors and smart devices that can perceive the external environment so that they can be used to perform and support services such as physical therapy and health. It has become a new type of electronic medical technology that can be used to obtain information on patient physical function indicators through small wearable devices or implantable medical devices, providing a powerful safeguard for human health (Han et al., 2020). Generally, most medical device manufacturers believe that focusing on more safety measures will only increase production costs and will not lead to more market gains (Sun et al., 2019). Therefore, they do not implement enough after-sales update services, which has led to many devices having high-risk vulnerabilities, such as default pass and unencrypted plaintext transmission keys (McMahon et al., 2017). Access control technology can protect network security effectively, which protects data privacy by controlling the access rights of users (Fang, Yin, Guo, & Fang, 2017). Therefore, access control under IoMT has become one of the current research hotspots.

At present, the integrated application of blockchain and the IoT has been widely valued by the industry and has been developed and practiced to a certain extent (Yang et al., 2019). The EOS (enterprise operation system, a commercially distributed design blockchain operating system) in the blockchain 3.0 era can handle thousands of transactions per second and has a much wider range of application scenarios. The introduction of a programmable society with smart contracts makes it possible to solve access control problems through blockchain technology. Blockchain technology has become a hot frontier technology in the Internet field and plays an extraordinary role in the field of Internet innovation. Some unscrupulous elements have taken the opportunity to attack users by exploiting imperfect management mechanisms and security loopholes in blockchain technology, which makes blockchain technology face many security threats and challenges (Ferrag et al., 2018; Nicolas et al., 2020; Puthal et al., 2018).

To address the above security issues, it is of far-reaching significance to clarify the concept, current research status and development trend of IoMT to specify the development strategy and conduct extensive and in-depth management and medical research. There is a discussion in the literature on IoMT security, but there are few blockchain-based access control applications in IoMT-related areas. This paper focuses on the following research work: analyzing the existing traditional blockchain system and the three-layer architecture of IoT, and optimizing the three-layer access control method; effectively solving the third-party trustworthiness problem by using blockchain access control, and finally realizing the effective management of IoMT system.

The content of this paper is as follows: Part 2 and Part 3 provide a brief introduction to the IoMT system and blockchain technology. Part 4 describes three access control models under the IoMT. Part 5 introduces the IoMT access control model with the introduction of blockchain technology, which enhances the computational and storage capabilities and solves the problem of third-party trustworthiness very well. Part 6 concludes the text and provides an outlook on future technology development.

2. IOMT SYSTEM

IoMT refers to the intelligent and convenient connection of medical staff, patients, and various medical equipment and facilities through IoT and communication technologies, which can fully support various

tasks, such as automatic identification, positioning, collection, tracking, management and sharing of medical data, and to better complete the intelligence of medical treatment (Elsayeh et al., 2021).

2.1 Overview of the IoMT and its Current Status

The continuous improvement of the IoMT system has greatly reduced the work pressure on the medical staff, improved the speed of response to medical treatment, enhanced the accuracy and convenience of medical work, and comprehensively improved the quality of clinical care (Yang, Yang, Han et al, 2018).

With the development of digital medicine, telemedicine, mobile medicine and wearable devices, the application of IoMT has penetrated all aspects of life. Once massive medical data information is leaked, it will cause immeasurable losses (Ding et al., 2020). Before 2016, FBI American information security experts found that there were exploitable security holes in infinite embedded medical devices such as cardiac pacemakers and insulin pumps (Martinez, 2018). Earthquake net viruses (Langner, 2011) have caused large-scale damage to medical industrial facilities. In 2016, the Mirai botnet launched a DDoS attack on Dyn Corporation, an Internet domain name resolution service provider in the United States, resulting in the inaccessibility of hundreds of important websites, such as Twitter, Amazon and the Wall Street Journal, and the paralysis of major public services, social platforms and public network services in the United States (Wikipedia, n.d.). The security of IoMT should be given more attention.

2.2 Application of IoMT

With the continuous improvement of medical network infrastructure, IoMT also has the basic characteristics of comprehensive perception, reliable transmission and intelligent processing of the IoT. As a low-power network with limited resources, it has been widely used in medical and health life scenarios, effectively improving people's medical levels (Ni et al., 2019). A forecast by market research firm IDC reports that more than 50 billion terminals and related devices will be connected to the Internet worldwide in 2020 (Novo, 2018). The introduction of electronic devices with radio frequency identification (RFID) sensors, which, based on their ability to capture the real-time status of patients, medical parameters and information on the distribution of medicines, will make it possible to set up a better system for monitoring and predicting diseases. Advances in sensor-related technologies have enabled the widespread use of inexpensive devices with built-in network communication and remote monitoring, allowing for higher levels of measurement and monitoring of human vital signs. Edible or degradable electronic chips are increasingly being used in internal organs of the human body, and in the future, the IoT will help and guide patients through various treatments (Chu, 2018). The application of the IoMT is shown in Figure 1.

2.3 A Three-Tier Architecture for the IoMT

IoMT differs from other IoT applications in that it is characterized by the refinement of the data collected, the diversity of the various devices and the complexity of the applications implemented. There are also a large number of heterogeneous interfaces, heterogeneous data and heterogeneous protocol communication conversions in the system. The IoMT has a huge structure and many requirements, which determines that it is a system with higher technical content requirements, maturity requirements and stability requirements among various IoT applications. With the existing IoT technology base and medical system, the logical architecture of IoMT can be divided into three levels from top to bottom: perception layer, transmission layer and application layer (Sun et al., 2018), as shown in Figure 2.

The perception layer captures medical data from smart medical devices and aims to fully sense and collect patient information. The transport layer transmits the data from the perception layer to the application layer after processing it through network communication (mobile, wired, and wireless networks). The application layer aggregates and processes data from the cloud, integrates medical

Figure 1. IoMT application

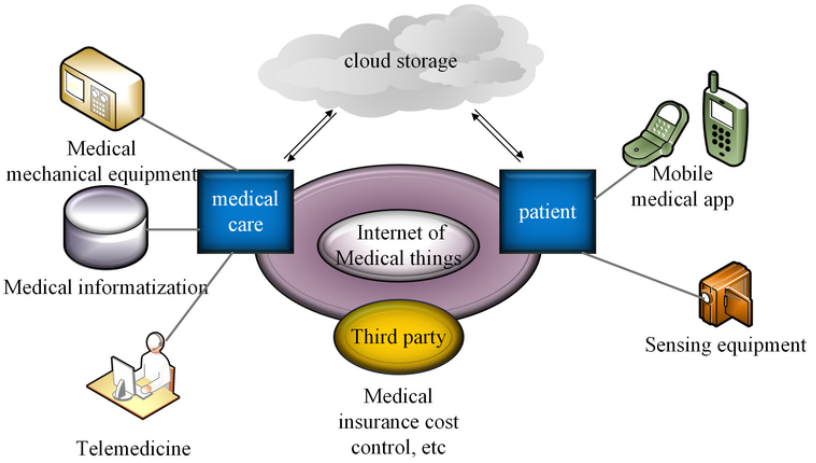
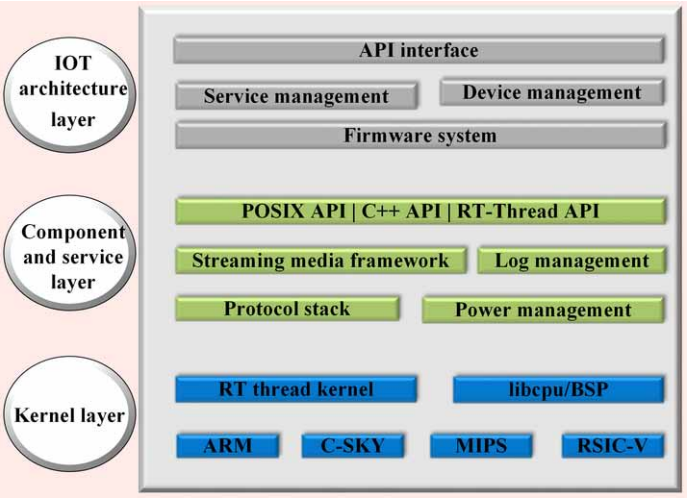


Figure 2. IoMT infrastructure



information resources and provides corresponding medical services to meet the needs of end users according to the reality and service requirements of the target users. The physical security of a perception layer device can be affected by real factors, its system security can be limited by resources, and it has to provide the basis for secure transport layer communication when using transport layer protocols for communication. Therefore, the security issues of the three aspects of the perception layer complement each other, and no one aspect should be neglected. The transport layer is primarily in charge of delivering the information collected by the perception layer, and the intermediate sensors are so distributed that they cannot ensure the privacy and security of each node. Network communication protocols will also grow as they develop. When data are passed between networks, it will involve authentication, key negotiation (Yang, Li, Kong et al, 2018), data confidentiality and integrity protection, and many other issues, and will also face more prominent security issues (Nguyen et al., 2016; Zhang et al., 2014). The process of processing and applying the medical data collected at the application layer requires security measures to protect it. With the increase in medical sensing

devices, the scale of DDoS attacks has increased significantly. Cloud-based servers also need to be upgraded to withstand DDoS attacks (Altmeier et al., 2015).

This paper cites (Zhang et al., 2017) as a listing and supplements the topics discussed in 363 papers from the first half of 2012-2021 in the field of IoT security from the Chinese Computer Society, as shown in Table 1.

3. BLOCKCHAIN TECHNOLOGY

Blockchain technology has its roots in Satoshi Nakamoto's 2008 paper "Bitcoin: A Peer-to-Peer Electronic Cash System" (Srinivas & Das, 2020). From an application perspective, it is a distributed shared ledger and database that is decentralized, tamper-proof, open and transparent (Zheng, Xie, Dai, Chen, & Wang, 2017)

3.1 Overview of Blockchain Development

Crypto-digital currencies, led by Bitcoin, ushered in the era of blockchain. With continuous development, the blockchain 2.0 era, represented by Ether, offers programmable scripts to users. However, due to latency and data throughput, Ether can only process a limited number of transactions per second and smart contracts can be deployed less efficiently. The 3.0 Fast Programmable Society of Blockchain (Merkle, 1987) realizes the performance expansion of distributed applications. EOS solves the problems of latency and data throughput through parallel chains and Delegated Proof of Stake (DPOS). EOS can even process thousands of transactions per second (Liu et al., 2019).

3.2 The Structural Hierarchy of the Blockchain

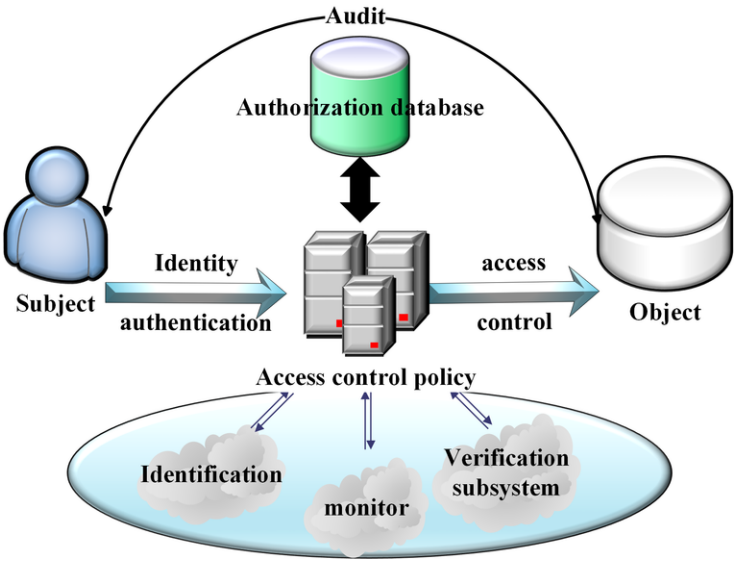
The current blockchain network is simply divided into a four-layer structure of a storage layer, network layer, extension layer and application layer (Wang, Wang, Cao et al, 2018), which are independent and interconnected with each other, as shown in Figure 3.

The storage layer is mainly used to store medical information and data, and is connected in a chain-like structure. The network layer mainly consists of a communication network between blockchain nodes, cryptography and a decentralized consensus mechanism. Both the private key and the encryption algorithm in its encryption mechanism can have security risks: a network hacker can use the publicly available parameters to replicate the user's private key (Mayer, 2016) and steal the user's signature secret key (Schmidt & Medwed, 2009). If two users in an ECDSA attack use the same random number of signatures, they are able to compute each other's private keys (Courtois et

Table 1. Ops of discussion for papers in the field of network security at CCS 2012-2021

Direction of discussion	The security issues faced
Sensing (120 papers)	1. Lightweight Cryptography Algorithm 2. Embedded System Defense Technology 3. Side Channel Attack and Defense 4. Cryptographic Algorithm Based on Biometrics and Device Physical Characteristics
Transport (141 papers)	1. Sensor Network 2. Privacy Data Protection in Communication Protocols 3. Secure Communication Protocol Against Remote Attacks (Middleman, Replay, DOS, etc.)
Application (102 papers)	1. Privacy Data Protection in Application 2. Equipment and Application Testing Framework in the Internet of Things 3. Intrusion and Defense Detection System

Figure 3. Blockchain network hierarchy



al., 2014). A password can be obtained by colliding a rainbow table with a hash function (Horalek et al., 2017), and a hash length extension attack can crack the hash function (Coron et al., 2005). There can be vulnerabilities in its consensus mechanism, such as blockchain network transaction latency and excessive consumption of arithmetic power. In terms of network communication, attackers may maliciously cause delay or isolation of the network to attack the blockchain system, mainly eclipse attacks (Heilman et al., 2015), scalable metric totals (Gervais et al., 2015), BGP hijacking attacks (Apostolaki et al., 2017) and balance attacks (Natoli & Gramoli, 2017). As shown in Table 2.

The extension layer is an extended implementation of blockchain technology based on "smart contracts" (decentralized shared code deployed on a blockchain system) (Wang, Yuan, Wang et al, 2018). Smart contracts may have transaction order dependency vulnerabilities, timestamp dependency vulnerabilities, handling exception vulnerabilities, and reentrant flaw vulnerabilities (Luu, Chu, Olickel et al, 2016), and smart contracts may consume significant fees or reduce block synchronization rates by exploiting gas vulnerabilities during operational deployment. The application layer is deployed based on various practical application scenarios, where users can interact with the blockchain system through applications. The user's privacy may be compromised when interacting with the blockchain system. Approximately half of the user information can be approximated by clustering analysis of the transaction behavior (Androulaki et al., 2013). It is also possible to use a single node to forge multiple identities, thus attacking the system and breaking the redundancy mechanism of the system (witch attack) (Douceur, 2002) to break the anonymity protocol, resulting in the compromise of user identities

Table 2. Network communication security issues

Attack type	Characteristic
Eclipse attack	Cut off and isolate the links between users and other nodes in the system
Scalable metric attack	Delay the transmission of transaction information
BGP hijacking attack	Delay network information transmission or block synchronization speed
Balanced attack	Disturb the communication between subgroups with the same computing power

(Bissias et al., 2014). In the course of a transaction, a trespasser is able to combine external sources of information with techniques such as information flow analysis to analyze data and information related to the account, ultimately stealing the user's transaction privacy (Fleder et al., 2015).

3.3 Application of Blockchain Technology in IoMT

Traditional storage strategies for healthcare data have resulted in large volumes of healthcare data being accumulated in the center of hospital information or regional data centers. The load carried by the center will therefore increase dramatically with the increase in data. Blockchain, as a new decentralized protocol, can be applied in IoMT to solve such problems. The distributed data storage approach enables secure storage of transaction information or other data, and information that is stored in the blockchain cannot be falsified or altered (Mattila, 2016).

In terms of recording and storing medical information, the centralized nature ensures that medical data are all on the same tier, which does not lead to global destruction due to node corruption and reduces storage costs. A hash function creates a mapping pointer to link the blocks into a line, ensuring that the patient's treatment record cannot be tampered with. In the field of medical insurance and electronic policy management applications, blockchain technology will fragment the file in terms of storage, and the 'hash value' must be obtained through the file uploader before the information can be restored, guaranteeing the rigor of medical compensation and the level of trust between the insurance company and the policyholder, and allowing comparison and reference of the policyholder's information to prevent duplication. It is also possible to compare the information of the insured to prevent duplication and reduce the incidence of fraud. In the field of pharmaceutical applications, blockchain technology adds credibility to the fact that information data such as drug products cannot be tampered with. Drug information can be checked against national standards in real-time, ensuring transparency and openness. Blockchain technology can transmit front-end businesses to back-end businesses via encryption, bypassing third parties and reducing the chances of commercial and medical secrets being stolen.

4. ACCESS CONTROL TECHNOLOGY

Access control is a strategy that defines or predefines a user's identity to prevent unauthorized users from accessing resources (Ourad et al., 2018).

4.1 The Need to Apply Access Control

With the proliferation of medical devices and end nodes, IoMT systems present new opportunities and unknown challenges. Because IoT devices are easy to build and widely distributed, it makes it very difficult to enforce strict security management for each node. Medical sensing devices require access to the internet for data transmission and are constantly exposed to various types of attacks from other malicious nodes. IoMT devices often contain a large amount of patient privacy and sensitive data, and malicious theft by others would cause immeasurable damage to the user, placing a higher

Table 3. Application of blockchain technology in health care

Related fields	Application advantages
Medical information	Reduce storage costs; Records cannot be tampered with; Increase transparency
Electronic policy management	The rigor of medical compensation Can make an accurate claim settlement plan
Medical field	Increased data reliability; Carry out big data information mining; Reduce the possibility of stealing trade secrets

demand on the protection of information and data. Therefore, the study of access control mechanisms in IoMT has become an important part of IoT information security (Lin et al., 2018).

4.2 Principle of Access Control

Access control in IoMT systems authenticates the control and legality of user access and use of medical resources, checks whether the user has the relevant authorization, controls access to specific resources and prevents unauthorized users from operating medical resources in breach of the law. Monitors medical resource access records by specifying user access rights and rules, and opens and revokes resource access rights to secure relevant medical information data (Fang, Yin, Guo, & Fang, 2017). The purpose of access control is to verify the legitimacy of user requests and operations for resources. The management of user access control enhances the security of system resources. This is shown in Figure 4. Access control, as an important means of information security and excellent control of security mechanisms, is widely used in several areas, such as firewalls, file systems, VPNs and infrastructure security in related medical fields.

Most IoT operating systems are software platforms based on RTOS and Linux operating systems, loaded with adapted file systems, UI libraries and other middleware, with multiuser and multitasking features (Kazmi et al., 2018). Figure 5 shows the hierarchy of the IoT operating system for RT threads, which are closely related to each other. Because a multiuser and multitasking system environment (Woo et al., 2018) provides multiple ways for unauthorized users to illegally request access to system resources, it is necessary to implement reasonable and efficient security measures for computer operating systems and middleware and their network services. This is to prevent the use of system resources by illegal users and the unreasonable use of the system by legitimate users. Therefore, the use of an access control system can handle the above problems efficiently.

The access control service includes two parts: the access control model, and the policy language. Access control consists of 3 basic elements: access policy rules, access subjects and access objects:

1. **Access principal:** The access to the target node information in the information system is initiated by the accessing user, who follows the rules of the accessed information node and can access the data of the information node within the scope of the authorization. The access user or the program developed by the user is usually the access subject.

Figure 4. Access control principle

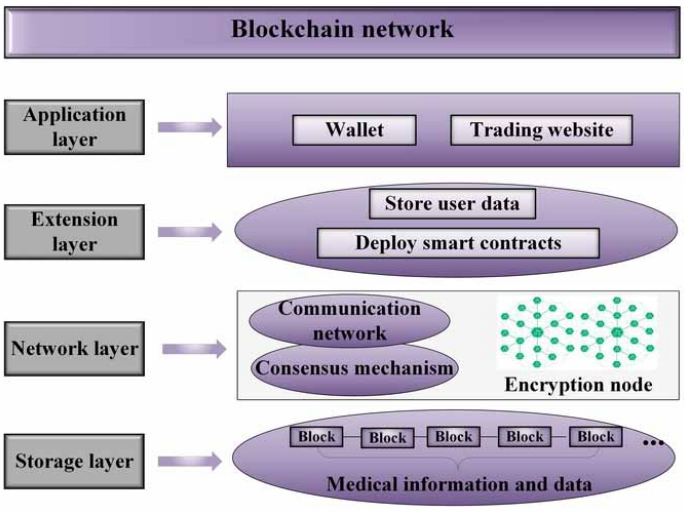
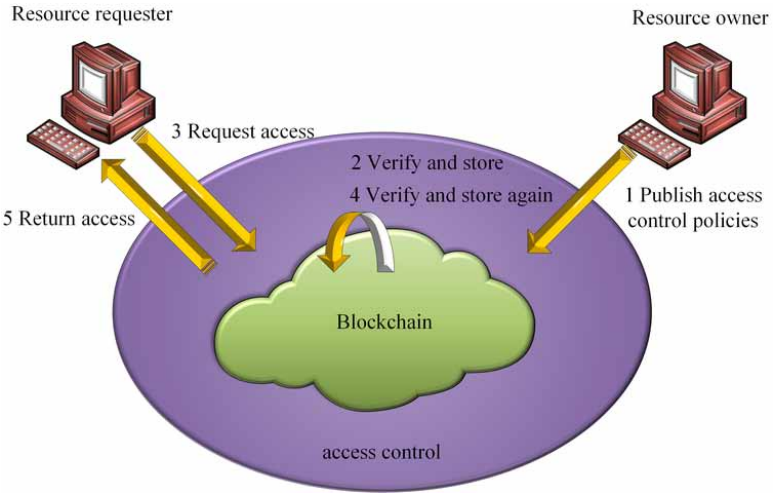


Figure 5. RT thread IoT operating system architecture



2. **Access object:** The access object, as an information carrier, is not restricted by the operating system and can be a database, file, directory, storage page, etc., or a bit, byte, or field. The access subject can sometimes also be accessed as an object. In an information system, the access object can be manipulated by the accessing subject for access actions.
3. **Security Access Policy:** This is a policy rule for securing data information of IoMT sensor devices, specifying whether the subject can access the object and what methods can be used to access the object.

As IoT-related technologies are rapidly developing, from the early days of connecting all items to the network through radio frequency identification and other information sensing devices to achieve intelligent management, to the "Internet of Things era" in which everything is connected (Luo & Yan, 2013). The access control methods for IoMT are also evolving iteratively, proposing role-based access control (RBAC), attribute-based access control (ABAC), usage control model (UCON) (Beltran & Skarmeta, 2018), etc.

RBAC is a role-based access control model that was proposed to solve the problem of access control in commercial-grade healthcare systems and was evaluated to select the access control technology that works better in practice (Alturi & Ferraiolo, 2011). In the RABC model, the link between the access subject and the access object occurs indirectly, with the addition of roles separating users and permissions. First, assign the permission to access the object to the designated role, and then the corresponding access subject obtains the corresponding role. The access subject also obtains the object access permission of the corresponding role, and indirectly obtains the authorization of the access object. The levels of users, roles, and objects are clear. This access authority management method simplifies the authority management of access objects and is easy to maintain (Moyer & Abamad, 2001). RABC does not support sequential operation access control mechanisms, so RABC access control is not suitable for IoMT systems with strict operational requirements.

ABAC is an attribute-based access control model and a convenient access control management model (Yuan & Tong, 2005). Compared with RABC, RABC needs to manage and maintain a large number of roles and authority relationships, while ABAC is more flexible and sorts out an independent and complete set of attributes according to the analysis of the subject and object characteristics (Zarezadeh et al., 2020). For the medical Internet of Things system managed by ABAC, when adding system resources, only less information needs to be updated to complete the synchronous update of the system. It is more scalable and more convenient to use.

UCON is an access control model based on usage control, it is mainly used to preserve medical data resources. In this way, all data resources, system resources, and network resources can be reasonably accessed and used by legitimate users, and it can also protect the digital resources of the client (Zhaofeng et al., 2019). UCON model introduces two new features "continuity" and "variability". Continuity means that access control monitors the process of accessing the subject and accessing object resources, and variability means that the attributes of the accessing subject are changeable during the process of obtaining authorization to access the object resources (Guoping & Wentao, 2012).

5. BLOCKCHAIN ACCESS CONTROL UNDER THE IOMT

IoMT terminal node equipment is generally composed of medical-related sensors, micro control units, communication interfaces and actuators, such as common cameras, smart watches, various medical monitoring instruments, etc. (Jain et al., 2021). These devices have certain independent computing and storage capabilities, which are limited by the functional positioning of the medical sensor devices themselves and cannot well support access control between devices. Common access control uses a centralized central decision-making method, which places a large amount of calculation and information storage in the central device for execution, and blockchain technology can provide the central device with the support of security technology (Liu et al., 2020). It has emerged as a technical solution to the data risks and associated privacy and security challenges posed by the centralized model. The access control model in the IoMT system relies on central authority decision-making, and performs access control management based on authorization rules and access subject attribute information. One of the applications of blockchain technology in the IoMT system is to replace the system-centric authority decision-making method.

5.1 Introducing the Access Control Method of Blockchain Technology

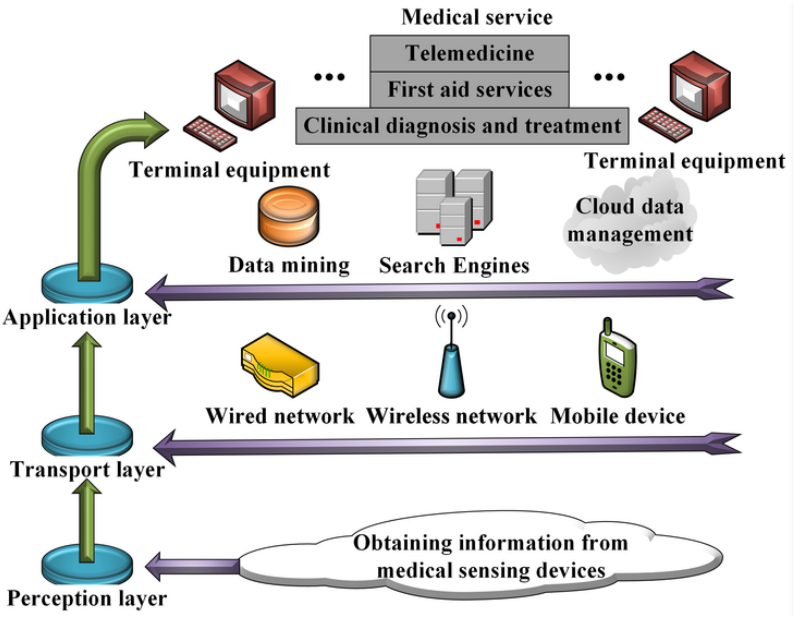
Blockchain technology has high requirements on the computing power and bandwidth of the nodes, and the exchange of information stored by the verification nodes leads to large network delays. These problems due to technical characteristics do not apply to the real-time requirements of some medical equipment, so blockchain technology cannot be directly used in IoMT systems (Watanabe et al., 2016). However, some other features of the blockchain are well suited to solve the security concerns of IoMT systems:

1. **Decentralization:** Without the control of a central trusted entity, all nodes on the chain participate together to ensure the scalability and maintainability of the model, reduce network delays and avoid single points of failure.
2. **Anonymity:** Blockchain has the characteristics of anonymity (Zheng, Xie, Dai, Chen, & Wang, 2017), and the anonymity of blockchain is applied in the IoMT system, which can realize the protection of the identity information and private data of medical and patient users.
3. **Security:** Blockchain technology can realize the construction of a secure network for information storage and verification between nodes that are uncertain whether they are trustworthy or not, which is suitable for the IoT, a generalized network built on the Internet. There are a large number of nodes in the IoT system, which requires the transmission of massive amounts of data information and the introduction of blockchain technology to ensure that the information is not tampered with (Alansari, Paci, & Sassone, 2017) the ensure the correctness of the data.

The execution process of the decentralized blockchain access control model is shown in Figure 6.

The access control models of RABC (Wu et al., 2014), ABAC and UCON (Park & Sandhu, 2002) under the traditional IoMT system all manage access control through centralized authority decision-making. Since the computing and storage capabilities of most IoT device nodes are insufficient to

Figure 6. Decentralized blockchain access control model



support access control management, the execution process of access control is mainly through third-party platforms or server devices other than IoT devices. Blockchain technology is introduced into the IoMT system, and the relevant policy rules for the access rights of the visiting subject to the object resources are stored on the nodes of the blockchain. Blockchain transactions or smart contracts (Liu et al., 2012) are used to manage access control permissions rules and policies. The resource access authority rules under the IoMT system are defined by creating transactions and published on the blockchain. Any user in the blockchain can view the node information on the chain at any time and obtain the operating authority of which system resource the current visitor has. The scope covered by this method includes resource owners, access subjects that manage multiple device nodes, and access objects (system resources, which can also be access subjects). The resource owner is responsible for controlling the access rights of existing resources, and updating and storing them on the blockchain node, using the script operation of the blockchain for updating and execution.

5.2 Optimized Access Control Model

The RABC access control model is managed and maintained by storing the three elements of the user, role, and authority information on a third-party platform or central server (Yavari et al., 2017). When faced with a scenario where the number of nodes in an IoMT system increases sharply, the scalability of the RABC access control model itself may only apply to a few IoMT systems. Facing the rapid growth of medical sensor equipment nodes, the application of blockchain access control can hierarchically simplify management, reduce storage pressure by compressing data or saving data outside the chain, and enhance the functionality of the blockchain by improving its structure or optimizing the consensus algorithm.

The ABAC access control model uses the attribute set of the access subject and the access object to determine whether to assign the corresponding access authority (Ouechtati & Azzouna, 2017). The execution of the ABAC access control module requires a variety of mechanisms to cooperate. The calculation and storage requirements generated in this process are often not met in most medical equipment. Therefore, the ACBC-based access control model needs to use a third party to store and

manage the attribute set of the access subject and resources to realize the ABAC access control model under the IoMT system. Blockchain can act as a trusted entity for the access control model.

The UCON access control model comprehensively considers the access subject, access object and authority strategy and also considers the two new attributes of continuity and variability. The design features of the structure of the blockchain itself support dynamics.

Since the computing and storage capacity of medical devices is weak and insufficient to support the implementation of access control functions and vulnerable to malicious attacks by illegal users, access control models such as RABC, ABAC, and UCON that apply blockchain technology also use a centralized approach to solve the access control decision problem, and the security of the blockchain system itself and the integrity of the access control policy are also issues that require attention (Zhang et al., 2018).

The blockchain technology itself has the characteristics of anonymity, distribution, and nontempering (Alansari, Paci, Margheri et al, 2017), which can enable nodes on the blockchain to exchange the information stored on the verification node in an untrusted state, to achieve the effect of "integrity". Using the technical characteristics of the blockchain, a transparent and reliable third-party platform can be built to provide computing and storage services for devices in the IoMT system. At present, the application of blockchain technology has gradually changed from being a trusted database to save access control strategies to using blockchain smart contracts to achieve automated access control.

Lounis et al. (2016) proposed a cloud-based medical wireless sensor network architecture and developed an access control that supports complex and dynamic security policies. This access control relies on ciphertext policy attribute-based encryption (CP-ABE). Li et al. (2012) proposed a new patient-centric framework and a set of mechanisms for access control to data stored in semi-trusted servers. The use of attribute-based encryption (ABE) technology allows for the encryption of each patient's health record, and the use of multiauthority ABE allows for a high level of patient privacy to be protected.

6. SUMMARY AND FUTURE RESEARCH DIRECTIONS

This article introduces the basic concepts of the IoMT and its logical architecture. The logical architecture is divided into a perception layer (perception and external information), a transmission layer (transmission of node device information from the perception layer to the application layer through the network) and the application layer (calculation, processing, storage and other operations on the data transmitted by the transmission layer) (Ara et al., 2016). A brief description of the origin and development of the blockchain is made, and the common security problems of the storage layer, network layer, extension layer, and application layer of the blockchain are summarized (Wang, Han, & Beynon-Davies, 2018). Public and private key security issues at the storage layer, various common attacks at the network layer (eclipse attacks (Chen et al., 2020), scalable measurement attacks, BGP hijacking attacks (Awe et al., 2020), balance attacks, etc.). The extension layer relies on vulnerabilities in the representative transaction sequence of smart contracts (Rifi, Rachkidi, Agoulmine, & Taher, 2017), timestamp dependency vulnerabilities, processing exception vulnerabilities (Perez & Livshits, 2019), etc. The disclosure of user privacy and identity information at the application layer.

6.1 Summary

In summary, first, the content of the IoMT and blockchain is introduced. The three common access control models (RBAC, ABAC, UCON) under the IoMT system are analyzed, and the security risks, privacy issues and shortcomings in the scenario of massive IoT devices are analyzed. The three access control models all implement system resource access control through the decision-making method of a centralized third-party platform. Whether the third-party platform is credible has become one of the

core security issues. The introduction of blockchain technology has solved the problem of third-party credibility. Even in the face of the rapidly growing IoT terminal devices, blockchain technology can solve some of the problems in the access control of massive devices through the three directions of hierarchical management, compressed storage and performance optimization.

Blockchain technology can be anonymous, distributed, and tamper-proof. Because of its decentralized characteristics (Karumba et al., 2020), it is very suitable for solving the security problems of untrusted third parties in the access control model of the IoMT system (Di Francesco Maesa, Mori, & Ricci, 2017):

1. **Blockchain provides trusted storage:** The tamper-evident feature can be used to store access control policies; it can store the massive amount of data generated in the IoT, using blockchain as a trusted transaction database; it can directly store access rights to prevent malicious users from destroying data.
2. **Blockchain provides trusted computing:** By storing data under the chain and storing only the hash pointing to the data on the blockchain, the blockchain provides a trusted platform for access control with executable smart contracts.
3. **Blockchain provides trusted computing and storage:** Some researchers take full advantage of both the computational and storage capabilities of the blockchain to store important data in the blockchain while also using the computational power of the blockchain for access control decisions.

6.2 Future Research Directions

1. The blockchain can achieve honest calculation and storage for the access control of the IoMT system, and the information stored on the blockchain node will be disclosed to other users on the chain. It is not a good practice for resource owners that the permission rules of access control can be arbitrarily viewed by other users. The privacy protection method of blockchain nodes is also one of the future research directions and trends. Currently, Microsoft proposes the Confidential Consortium Blockchain to ensure the privacy of smart contract code, which uses Intel SGX and Windows virtual security model to create a trusted computing environment in which to prove the security of the code placed and to ensure that internal data is not visible to the outside world and cannot be tampered with (Saleh et al., 2020).
2. The development of IoMT systems is becoming increasingly complex. The RABC, ABAC, and UCON access control models are well adapted to simple application scenarios. In the complex real-world production environment, there are often access control requests between different network organizations (Cruz et al., 2018), and whether the blockchain can act as a trusted third party to resolve access control requests between different IoT networks is also a direction that needs attention. The same problem may also appear in different blockchains, and nodes on different chains may have access control requirements. At this time, there are comprehensive issues such as the processing of cross-chain requests, the conflict of access control strategies, and whether the smart contract (Ramachandran & Kantarcioglu, 2017) is adapted.
3. How to improve the time performance of the blockchain is a problem that must be solved in the future. At present, there are three main ways to improve the performance of blockchain access control: First, by designing a new consensus algorithm to improve the speed of consensus, which can increase the speed of blockchain generation (Eyal et al., 2016; Kogias et al., 2016; Luu, Narayanan, Zheng et al, 2016); Second, change the chain structure of the blockchain to a network structure so that multiple blocks can be generated in parallel (Boyen et al., 2016; Coelho, 2018). Third, using multiple side chains to cooperate with the main chain, the main chain guarantees security, the side chain realizes specific business functions, and the performance is improved through the parallel work of multiple chains (Back et al., 2014; Hueber, 2018).

4. The nodes of the blockchain can only be increased but not reduced. This mechanism has brought huge storage pressure to the access control management of the IoMT system. It is also worth considering how to reduce the pressure of blockchain storage and improve the storage efficiency of node information. One of the current solutions is to compress the information in the node so that more data can be represented on the unit node (Di Francesco Maesa, Mori, & Ricci, 2017). The other is to store data outside the chain (Yu et al., 2018) and generate a unique hash value (Rifi, Rachkidi, Agoulmine, & Taher, 2017). The storage pressure of the blockchain is reduced by storing the hash value on the chain.
5. The issue of access control in cloud computing is also one of the most important issues in the current security field (Huang et al., 2021). The issue of access control in cloud computing is not only a technical issue but also involves many aspects such as standardization, laws and regulations, and codes of conduct. An appropriate environment and strict supervision model should be created to address the current access control dilemma faced by the current cloud computing environment.

ACKNOWLEDGMENT

This research was supported by the State Key Laboratory of Process Automation in Mining & Metallurgy and Beijing Key Laboratory of Process Automation in Mining & Metallurgy[grant number BGRIMM-KZSKL-2018-10]; the Research Project of Basic Scientific Research Business Expenses of Hebei Provincial Universities - Medical-Industrial Integration Project [grant number JYG2020001]; the science and technology basic research project (natural science) [grant number JQN2021027]; and the Natural Science Foundation of Hebei Province [grant number E2021209024].

REFERENCES

Alansari, S., Paci, F., Margheri, A., & Sassone, V. (2017, June). Privacy-preserving access control in cloud federations. In *2017 IEEE 10th International Conference on Cloud Computing (CLOUD)* (pp. 757-760). IEEE. doi:10.1109/CLOUD.2017.108

Alansari, S., Paci, F., & Sassone, V. (2017, June). A distributed access control system for cloud federations. In *2017 IEEE 37th international conference on distributed computing systems (ICDCS)* (pp. 2131-2136). IEEE. doi:10.1109/ICDCS.2017.241

Altmeier, C., Mainka, C., Somorovsky, J., & Schwenk, J. (2015). Adidos–adaptive and intelligent fully-automatic detection of denial-of-service weaknesses in web services. In *Data Privacy Management, and Security Assurance* (pp. 65–80). Springer.

Alturi, V., & Ferraiolo, D. F. (2011). *Role-Based Access Control*. Academic Press.

Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., & Capkun, S. (2013, April). Evaluating user privacy in bitcoin. In *International conference on financial cryptography and data security* (pp. 34-51). Springer. doi:10.1007/978-3-642-39884-1_4

Apostolaki, M., Zohar, A., & Vanbever, L. (2017, May). Hijacking bitcoin: Routing attacks on cryptocurrencies. In 2017 IEEE symposium on security and privacy (SP) (pp. 375-392). IEEE.

Ara, T., Shah, P. G., & Prabhakar, M. (2016). Internet of Things architecture and applications: A survey. *Indian Journal of Science and Technology*, *9*(45), 1–7. doi:10.17485/ijst/2016/v9i45/106507

Awe, K. F., Malik, Y., Zavarsky, P., & Jaafar, F. (2020). Validating BGP update using blockchain-based infrastructure. In *Decentralised Internet of Things* (pp. 151–165). Springer. doi:10.1007/978-3-030-38677-1_7

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., . . . Wuille, P. (2014). *Enabling blockchain innovations with pegged sidechains.* http://www. opensciencereview. com/papers/123/ enablingblockchain-innovations-with-pegged-sidechains

Beltran, V., & Skarmeta, A. F. (2018). Overview of device access control in the iot and its challenges. *IEEE Communications Magazine*, *57*(1), 154–160. doi:10.1109/MCOM.2017.1700433

Bissias, G., Ozisik, A. P., Levine, B. N., & Liberatore, M. (2014, November). Sybil-resistant mixing for bitcoin. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society* (pp. 149-158). doi:10.1145/2665943.2665955

Boyen, X., Carr, C., & Haines, T. (2016). *Blockchain-Free Cryptocurrencies. A Rational Framework for Truly Decentralised Fast Transactions*. Academic Press.

Chen, H., Pendleton, M., Njilla, L., & Xu, S. (2020). A survey on ethereum systems security: Vulnerabilities, attacks, and defenses. *ACM Computing Surveys*, *53*(3), 1–43. doi:10.1145/3391195

Chu, M. (2018). The application of Internet of Things technology in medical equipment. *Digital Technology and Application*, *36*(6), 131.

Coelho, F. C. (2018). Optimizing disease surveillance with blockchain. *bioRxiv*, 278473.

Coron, J. S., Dodis, Y., Malinaud, C., & Puniya, P. (2005, August). Merkle-Damgård revisited: How to construct a hash function. In *Annual International Cryptology Conference* (pp. 430-448). Springer. doi:10.1007/11535218_26

Courtois, N. T., Emirdag, P., & Valsorda, F. (2014). Private key recovery combination attacks: On extreme fragility of popular bitcoin key management, wallet and cold storage solutions in presence of poor RNG events. *Cryptology ePrint Archive*.

Cruz, J. P., Kaji, Y., & Yanai, N. (2018). RBAC-SC: Role-based access control using smart contract. *IEEE Access : Practical Innovations, Open Solutions*, *6*, 12240–12251. doi:10.1109/ACCESS.2018.2812844

Di Francesco Maesa, D., Mori, P., & Ricci, L. (2017, June). Blockchain based access control. In *IFIP international conference on distributed applications and interoperable systems* (pp. 206–220). Springer.

Ding, Y., Wu, G., Chen, D., Zhang, N., Gong, L., Cao, M., & Qin, Z. (2020). DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things. *IEEE Internet of Things Journal*, *8*(3), 1504–1518. doi:10.1109/JIOT.2020.3012452

Douceur, J. R. (2002, March). The sybil attack. In *International workshop on peer-to-peer systems* (pp. 251-260). Springer. doi:10.1007/3-540-45748-8_24

Elsayeh, M., Ezzat, K. A., El-Nashar, H., & Omran, L. N. (2021). Cybersecurity architecture for the internet of medical things and connected devices using blockchain. *Biomedical Engineering: Applications, Basis and Communications*, *33*(2), 2150013.

Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R. (2016). {Bitcoin-NG}: A scalable blockchain protocol. In *13th USENIX symposium on networked systems design and implementation (NSDI 16)* (pp. 45-59). USENIX.

Fang, L., Yin, L. H., Guo, Y. C., & Fang, B. X. (2017). A survey of key technologies in attribute-based access control scheme. *Chinese Journal of Computers*, *40*(7), 1680–1698.

Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2018). Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet of Things Journal*, *6*(2), 2188–2204. doi:10.1109/JIOT.2018.2882794

Fleder, M., Kester, M. S., & Pillai, S. (2015). *Bitcoin transaction graph analysis.* arXiv preprint arXiv:1502.01657.

Gervais, A., Ritzdorf, H., Karame, G. O., & Capkun, S. (2015, October). Tampering with the delivery of blocks and transactions in bitcoin. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 692-705). doi:10.1145/2810103.2813655

Guoping, Z., & Wentao, G. (2012). The research of access control in the application of VANET based on UCON. *Procedia Engineering*, *29*, 4091–4095. doi:10.1016/j.proeng.2012.01.625

Gupta, B. B., & Quamara, M. (2020). An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurrency and Computation*, *32*(21), e4946. doi:10.1002/cpe.4946

Han, Y., Han, Z., Wu, J., Yu, Y., Gao, S., Hua, D., & Yang, A. (2020). Artificial intelligence recommendation system of cancer rehabilitation scheme based on IoT technology. *IEEE Access : Practical Innovations, Open Solutions*, *8*, 44924–44935. doi:10.1109/ACCESS.2020.2978078

Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015). Eclipse attacks on {Bitcoin's}{peer-to-peer} network. In *24th USENIX Security Symposium (USENIX Security 15)* (pp. 129-144). USENIX.

Horalek, J., Holík, F., Horák, O., Petr, L., & Sobeslav, V. (2017). Analysis of the use of Rainbow Tables to break hash. *Journal of Intelligent & Fuzzy Systems*, *32*(2), 1523–1534. doi:10.3233/JIFS-169147

Huang, Q., Yue, W., Yang, Y., & Chen, L. (2021). P2gt: Fine-grained genomic data access control with privacy-preserving testing in cloud computing. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*. PMID:33656996

Hueber, O. (2018). The blockchain and the sidechain innovations for the electronic commerce beyond the Bitcoin's framework. *International Journal of Transitions and Innovation Systems*, *6*(1), 88–102. doi:10.1504/IJTIS.2018.090770

Jain, S., Nehra, M., Kumar, R., Dilbaghi, N., Hu, T., Kumar, S., Kaushik, A., & Li, C. Z. (2021). Internet of medical things (IoMT)-integrated biosensors for point-of-care testing of infectious diseases. *Biosensors & Bioelectronics*, *179*, 113074. doi:10.1016/j.bios.2021.113074 PMID:33596516

Karumba, S., Kanhere, S. S., Jurdak, R., & Sethuvenkatraman, S. (2020). *HARB: A hypergraph-based adaptive consortium blockchain for decentralised energy trading*. IEEE Internet of Things Journal.

Kazmi, A., Serrano, M., & Soldatos, J. (2018). Vital-os: An open source iot operating system for smart cities. *IEEE Communications Standards Magazine*, *2*(2), 71–77. doi:10.1109/MCOMSTD.2018.1700016

Kogias, E. K., Jovanovic, P., Gailly, N., Khoffi, I., Gasser, L., & Ford, B. (2016). Enhancing bitcoin security and performance with strong consistency via collective signing. In *25th USENIX security symposium (USENIX security 16)* (pp. 279-296). USENIX.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security and Privacy*, *9*(3), 49–51. doi:10.1109/MSP.2011.67

Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2012). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Transactions on Parallel and Distributed Systems*, *24*(1), 131–143. doi:10.1109/TPDS.2012.97

Lin, C., He, D., Huang, X., Choo, K. K. R., & Vasilakos, A. V. (2018). BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. *Journal of Network and Computer Applications*, *116*, 42–52. doi:10.1016/j.jnca.2018.05.005

Liu, H., Han, D., & Li, D. (2020). Fabric-IoT: A blockchain-based access control system in IoT. *IEEE Access : Practical Innovations, Open Solutions*, *8*, 18207–18218. doi:10.1109/ACCESS.2020.2968492

Liu, J., Fu, Z., & Sun, X. (2019). A survey on the security of blockchain. *Nanjing Xinxi Gongcheng Daxue Xuebao*, *11*(5), 513–522.

Liu, J., Xiao, Y., & Chen, C. P. (2012, June). Authentication and access control in the internet of things. In *2012 32nd international conference on distributed computing systems workshops* (pp. 588-592). IEEE. doi:10.1109/ICDCSW.2012.23

Lounis, A., Hadjidj, A., Bouabdallah, A., & Challal, Y. (2016). Healing on the cloud: Secure cloud architecture for medical wireless sensor networks. *Future Generation Computer Systems*, *55*, 266–277. doi:10.1016/j.future.2015.01.009

Luo, J., & Yan, L. (2013, June). Internet of things RFID anti-collision algorithm. In *2013 Fourth International Conference on Digital Manufacturing & Automation* (pp. 721-724). IEEE. doi:10.1109/ICDMA.2013.171

Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016, October). Making smart contracts smarter. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 254-269). doi:10.1145/2976749.2978309

Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016, October). A secure sharding protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 17-30). doi:10.1145/2976749.2978389

Martinez, J. B. (2018, November). Medical device security in the iot age. In 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 128-134). IEEE. doi:10.1109/UEMCON.2018.8796531

Mattila, J. (2016). *The blockchain phenomenon–the disruptive potential of distributed consensus architectures* (No. 38). ETLA Working Papers.

Mayer, H. (2016). ECDSA security in bitcoin and Ethereum: A research survey. *CoinFaabrik*, *28*(126), 50.

McMahon, E., Williams, R., El, M., Samtani, S., Patton, M., & Chen, H. (2017, July). Assessing medical device vulnerabilities on the Internet of Things. In *2017 IEEE international conference on intelligence and security informatics (ISI)* (pp. 176-178). IEEE.

Merkle, R. C. (1987, August). A digital signature based on a conventional encryption function. In *Conference on the theory and application of cryptographic techniques* (pp. 369-378). Springer.

Moyer, M. J., & Abamad, M. (2001, April). Generalized role-based access control. In *Proceedings 21st International Conference on Distributed Computing Systems* (pp. 391-398). IEEE. doi:10.1109/ICDSC.2001.918969

Natoli, C., & Gramoli, V. (2017, June). The balance attack or why forkable blockchains are ill-suited for consortium. In *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)* (pp. 579-590). IEEE. doi:10.1109/DSN.2017.44

Nguyen, K. T., Oualha, N., & Laurent, M. (2016, September). Authenticated key agreement mediated by a proxy re-encryptor for the internet of things. In *European symposium on research in computer security* (pp. 339-358). Springer. doi:10.1007/978-3-319-45741-3_18

Ni, J., Lin, X., & Shen, X. S. (2019). Toward edge-assisted Internet of Things: From security and efficiency perspectives. *IEEE Network*, *33*(2), 50–57. doi:10.1109/MNET.2019.1800229

Nicolas, K., Wang, Y., Giakos, G. C., Wei, B., & Shen, H. (2020). Blockchain system defensive overview for double-spend and selfish mining attacks: A systematic approach. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 3838–3857. doi:10.1109/ACCESS.2020.3047365

Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal, 5*(2), 1184-1195.

Ouechtati, H., & Azzouna, N. B. (2017, May). Trust-abac towards an access control system for the internet of things. In *International Conference on Green, Pervasive, and Cloud Computing* (pp. 75-89). Springer. doi:10.1007/978-3-319-57186-7_7

Ourad, A. Z., Belgacem, B., & Salah, K. (2018, June). Using blockchain for IOT access control and authentication management. In *International Conference on Internet of Things* (pp. 150-164). Springer. doi:10.1007/978-3-319-94370-1_11

Park, J., & Sandhu, R. (2002, June). Towards usage control models: beyond traditional access control. In *Proceedings of the seventh ACM symposium on Access control models and technologies* (pp. 57-64). doi:10.1145/507711.507722

Perez, D., & Livshits, B. (2019). *Smart contract vulnerabilities: Does anyone care?* arXiv preprint arXiv:1902.06710.

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). The blockchain as a decentralized security framework. *IEEE Consumer Electronics Magazine*, *7*(2), 18–21. doi:10.1109/MCE.2017.2776459

Ramachandran, A., & Kantarcioglu, D. (2017). *Using blockchain and smart contracts for secure data provenance management.* arXiv preprint arXiv:1709.10000.

Rifi, N., Rachkidi, E., Agoulmine, N., & Taher, N. C. (2017, September). Towards using blockchain technology for IoT data access protection. In *2017 IEEE 17th international conference on ubiquitous wireless broadband (ICUWB)* (pp. 1-5). IEEE. doi:10.1109/ICUWB.2017.8251003

Rifi, N., Rachkidi, E., Agoulmine, N., & Taher, N. C. (2017, September). Towards using blockchain technology for IoT data access protection. In *2017 IEEE 17th international conference on ubiquitous wireless broadband (ICUWB)* (pp. 1-5). IEEE. doi:10.1109/ICUWB.2017.8251003

Saleh, O. S., Ghazali, O., & Rana, M. E. (2020). Blockchain based framework for educational certificates verification. *Journal of Critical Reviews, 7*(3), 79-84.

Schmidt, J. M., & Medwed, M. (2009, September). A fault attack on ECDSA. In *2009 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)* (pp. 93-99). IEEE. doi:10.1109/FDTC.2009.38

Srinivas, J., & Das, A. K. (2020). Lightweight Security Protocols for Blockchain Technology. In *Cyber Defense Mechanisms* (pp. 131–156). CRC Press. doi:10.1201/9780367816438-9

Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and privacy in the medical internet of things: A review. *Security and Communication Networks*, *2018*, 2018. doi:10.1155/2018/5978636

Sun, Y., Lo, F. P. W., & Lo, B. (2019). Security and privacy for the internet of medical things enabled healthcare systems: A survey. *IEEE Access : Practical Innovations, Open Solutions*, *7*, 183339–183355. doi:10.1109/ACCESS.2019.2960617

Wang, H., Wang, Y., Cao, Z., Li, Z., & Xiong, G. (2018, August). An overview of blockchain security analysis. In *China Cyber Security Annual Conference* (pp. 55-72). Springer.

Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R., & Wang, F. Y. (2018, June). An overview of smart contract: architecture, applications, and future trends. In *2018 IEEE Intelligent Vehicles Symposium (IV)* (pp. 108-113). IEEE. doi:10.1109/IVS.2018.8500488

Wang, Y., Han, J. H., & Beynon-Davies, P. (2018). Understanding blockchain technology for future supply chains: A systematic literature review and research agenda. *Supply Chain Management*.

Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., & Kishigami, J. (2016, January). Blockchain contract: Securing a blockchain applied to smart contracts. In 2016 IEEE international conference on consumer electronics (ICCE) (pp. 467-468). IEEE.

Wikipedia. (n.d.). *2016 dyn cyberattack [EB/OL]*. https://en.wikipedia.Org/w/index.Php?Title=2016_Dyn_cyberattack&oldid=763071700

Woo, M. W., Lee, J., & Park, K. (2018). A reliable IoT system for personal healthcare devices. *Future Generation Computer Systems*, *78*, 626–640. doi:10.1016/j.future.2017.04.004

Wu, J., Dong, M., Ota, K., Li, J., & Pei, B. (2014, December). A fine-grained cross-domain access control mechanism for social internet of things. In *2014 IEEE 11th Intl Conf on Ubiquitous Intelligence and Computing and 2014 IEEE 11th Intl Conf on Autonomic and Trusted Computing and 2014 IEEE 14th Intl Conf on Scalable Computing and Communications and Its Associated Workshops* (pp. 666-671). IEEE. doi:10.1109/UIC-ATC-ScalCom.2014.140

Yang, A., Li, Y., Kong, F., Wang, G., & Chen, E. (2018). Security control redundancy allocation technology and security keys based on Internet of Things. *IEEE Access : Practical Innovations, Open Solutions*, *6*, 50187–50196. doi:10.1109/ACCESS.2018.2868951

Yang, A. M., Yang, X. L., Han, Y., Guo, Y. K., Liu, J. M., & Zhang, H. Q. (2018). Wireless channel optimization of Internet of things. *IEEE Access : Practical Innovations, Open Solutions*, *6*, 54064–54074. doi:10.1109/ACCESS.2018.2871364

Yang, Q., Lu, R., Rong, C., Challal, Y., Laurent, M., & Wang, S. (2019). Guest editorial the convergence of blockchain and IoT: Opportunities, challenges and solutions. *IEEE Internet of Things Journal*, *6*(3), 4556–4560. doi:10.1109/JIOT.2019.2921235

Yavari, A., Panah, A. S., Georgakopoulos, D., Jayaraman, P. P., & van Schyndel, R. (2017, June). Scalable role-based data disclosure control for the internet of things. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)* (pp. 2226-2233). IEEE. doi:10.1109/ICDCS.2017.307

Yu, F. R., Liu, J., He, Y., Si, P., & Zhang, Y. (2018). Virtualization for distributed ledger technology (vDLT). *IEEE Access : Practical Innovations, Open Solutions*, *6*, 25019–25028. doi:10.1109/ACCESS.2018.2829141

Yuan, E., & Tong, J. (2005, July). Attributed based access control (ABAC) for web services. In *IEEE International Conference on Web Services (ICWS'05)*. IEEE. doi:10.1109/ICWS.2005.25

Zarezadeh, M., Taluki, M. A., & Siavashi, M. (2020). Attribute-based Access Control for Cloud-based Electronic Health Record (EHR) Systems. *ISeCure, 12*(2).

Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart contract-based access control for the internet of things. *IEEE Internet of Things Journal*, *6*(2), 1594–1605. doi:10.1109/JIOT.2018.2847705

Zhang, Y., Xiang, Y., Huang, X., & Xu, L. (2014, September). A cross-layer key establishment scheme in wireless mesh networks. In *European Symposium on Research in Computer Security* (pp. 526-541). Springer. doi:10.1007/978-3-319-11203-9_30

Zhang, Y. Q., Zhou, W., & Peng, A. N. (2017). Survey of Internet of Things security. *Journal of Computer Research and Development*, *54*(10), 2130–2143.

Zhaofeng, M., Lingyun, W., Xiaochang, W., Zhen, W., & Weizhe, Z. (2019). Blockchain-enabled decentralized trust management and secure usage control of IoT big data. *IEEE Internet of Things Journal*, *7*(5), 4000–4015. doi:10.1109/JIOT.2019.2960526

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). *An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress).* IEEE.

Yikai Liu, Master in Cyberspace Security. His main research interests are network security, intrusion detection, blockchain, machine learning.

Fenglan Ju, Master of Health Statistics. Director of Finance Division, North China University of Science and Technology.

Qunwei Zhang, whose main areas are fractional differential equations, numerical computation and mathematical modeling.

Meng Zhang, whose main research interests include machine learning, computer vision, and pattern recognition.

Zezhong Ma, whose main research areas are network security, federal learning, privacy protection, and deep learning.

Mingduo Li received the B.S. degree in electrical engineering from Hebei University of Technology, Tianjin, China, in 2012, and the M.S. degree in electrical engineering from Northeastern University, Boston, USA, in 2015. She is currently pursuing her PhD in mineral engineering at the School of Mining Engineering, North China University of Science and Technology, Tangshan, China. Her research interests include safety science and engineering, automatic control, and microelectromechanical systems.

Fengchun Liu, Ph. His main research interests are machine learning, big data and cyber security.