Efficient Privacy-preserving in IoMT with Blockchain and Lightweight Secret Sharing

Chaoyang Li, Mianxiong Dong, *Member, IEEE*, Xiangjun Xin, Jian Li, Xiu-Bo Chen, and Kaoru Ota, *Member, IEEE*

***Abstract*—Internet of medical things (IoMT) aggregates a series of smart medical devices and fully uses the collected health data to improve user experience, medical resource utilization, and full life cycle protection. However, privacy leakage, data loss, and inefficient sharing problems are still serious in the data-sharing process between different smart medical devices. This paper first introduces an efficient privacy-preserving model with blockchain to construct a secure data-sharing mechanism between different device nodes. This model utilizes distributed storage form to solve the centralized management problem and provides a fundamental secret reconstruction and retrieval framework. Then, a lightweight (t, n)-threshold secret sharing (t/n-SS) scheme is designed to strengthen the medical data-sharing security and efficiency. It utilizes the interleaving encode technology to decrease the length of original message into n small shares. These small shares are also suitable for data transmission and processing with a more energy-efficient way. It can protect privacy by destroying the data's semantic meaning. Meanwhile, it only needs less than $t(t \leq n)$ shares to recover the original secrets, making the sharing process more efficient. Moreover, the performance evaluations of transaction processing in IoMT show that the proposed model is very stable. The simulation and performance evaluation results show that this t/n-SS scheme is energy efficient, storage saving, and strong fault tolerance than similar literature.**

***Index Terms*—Privacy-preserving, Internet of Medical Things, Blockchain, Secret Sharing.**

I. Introduction

INTERNET of medical things (IoMT) establishes a network of interconnected smart medical devices, wearable health devices, and other Internet medical hardware devices [1], [2]. It is increasingly important in people's daily health management, disease diagnosis, and rehabilitation treatment with more comprehensive health data. However, with the increasing number of smart medical devices, privacy leakage problem in health data sharing processes among different devices becomes more and more serious. Although blockchain technology has been utilized to establish a distributed data organization mode for traditional IoMT systems [3], [4], the transparency of transaction records in the public blockchain ledger also challenges the privacy-preserving of health data. Therefore, to improve the privacy security in medical data-sharing process through IoMT system, the lightweight data-sharing algorithm is needed along with the increasing demands of high throughput and low latency for smart medical devices.

Secure data-sharing model is the cornerstone for health management, value play, and privacy security. Along with the developments of informatization and digitization of health data management [5], the patient's health data are continually transferred and exchanged between medical institutions, medical workers, medical devices, and medical applications as shown in Fig. 1. In most instances, the medical institution does not want to share its health data with others due to the competition mechanism. However, sensitive information, such as the patient's privacy, and medical institution's secret information, inserted in the health data is also transferred here and there. It will bring serious detriments to the security of persons and property, threaten medical institutions, and even endanger national security. The traditional management forms not only do not prevent data leakage but also restrict the sharing and exploitation of data value [6], [7]. Blockchain technology can well solve the centralized management problem to establish a distributed health data-sharing platform. Some blockchain-based frameworks, such as Healthchain [8], [9], Fortified-chain [10], and MedShare [11], have been proposed to realize secure management and sharing of health data. These blockchain-based IoMT systems provide a secure and distributed health data-sharing platform, and establish a traceability mechanism in case of data loss and privacy leakage problem. Nevertheless, these proposals mainly focus on the data management and utilization processes but rarely care about the data collection process from smart medical devices through IoMT. How to establish a more secure and efficient medical data cross-device sharing model becomes one of the main challenges for privacy-preserving in IoMT.

Security of user privacy and health data is essential for the patient and medical institution. In practice, the electronic clinical thermometer only measures the body temperature, the electronic glucometer only measures the blood sugar concentration, the electronic blood pressure meter only measures the blood pressure, and the smartwatch can record a human's heart rate. Human health data contain many different kinds, which need many different medical devices to collect and analyze, and there does not exist integrated equipment that can measure all kinds of health data. The IoMT integrates smart medical devices and aggregates the fragmented health data from different devices into a unified ledger [12]. However, the secure transmission mechanism is a significant problem related to health data security and user privacy. As in other areas, there exist some "blockchain +" data-sharing mechanisms and algorithms, such as the blockchain + attribute-

Chaoyang Li and Xiangjun Xin are with the College of Software Engineering, Zhengzhou University of Light Industry, Zhengzhou 450001, China.

Mianxiong Dong and Kaoru Ota are with Muroran Institution of Technology, Muroran 050-8585, Japan.

Jian Li and Xiu-Bo Chen are with the School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China.

Corresponding author: Mianxiong Dong (mx.dong@csse.muroran-it.ac.jp)

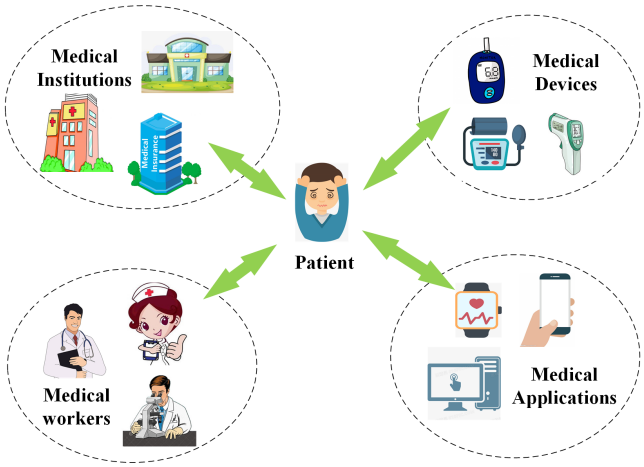


Fig. 1. Health data sharing through IoMT.

based encryption in 5G flying drones [13], blockchain + access control scheme in IIoT [14], blockchain + auditable private data sharing in smart grid [15], blockchain + credit-based consensus algorithm in disaster rescue [16], blockchain + delegated proof-of-stake consensus algorithm in the Internet of vehicles [17], blockchain + deniable ring signature in IoT [18], blockchain + oblivious random access memory in cloud computing [19]. Although blockchain technology can solve the centralized management problem in traditional IoMT systems, it also needs cryptographic algorithms to strengthen health data and user privacy security. In general, the smart medical devices generally have small storage space and low computing power, which results in highly complex algorithms that are not suitable. The lightweight secret sharing is one secure multi-party computation (SMC) algorithm that can improve computing efficiency while ensuring safety.

The secret sharing scheme can guarantee health data security in the sharing processes between smart medical devices and medical institutions [20]. Instead, it divides the original secrets into small shares to lighten the management difficulties and security risks associated with message concentration and stores the shares in different nodes to improve the sharing efficiency and data security. Then, the original secrets can be recovered by a retrieval mechanism with partial or total shares. This lightweight secret-sharing algorithm will be more suitable for secure health data transmission through these devices to satisfy the demands of high efficiency and low latency. Therefore, to strengthen the security of cross-device health data sharing, this paper first introduces a data privacy-preserving model empowered by blockchain technology for the IoMT system. We also propose a lightweight t/n-SS scheme for health data sharing among different smart medical devices through IoMT. The following three items are the summarized contributions:

- We introduce a novel data privacy-preserving model for secure health data sharing in IoMT with blockchain. This model establishes a secure health data-sharing mechanism between smart medical devices, medical workers, and medical institutions. It also constructs a fundamental secret reconstruction and retrieval framework to improve the data-sharing security and efficiency.
- We propose a lightweight t/n-SS scheme for medical data-sharing in blockchain-based IoMT. This scheme first divides the original message into n shares to prevent privacy theft by destroying semantic meaning. Then, it recovers this message with no less than t shares, improving data-sharing efficiency. This scheme also improves the fault tolerance ability with the (t, n)-threshold function when some shares are missing.
- We provide the performance evaluations of transaction processing in blockchain-based IoMT in concerning the transaction throughput (TSP) and transaction latency (TL). Meanwhile, the simulation and comparison of energy consumption, storage space, and network fault tolerance between the proposed t/n-SS and other similar literature are also provided.

In the following, Sec. II gives some related works review, Sec. III provides the data privacy-preserving model for blockchain-based IoMT, Sec. IV describes the proposed t/n-SS, Sec. V presents the security proof for the proposed scheme, Sec. VI gives the performance simulation and comparison, and the last Sec. VII concludes.

II. Relate Works

As in the data sharing process, privacy-preserving and data security are two significant parts which caused much-related research in recent years. This section reviews the privacy-preserving for IoMT and the data-sharing schemes in recent years.

A. Privacy-preserving for IoMT

Data tampering and privacy leakage are more serious in traditional IoMT, blockchain technology has been applied to design decentralized data management platforms. These privacy-preserving models are compared in Tab. I. Xu et al. introduced a double chain management model for large-scale health data by InterPlanetary File System (IPFS), where the doctor chain mainly contained the doctor's diagnostic results, and the user chain mainly contained the medical records [8]. Meanwhile, our former work designed a health data management platform based on a consortium blockchain called Healthchain. It also supported fair data trading with the Stackelgerg pricing model [9]. Egala et al. constructed a fortified-chain system for health data secure sharing and introduced a ring-based access control model to protect user privacy [10]. Wang et al. designed a Medshare platform with the smart contract for secure health data sharing and utilized attribute-based encryption to protect data privacy by the fine-grained access control mechanism [11]. Stafford and Treiblmaier developed a blockchain-enabled health data-sharing platform and utilized a grounded theory approach to analyze the health data for best treatment [21]. Du et al. utilized the consortium blockchain to construct a medical information-sharing platform, and they also proposed a consensus algorithm to achieve universal anonymous sharing [22]. Liu et al. gave a data-sharing scheme for blockchain-based mobile edge computing and designed a privacy-preserving mechanism to satisfy the privacy demand [23]. Abdellatif et al. presented a MEdge-chain system for edge computing based

TABLE I
RELATE WORK COMPARISON

Literature	Sharing technology	Advantage	Limitation	Lightweight
Xu *et al*. [8]	Public blockchain; IPFS	Double chain cooperation; Scalability	EMRs rights confusion; Cross-institution sharing	No
Li *et al*. [9]	Consortium blockchain; Stackelgerg game	Distributed management; Data sharing incentives	Access control ability; Interoperability	No
Egala *et al*. [10]	Public blockchain; Hybrid computing paradigm	Access control ability; Interoperability	EMRs rights confusion	No
Wang *et al*. [22]	Smart contract; Attribute-based encryption	Access control ability	EMRs rights confusion; Interoperability	No
Stafford *et al*. [21]	Public blockchain; Grounded theory	Interoperability	EMRs rights confusion; Access control ability	No
Du *et al*. [22]	Consortium blockchain; Mixed Byzantine fault tolerance	Universal anonymous sharing model	Access control ability; Interoperability	No
Liu *et al*. [23]	Public blockchain; Mobile-edge computing	Data sharing efficiency	Access control ability; Interoperability	No
Abdellatif *et al*. [24]	Public blockchain; Edge computing	Automated patients monitoring; Cross-institution sharing	EMRs right confusion; Access control ability	No
AI-Sumaidaee *et al*. [25]	Private blockchain; Hyperledger fabric	Cross-institution sharing	Access control ability; Interoperability	No
Zhao *et al*. [26]	Public blockchain; Quantum Byzantine agreement	Data fair exchange	Access control ability; Interoperability	No

on blockchain technology, which could guarantee secure and efficient health data exchange between different edge medical devices [24]. AI-Sumaidaee et al. established a distributed healthcare service system based on Hyperledger Fabric, which could weak the fragmentation problem and promote the information flow efficiency [25]. Zhao et al. introduced IoT-based blockchain networking for smart healthcare with Brooks-lyengar and quantum Byzantine agreement algorithms [26]. The comparison results in Tab. I show that the architecture of blockchain-enabled IoMT can provide a secure data-sharing platform. However, these literatures also have some limitations of EMRs rights confusion, access control ability, interoperability, etc. They do not lightweight because there is no lightweight SMC algorithm embedded in such blockchain-based IoMT systems.

With the developments of science and technology, many new technologies have been applied to promote the progress of healthcare services. Yang et al. reviewed the visions and features of cyber-physical system empowered robotic home-care system, and they also provided the future perspectives and challenges for the healthcare 4.0 [27]. Majumder et al. created a conceptual framework for a blockchain-enabled health data management platform, but it cannot realize the claimed intelligent data management [28]. Aujla and Jindal introduced a blockchain-enabled mechanism to establish a secure transmission channel between the home health monitoring sensors and edge device nodes [29]. Then, some privacy-preserving methods by utilizing artificial intelligence technologies are proposed to strengthen the security and efficiency of data-sharing process in IoMT. Jin et al. utilized federated learning and blockchain technologies to decrease the communication latency between medical devices in IoMT [30]. Lakhan et al. utilized federated learning and blockchain technologies to improve privacy security in IoMT systems [31]. Kumar et al. presented a data-sharing protocol for industrial healthcare systems with permission blockchain and deep-learning [32]. Belhadi et al. presented an end-to-end intelligent framework with blockchain technology, ensemble learning, and genetic algorithm for training complicated health data in IoMT [33]. However, these non-cryptographic designs are often vulnerable to system or network attacks and easily cause privacy leakage problems.

B. Data Sharing Scheme

The cryptographic secret sharing belongs to SMC, which can guarantee message security among the sharing processes in different parties. Luo et al. presented a data collection model with the secret sharing scheme to improve patient privacy security in IoMT [34]. Tang et al. introduced a health data sharing scheme by utilizing the fog computing technology [35], and their teams also gave a data aggregation scheme based on a fair incentives method with lightweight e-health IoT devices [36]. These two schemes all focus on the privacy security problem in the healthcare service system. Wei et al. provided a health data sharing scheme in a public cloud, which could realize revocable storage and hierarchical attribute-based access control [37]. Sarosh et al. proposed a secret sharing scheme for personal data exchange in the IoMT system [38]. Ma et al. applied edge computing technology to establish a privacy-preserving model for medical diagnosis [39]. Tan et al. gave a security and privacy-preserving protocol by utilizing the blockchain and ciphertext policy attribute-based encryption. Its security reduces to the secure access mechanism with the data and user attributes [40]. Chen et al. utilized the cloud computing and proxy re-encryption to realize secure data sharing through blockchain-enabled IoMT system [41]. Zhang et al. presented an identity-based decryption protocol for health data sharing. It can weaken the key escrow problem by applying the identity-based public key [42]. Deebak and AI-Turjman presented a mutual authenticity approach for cross-examine the common secret session key between smart devices in different communication entities [43]. Li et al. introduced a keyword-searchable encryption scheme for health data management, which can guarantee data-sharing security in the Healthchain system [44]. Meanwhile, a four layers architecture of the

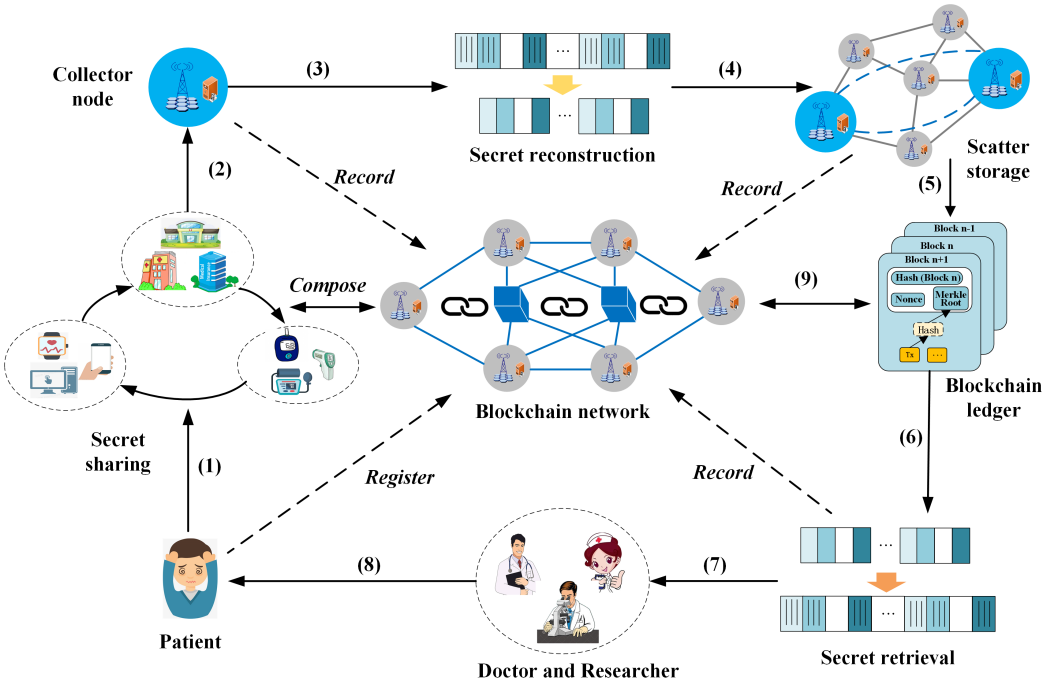


Fig. 2. The framework of privacy-preserving model.

perceptual, network, platform, and application for blockchain-based IoMT was introduced, and a group blind signature scheme was proposed to strengthen the health data-sharing process through this system [45]. Qu et al. gave a new sight for privacy protection in IoMT with quantum blockchain which was composed of the quantum signature and quantum identity authentication [46]. However, these schemes are generally with high complexity based on the bilinear pairings, lattice, or quantum algorithm.

The lightweight secret sharing schemes are mainly constructed with lightweight coding algorithms, such as Lagrangian interpolation formula (LIF), Chinese remainder theorem (CRT). These schemes are generally called (t, n)-threshold scheme as it divides the original secrets into n different pieces for distributed storage and then recovers them with only t $(t \leq n)$ pieces. Wang et al. proposed two such schemes based on the LIF, and these two schemes all contribute to improving source-location privacy security in wireless sensor networks (WSM) [47], [48]. Jia et al. applied the CRT to create such a protocol, but they did not care about the dynamic nature of the security environment [49]. Bitar et al. designed a staircase code-based secret sharing scheme for intensive computations tasks allocation [50]. Jia et al. utilized CRT to establish a general access structure strategy for group key management [51]. Hua et al. introduced a cipher-feedback secret sharing technique with (r, n)-threshold mechanism, which could improve the reversible data security in encrypted images in a lightweight way [52]. Kim et al. proposed a vertical mixing method by the additive secret sharing to improve cryptographic private web search solutions [53]. These secret sharing schemes are designed with CRT and LIF, which can make the scheme more efficient in a lightweight way. Considering the privacy-preserving data-sharing process among different medical devices in IoMT, this kind of cryptographic data-sharing scheme is more suitable. Therefore, the following sections first design a privacy-preserving model for health data sharing in the blockchain-based IoMT and introduce a new t/n-SS scheme to strengthen the model.

III. Data Privacy-preserving Model for IoMT

This section gives detailed descriptions of a data privacy-preserving model for IoMT.

A. Main Idea

Considering the privacy security in the IoMT, this article constructs a data privacy-preserving model with blockchain technology and lightweight secret sharing, shown in Fig. 2. It changes the data management forms in traditional IoMT systems and applies the lightweight secret sharing mechanism to realize secure health data storage and sharing. It first establishes a distributed health data management platform for secure data sharing in blockchain-based IoMT. Then it inserts a t/n-SS scheme to improve privacy security and data sharing efficiency. Then, this model's framework and concrete construction are given in the following subsections.

B. Framework of Privacy-preserving Model for blockchain-based IoMT

From the generation of health data, the data-sharing processes will undergo collection, authentication, reconstruction, and retrieval, and then the health data can be viewed by other users. First and foremost, the medical institutions, smart medical devices, patients, doctors, and researchers compose

the Blockchain-based IoMT system, which supports secure health data-sharing through these different entities. Then, the working mechanism of this model in the blockchain-based IoMT system is shown in Fig. 2. (1) The patient first should register as a legal user in the blockchain-based IoMT system, and the wearable and smart medical devices collect his health indicator data. (2) The collected health data are verified first, uploaded to the blockchain network, and then transmitted between the medical devices, apps, and medical institutions. (3) The collector node stores these data in native server and uploads processing records into the blockchain network. The storage process is a secret reconstruction performed, which can guarantee security against the tamper, deletion, and other destructive behaviors, and the original secrets M (health data) are divided into n pieces of sub-messages. (4) The divided sub-messages are stored in different nodes in the blockchain-based IoMT system. (5) The storage address and operational processes are recorded in the blockchain ledger, and the transaction in this ledger will become immutable records. (6) The secret retrieval process recovers original secrets with only t ($t \leq n$) pieces of sub-message. (7) The authorized doctor and researcher can view the original medical, then (8) make the diagnosis and perform research based on these health data. In addition, (9) all the operational processes in the former steps are uploaded to the blockchain-based IoMT system and recorded in the blockchain ledger for traceability. This public ledger servers as the one of only record list which store the health data indexes and processing operations.

Here, to lighten the blockchain ledger, we utilize the on-chain ledger and off-chain storage (OLOS) model to record transactions and store the health data. The OLOS model was proposed in our former work [47], as the storage addresses and operating records of health data were recorded into public ledger, and the real health data resources were deposited in native server. Based on this OLOS mechanism, the proposed privacy-preserving model can improve health data and system users' privacy security. In addition to the patient, doctor, and research nodes participating in the former, some other bank and insurance nodes also participate in the health data-sharing process in blockchain-based IoMT. The next section provides the concrete construction of this model.

C. Model Concrete Construction

The detailed data-sharing processes are shown in Fig. 3. When a patient sees a doctor in another medical institution, the health data will be shared through the blockchain network from the patient node to the doctor node. Meanwhile, other nodes are also participating in this blockchain network, such as the research node, bank node, insurance node, etc. Following are the descriptions of these main participants in the proposed model:

- *Blockchain network:* Blockchain network is the core part of the data privacy-preserving model in blockchain-based IoMT, which undertakes the responsibilities of user authentication, data management, trust agreement, and privacy-preserving. Firstly, the patient, doctor, researcher, medical institution, bank, and insurance parties should all register as legal users in the blockchain-based IoMT system. Then they can participate in the system transaction of data processing. Secondly, from data generation to destruction, the processing records are recorded into the public ledger, providing evidence for the medical dispute. Thirdly, a consensus algorithm is needed to achieve system consistency between the distributed peer-to-peer strange nodes. This blockchain-based IoMT system is a union of medical institutions, so the proof of stake is suitable for achieving system trust. Lastly, a non-tamper blockchain ledger guarantees health data security against data leakage, tampering, and island problems in traditional centralized storage forms. The cryptography and signature algorithms inserted in the blockchain system protect user privacy. Moreover, the patient, doctor, and researcher act in different roles in the IoMT system to promote health data sharing.

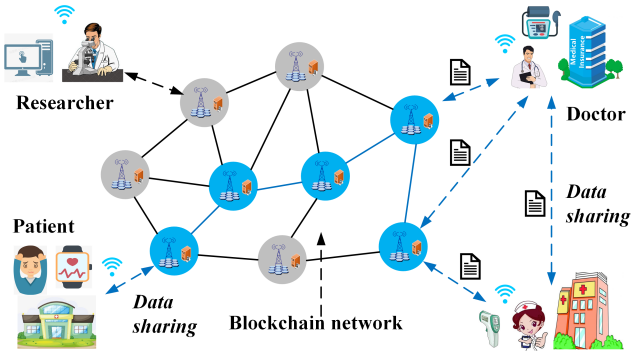


Fig. 3. The data privacy-preserving model.

- *Patient node:* Patient serves as the creator of health data who does not have his electronic medical records and cannot take the health data to other institutions because of the limitations of competition between different medical institutions. Health data are essential resources to determine the condition and diagnose a new patient, and the limitations lead to many duplicate checks and add to the patient's burden. Through this blockchain-based IoMT system, the daily health indicator data can be collected and recorded into the blockchain private ledger. When the patient comes to a new medical institution, his historical health data can be shared with a needed doctor by the authorization mechanism, which can help the doctor make a more accurate diagnosis. This also can decrease the time of medical checks and improve treatment efficiency.
- *Doctor node:* Doctor gives a diagnosis according to the checking results, but it will waste much time for the patient to check the health indexes individually. For an emergency case, historic health records are essential for selecting an appropriate therapeutic schedule. Meanwhile, the doctor needs to learn more cases to improve his professional skills, especially in a small medical institution. Therefore, health data sharing between different medical institutions can guarantee timely diagnosis and treatment of disease, and the blockchain-based IoMT system can promote health data sharing more securely and efficiently.

Moreover, as the doctor participates in the generation of health data, he can view the health data he created.

- *Researcher node:* Researcher performs drug discovery and device development with many health data. However, the health data in the current healthcare service system have the problems of decentralization, format complexity, and human destruction, limiting the exploitation of data value. The blockchain-based IoMT system can help aggregate the decentralized data and uniform their format. The researcher can discover more effective drugs and develop safe and reliable medical devices based on these rich health data resources.
- *Bank node:* Bank node plays the financial payment and settlement for the medical service. All transaction information is recorded in the blockchain ledger, which can provide integrated historic records for auditing regulation.
- *Insurance node:* Insurance node is also the critical node for blockchain-based IoMT, which takes responsibility for medical reimbursement. This kind of node generally cooperates with the bank node to finish the financial service for medical service transactions.

Some other nodes in this blockchain network exist, such as audit, drug supply, and other related medical service nodes. These different kinds of nodes establish the medical service ecology, and parts of these nodes help maintain the system consensus. This data privacy-preserving model establishes a secure sharing mechanism for data sharing in blockchain-based IoMT. Then a lightweight t/n-SS scheme has been proposed to strengthen the security and efficiency of sharing process in next section.

IV. Lightweight Secret Sharing Scheme

This section first provides the scheme and security models of a lightweight secret sharing scheme and then gives detailed descriptions of the proposed scheme.

A. Scheme Models

The Shamir protocol is a threshold secret segmentation scheme based on the LIF [54]. The definitions of the scheme and security models are given in this part.

(1) *Scheme model*

A t/n-SS scheme mainly contains two parts: secret reconstruction and secret retrieval.

a) *Secret reconstruction:*

- Select a prime p;
- Confirm the subkey holders n;
- Confirm the threshold t;
- Select $t-1$ number $a_1, a_2, ..., a_{t-1} \in [1, p]$;
- For secret s, set a polynomial $f(x) = s + a_1 x + a_2 x^2 + ... + a_{t-1} x^{t-1}$;
- Assign $s_i = f(i), (i = 1, 2, ..., n)$ to n holders $P_1, P_2, ..., P_n$ respectively;
- Destroy the polynomial $f(x)$.

b) *Secret retrieval:*

- Aggregate t subkeys $\{s_1, s_2, ..., s_t\} \rightarrow \{f(1), f(2), ..., f(t)\}$;
- Establish a secret retrieval polynomial $f(x) = \sum_{j=1}^{t} f(i_j) \prod_{l=1, l!=j}^{t} \frac{x - i_l}{i_j - i_l} modp$.
- Compute and output $s = f(0)$.

(2) *Security model* To steal the secret information s, some adversaries always attempt to collect more subkeys or obtain information about the polynomial. These adversaries are the internal subkey holders or the external opponents, which are classified into two types, as shown in the following.

- *Type I - Half honest adversary*: This type of adversary will comply with the protocol requirements but will actively collect the subkeys.
- *Type II - Malicious adversary*: This adversary is no longer following the protocol honestly and will send false or forged calculation results to other participants.

Here, it is generally assumed that the number of these adversaries does not exceed t for the internal subkey holders. In the t/n-SS scheme, LIF is an essential security barrier. Even though these adversaries obtain no less than t subkeys, they cannot derive s without secret reconstruction and retrieval principles. Then, for the scheme fault tolerance in resisting these two types of adversaries, it must prove that no less than t subkeys can recover s and less than t subkeys cannot recover it. Then, the security of one t/n-SS scheme against these two types of adversaries can be reduced to the following two lemmas.

Lemma 1: The original secret s can be recovered with j $(t \leq j \leq n)$ pieces of subkeys $\{s_{i_1}, s_{i_2}, ..., s_{i_j}\} \subseteq \{s_1, s_2, ..., s_n\}$ $(i_j \in \{1, 2, ..., n\})$.

Lemma 2: The original secrets s can not be recovered with j' $(j' < t)$ pieces of shares $\{s_{i_1}, s_{i_2}, ..., s_{i_{j'}}\} \subseteq \{s_1, s_2, ..., s_n\}$ $(i_{j'} \in \{1, 2, ..., n\})$.

Here, *Lemma 1* presents that s can be successfully recovered with no less than t subkeys. In general, the worst case of t subkeys is considered as the cases beyond t are always established when this case succeeds. *Lemma 2* shows that s cannot be recovered with less than t subkeys. Here, it usually considers the worst case of $t-1$ subkeys as the cases of less than $t-1$ are not true when this case does not work. Based on these two lemmas, it can prove that it can derive s with enough subkeys successfully. These two lemmas can prove that a t/n-SS scheme can resist the former two adversaries and has good fault tolerance.

B. t/n-SS Scheme

The health data are divided firstly to destroy semantic meaning, then managed with the OLOS model in the blockchain-based IoMT system. When someone obtains access rights to these data, they can be derived with no less than t shares. Following are the detailed descriptions of this t/n-SS scheme.

(1) *Secret reconstruction* This process contains two operations: interleaving encoding and message reorganization, shown in Fig. 4. Firstly, the interleaving encoder algorithm encodes secrets M into t sub-messages $\{m_1, m_2, ..., m_t\}$, and the length of every sub-message is $\lceil l/t \rceil (1 < t \leq n)$. Here, M with based 2 length l are divided into $\lceil l/t \rceil$ pieces, and every piece has t bits. Meanwhile, in order to well perform

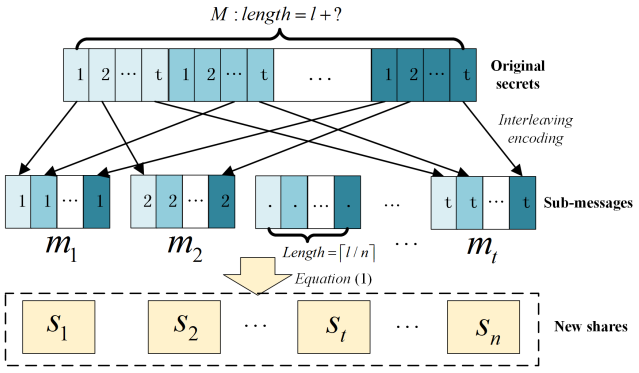


Fig. 4. The secret reconstruction process.

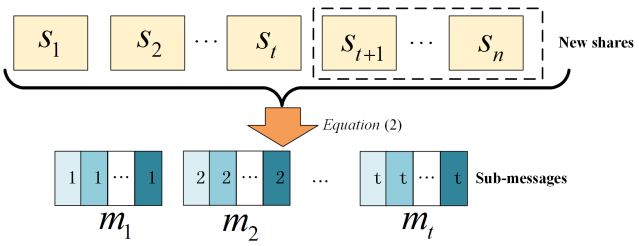


Fig. 5. The secret retrieval process.

the following operations, there also adds $(t-(l \mod t))$ bits 0 in the end to guarantee that secret M is sufficiently segmented. This encoding algorithm destroys the semantic meaning of original secrets, preventing the statistical attack from the adversary who does not know the code rule.

Then, to improve the data sharing security, t sub-messages are $\{m_1, m_2, ..., m_t\}$ reorganized into n new shares $s_i (i = 1, 2, ..., n)$ according to the principle in Eq. (1). Here, p $(p \leq 2^{\lceil l/t \rceil})$ is a larger prime number. These n new shares are recorded and managed by n nodes, and they do not have any information about the original secrets. Therefore, it will be safer for health data security and user privacy to record these fragmented shares in the public blockchain ledger. Moreover, the size of s_i is much more small in comparing wit m_i with $\lceil l/t \rceil$, and $\lceil l/t \rceil$ is also smaller than that of original secrets with l. The new small shares can make the secret data-sharing scheme more lightweight as it needs less storage space and data processing time.

$$s_i = \begin{cases} m_1 + \cdots + im_i \cdots + m_t \mod p, \text{if } 1 \leq i \leq t \\ 2^{i-t+1}s_1 + \cdots + 2^{i-t+t}s_t \mod p, \text{if } t < i \leq n \end{cases} \quad (1)$$

(2) *Secret retrieval* When one user obtains the data access rights, he can recover the original secrets with no less than t pieces of shares shown in Fig. 5. If there exist j $(t \leq j \leq n)$ pieces of shares $\{s_{k_1}, s_{k_2}, ..., s_{k_j}\} \subseteq \{s_1, s_2, ..., s_n\}$ $(k_j \in \{1, 2, ..., n\})$, these sub-messages $\{m_1, m_2, ..., m_t\}$ can be recovered by the following Eq. (2).

$$(m_1, m_2, ..., m_t)^T = D^{-1}_{t \times j} \cdot (s_{k_1}, s_{k_2}, ..., s_{k_j})^T \quad (2)$$

Here, the specific coefficient matrix $D^{-1}_{t \times j}$ represents the relation of the shares set and sub-message set, which is discussed with two cases D_1 and D_2 in detail in the following Sec. IV. This t/n-SS scheme provides the fault-tolerant ability for the secret retrieval process in the blockchain-based IoMT system if some share pieces are tampered with or destroyed. Meanwhile, it can improve the data retrieval efficiency as it needs less than n shares for remote retrieval.

C. Data Recordation in Blockchain Ledger

This blockchain ledger takes responsibility for recording the storage address and operating records of health data in blockchain-based IoMT. As shown in Fig. 6, these records serve as transactions in the public ledger. These transactions are organized as the leaf node of the Merkle tree, and its root nodes represent the Hash value of all the transaction data in this block. It performs layer-by-layer hash operations on transactions by using the structure of binary tree to guarantee the transaction security. Then, the blocks are linked according to chronological order, and the new block is also signed with the signature of the former block creator. This signature guarantees the connection of each block and establishes a transaction secure traceability mechanism. Finally, this ledger establishes a platform for data-sharing among medical institutions, doctors, researchers, and patients and provides traceable data for medical disputes. This ledger is also public, which guarantees the credibility of health data and operant behaviors on the base of protecting user privacy. Every valid nodes can view the transactions in this public ledger, but they cannot obtain anything about the real health data as the semantic meaning is scrambled. Only users who have obtained the correct data shares and encoding rules can correctly recover the original real health data.

For example, as one patient goes to see a doctor in one medical institution, the health data will pass through the following four steps to play its own value. (1) The patient initializes medical history sheet to store the health data; (2) For the nurse, she writes the visit and treatment records into this medical history sheet, signs with her signature and uploads them in the blockchain ledger; (3) For the doctor, he writes the diagnosis and medication records and also signs with his signature; (4) If this piece of health data is utilized by medical researcher, the processing operations and researcher's signature must be recorded and uploaded in the blockchain ledger. Note that, all the related records should be recorded, all the related operators' signatures should be signed, and then this blockchain ledger can provide more secure and traceable medical records for systems users.

V. Security Proof for t/n-SS Scheme

The security proof for the former t/n-SS scheme is given according to the *Lemma 1* and *Lemma 2* defined in the security model in Section IV.A. Here, we first give the security proof for secret retrieval with t pieces of shares as shown in *Theorem 1*, and then prove that any less than t shares do not recover original secrets as shown in *Theorem 2*.

Theorem 1: The original secrets M can be recovered with j $(t \leq j \leq n)$ pieces of shares $\{s_{k_1}, s_{k_2}, ..., s_{k_j}\} \subseteq \{s_1, s_2, ..., s_n\}$ $(k_j \in \{1, 2, ..., n\})$.

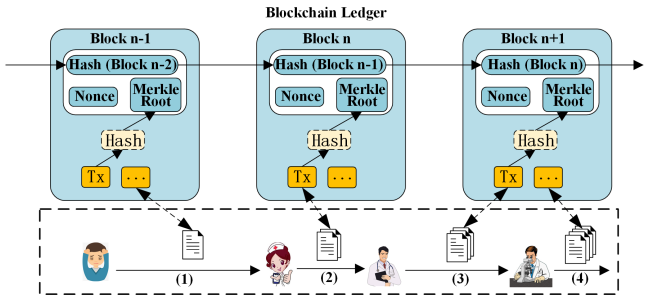


Fig. 6. Data recordation in blockchain ledger.

Proof: We show the proof that secrets M can be recovered with t shares. If this is a worst-case success, those cases with more than t shares are also valid. We divide this proof analysis into two cases: *Case 1* is the retrieval with first t shares, and *Case 2* is the retrieval with t shares chosen from two parts of the first t and last $n-t$. The detailed analyses are given below.

Case 1: Given the first t pieces $\{s_1, s_2, ..., s_t\} \subseteq \{s_1, s_2, ..., s_n\}$, the sub-messages $\{m_1, m_2, ..., m_t\}$ can be recovered by the coefficient matrix D_1 as Eq. (3).

$$(m_1, m_2, ..., m_t)^T = D_1^{-1} \cdot (s_1, s_2, ..., s_t)^T \tag{3}$$

Due to the shares $\{s_1, s_2, ..., s_t\}$ are reconstructed according to the principle of Eq. (1) with $1 \leq i \leq t$, they can be described as Eq. (4):

$$\begin{cases} s_1 = m_1 + m_2 + \cdots + m_t \mod p \\ s_2 = m_1 + 2m_2 + \cdots + m_t \mod p \\ \quad \vdots \\ s_t = m_1 + m_2 + \cdots + tm_t \mod p \end{cases} \tag{4}$$

Therefore, the coefficient matrix D_1 is shown in Eq. (5):

$$D_1 = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & t \end{pmatrix} \tag{5}$$

Then, we calculate the determinant of D_1 and find $|D_1| = (t-1)!$. Hence, the coefficient matrix D_1 is invertible with the non-zero determinant $(t-1)!$ $(t > 1)$, and the sub-messages $\{m_1, m_2, ..., m_t\}$ can be recovered by matrix D_1^{-1} with t shares of $\{s_1, s_2, ..., s_t\}$.

Case 2: Given t shares chosen from two parts are $\{s_{k_1}, ..., s_{k_i}, s_{t+k_{i+1}}+, ..., s_{t+k_t}\}$, $1 \leq k_1 < \cdots < k_i \leq t < s_{t+k_{i+1}} < \cdots < s_{t+k_t} \leq n$ the sub-messages $\{m_1, m_2, ..., m_t\}$ can be recovered by the coefficient matrix D_2 as Eq. (6).

$$\begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_t \end{pmatrix} = D_2^{-1} \begin{pmatrix} s_{k_1} \\ \vdots \\ s_{k_i} \\ s_{t+k_{i+1}} \\ \vdots \\ s_{t+k_t} \end{pmatrix} \tag{6}$$

Where first i $(0 \leq i \leq t)$ equations are randomly selected from the congruence equations in Eq. (4), and the last $t-i$ equations are randomly selected from the congruence equations in the following Eq. (7), which are reconstructed according to the principle of Eq. (1) with $t < i \leq n$.

$$\begin{cases} s_{t+1} = 2^2 s_1 + 2^3 s_2 + \cdots + 2^{t+1} s_t \mod p \\ s_{t+2} = 2^3 s_1 + 2^4 s_2 + \cdots + 2^{t+2} s_t \mod p \\ \quad \vdots \\ s_n = 2^{n-t+1} s_1 + 2^{n-t+2} s_2 + \cdots + 2^n s_t \mod p \end{cases} \tag{7}$$

Now, we do not need directly prove the relations between the sub-messages set $\{m_1, m_2, ..., m_t\}$ and shares set $\{s_{k_1}, ..., s_{k_i}, s_{t+k_{i+1}}+, ..., s_{t+k_t}\}$. We only need find the transformation matrix F transmitted from the shares set $\{s_1, s_2, ..., s_t\}$, which is shown in Eq. (8).

$$(s_{k_1}, ..., s_{k_i}, s_{t+k_{i+1}}+, ..., s_{t+k_t})^T = F \cdot (s_1, s_2, ..., s_t)^T \tag{8}$$

Therefore, we only need to prove the matrix F is invertible, which declares that the coefficient matrix D_2 is existing and invertible.

Then, the newly formed congruence equations are shown in Eq. (9), which are composed of one part of i shares $\{s_{k_1}, s_{k_2}, ..., s_{k_i}\} \subseteq \{s_1, s_2, ..., s_t\}$, and the other part $t-i$ shares $\{s_{t+k_{i+1}}, s_{t+k_{i+2}}, ..., s_{t+k_t}\} \subseteq \{s_{t+1}, s_{t+2}, ..., s_n\}$.

$$\begin{cases} s_{k_1} = s_{k_1} \mod p \\ \quad \vdots \\ s_{k_i} = s_{k_i} \mod p \\ s_{t+k_{i+1}} = 2^{k_{i+1}+1} s_1 + \cdots + 2^{k_{i+1}+t} s_t \mod p \\ \quad \vdots \\ s_{t+k_t} = 2^{k_t+1} s_1 + \cdots + 2^{k_t+t} s_t \mod p \end{cases} \tag{9}$$

Next, the coefficient matrix F can can be described in Eq. (10):

$$F = \begin{pmatrix} 0 \cdots & 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 \cdots & 0 & \cdots & 1 & \cdots & 0 \\ 1 \cdots & k_1^{k_{i+1}+k_1} & \cdots & k_i^{k_{i+1}+k_i} & \cdots & t^{k_{i+1}+t} \\ \vdots & \vdots & & \vdots & & \vdots \\ 1 \cdots & k_1^{k_t+k_1} & \cdots & k_i^{k_t+k_i} & \cdots & t^{k_t+t} \end{pmatrix} \tag{10}$$

The determinant of F can be calculated by the method as shown in Eq. (11), where $a_1, a_2, ..., a_{i-1} \in \{1, 2, ..., t\} - \{k_1, k_2, ..., k_i\}$, $a_1 < a_2 < ... < a_{i-1}$.

$$|F| = (-1)^{\sum_{j=1,2,...,i} k_j} \cdot E \tag{11}$$

where E shown in Eq. (12) is a generalized Vandermonde Determinant [55], and $E \neq 0$ with the condition of $a_1 < a_2 < ... < a_{i-1}$.

$$E = \begin{vmatrix} a_1^{k_{i+1}+k_1} & a_2^{k_{i+1}+k_i} & \cdots & a_{t-i}^{k_{i+1}+t} \\ a_1^{k_{i+2}+k_1} & a_2^{k_{i+2}+k_i} & \cdots & a_{t-i}^{k_{i+2}+t} \\ \vdots & \vdots & \ddots & \vdots \\ a k_1^{k_t+k_1} & a_2^{k_t+k_i} & \cdots & a_{t-i}^{k_t+t} \end{vmatrix}_{t-i} \tag{12}$$

Therefore, the coefficient matrix F is invertible with the non-zero determinant $|F|$. From the above proofs of *case 1*

and *case 2*, we can derive that Eq. (2) holds with $k_j = t$. Meanwhile, as t shares can recover the original secrets correctly, it declares that no less than t $(t \leq n)$ shares can always recover them correctly. *Theorem 1* has been proved, showing that the proposed secret sharing scheme has a strong fault-tolerant capability for data retrieval. Although the system or natural problems destroy some shares, it can successfully recover the original secrets M with no less than t shares.

In addition, the threshold t is a more critical parameter for the proposed scheme, which decides the fault-tolerant capability for the data-sharing process between different medical devices. Next, to explain that the proposed secret sharing scheme strictly satisfies t-threshold, we present another *Theorem 2* in the following to show that no more than t shares do not recover secrets M.

Theorem 2: The original secrets M can not be recovered with j' $(j' < t)$ pieces of shares $\{s_{k_1}, s_{k_2}, ..., s_{k_{j'}}\} \subseteq \{s_1, s_2, ..., s_n\}$ $(k_{j'} \in \{1, 2, ..., n\})$.

Proof: Assume one adversary can obtain a shares set $A : \{s_{k_1}, s_{k_2}, ..., s_{k_{j'}}\}$, he attempts to recover the sub-messages set $B : \{x_1, x_2, ..., x_t\}$ with coefficient matrix $D_{j' \times t}$ as shown in Eq. (13).

$$A = D_{j' \times t} B \tag{13}$$

Now, the problem becomes whether the congruence equations Eq. (13) have a solution. We consider the best case as the adversary who obtains $j' = t - 1$ pieces of shares can derive M, and then the cases with less than $t - 1$ shares are also false.

As the coefficient matrix $D_{(t-1)\times t}$ is over a field $\mathbb{F}$, we set a new matrix D' over $\mathbb{F}_p$. The augmented matrix of $D_{j' \times t}$ can be denoted as $(D'|A)_{(t-1)\times(t+1)}$, and $(D'|A)_{(t-1)\times(t+1)} = D'_{(t-1)\times t} A$. Here, there exist two cases: one is that the rank of $D_{(t-1)\times t}$ is less than $(D'|A)_{(t-1)\times(t+1)}$, and the other is that the rank of $D_{(t-1)\times t}$ is the same as $(D'|A)_{(t-1)\times(t+1)}$. The first case has no solution for the congruence equations Eq. (13). The second case can not derive a lawful solution as the congruence equations Eq. (13) have infinitely many solutions under the condition of the rank of $D_{(t-1)\times t}$ and $(D'|A)_{(t-1)\times(t+1)}$ are less than the number of variable t. Therefore, $t-1$ shares can not successfully recover the original secrets, and less than $t - 1$ shares can not succeed.

The above two theorems show that the proposed secret sharing scheme strictly satisfies the t threshold, and only less than t pieces of shares can successfully recover secrets M. The interleaving coding algorithm has reconstructed the original secrets, and the semantic meaning has been destroyed. Even though the adversary obtains more than t pieces shares, he can still not recover secrets M as he needs more information about the interleaving coding principle. Therefore, this t/n-SS scheme can well resist the attacks from both types adversaries no matter who can obtain less or more than t pieces shares. In addition, fragmented storage forms can weaken the storage stress and improve health data security and user privacy. This scheme also provides fault-tolerant capability once some shares have been tampered with or destroyed.

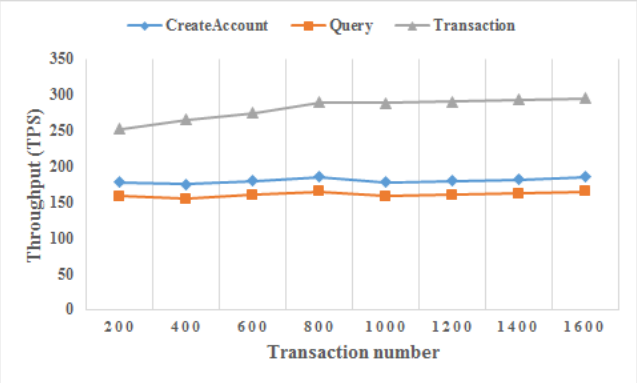


Fig. 7. Transaction throughput

VI. Performance Analysis

This part gives the performance evaluation and security analysis of the data privacy-preserving model. We perform the proposed t/n-SS scheme and other similar schemes on a Windows 10 laptop with Intel(R) Core (TM) i9 CPU 438 3.0 GHz and 16G RAM.

A. Transaction Processing in blockchain-based IoMT

For the blockchain-based IoMT system, we perform the health data sharing transaction processing on the Hyperledger Fabric concerning the transaction throughput (TSP) and transaction latency (TL). We select three items, such as "CreateAccount", "Query", and "Transaction", to describe the variation of TSP and TL based on the increase of the transaction number. Here, we perform it with the transaction number increasing from 200 to 1600 and present the simulation results in the following two figures. Fig. 7 is the trend chart of transaction throughput, and Fig. 8 is the trend chart of average transaction latency. As the transaction throughput, the items "CreateAccount" and "Transaction" keep stable, and the "Query" increases slightly. As the transaction latency, the items "CreateAccount" and "Query" keep stable, and the "Transaction" increases slightly. Meanwhile, the transaction latency of these three items is low, as the latency of "CreateAccount" is not exceeding 0.53 ms, the latency of "Query" is not exceeding 0.05 ms, and the latency of "Transaction" is not exceeding 0.24 ms. Therefore, it can derive that the TSP and TL are less affected by the test environment, and the proposed data privacy preserving model is practical for health data sharing in the blockchain-based IoMT system.

B. Performance Comparison

The performance comparisons of the proposed t/n-SS scheme with similar secret sharing schemes with the shares number, method, security, and application areas are shown in Tab. II, where m is a random integer exceeding 1. As the scheme in [50], it needs to send multiple shares to one participant because the staircase codes allow one participant to have no less than two shares to guarantee the connectivity of divided shares. The other schemes include our t/n-SS scheme only needs one share. For the security, the threshold schemes

TABLE II
PERFORMANCE COMPARISON

Schemes	Shares number	Method	Security	Application areas
Wang et al. [47]	1	LIF for integer ring	Asymptotically prefect	Source-location privacy in WSN
Wang et al. [48]	1	LIF for integer ring	Asymptotically prefect	Source-location privacy in WSN
Jia et al. [49]	1	CRT for polynomial ring	Prefect	Threshold changeable secret sharing
Bitar et al. [50]	m	Staircase codes	Not prefect	Distributed computing
Jia et al. [51]	1	CRT for polynomial ring	Perfect	General access structures
Our t/n-SS	1	LIF for polynomial ring	Prefect	Data privacy in blockchain-based IoMT

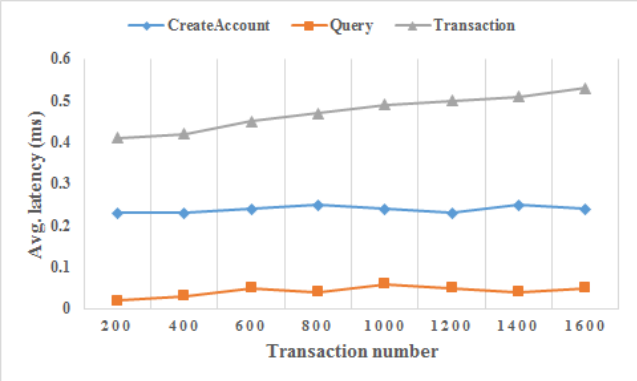


Fig. 8. Transaction latency

in [47], [48] are asymptotically perfect with the LIF for integer ring, and the scheme in [50] is not perfect since the multiple shares will affect the efficiency and increase the storage space. The proposed t/n-SS scheme used LIF for polynomial ring can achieve perfect security. For the application areas, schemes in [47], [48] are designed for source-location privacy in WSN, scheme in [49] is constructed for threshold changeable secret sharing, scheme in [50] is proposed for distributed computing, scheme in [51] is introduced for general access computing, and our t/n-SS scheme health data privacy-preserving in blockchain-based IoMT. For the application areas, this item comparison shows that this secret-sharing scheme fits for data privacy-preserving in information systems. Therefore, this data privacy-preserving model can improve health data security and user privacy in blockchain-based IoMT.

C. Comparison with Other Secret Sharing Schemes

We chose three representative schemes for comparison as the cloud-based secret sharing (CSS) scheme in Ref. [37], which is operated in public could, the perfect secret sharing (PSS) scheme in Ref. [38], which is created for the centralized IoMT system, and the CRT-based secret sharing (CRSS) scheme in Ref. [49] is a universal threshold secret sharing scheme. These three kinds of schemes represent similar health data-sharing methods for privacy-preserving in the data-sharing process between different smart medical devices. Although some other similar secret sharing approaches exist, we cannot address them in comparison with the proposed t/n-SS scheme as the performance evaluations are similar to these three selected schemes. Note that some of the parameter settings are listed in Tab. III, and the energy consumption,

TABLE III
SIMULATION PARAMETERS

Items	Parameter	Value
Block time	τ	12 sec
Length of health data	3	100,200,...,1000 bits
Threshold	(t, n)	(4,7)
System nodes	N	100
User Number	M	80

storage space efficiency, and network fault tolerance have been performed. Detailed descriptions are shown in the following.

(1) *Energy consumption*

Through the proposed data sharing model, the collected health data need to go through four steps, reconstruction, verification, confirmation, and retrieval, to realize transmission from one device entity to the other. For one piece of health data, the energy consumption of verification and confirmation processes is negligible, but the computation of the reconstruction process is more complex. Therefore, we mainly consider the energy consumption for these processes. By the interleaving encoding and the reconfiguration principle in Eq. (1), the original secrets M have been divided into n shares. In this process, there need n modulo operations, $t(n-t)$ multiply operations, and $t(t-2)+\frac{1}{2}t(t+1)+(n-t)(t-1)$ add operations. Here, we consider the lowest energy consumption for the retrieval process with only t shares. These operations are more energy-efficient than any other operation of bilinear pairing and exponentiation. The general running time consumption is the one add operation with 41.45 ms, one multiply operation with 57.25 ms, and one modulo operation with 1178.15 ms. The energy consumption is also influenced by the wireless sensor node, which is generally with power level of 3.0 V and 8.0 mA for MICA 2. For the $(4, 7)$-SS scheme, the energy consumption of this process is $3.0 * 8.0 * (27 * 41.45 + 10 * 57.25 + 7 * 1178.15)/1000 = 10.05mJ$.

In addition, the delivery of the shares to different n devices nodes is also energy consumption, and one node needs to verify and confirm $(l/t) \times n \times n$ bits with l bits health data in the proposed t/n-SS scheme. However, the other three CSS, PSS, and CRSS schemes have $l \times n \times n$ operations for one transaction. Then, by aggregating all the energy consumption operations mentioned above, the performance and comparison results and the increase of secrets length from 100 bits to 1000 bits are shown in Fig. 9. Although composed with former $10.05mJ$ energy consumption, the proposed t/n-SS is also energy saving with the small length shares comparing with the other three schemes.

(2) *Storage space efficiency*

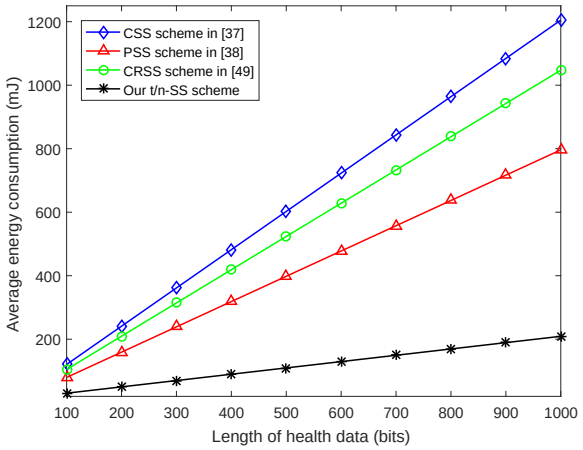


Fig. 9. The average energy consumption with different shares' length

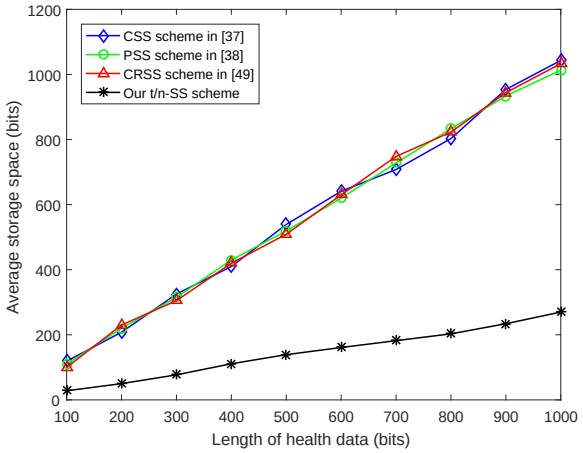


Fig. 10. The average storage space with different shares' length

Smart medical devices are usually designed with insufficient storage space to carry more computational processing components to realize high data processing ability. Meanwhile, the blockchain ledger also has a limited block size. Therefore, a minor transaction size will suit health data sharing between different smart medical device nodes. The proposed t/n-SS scheme has divided the long-length message into shares with small lengths, the distributed storage form fully uses the storage space in the device nodes, and the small shares make the transaction processing more efficient. However, the other three schemes executing the entire length of original messages take up much storage space. Results are shown in Fig. 10, and it is almost the linear growth relationship between the average storage space and the length of health data for all four schemes. The proposed t/n-SS scheme needs smaller storage spaces than the other three schemes.

(3) *Network fault tolerance*

In the practical situation, the smart medical device node sometimes occurs an outage, so the network fault tolerance ability is a more critical index for system stability. The success rate of secret sharing related to the node failure probability is

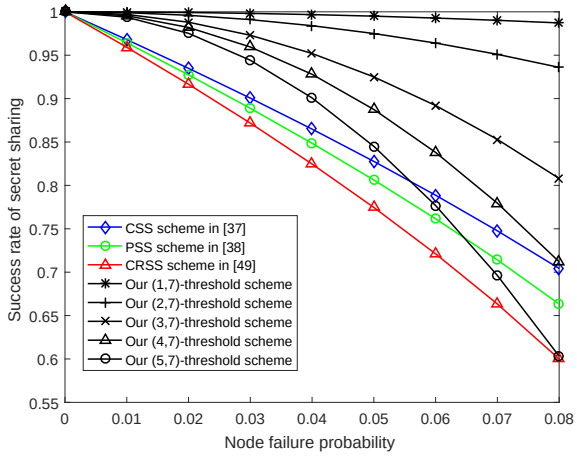


Fig. 11. The secrets successful sharing rate with node failure probability.

shown in Fig. 11. The success rates are linear decline with the increasing node failure probability in the other three CSS, PSS, and CRSS schemes, as they execute the data-sharing operations with a full-length message. For the general storage form, single node failure will seriously damage the healthcare service system. It also quickly brings data leakage, tampers with centralized management, and damages the security of users' privacy and property. However, the success rate in the proposed t/n-SS scheme declines gradually as it has a certain fault tolerance ability. We also provide the performance comparison with different $t = \{1, 2, 3, 4, 5\}$ shares, and the proposed t/n-SS scheme outperforms the other three schemes with node failure probability $[0, 0.08]$ when $1 \leq t \leq 4$. But when t increases to 5, the success rate declines quickly, and the worst case is down to 0.6, which is not practical. If the system stability requires a 90% success rate, the proposed t/n-SS scheme with the threshold $(1, 7)$ and $(2, 7)$ can satisfy 0.08 node failure probability. However, the other three schemes satisfy no less than 0.25 node failure probability. Therefore, this scheme can improve the network fault tolerance ability and make the shared health data more reliable.

D. Security Analysis for blockchain-based IoMT

- *Health data secret sharing*: Through the proposed data sharing model, the health data can be securely transmitted among different smart medical devices in the blockchain-based IoMT system.
- *User privacy-preserving*: Through the reconstruction process, the semantic meaning of health data has been destroyed. The adversary cannot obtain any information from the network's transmitted shares or the blockchain ledger's public transaction records.
- *Health data lightweight storage*: The original health data have been divided into different shares with small lengths, improving the data processing efficiency. Meanwhile, decentralized storage improves health data security and saves space for smart medical devices.
- *Network fault tolerance*: The proposed t/n-SS scheme makes the data-sharing process in the blockchain-based

IoMT system more robust against secret share damage or loss.

VII. Conclusions and Future Works

This paper focuses on the privacy-preserving problem in the data-sharing process between different smart medical devices and designs a data privacy-preserving model based on blockchain technology for secure data sharing. This model can guarantee health data security and user privacy when the data are transmitted among the patient, doctor, researcher, and other nodes through the blockchain-based IoMT system. Then, a (t, n)-SS scheme has been proposed to strengthen the data-sharing security and efficiency. This scheme divides the original secrets into small shares for storage and sharing, which can significantly save storage space and guarantee privacy security in the public ledger. Meanwhile, the original secrets are recovered with only t $(t \leq n)$ pieces of shares, which improves the efficiency and the fault tolerance ability of the health data-sharing process. Finally, the security proof shows that this (t, n)-SS scheme is correct and theoretical security, and the performance results show that the privacy-preserving model is energy-saving, storage space efficient, and network fault tolerant.

However, other problems exist, such as user authentication data access control, in the data utilization process of cross-device data sharing, which should be considered more. For example, when health data are transmitted to other smart medical devices, the legality of the device owner refers to privacy security. When the patient takes his health data to a new medical institution, authorizing the needed medical workers to view the data is also a significant security problem. Therefore, we will continue to put efforts into the privacy-preserving methods for the blockchain-based IoMT system.

Acknowledgment

This work was supported by the National Natural Science Foundation of China under Grant 62272090, 61962009, the JSPS KAKENHI Grant Numbers JP19K20250, JP20H04174, JP22K11989, Leading Initiative for Excellent Young Researchers (LEADER), MEXT, Japan, and JST, PRESTO Grant Number JPMJPR21P3, Japan. Mianxiong Dong is the corresponding author, the Doctor Scientific Research Fund of Zhengzhou University of Light Industry under Grant 2021B-SJJ033.

References

[1] A. Gatouillat, Y. Badr, B. Massot, and E. Sejdić, "Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3810-3822, Oct. 2018.

[2] N. Y. Philip, J. J. Rodrigues, H. Wang, S. J. Fong, and J. Chen, "Internet of Things for in-home health monitoring systems: current advances, challenges and future directions," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 300-310, Feb. 2021.

[3] R. Wang, H. Liu, H. Wang, Q. Yang, and D. Wu, "Distributed security architecture based on blockchain for connected health: architecture, challenges, and approaches," *IEEE Wireless Commun.*, vol. 26, no. 6, pp. 30-36, Dec. 2019.

[4] L. Soltanisehat, R. Alizadeh, H. Hao, and K. K. R. Choo, "Technical, temporal, and spatial research challenges and opportunities in blockchain-based healthcare: A systematic literature review" *IEEE Transactions Eng. Manag.*, early access, vol.70, no. 1, pp. 353-368, Sept. 2, 2020.

[5] H. Qiu, M. Qiu, M. Liu, and G. Memmi, "Secure health data sharing for medical cyber-physical systems for the healthcare 4.0," *IEEE J. Biomed. Health Inform.*, vol. 24, no. 9, pp. 2499-2505, Sept. 2020.

[6] M. Seliem, and K. Elgazzar, "BIoMT: Blockchain for the internet of medical things," *2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom). IEEE*, Jun. 2019, pp. 1-4.

[7] C. Li, Y. Tian, X. Chen, and J. Li, "An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems," *Inf. Sci.*, vol. 546, pp. 253-264, Feb. 2020.

[8] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8770-8781, Oct. 2019.

[9] C. Li, M. Dong, J. Li, G. Xu, X. Chen, and K. Ota, "Healthchain: Secure EMRs Management and Trading in Distributed Healthcare Service System," *IEEE Internet Things J.*, vol. 8, no. 9, pp. 7192-7202, May 2021.

[10] B. S. Egala, A. K. Pradhan, V. R. Badarla, and S. P. Mohanty, "Fortified-chain: a blockchain based framework for security and privacy assured internet of medical things with effective access control," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11717-11731, Jul. 2021.

[11] M. Wang, Y. Guo, C. Zhang, C. Wang, H. Huang, and X. Jia, "MedShare: a privacy-preserving medical data sharing system by using blockchain," *IEEE Trans. Serv. Comput.*, 2021. [Online]. Availabe: https://ieeexplore.ieee.org/abstract/document/9547814

[12] S. Pirbhulal, W. Wu, G. Li, and A. K. Sangaiah, "Medical information security for wearable body sensor networks in smart healthcare," *IEEE Consum. Electron. Mag.*, vol. 8, no. 5, pp. 37-41, Sept. 2019.

[13] C. Feng, K. Yu, A. K. Bashir, Y. D. Al-Otaibi, Y. Lu, S. Chen, and D. Zhang, "Efficient and secure data sharing for 5G flying drones: a blockchain-enabled approach," *IEEE Netw.*, vol. 35, no. 1, pp. 130-137, Jan.-Feb. 2021.

[14] K. Yu, L. Tan, M. Aloqaily, H. Yang, and Y. Jararweh, "Blockchain-enhanced data sharing with traceable and direct revocation in IIoT," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, no. 11, pp. 7669-7678, Nov. 2021.

[15] Y. Wang, Z. Su, N. Zhang, J. Chen, X. Sun, Z. Ye, and Z. Zhou, "SPDS: A secure and auditable private data sharing scheme for smart grid based on blockchain," *IEEE Trans. Industr. Infor.*, vol. 17, no. 11, pp. 7688-7699, Nov. 2021.

[16] Z. Su, Y. Wang, Q. Xu, and N. Zhang, "LVBS: Lightweight vehicular blockchain for secure data sharing in disaster rescue," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 11, pp. 19-32, Jan.-Feb. 2022.

[17] J. Cui, F. Ouyang, Z. Ying, L. Wei, and H. Zhong, "Secure and efficient data sharing among vehicles based on consortium blockchain," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 8857-8867, Jul. 2022.

[18] T. Li, H. Wang, D. He, and J. Yu, "Blockchain-based privacy-preserving and rewarding private data sharing for IoT," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 15138-15149, Aug. 2022.

[19] J. Shen, H. Yang, P. Vijayakumar, and N. Kumar, "A privacy-preserving and untraceable group data sharing scheme in cloud computing," *IEEE Transa. Dependable Secure Comput.*, vol. 19, no. 4, pp. 2198-2210, Jul.-Aug. 2022.

[20] C. C. Yang, T. Y. Chang, and M. S. Hwang, "A (t, n) multi-secret sharing scheme," *Appl. Math. Comput.*, vol. 151, no. 2, pp. 483-490, Apr. 2004.

[21] T. F. Stafford, and H. Treiblmaier, "Characteristics of a blockchain ecosystem for secure and sharable electronic medical records," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1340-1362, Nov. 2020.

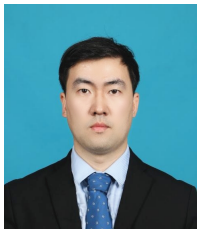
[22] M. Du, Q. Chen, J. Chen, and X. Ma, "An optimized consortium blockchain for medical information sharing," *IEEE Trans. Eng. Manag.*, vol. 68, no. 6, pp. 1677-1689, Dec. 2021.

[23] L. Liu, J. Feng, Q. Pei, C. Chen, Y. Ming, B. Shang, and M. Dong, "Blockchain-enabled secure data sharing scheme in mobile-edge computing: An asynchronous advantage actor-critic learning approach," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2342-2353, Feb. 2021.

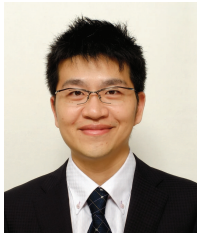
[24] A. A. Abdellatif, L. Samara, A. Mohamed, A. Erbad, C. F. Chiasserini, M. Guizani, M. D. Connor, and J. Laughton, "MEdge-Chain: Leveraging Edge Computing and Blockchain for Efficient Medical Data Exchange," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15762-15775, Nov. 2021.

[25] G. Al-Sumaidaee, R. Alkhudary, Z. Zilic, and A. Swidan, "Performance analysis of a private blockchain network built on Hyperledger fabric for healthcare," *Inf. Process. Manage.*, vol. 60, no. 2, p. 103160, Mar. 2023.

[26] Z. Zhao, X. Li, B. Luan, W. Jiang, W. Gao, and S. Neelakandan, "Secure Internet of Things (IoT) using a Novel Brooks Iyengar Quantum Byzantine Agreement-centered Blockchain Networking (BIQBA-BCN) Model in Smart Healthcare," *Inf. Sci.*, vol.629, pp. 440-455, Jun. 2023.
[27] G. Yang, Z. Pang, M. J. Deen, M. Dong, Y. T. Zhang, N. Lovell, and A. M. Rahmani, "Homecare robotic systems for healthcare 4.0: visions and enabling technologies," *IEEE J. Biomed. Health Inform.*, vol. 24, no. 9, pp. 2535-2549, Sept. 2020 .
[28] A. Majumder, S. Saha, T. Bhowmik, and A. Basu, "A Conceptual Framework for Blockchain-based Intelligent Healthcare Data Management," *2021 IEEE Bombay Section Signature Conference (IBSSC). IEEE*, Nov. 2021, pp. 1-6.
[29] G. S. Aujla, and A. Jindal, "A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 491-499, Feb. 2020.
[30] H. Jin, X. Dai, J. Xiao, B. Li, H. Li, and Y. Zhang, "Cross-Cluster Federated Learning and Blockchain for Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 21, pp, 15776-12784, Nov. 2021.
[31] A. Lakhan, M.A. Mohammed, J. Nedoma, R. Martinek, P. Tiwari, A. Vidyarthi, A. Alkhayyat, and W. Wang, "Federated-Learning Based Privacy Preservation and Fraud-Enabled Blockchain IoMT System for Healthcare," *IEEE J. Biomed. Health Inform.*, Apr. 2022. [Online]. Availabe: https://ieeexplore.ieee.org/abstract/document/9754271
[32] R. Kumar, P. Kumar, R. Tripathi, G.P. Gupta, A.N. Islam, and M. Shorfuzzaman, "Permissioned blockchain and deep-learning for secure and efficient data sharing in industrial healthcare systems," *IEEE Trans. Industr. Inform.*, vol.18, no. 11, pp. 8065-8073, Nov. 2022.
[33] A. Belhadi, J. O. Holland, A. Yazidi, G. Srivastava, J. C. W. Lin, and Y. Djenouri, BIoMT-ISeg: Blockchain internet of medical things for intelligent segmentation," *Front. Physiol.*, vol. 13, p.2744, Jan. 2023.
[34] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and M. Atiquzzaman, "PrivacyProtector: Privacy-protected patient data collection in IoT-based healthcare systems," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 163-168, Feb. 2018.
[35] W. Tang, J. Ren, K. Zhang, D. Zhang, Y. Zhang, and X. Shen, "Efficient and privacy-preserving fog-assisted health data sharing scheme," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 6, pp. 1-23, Nov. 2019.
[36] W. Tang, J. Ren, K. Deng, and Y. Zhang, "Secure data aggregation of lightweight e-healthcare iot devices with fair incentives," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8714-8726, Oct. 2019.
[37] J. Wei, X. Chen, X. Huang, X. Hu, and W. Susilo, "RS-HABE: Revocable-storage and hierarchical attribute-based access scheme for secure sharing of e-health records in public cloud," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 5, pp. 2301-2315, Oct. 2019.
[38] P. Sarosh, S. A. Parah, G. M. Bhat, A. A. Heidari, and K. Muhammad, "Secret sharing-based personal health records management for the Internet of health things," *Sustain. Cities Soc.*, vol. 74, pp. 103129, Nov. 2021.
[39] Z. Ma, J. Ma, Y. Miao, X. Liu, K. K. R. Choo, R. Yang, and X. Wang, "Lightweight privacy-preserving medical diagnosis in edge computing," *IEEE Trans. Serv. Comput.*, vol. 15, no. 3, pp. 1606-1618, Jun. 2020.
[40] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei, and H. Lu, "Towards secure and privacy-preserving data sharing for covid-19 medical records: A blockchain-empowered approach," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 1, pp. 271-281, Aug. 2021.
[41] Z. Chen, W. Xu, B. Wang, and H. Yu, "A blockchain-based preserving and sharing system for medical data privacy," *Future Gener. Comput. Syst.*, vol. 124, pp. 338-350, Nov. 2021.
[42] Y. Zhang, D. He, M. S. Obaidat,, P. Vijayakumar, and K. F. Hsiao, "Efficient identity-based distributed decryption scheme for electronic personal health record sharing system," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 384-395, Feb. 2020.
[43] B. D. Deebak, and F. Al-Turjman, "Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 346-360, Feb. 2020.
[44] C. Li, M. Dong, J. Li, G. Xu, X.B. Chen, W. Liu, and K. Ota, "Efficient Medical Big Data Management With Keyword-Searchable Encryption in Healthchain," *IEEE Syst. J.*, vol.16, no. 2, pp. 5521-5532, Dec. 2022.
[45] C. Li, B. Jiang, Y. Guo, and X. Xin, "Efficient group blind signature for medical data anonymous authentication in blockchain-enabled IoMT," *Comput. Mater. Contin.*, vol. 76, no. 1, pp. 591-606, Jun. 2023.
[46] Z. Qu, Y. Meng, B. Liu, G. Muhammad, and P. Tiwari, "QB-IMD: A secure medical data processing system with privacy protection based on quantum blockchain for IoMT," *IEEE Internet Things J.*, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10149070
[47] N. Wang, J. Fu, J. Zeng, and B. K. Bhargava, "Source-location privacy full protection in wireless sensor networks," *Inf. Sci.*, vol. 444, pp. 105-121, May 2018.
[48] N. Wang, J. Fu, J. Li, and B. K. Bhargava, "Source-location privacy protection based on anonymity cloud in wireless sensor networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 100-114, May 2019.
[49] X. Jia, D. Wang, D. Nie, X. Luo, and J. Z. Sun, "A new threshold changeable secret sharing scheme based on the Chinese remainder theorem," *Inf. sci.*, vol. 473, pp. 13-30, Jan. 2019.
[50] R. Bitar, P. Parag, and S. El Rouayheb, "Minimizing latency for secure coded computing using secret sharing via staircase codes," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 4609-4619, Aug. 2020.
[51] X. Jia, Y. Guo, X. Luo, D. Wang, and C. Zhang, "A perfect secret sharing scheme for general access structures," *Inf. Sci.*, vol. 595, pp. 54-69, Apr. 2022.
[52] Z. Hua, Y. Wang, S. Yi, Y. Zhou, and X. Jia, "Reversible data hiding in encrypted images using cipher-feedback secret sharing," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 8, pp. 4968-4982, Aug. 2022.
[53] M. Kim, and I. Lee, "Taming the round efficiency of cryptographic protocols for private web search schemes," *Inf. Sci.*, vol. 621, pp. 1-21, 2023.
[54] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612-613, Nov. 1979.
[55] A. Chandler, "A categorification of the Vandermonde determinant," *J. Knot Theory Ramif.*, vol. 30, no. 13, p. 2141005, Feb. 2021.



Chaoyang Li received the Ph.D. degree in intelligent science and technology from the Beijing University of Posts and Telecommunications, Beijing, China, in 2021. He is currently a Lecturer with the College of Software Engineering, Zhengzhou University of Light Industry, Zhengzhou, China. He was a visiting student with the ENeS lab at Muroran Institution of Technology, Muroran, Japan, supported by the China Scholarship Council (CSC) Program from October 2019 to September 2020. His interests include information security, cryptography and blockchain.



Mianxiong Dong received B.S., M.S. and Ph.D. in Computer Science and Engineering from The University of Aizu, Japan. He is the Vice President and Professor of Muroran Institute of Technology, Japan. He was a JSPS Research Fellow with School of Computer Science and Engineering, The University of Aizu, Japan and was a visiting scholar with BBCR group at the University of Waterloo, Canada supported by JSPS Excellent Young Researcher Overseas Visit Program from April 2010 to August 2011. Dr. Dong was selected as a Foreigner Research Fellow (a total of 3 recipients all over Japan) by NEC C&C Foundation in 2011. He is the recipient of The 12th IEEE ComSoc Asia-Pacific Young Researcher Award 2017, Funai Research Award 2018, NISTEP Researcher 2018 (one of only 11 people in Japan) in recognition of significant contributions in science and technology, The Young Scientists Award from MEXT in 2021, SUEMATSU-Yasuharu Award from IEIEC in 2021, IEEE TCSC Middle Career Award in 2021. He is Clarivate Analytics 2019, 2021, 2022 Highly Cited Researcher (Web of Science) and Foreign Fellow of EAJ.

Xiangjun Xin received the Ph.D. degree from Xidian University in 2009. He is currently a Professor in the College of Software Engineering, Zhengzhou University of Light Industry, Zhengzhou, China. His current research interests include quantum cryptography and information security.

Jian Li received the Ph.D. degree in computer application technology from the Beijing Institute of Technology, Beijing, China, in 2005. He is currently a Professor in the School of Cyberspace Security at Beijing University of Posts and Telecommunications, Beijing, China. His current research interests include quantum cryptography, blockchain and information security.

Xiu-Bo Chen received the Ph.D. degree in cryptography from the Beijing University of Posts and Telecommunications, Beijing, China, in 2009. She is currently a Professor in the School of Cyberspace Security at Beijing University of Posts and Telecommunications, Beijing, China. Her research interests include information security, blockchain, cryptography and quantum network coding.

Kaoru Ota was born in Aizu-Wakamatsu, Japan. She received M.S. degree in Computer Science from Oklahoma State University, the USA in 2008, B.S. and Ph.D. degrees in Computer Science and Engineering from The University of Aizu, Japan in 2006, 2012, respectively. Kaoru is currently a Professor and Ministry of Education, Culture, Sports, Science and Technology (MEXT) Excellent Young Researcher with the Department of Sciences and Informatics, Muroran Institute of Technology, Japan. From March 2010 to March 2011, she was a visiting scholar at the University of Waterloo, Canada. Also, she was a Japan Society of the Promotion of Science (JSPS) research fellow at Tohoku University, Japan from April 2012 to April 2013. Kaoru is the recipient of IEEE TCSC Early Career Award 2017, The 13th IEEE ComSoc Asia-Pacific Young Researcher Award 2018, 2020 N2Women: Rising Stars in Computer Networking and Communications, 2020 KDDI Foundation Encouragement Award, and 2021 IEEE Sapporo Young Professionals Best Researcher Award. She is Clarivate Analytics 2019, 2021, 2022 Highly Cited Researcher (Web of Science) and is selected as JST-PRESTO researcher in 2021, Fellow of EAJ in 2022.