J Med Syst (2018) 42: 147
https://doi.org/10.1007/s10916-018-0998-2

MOBILE & WIRELESS HEALTH

BMPLS: Blockchain-Based Multi-level Privacy-Preserving Location Sharing Scheme for Telecare Medical Information Systems

Yaxian Ji[1] · Junwei Zhang[1] · Jianfeng Ma[1] · Chao Yang[1] · Xin Yao[2]

Received: 28 February 2018 / Accepted: 18 June 2018 / Published online: 30 June 2018

Abstract

The sharing of patients' locations is an important part in mobile medical services and modern smart healthcare. Although location sharing based on blockchains has advantages on decentralization and openness, there is also a challenge to guarantee the security and the privacy of locations recorded in a blockchain. To this end, this paper investigates the location sharing based on blockchains for telecare medical information systems. Firstly, we define the basic requirements of blockchain-based location sharing including decentralization, unforgeability, confidentiality, multi-level privacy protection, retrievability and verifiability. Then, using order-preserving encryption and merkle tree, we propose a blockchain-based multi-level location sharing scheme, i.e. BMPLS. The analysis results show that our scheme satisfies the above requirements. Finally, the performance of our scheme is evaluated and the experiment results show that our scheme is efficient and feasible for both patients and medical workers. In a word, our scheme can be applied to realize privacy-preserving location sharing based on blockchains for telecare medical information systems.

Keywords Location sharing · Multi-level privacy preserving · Blockchain · Order-preserving encryption · Merkle tree

Introduction

To make healthcare smarter, hospitals trend to apply advanced information technology to implement dynamic intelligent management. With the development of wireless mobile network [1–3] and wearable technology [4, 5], mobile medical service [6, 7] and tele-medicine [8, 9] have emerged into telecare medical information systems (TMIS). For instance, IBM corporation integrates real time asset locator (RTAL) for medical applications to track and manage the location of patients, healthcare staff and devices. Furthermore, the location management of patients plays an important role in telecare for patients, such as the health management of chronic patients, the analysis of the distribution of patients with infectious diseases, long-term care for special patients and so on.

Traditional data sharing schemes [10, 11] are based on centralized management system, which is not conducive to the secure sharing of information with other medical institutions. At the same time, the records are at risk of being used illegally without the characteristic of openness because the regulatory agencies cannot access the data controlled by an institution in general. Therefore, the location sharing schemes based on centralized management system are not conducive to the development of TMIS from the view of resource sharing.

Different from centralized management system, peer-to-peer network [12] is decentralized which has advantages on the sharing of resource. In a peer-to-peer network, each participant can obtain and share information directly, i.e. each one can not only act as a user, but also as a provider to provide services for other parties.

A blockchain [13, 14], which is typically managed based on a peer-to-peer network, in an open, distributed ledger that can record transactions efficiently in a verifiable and permanent way. Due to the above characteristics, the blockchain technology has the potential to achieve a location sharing scheme for TMIS.

This article is part of the Topical Collection on *Blockchain-based Medical Data Management System: Security and Privacy Challenges and Opportunities*

✉ Junwei Zhang
jwzhang@xidian.edu.cn

[1] School of Cyber Engineering, Xidian University, Xi'an 710071, China

[2] School of Software, Central South University, Changsha 410075, China

Related works In 2008, S.Nakamoto [13] proposed Bitcoin based on blockchains as a cryptocurrency and worldwide payment system, which makes blockchains the core of the electronic currency in the following years. After Bitcoin, lots of cryptocurrency [15, 16] systems based on blockchains have being developed and widely used in many fields gradually.

However, the location sharing schemes based on blockchains are vulnerable to privacy illegal leakage from the perspective of patients. Guy Zyskind et al. [17] proposed a data storage scheme to protect personal data such as locations and contacts in a blockchain. Personal data is encrypted before it is stored into the blockchain in order to realize the confidentiality of records. Giacomo Brambilla et al. [18] proposed a location proof scheme in the blockchain. The proved location information is signed before it is recorded in the blockchain in order to achieve the verifiability of records in a blockchain. Obviously, the above two works cannot provide privacy protection on records in a blockchain.

It is well known that privacy protection, as an important issue in medical environment [19, 20] and many other applications [21–23], has been widely studied. K-anonymity [22] and differential privacy [23] are commonly used techniques for location privacy protection. However, these approaches will lead to the loss of information so that we cannot retrieve the intact location. As a result, they are not suitable for location sharing in TMIS when we need the intact location to obtain a precise medical care.

Location sharing in TMIS Compared to the location sharing schemes based on centralized management structure, blockchain-based location sharing in TMIS should satisfy not only confidentiality and privacy preserving but also the following requirements.

First, multi-level privacy protection should be provided for the location of patients in TMIS. One hand, location privacy perserving, as a basic security requirement of location-related services, should be provided in order to prevent the illegal leakage of personal location information in TMIS. The other hand, the location privacy in TMIS should be divided by multi-level for various services with differentiation on privacy requirements, since the different location-related services may have different privacy requirements. For example, we consider two researches on epidemic spread based on data from TMIS: the first one is to analyze the distribution of infectious diseases in a country, and the second one is to analyze the distribution of infectious diseases in the world. Obviously, the above two researches have different requirements on location privacy. Thus, multi-level privacy preserving is one of the required properties for location sharing in TMIS.

Second, retrievability of the intact location should be guaranteed to retrieve the real location from the records in a blockchain for some precise medical care applications, such as emergency medical assistance and so on. Obviously, the privacy protection schemes with information loss, such as k-anonymity, can not satisfy this property.

Third, verifiability of the shared location with privacy protection should be necessary for location sharing in TMIS, because a false information may lead to a wrong medical diagnosis which is unacceptable in TMIS. Therefore, medical workers, e.g. doctors, should be able to verify the validity of a shared location in order to give appropriate medical services in TMIS.

Our contributions Due to that a blockchain can only provide the anonymity of users but not the privacy preserving for the location information recorded on blocks, we need to use a privacy preserving technology to realize multi-level privacy protection for the records with location in blockchains. However, this study is very challenging with the following reasons. First, that the information recorded in a valid blockchain is fixed and hard to modify makes it difficult to realize the multi-level location privacy protection for various medical applications. Second, it is hard to verify the validity of the shared location when they are protected by multi-level privacy.

In this paper, we put emphasis on realization of multi-level privacy perserving location sharing based on blockchains for TMIS. First, in order to realize multi-level privacy, we adopt order-preserving encryption scheme(OPE) [24, 25], which allows comparison operations to be directly applied on encrypted data without decrypting the operands. Second, we apply merkle tree [26], which supports efficient and secure verification of large data structures, to provide verifiability of the shared location, i.e. the user can verify whether the location information received from other peers in a peer-to-peer network are undamaged and unaltered.

Our contributions in this paper are fourfold.

1. We classify the required properties of blockchain-based location sharing for TMIS including decentralization, unforgeability, confidentiality, multi-level privacy preserving, retrievability and verifiability.
2. We propose BMPLS, a novel blockchain-based privacy preserving location sharing scheme for TMIS. Scheme BMPLS can provide the location-based medical services between patients, medical workers, medical researchers and so on.
3. We theoretically analyze the security of BMPLS. We show that BMPLS satisfies the above required properties. At the same time, BMPLS is much more secure than the existing schemes.

4. We report experimental evaluations of BMPLS. Our results show that BMPLS is efficient and feasible for both patients and medical workers in TMIS.

Preliminaries

Order-preserving encryption

An order-preserving encryption (OPE) is a deterministic symmetric encryption scheme which preserves the order of plaintexts [24]. The definition is as follows.

Definition 1 (OPE) For $m \leq n, [m] = \{i|1 \leq i \leq m\}$ denotes the plaintext-space, $[n] = \{j|1 \leq j \leq n\}$ denotes the ciphertext-space. Suppose that $SE_{m,n} = (k, E_{m,n}, D_{m,n})$ is a deterministic symmetric encryption scheme, where k is the symmetric encryption key, $E_{m,n}$ is the deterministic symmetric encryption algorithm, and $D_{m,n}$ is the decryption algorithm satisfying: $D_{m,n}(E_{m,n}(x,k),k) = x$. We say that $SE_{m,n}$ is an OPE symmetric scheme if:

$$x < x' \Leftrightarrow E_{m,n}(x,k) < E_{m,n}(x',k) \quad (1)$$

Note that OPE in [27] has been proven that if the number x of known plaintext/ciphertext pairs satisfies $x = o(m^e)$, $0 < e < 1$ and $m^3 \leq n$,the probability of adversaries uncovering a plaintext is negligible.

Merkle tree

The main idea of merkle tree [26] is to construct a binary tree using a one-way hash function. The values of leaf nodes are the hash values of the data blocks. The values of the internal nodes are calculated from their child nodes. For example, if $node_i$ is the parent node of $node_j$ and $node_k$, then $node_i = Hash(node_j||node_k)$.

Each leaf value of the tree can be verified through its authentication path according to the known root. Therefore, the merkle tree can be used to verify integrity of data, and we only need to store the root of the merkle tree to authenticate any leaf nodes. Simultaneously, since only hash functions are calculated in the verification process, the computational costs of verification are quite low.

Problem formulations

System model

The system model is shown in Fig. 1. In this model, the parties can be classified as three entities including location data owner(LDO), location data requestor(LDR), and the miners. Regularly, LDO records the location-related information into a blockchain. As shown in Fig. 1, LDRs who want to derive the information may need to interact with the LDO before obtaining the location-related information from the blockchain. Each block of the blockchain in our scheme is composed of multiple records from different LDOs. Moreover, the location records with different timestamps from a same LDO should be connected in chronological order. More specifically,

LDO LDO can generate the location-related data and record it on the blockchain for sharing with LDR in TMIS. In the sharing procedure, LDO may send LDR different size of areas instead of precise location to achieve multi-level privacy protection according to different requirements.

LDR LDR can retrieve the location-related information with the help of LDO according to the data in the blockchain. Different LDRs have different requirements of location accuracy. For example, medical caregivers need exact locations, chronic disease management personnel need small areas to distinguish LDO's approximate locations and the doctors in the infectious disease control center need different size of regions according to the risk of infection.

Miners Miners are responsible for the blockchain mining to maintain the blockchain. They aim to complete the proof-of-work tasks and gain rewards from blockchains in TMIS.

Threat model

The members in the system have potential to play the role of the attackers:

LDO LDOs as providers of location data may have the following dishonest behaviors: First, some LDOs may repudiate the location data recorded in the blockchain. Second, they may return the deceptive result about the recorded location information to LDRs.

LDR LDRs as requestors of location under privacy protection maybe want to obtain more detail information about LDOs' locations for some personal reasons. In other word, LDRs may attempt to infer a more accurate area according to the area obtained by LDOs. Furthermore, LDRs may attempt to completely retrieve the precise location of LDOs.

Miners Miners as the blockchain users may try to modify the records in a blockchain, launch an unauthorized access to the personal medical data, leak the private location information and so on.

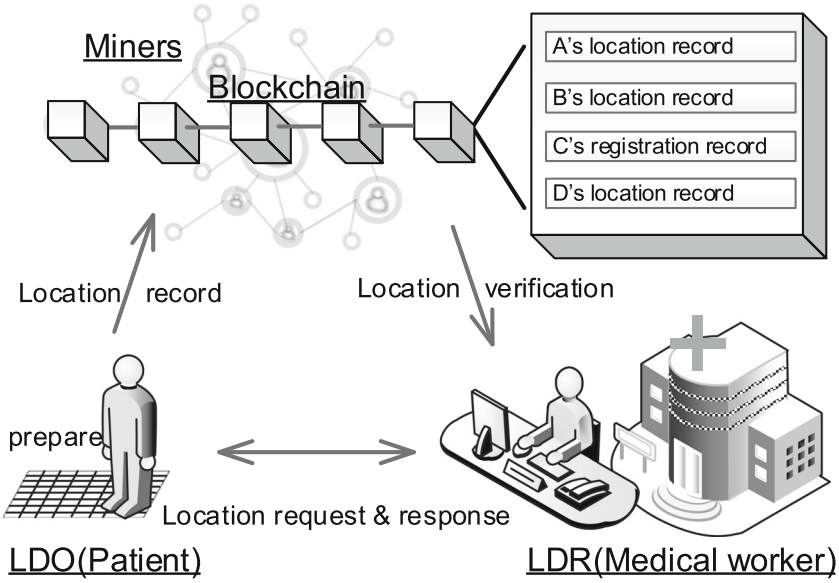

Fig. 1 System model

Design goals

Accoring to the requirements and the adversary model of location sharing based on blockchains for TMIS, the proposed scheme BMPLS should satisfy the following properties:

1. Decentralization. Our scheme should achieve a decentralized management for location records between patients and medical workers from several medical institutions.
2. Unforgeability. Our scheme should ensure unforgeability of patients' location records. For instance, an illegal modification on the patients' locations may lead to an unpredictable deviation in medical analysis results which may trigger an irreversible medical accident.
3. Confidentiality. Our scheme should guarantee the confidentiality to prevent the disclosure of location records to unauthorized users because any TMIS cannot be considered secure if it could not resist to unauthorized access to the medical data.
4. Multi-level privacy protection. Our scheme should provide multi-level privacy perserving for the location of patients in TMIS.
5. Retrievability. Our scheme should achieve retrievability on patients' location records for some special or urgent medical conditions.
6. Verifiability. Our scheme should provide verifiability of the shared location with privacy protection in order to avoid the wrong medical diagnosis based on false location information.

The proposed scheme

Scheme BMPLS is designed under a reasonable assumption that the location information generated by LDOs are correct and authentic during the submission procedure. Note that there are some very efficient solutions [28] to provide location verification services which can be used to guarantee the authenticity of the submitted location information. But it is out of scope since our scheme focuses on privacy protection of the location sharing process.

Scheme BMPLS consists of the following three phases: the initialization phase, the record generation phase and the location sharing phase.

Initialization

Registration record is the first record of a LDO to keep the initialization information for the followed location sharing. First, a rectangular region which denotes the whole region that the LDO can visit should be determined. Second, the LDO translates the geographic coordinate (longitude and latitude) of the location into a cartesian coordinate, where the vertex at the left bottom of the region is the origin of the cartesian coordinate. In such a cartesian coordinate, the region can be set as $S = \{(x, y)|0 \leq x \leq X, 0 \leq y \leq Y\}$. Third, the LDO partitions the region recursively into grids according to the quad-tree function. Let N denote the number of the LDO's partition levels. According to the security requirements of OPE [27], N should satisfy:

$$2^N = o(min\{X, Y\}^e), 0 < e < 1 \quad (2)$$

We define the function $Parti(S, N)$ to partition the region S according to partition level N, as shown in Eq. 3:

$$Parti(S,N) = \{x_i | 1 \le i \le 2^N \wedge x_i = i \times \frac{X}{2^N}\} \cup \{y_i | 1 \le i \le 2^N \wedge y_i = i \times \frac{Y}{2^N}\} \quad (3)$$

A merkle tree named $verTree$ is generated according to $\{x_1, x_2, ..., x_{2^N}\}$, and a merkle tree named $horTree$ is generated according to $\{y_1, y_2, ..., y_{2^N}\}$. Figure 2 shows an example of generation of merkle tree when $N = 3$. Finally, the LDO puts the registration record $regRec$ into a block of the blockchain. Algorithm 1 shows the details of generation of registration record.

Note that in lines 3-4 of Algorithm 1, $E_{X,X'}()$ and $E_{Y,Y'}()$ denote the OPE function with plaintext-spaces X, Y and ciphertext-spaces X', Y' respectively, where $X^3 \le X', Y^3 \le Y'$. In lines 8-9, $genMT()$ denotes the function to generate the merkle tree using leaf nodes. In line 10, $Translate^{-1}$ denotes the function for LDRs to retrieve the location record into the real geographical location. The LDO should sign the registration record and broadcast to the network after running of Algorithm 1. After miners generate a valid block including the registration record of LDO, the initialization phase is finished. The specific realizations of signature and mining are not a focus of our paper, readers can refer to [13, 14, 29].

Algorithm 1 Generation of registration record

Input:
Region $S = \{(x, y) | 0 \le x \le X, 0 \le y \le Y\}$; Maximum level of location partition N; LDO's secret key $k_{LDO} = k^x_{LDO} || k^y_{LDO}$

Output:
Registration record $regRec$

1: $\{x_1, x_2, ..., x_{2^N}\} \cup \{y_1, y_2, ..., y_{2^N}\} \leftarrow Parti(S, N)$;
2: **for** $i = 1; i \le 2^N; i++$ **do**
3: $\quad ciph^x_i = E_{X,X'}(k^x_{LDO}, x_i)$;
4: $\quad ciph^y_i = E_{Y,Y'}(k^y_{LDO}, y_i)$;
5: $\quad node^x_i = Hash(i || x_i || ciph^x_i)$;
6: $\quad node^y_i = Hash(i || y_i || ciph^y_i)$;
7: **end for**
8: $horTree \leftarrow genMT(node^x_1, node^x_2, ..., x^x_{2^N})$;
9: $verTree \leftarrow genMT(node^y_1, node^y_2, ..., node^y_{2^N})$;
10: $regRec \leftarrow Sig_{LDO}(Translate^{-1} || horTree_{root} || verTree_{root})$;
11: **return** $regRec$;

Location record

In this phase, the process of a LDO recording location information into the blockchain is illustrated. Unlike bitcoin, each block of the blockchain in our scheme is not composed of transactions, but registration records (generated in initialization phase) and location records, as shown in Fig. 1. Without loss of generality, we assume that LDO wants to put one location record $record^{LDO}_j$ into the blockchain. Algorithm 2 shows the detailed generation process of location record.

Note that in lines 5 and 6 of Algorithm 2, the hash value of location plaintext $LocHash_j$ and OPE ciphertext $OpeHash_j$ are recorded in order to make LDRs have access to the verification of the shared location records in location sharing phase. In the line 7, $Enc()$ denotes symmetric encryption function, $SymCiph_j$ is recorded to provide the retrievability for some special medical conditions. In the line 9, $record^{LDO}_j$ references previous record's identity $recId^{LDO}_{j-1}$. The structure of location records is illustrated in Fig. 3.

Algorithm 2 Generation of location record

Input:
LDO's j-th location(x_j, y_j); LDO's secret keys $k_{LDO} = k^x_{LDO} || k^y_{LDO}, k_{sym}$

Output:
Location record $record^{LDO}_j$

1: **LDO executes:**
2: $ciph^x_j \leftarrow E_{X,X'}(k^x_{LDO}, x_j)$;
3: $ciph^y_j \leftarrow E_{Y,Y'}(k^y_{LDO}, y_j)$;
4: $ciph_j \leftarrow ciph^x_j || ciph^y_j$;
5: $OpeHash_j \leftarrow Hash(ciph_j)$;
6: $LocHash_j \leftarrow Hash(x_j || y_j)$;
7: $SymCiph_j \leftarrow Enc(k_{sym}, x_j || y_j)$;
8: $LocInfo_j \leftarrow OpeHash_j || LocHash_j || SymCiph_j || timestamp_j$;
9: $record^{LDO}_j \leftarrow Pub_{LDO} || LocInfo_j || recId^{LDO}_{j-1} || signature_{LDO}$;
10: **return** $record^{LDO}_j$;

Location sharing

The location sharing phase consists of location sharing stage and location verification stage. Without loss of generality, we assume that LDR wants to obtain one location information $record^{LDO}_k$ of LDO.

Step1 Location sharing

According to the requirement of location sharing with LDR, LDO makes varying levels of privacy protection. (1) If LDR is totally trusted and the intact location should be provided to LDR, the concrete location record will be

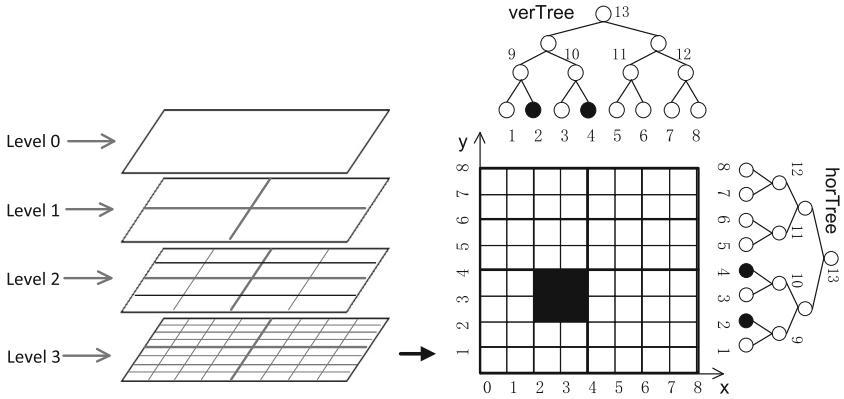

Fig. 2 Generation of merkle trees

decrypted and sent to LDR by LDO(we denote $n = \infty$ for short in this case). (2) If LDR is semi-trusted with a privacy protection level n, LDO will determine the size of the rectangular border according to n and return the response to LDR. The response consists of the OPE ciphertexts of the location, location border information and some required nodes of merkle tree to help LDR to compute the root of this merkle tree and verify the shared location information. The details of location sharing stage are illustrated in Algorithm 3.

Algorithm 3 Location sharing

Input:
location record ID $recoId_k^{LDO}$; session key between LDO and LDR $k_{session}$; privacy protection level n

Output:
shared location information $response$

1: **LDR executes:**
2: $request \leftarrow Pub_{LDR}||recId_k^{LDO}||n||signature_{LDR}$;
3: LDR sends $request$ to LDO;
4: **LDO executes:**
5: **if** $n = \infty$ **then**
6: $response \leftarrow Enc(k_{session}, x_k||y_k)||Pub_{LDR}(k_{session})$;
7: **else if** $0 \leq n \leq N$ **then**
8: find the border$\{x_{min}, x_{max}, y_{min}, y_{max}\}$ in level n;
9: $borInfo_{id_1} \leftarrow id_1||x_{min}||ciph^x_{id_1}$;
10: $borInfo_{id_2} \leftarrow id_2||x_{max}||ciph^x_{id_2}$;
11: $borInfo_{id_3} \leftarrow id_3||y_{min}||ciph^y_{id_3}$;
12: $borInfo_{id_4} \leftarrow id_4||x_{max}||ciph^y_{id_4}$;
13: $borInfo \leftarrow borInfo_{id_1}||borInfo_{id_2}||borInfo_{id_3}||borInfo_{id_4}$;
14: $nodes^x \leftarrow \{node^x_{x1}, node^x_{x2}, ...\}$;
15: $nodes^y \leftarrow \{node^y_{y1}, node^y_{y2}, ...\}$;
16: $response \leftarrow Enc(k_{session}, ciph_k||borInfo||nodes^x||nodes^y)||Pub_{LDR}(k_{session})$;
17: **end if**
18: **return** $response$;

In lines 14-15, $nodes^x$ and $nodes^y$ are the required nodes for LDR to calculate the $horTree_{root}$ and $verTree_{root}$. At the same time, privacy level n should be determined according to the requirement of the forthcoming medical service and the authentication result between LDO and LDR. As far as we know, the most popular authentication methods can be classified as password authentication [30], multi-factors authentication [31, 32], biometrics-based authentication [33], group-based authentication [34, 35] and so on. However, the authentication of LDR is not the main concern of BMPLS.

Step2 location verification

After receiving the response from LDO, LDR verifies the location by means of location records and registration record in the blockchain in order to prevent LDO from deception of the location. The border information has been determined when LDO registered before, and the merkle tree's root can be used to verify the response information. The details of location verification are illustrated in Algorithm 4.

(1) When LDR is totally trusted, LDR receives intact location information. As shown in lines 2-5 of Algorithm 4, if the hash value of the location plaintext equals the hash value $LocHash_k$ in the blockchain, LDR accepts the location records .
(2) When the LDR is semi-trusted, LDR checks whether the border information is consistent with that in the registration record, as shown in lines 7-13 of Algorithm 4. Further, LDR judges whether the $ciph_k$ is consistent with that in the location record by hash function and whether the location point is located in the location borders by comparison of OPE ciphertexts in line 15.

Algorithm 4 Location verification

Input:
response from LDO $response$; record in the blockchian $record_k^{LDO}$; session key with LDO $k_{session}$

Output:
Bool varaiable $isAccepted$

initialize $isAccepted \leftarrow False$;
if $x'_k||y'_k \leftarrow Dec(k_{session}, response)$ **then**
  if $Hash(x'_k||y'_k) = record_k^{LDO}.LocInfo_k.LocHash_k$ **then**
    $isAccepted \leftarrow True$;
  end if
else if $ciph_k||borInfo||nodes^x||nodes^y \leftarrow Dec(k_{session}, response)$ **then**
  $borInfo_{id_1}||borInfo_{id_2}||borInfo_{id_3}||borInfo_{id_4} \leftarrow borInfo$;
  $node^x_{id_1} \leftarrow Hash(borInfo_{id_1})$;
  $node^x_{id_2} \leftarrow Hash(borInfo_{id_2})$;
  $node^y_{id_3} \leftarrow Hash(borInfo_{id_3})$;
  $node^y_{id_4} \leftarrow Hash(borInfo_{id_4})$;
  $horTree_{root'} \leftarrow MerkleHash\{nodes^x, node^x_{id_1}, node^x_{id_2}\}$;
  $verTree_{root'} \leftarrow MerkleHash\{nodes^y, node^y_{id_3}, node^y_{id_4}\}$;
  if $horTree_{root'} = horTree_{root}$ **and** $verTree_{root'} = verTree_{root}$ **then**
    if $Hash(ciph_k) = record_k^u.LocInfo_k.OpeHash_k$ **and** $borInfo_{id_1}.ciph^x_{id_1} < ciph_k.ciph^x_k < borInfo_{id_2}.ciph^x_{id_2}$ **and** $borInfo_{id_3}.ciph^y_{id_3} < ciph_k.ciph^y_k < borInfo_{id_4}.ciph^y_{id_4}$ **then**
      $isAccepted \leftarrow True$;
    end if
  end if
end if
return $isAccepted$;

Discussion of scheme BMPLS

Appropriate values of *N* To satisfy the requirements of multi-level location privacy preserving in telecare medical information systems, we discuss the appropriate values of N to be set in reality.

According to initialization phase of BMPLS, N denotes the total number of selectable location privacy preserving levels. Given an acceptable minimum privacy protect area with side length l, and whole region to be covered with side length L, $N = \lfloor log_2 \frac{L}{l} \rfloor$. If $\frac{L}{l} = 3 \times 10^4$, the value of N just reaches 14. To facilitate the understanding, we suppose that the acceptable minimum privacy preserving region of a LDO are squares with side length of 150 meters(street level). If the area of required whole region to be covered which approaches to the area of city such as Phoenix, then $N = 8$; If the area of required region which is bigger than that of State of Arizona, then $N = 12$; If covered area reaches around $609km^2$ which is larger than most countries all over the world, then $N = 14$.

Consequently, even if the system needs to cover a huge region, the value of N will not be large. Moreover, the height of merkle tree generated by LDO in initialization phase which equals N would be low. Furthermore, the computational costs of LDR in location verification stage is small.

Decentralized consensus and incentives Based on different requirements, medical systems can select applicable decentralized consensus. Here, proof-of-work is available and applicable. If proof-of-work is implemented in our scheme to achieve decentralized consensus like bitcoin, miners need to randomly append a nonce to calculate hash value of the block that satisfy the required zero bits. Once a new block is generated, it is added to the blockchain after broadcast. The system can support large amounts of network nodes under this mechanism.

Incentives are the key factors to maintain the sustainable running of the blockchain. We come up with an optional and simple scheme as follows. Miners maintain the blockchain to gain subsidies in the form of medical credits as rewards only if they generate valid block. Patients who hold medical credits have access to location-based medical services, in other words, they need medical credits to upload location records into the blockchain to share their location information with medical workers. If medical workers need location information for medical analysis, they also need to disburse medical credits. Obviously, BMPLS can implement more elaborate incentives to meet specific requirements in complex medical environments.

Analysis of scheme BMPLS

In this section, we demonstrate that scheme BMPLS satisfies all the required properties. At the same time, we compare BMPLS with related works.

Decentralization

Decentralization is the core property of blockchains due to its peer-to-peer structure. Therefore, by storing data across its distributed network, blockchains eliminate the risk of data being held centrally and entire system is not centralized managed by any third party. Every node of its network has a copy of the blockchain, and data on the blockchain is maintained by massive database replication. Moreover, The rights and duties of all the nodes are equal.

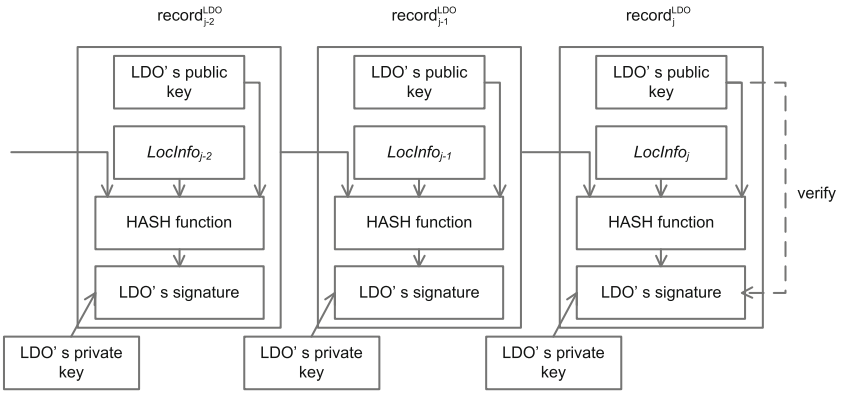

Fig. 3 Structure of location records

We adopt the blockchain to store the LDO's registration records such as $regRec$ which are used to verify the correctness of $borInfo$, and location records such as $record_i^{LDO}$ for arbitrary i which are used to verify the location points(x_i, y_i). So location information is not controlled by any third party and all the entities of the network have access to all the recorded location information. For this reason, the sharing of location information between the patients and medical workers can be achieved in BMPLS.

Unforgeability

In blockchains, each block $block_i$ except for the first block, contains the hash value of last block $Hash(block_{i-1})$, and links after $block_{i-1}$. To tamper with a record in a pasted block $block_{i-1}$, adversaries have to redo proor-of-work of the $block_{i-1}$ and all the following blocks. Additionally, they must catch up with all other honest entities to make modified blockchain the longest one since entities store longest chain as a copy each time. Adversaries have a negligible probability to catch up with honest entities unless they can control more than 51% of the nodes in the blockchain network.

In BMPLS, all the location information including LDO's registration $regRec$ and location records such as $record_i^{LDO}$ for arbitrary i is stored in the blockchain. Therefore, unforgeability is also guaranteed in our scheme to protect our location data from being tempered with.

Confidentiality

Location information in the blockchain including registration records such as $regRec$ and location records such as $record_i^{LDO}$ for arbitrary i. In $regRec$, $horTree_{root}$ and $verTree_{root}$ are the roots of hash merkle trees. Network nodes can recover nothing because of hash function's property of non-invertible. In $record_i^{LDO}$, location (x_j, y_j) is presented by means of $LocInfo_i$, which contains $OpeHash_i = Hash(ciph_j)$, $LocHash_i = Hash(x_j||y_j)$ and $SymCiph_i = Enc(k_{sym}, x_j||y_j)$. Because Hash function is non-invertible, and k_{sym} is the secrete key of symmetric encryption which is kept by LDO secretly, so ciphertext of symmetric encryption function cannot be decrypted without the encryption key k_{sym}. Consequently, adversaries have a negligible probability to recover the location information without communicating with LDO in BMPLS.

Multi-level location privacy protection

LDO can achieve multi-level location privacy protection. As shown in Fig. 2, LDO partitions the region into N levels. For one location request such as request for $record_j^{LDO}$, LDO chooses appropriate level $n(1 \leq n \leq N)$, and returns borders' information of (x_j, y_j) which corresponds to the merkle trees' nodes as illustrated in the black parts of Fig. 2 as well as OPE encryption $ciph_j$. As a result, LDR obtains the plaintexts of border $\{x_{min}, x_{max}, y_{min}, y_{max}\}$ which determined by LDO.

– Semi-trusted LDR has a negligible probability to reduce the LDO's privacy protection region for the following reasons:

  (1) In our scheme, borders are strictly aligned and have no overlapped region, so adversaries cannot reduce the privacy protection level by requesting overlapped regions to generate smaller region.

  (2) The LDR has a negligible probability to get other relations except for the order between the ciphertexts such as arbitrary $ciph_i^x$ and $ciph_j^x$. Since the adopted OPE algorithm is POPF-CCA(pseudorandom order-preserving function against chosen-ciphertext attack) secure, so $Ditance(x_j, y_j)$ cannot be reflected from $Ditance(ciph_i, ciph_j)$.

  (3) Ciphertexts of vertical lines such as $ciph_i^x = E_{X,X'}(k_{LDO}^x, x_i)$ and Ciphertexts of horizontal lines such as $ciph_j^y = E_{Y,Y'}(k_{LDO}^y, y_j)$ cannot leak location privacy of each other. Where $E_{X,X'}()$ denotes OPE encryption, X denotes plaintext-space, X' denotes ciphertext-space, k_{LDO}^x denotes key of OPE, and

x_i denotes horizontal axis of the location point. Accordingly, $ciph_i^x$ is determined by above parameters. Because $ciph_i^x$ and $ciph_i^y$ are calculated with different secret keys named k_{LDO}^x and k_{LDO}^x which are generated by the randomized key generation algorithm κ separately, with different plaintext-spaces X and Y, and with different ciphertext-spaces X' and Y' as well. So there is no correlation between $ciph_i^x$ and $ciph_i^y$ even though the x_i is the same as y_i. Therefore, there is no location privacy disclosure between $ciph_i^x$ and $ciph_j^y$ for arbitrary i and j.

– Semi-trusted LDR has a negligible probability to retrieve the location plaintext. LDO produced 2^N numbers of $(x_i||ciph_i^x)$ and 2^N numbers of $(y_i||ciph_i^y)$ in total. To prevent the location plaintexts from being retrieved, we have set $2^N = o(min\{X, Y\}^e), 0 < e < 1, X^3 \leq X'$ and $Y^3 \leq Y'$, which indicates the relationship between the all the plaintext/ciphertext pairs and the plaintext-spaces according to [27]. Therefore, there is a negligible probability to retrieve the location plaintexts even though adversaries hold all $(x_i||ciph_i^x)$ and $(y_i||ciph_i^y)$ in total $(1 \leq i \leq 2^N)$.

Retrievability

Arbitrary location record $record_j^{LDO}$ contains $SymCiph_j = Enc(k_{sym}, x_j||y_j)$, where $Enc()$ denotes symmetric encryption, and k_{sym} is kept secretely by LDO. In some emergent or special medical situation, location information $(x_j||y_j)$ of LDO in the blockchain must be completely retrieved. LDO can use k_{sym} to decrypt arbitrary $SymCiph_j$ so as to implement the retrievability property. To ensure the confidentiality, k_{sym} should not be propagated to others except in some special cases or for some special trusted requestors. Therefore, BMPLS can retrieve location points while implementing multi-level privacy preserving.

Verifiability

Semi-trusted LDR can verify the correctness and integrity of borders. If LDO returns false border information, such as $borInfo^* = id_1||x_{id_1}||ciph_{id_2}^x$, LDR could calculate $horTree_{root}^*$ according to the authentication path of merkle tree. For LDO, the probability of finding other numerical values to calculate with $borInfo^*$ together to achieve that $horTree_{root}^* = horTree_{root}$ is negligible due to collision resistance of hash function. Moreover, if LDO returns OPE ciphertext $ciph_j^* \neq ciph_j$, LDR could verify $ciph_j^*$ he received by $OpeHash_j$ in the blockchain. Finally, LDR determines whether the $location_j$ surrounded by the border by simple numerical comparisons.

Totally trusted LDR can verify the location(x_j, y_j) according to $LocHash_j$ in the $record_j^{LDO}$. If LDO returns false location information, such as $Enc(k_{session}, x_j^*||y_j)$, LDR could decrypt the message and calculate $LocHash_j^* = Hash(x_j^*||y_j)$. For LDO, the probability of finding x_j^* different from x_j to ensure $LocHash_j^* = LocHash_j$ is negligible due to collision resistance of hash function.

Comparison

In this section, we compare our scheme with the related schemes including UBFP-POL [18], UB-PPD [17] and k-anonymity [22]. Table 1 shows the comparison results, where "√" means satisfied, "×" means dissatisfied and "–" means uninvolved.

It is obvious that UBFP-POL [18] and UB-PPD [17] cannot provide multi-level privacy protection, while k-anonymity [22] cannot realize the property of retrievability. Therefore, our scheme BMPLS, which satisfies all the required properties, can be applied to provide privacy preserving location sharing for TMIS.

Performance evaluation

In this section, we mainly focus on evaluation of computation overhead of our proposed scheme. The performance evaluation consists of three parts according to three phases of scheme BMPLS, i.e. initialization, location record and location sharing. The experiments are implemented on a PC(CPU:Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz 2.71GHz, RAM:8G, OS:Windows 10) using python-3.6.1.

Table 1 Comparison with related works

Schemes	UBFP-POL [18]	UB-PPD [17]	K-anonymity [22]	Our scheme
Decentralization	√	√	-	√
Unforgeability	√	√	-	√
Confidentiality	×	√	√	√
Multi-level protection	×	×	√	√
Retrievability	-	-	×	√
Verifiability	-	-	-	√

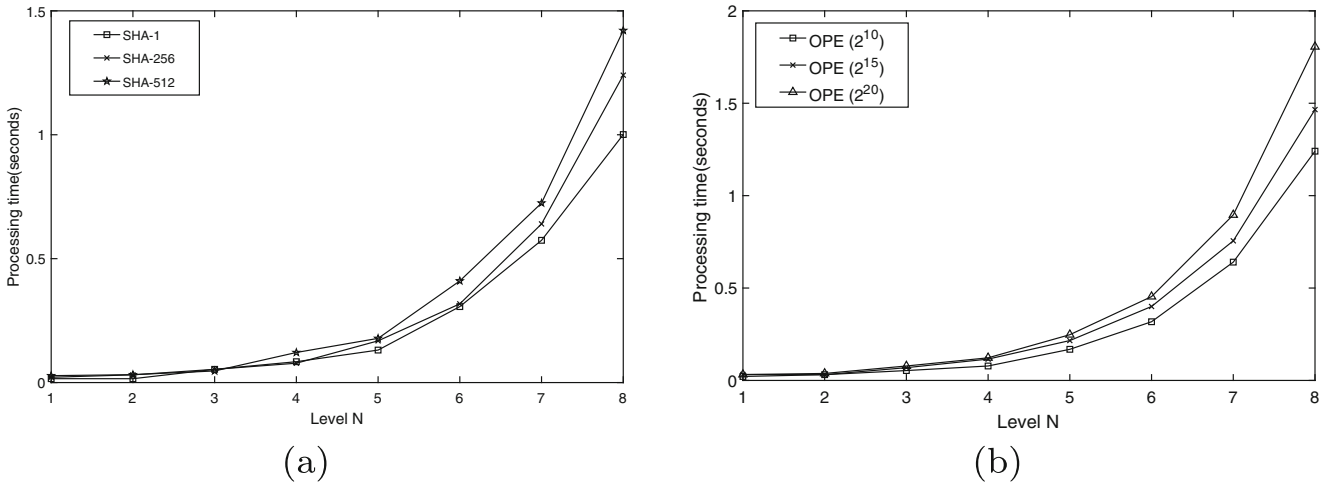

Fig. 4 Computation overhead in initialization phase: (**a**) Evaluation with different hash functions; (**b**) Evaluation with different OPEs

Initialization On the initialization phase of our scheme, a LDO who wants to record the locations into the blockchain must partition the domain recursively into grids. Next, the LDO needs to calculate the OPE ciphertexts of all the dividing lines and use the ciphertexts to generate two merkle trees.

In Fig. 4a, we adopt different hash functions to evaluate the performance in the initialization phase when the plaintext-space of OPE is $0 - 2^{10}$(OPE(2^{10}) for short). We notice that different hash functions lead to slightly different computation overhead. As illustrated in Fig. 4b, we evaluate the performance of the initialization phase based on OPE with different plaintext-spaces when hash function is SHA-256. The results show that larger plaintext-spaces of OPE will lead to slightly higher computation costs. At the same time, we find that the computation overhead is approximately following an exponential relationship with the partition level N. When $N = 10$, the number of minimum grids in the region is up to $4^{10} = 1048576$ with around 5 seconds of computation cost. Although the initialization phase is time-consuming compared to related works such as UBFP-POL [18], this phase, which can be implemented off-line, needs to be executed only once during the running of our scheme.

Location record In this phase, we evaluate the computation overhead of generation of location record. In the first experiment shown in Fig. 5a, we select OPE(2^{10}), SHA-256, and compare our scheme BMPLS with scheme UBFP-POL [18] using RSA-1024 and RSA-2048 respectively. In the second experiment shown in Fig. 5b, we select RSA-1024 and SHA-256, and evaluate the computation overhead with OPE under different plaintext-spaces. Because scheme BMPLS applies OPE to guarantee the security and privacy

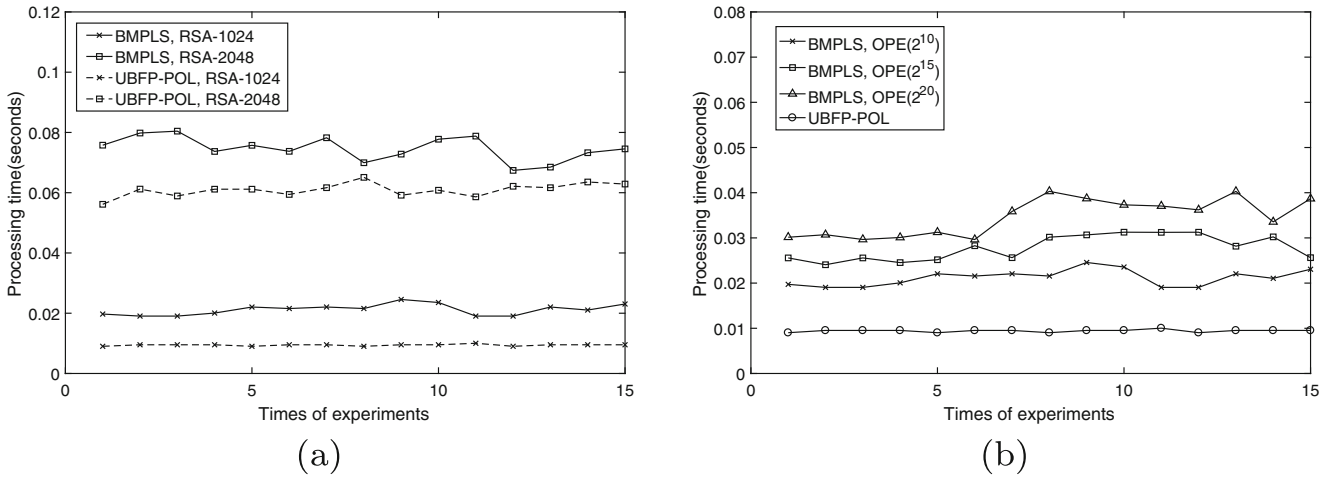

Fig. 5 Computation overhead of location record in different cryptographic algorithms: (**a**) Evaluation with different RSA algorithms; (**b**) Evaluation with different OPEs

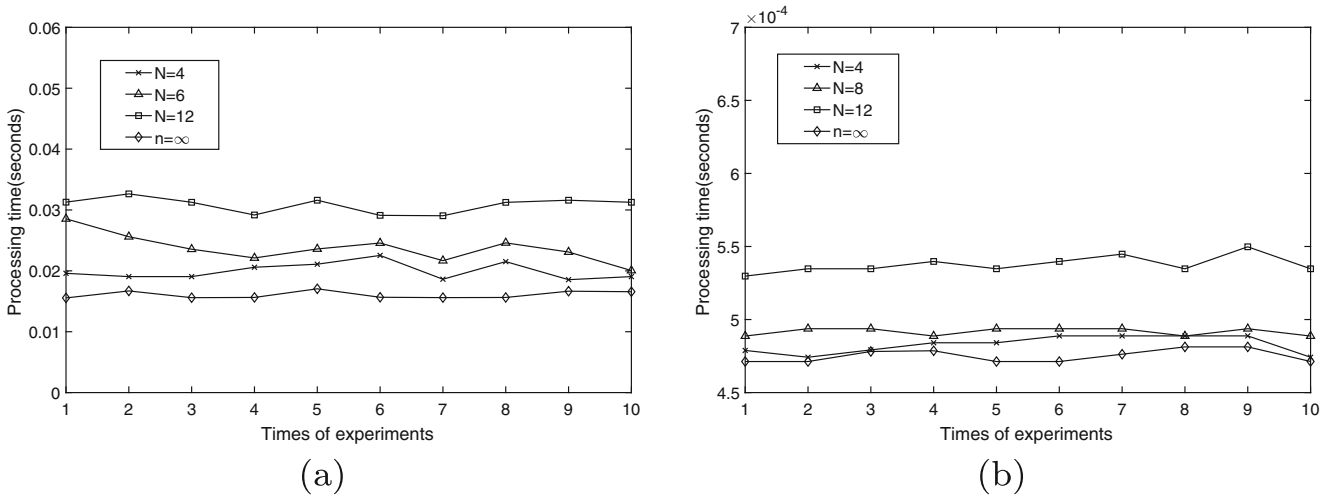

Fig. 6 Computation overhead in the location sharing phase: (**a**) Computation overhead of LDR; (**b**) Computation overhead of LDO

requirements of location sharing for TMIS, our scheme has slightly higher computation overhead than UBFP-POL which records location plaintexts into the blockchain and does not provide privacy protection.

Location sharing In this phase, a LDO can share location information based on multi-level privacy protection for different LDRs in our scheme. According to the region's partition levels N, we use OPE(2^{20}), SHA-256, RSA-1024, and evaluate the computation overhead of LDR and LDO respectively, shown in Fig. 6a and b. We can find that the processing of sharing intact location information ($n = \infty$) has the lowest computation burden, and the computation overhead of sharing location with higher partition level will be larger than that of sharing location with lower partition level.

In many medical applications, such as treatment of chronic diseases, the trajectory of a patient, which consists of lots of discrete locations, should be shared for medical workers in order to obtain a long term medical care. Thus, the performance of a location sharing scheme should be also efficient in case of multi-location sharing for TMIS.

We denote the multi-location set as $S = \{record_1, \ldots, record_i\}$ which consists of discrete locations of LDO. We assume that all the locations in S are distributed in different borders which is the worst case for multi-location sharing in our scheme. According to the number of locations in S, i.e.$|S|$, we use OPE(2^{20}), SHA-256, N=12, RSA-1024, and evaluate the computation overhead of LDR and LDO respectively in different schemes. As illustrated in Fig. 7a, the computation cost of LDR in UBFP-POL increases almost linearly with $|S|$ rapidly. Notably, LDRs

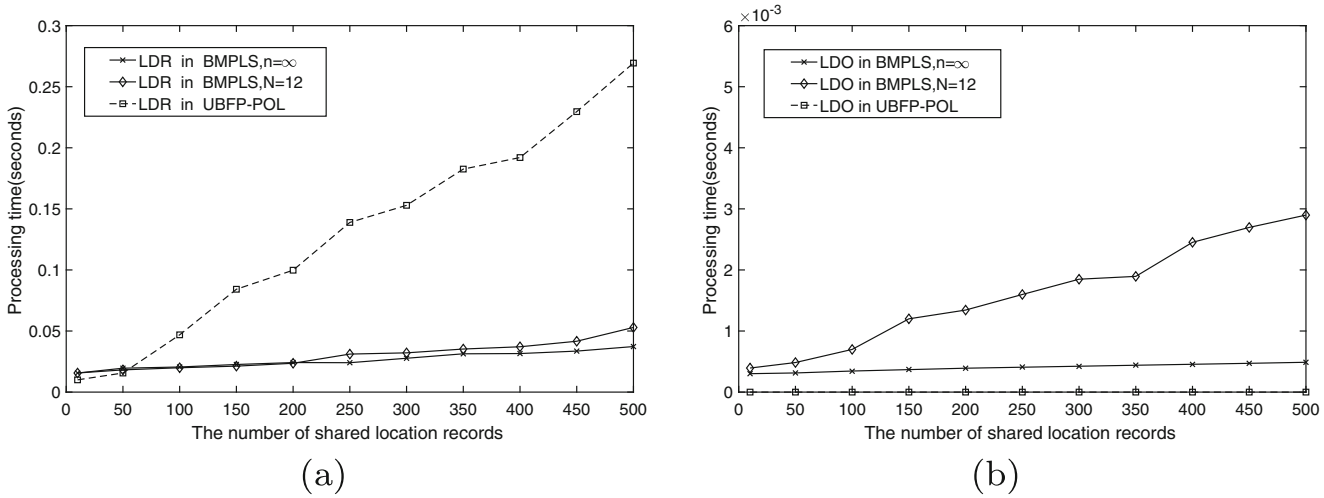

Fig. 7 Computation overhead of multi-location sharing in different schemes: (**a**) Computation overhead of LDR; (**b**) Computation overhead of LDO

in our scheme have much lower computation overhead than that of UBFP-POL when $|S| >> 50$. Furthermore, semi-trusted LDRs have a slightly higher computation overhead than trusted LDRs who can retrieve intact locations. As shown in Fig. 7b, there is no computation overhead for LDO in scheme UBFP-POL. Although our scheme has worse performance in LDO of multi-location sharing than scheme UBFP-POL, the computation overhead of returning locations borders and intact locations are just 3ms where $N = 12$ and 0.5ms where $n = \infty$ when $|S| = 500$ which is still efficient and acceptable for a long term medical care in TMIS.

Above all, our scheme is still efficient and feasible for TMIS in practice. In comparison with related works, our scheme enhances both the security and multi-level privacy of location sharing without sacrificing too much computation overhead.

Conclusions

In this paper, we propose BMPLS, a novel multi-level privacy preserving location sharing scheme based on blockchains for TMIS. LDOs could share their location records with different LDRs and achieve muti-level privacy protection for different LDRs. Different from existing schemes, our scheme enhances security and flexibility of privacy protection. In particular, our scheme can achieve complete retrievability of the location without loss of information. As a further contribution, analysis proves that our scheme can satisfy all the requirements we proposed. Finally, the experimental results show its efficiency in practice.

Funding Information This study was funded by National Natural Science Foundation of China (61472310, U1536202, U1405255, 61672413, 61672415, 61671360, 61602360, 61702404), the China 111 project (grant B16037).

Compliance with Ethical Standards

Conflict of interests The authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. He, D., Kumar, N., and Chilamkurti, N., A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. *Inf. Sci.* 321:263, 2015.
2. He, D., Zeadally, S., and Wu, L., Certificateless public auditing scheme for cloud-assisted wireless body area networks. *IEEE Systems Journal*, 2015.
3. Wang, D., Cheng, H., He, D., and Wang, P., On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices. *IEEE Systems Journal*, 2016.
4. Chao, H. C., Zeadally, S., and Hu, B., Wearable computing for health care. *J. Med. Syst.* 40(4):87, 2016.
5. Mezghani, E., Exposito, E., Drira, K., and Silveira, M. D., A semantic big data platform for integrating heterogeneous wearable data in healthcare. *J. Med. Syst.* 39(12):185, 2015.
6. He, D., Zeadally, S., Kumar, N., and Lee, J. H., Anonymous authentication for wireless body area networks with provable security. *IEEE Syst. J.* 11(4):2590, 2017.
7. Jiang, Q., Ma, J., Yang, C., Ma, X., Shen, J., and Chaudhry, S. A., Efficient end-to-end authentication protocol for wearable health monitoring systems. *Comput. Electr. Eng.* 63:182, 2017.
8. He, D., Chen, J., and Zhang, R., A more secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(3):1989, 2012.
9. He, D., and Zeadally, S., Authentication protocol for an ambient assisted living system. *IEEE Communications Magazine* 53(1):71, 2015.
10. Shen, J., Shen, J., Chen, X., Huang, X., and Susilo, W., An efficient public auditing protocol with novel dynamic structure for cloud data. *IEEE Trans. Inf. Forensic. Secur.* 12(10):2402, 2017.
11. Shen, J., Liu, D., Bhuiyan, M. Z. A., Shen, J., Sun, X., and Castiglione, A., Secure verifiable database supporting efficient dynamic operations in cloud computing. *IEEE Transactions on Emerging Topics in Computing*, 2017.
12. Bandara, H. D., and Jayasumana, A. P., Collaborative applications over peer-to-peer systems–challenges and solutions. *Peer-to-Peer Netw. Appl.* 6(3):257, 2013.
13. Nakamoto, S., Bitcoin: A peer-to-peer electronic cash system, Consulted, 2008.
14. Swan, M., Blockchain: Blueprint for a new economy. O'Reilly Media, Inc, 2015.
15. Park, S., Pietrzak, K., Alwen, J., Fuchsbauer, G., and Gazi, P., Spacecoin: A cryptocurrency based on proofs of space. *Cryptology ePrint Archive*, Report 2015/528, 2015. http://eprint.iacr.org/2015/528.
16. Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S., *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton: Princeton University Press, 2016.
17. Zyskind, G., Nathan, O., and Pentland, A. S., Decentralizing privacy: Using blockchain to protect personal data. In: *Proceedings of the 2015 IEEE Security and Privacy Workshops, pp. 180–184*, 2015.
18. Brambilla, G., Amoretti, M., and Zanichelli, F., Using blockchain for peer-to-peer proof-of-location, arXiv:1607.00174, 2016.
19. Yao, X., Lin, Y., Liu, Q., and Zhang, J., Privacy-preserving search over encrypted personal health record in multi-source cloud. *IEEE Access* 6:3809, 2018.
20. Miyaji, A., Nakasho, K., and Nishida, S., Privacy-preserving integration of medical data. *J. Med. Syst.* 41(3):37, 2017.
21. Shen, J., Zhou, T., Wei, F., Sun, X., and Xiang, Y., Privacy-preserving and lightweight key agreement protocol for V2G in the social internet of things. *IEEE Internet of Things Journal*, 2017.
22. Gedik, B., and Liu, L., A Customizable k-Anonymity Model for Protecting Location Privacy. In: *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS '05), pp. 620–629*, 2005.
23. Andrés, M. E., Bordenabe, N. E., Chatzikokolakis, K., and Palamidessi, C., Geo-indistinguishability: Differential privacy for location-based systems. In: *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 901–914, 2013.

24. Boldyreva, A., Chenette, N., Lee, Y., and O'Neill, A., Order-preserving symmetric encryption, *Advances in Cryptology - EUROCRYPT 2009, International Conference on the Theory and Applications of Cryptographic Techniques*. Cologne: Proceedings, pp. 224–241, 2009.
25. Peng, Y., Li, H., Cui, J., Zhang, J., Ma, J., and Peng, C., Hope: improved order preserving encryption with the power to homomorphic operations of ciphertexts. *Sci. China Inf. Sci.* 60(6):062101, 2017.
26. Merkle, R. C., A certified digital signature. In: *Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology, pp. 218–238*, 1989.
27. Xiao, L., and Yen, I. L., Security analysis for order preserving encryption schemes. In: *Proceedings of the 46th Annual Conference on Information Sciences and Systems (CISS), pp. 1–6*, 2012.
28. Zhang, J., Ma, J., Yang, C., and Yang, L., Universally composable secure positioning in the bounded retrieval model. *Sci. China Inf. Sci.* 58(11):1, 2015.
29. Shamir, A., Identity-based cryptosystems and signature schemes. *Lect. Notes Comput. Sci.* 196(2):47, 1985.
30. Wang, D., Cheng, H., Wang, P., Huang, X., and Jian, G., Zipf's law in passwords. *IEEE Trans. Inf. Forensic. Secur.* PP(99):1, 2017.
31. Jiang, Q., Chen, Z., Li, B., Shen, J., Yang, L., and Ma, J., Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems. *Journal of Ambient Intelligence and Humanized Computing*, 2017. https://doi.org/10.1007/s12652-017-0516-2.
32. Wang, D., and Wang, P., Two birds with one stone: Two-factor authentication with security beyond conventional bound. *IEEE Trans. Dependable Secure Comput.* PP(99):1, 2016.
33. He, D., and Wang, D., Robust biometrics-based authentication scheme for multiserver environment. *IEEE Syst. J.* 9(3):816, 2015.
34. Shen, J., Zhou, T., He, D., Zhang, Y., Sun, X., and Xiang, Y., Block design-based key agreement for group data sharing in cloud computing. *IEEE Transactions on Dependable and Secure Computing*, 2017.
35. Shen, J., Zhou, T., Chen, X., Li, J., and Susilo, W., Anonymous and traceable group data sharing in cloud computing. *IEEE Trans. Inf. Forensic. Secur.* 13(4):912, 2018.