Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Computer Standards & Interfaces 77 (2021) 103520

Contents lists available at ScienceDirect

Computer Standards & Interfaces

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

Privacy-preserving contact tracing in 5G-integrated and blockchain-based medical applications

Can Zhang [a], Chang Xu [*,b], Kashif Sharif [a], Liehuang Zhu [b]

[a] School of Computer Science & Technology, Beijing Institute of Technology, Beijing, China
[b] School of Cyberspace Science & Technology, Beijing Institute of Technology, Beijing, China

ARTICLE INFO

Keywords:
5G
Blockchain
Contact tracing
Medical applications
Privacy protection

ABSTRACT

The current pandemic situation due to COVID-19 is seriously affecting our daily work and life. To block the propagation of infectious diseases, an effective contact tracing mechanism needs to be implemented. Unfortunately, existing schemes have severe privacy issues that jeopardize the identity-privacy and location-privacy for both users and patients. Although some privacy-preserving systems have been proposed, there remain several issues caused by centralization. To mitigate this issues, we propose a **P**rivacy-preserving contact **T**racing scheme in 5G-integrated and **B**lockchain-based **M**edical applications, named PTBM. In PTBM, the 5G-integrated network is leveraged as the underlying infrastructure where everyone can perform location checking with his mobile phones or even wearable devices connected to 5G network to find whether they have been in possible contact with a diagnosed patient without violating their privacy. A trusted medical center can effectively trace the patients and their corresponding close contacts. Thorough security and performance analysis show that the proposed PTBM scheme achieves privacy protection, traceability, reliability, and authentication, with high computation & communication efficiency and low latency.

1. Introduction

We are currently in a critical period of fighting the corona virus (COVID-19) epidemic, where everyone hopes that the whole society will restore to the original order as soon as possible. To achieve this, both commercial healthcare/pharmaceutical organizations and academic researchers in related fields are actively contributing. Until now, hundreds of COVID-19-related papers have been published that have enabled researchers and the general public to know more about overcoming the spread of disease. For example, researchers in [21] used natural language processing techniques to find the propagation characteristics of situation information related to COVID-19 in social media such as Sina Weibo[1].

Besides, more novel technicians have been used to help people fight for this aggressive epidemic. The 5G technology has been considered as one of the promising technicians during the COVID-19 pandemic, which enables higher communication resources with low latency. A report of the World Economic Forum (WEF) [14] shows that COVID-19 rises 5G to the *2nd* rank of most discussed tech topics (before COVID-19 is *7th* rank). Another report [13] figures that COVID-19 is accelerating 5G demand in some industries such as healthcare. Under this circumstance, more research papers related to 5G and healthcare [1,9,23,31,42] have been published, which indicates that it is valuable to research 5G-based medical applications especially COVID-19-related applications.

During those medical applications, contact tracing can be considered as an important step in the prevention and control of infectious diseases such as COVID-19. In a typical contact tracing scenario, the close contacts of a patient will be traced and advised to seek proactive treatment from medical organizations as they have a higher probability to be infected compared to non-contacts. A recent study published in *Lancet* [5] shows that aggressive close contact tracking and isolation is the key measure to Shenzhen city's control of COVID-19 transmission. Hence, it will be helpful to stop the infectious virus from spreading further, if an effective solution of contact tracing is established.

In the current pandemic situation, the privacy of information has become an extremely sensitive issue, as, on one hand, immediate information sharing related to contacts is necessary, while on the flip side medical records (and identity) have to be kept confidential. Because users' medical data seems to be more sensitive, medical-related privacy issues appear to be more serious and will cause greater losses compared

* Corresponding author.
E-mail address: xuchang@bit.edu.cn (C. Xu).
[1] https://weibo.com/

https://doi.org/10.1016/j.csi.2021.103520
Received 28 August 2020; Received in revised form 20 January 2021; Accepted 4 February 2021
Available online 9 February 2021

with privacy issues in scenarios like IoT [35,38], vehicular network [40], smart grid [36], and cloud computing [33,34,37,39]. A report of IBM in 2019 [18] shows that the average cost of data loss per leakage has risen to $3.92 million, where healthcare suffers from the highest loss of $6.45 million per security breach. To mitigate these severe issues caused by privacy leakage, research in both academic and industrial areas has tried to propose new medical applications with the privacy-preserving properties. For example, MIT [27] uses Bluetooth signals from smartphones to perform automated contact tracing privately. Besides, Apple and Google jointly announced a contact tracing system that also makes use of Bluetooth-based proximity-detection technology to find close contacts without compromising location privacy [3].

Unfortunately, there are still some issues with existing contact tracing solutions that need to be solved. More specifically:

- **Centralized Architecture**: All the existing schemes are based on a centralized architecture. In that case, the system may suffer from single-point failure (data breach) that will affect the availability of the whole system.
- **Unreliable Data Storage**: Data stored on a centralized server can be easily deleted or tampered with, by malicious system administrators. Besides, malicious users may upload fake information to the system to evade supervision.
- **Limited Privacy Protection**: Privacy protection cannot be fully guaranteed. Existing privacy-preserving solutions can prevent privacy from violating by external adversaries. However, different companies, entities, and agencies who possess the user's private data have unlimited access privileges to them, which may also lead to privacy abuse.

In light of these issues that limit the practical use of existing contact tracing systems, we propose a novel privacy-preserving contact tracing scheme in blockchain-based medical applications, named PTBM. More specifically, the 5G-integrated network architecture is leveraged to achieve high communication bandwidth with low propagation & response latency. Blockchain is used to achieve reliable data storage & verification, and secure cryptographic primitives are also leveraged to protect identity privacy and location privacy for both users and patients. To the best of our knowledge, this is the first privacy-preserving contact tracing scheme with a decentralized architecture that achieves reliability in large scale emergency systems.

Following are the major contributions of this work.

- We design a novel decentralized architecture of contact tracing applications, where the 5G-integrated blockchain network is leveraged as underlying infrastructures. Both permissionless and permissioned blockchains are used to achieve public location checking and supervised data storage & tracing, respectively.
- We propose PTBM, a decentralized contact tracing scheme based on the hierarchy of blockchain and secure cryptographic primitives to protect the identity privacy and location privacy for both public users and patients without losing the tracing ability of trusted medical center.
- We make thorough security analysis and performance evaluation to prove that the proposed PTBM scheme achieves privacy protection, reliability, authentication, and traceability with high computation & communication efficiency and low latency.

The rest of the paper is organized into seven sections. Section 2 gives the background and motivation of the scheme including the related works. Section 3 introduces the fundamentals of blockchain, PCSD cryptosystem, and the bloom filter. Section 4 presents the formalized system model, security model, and design goals of PTBM. In Section 5, we elaborate on the complete working of the proposed scheme, followed by the security analysis and performance evaluation in sections 6 and 7, respectively. Finally, Section 8 concludes the paper.

2. Related works and motivations

In this section, some related works about blockchain with 5G, existing contact tracing mechanism and blockchain-based medical applications are introduced, which prove the novelty of the proposed scheme because to the best of our knowledge, none of the existing schemes supports reliable and privacy-preserving contact tracing with low latency.

2.1. Blockchain with 5G technology

Both the blockchain and 5G can be considered as the next-generations technology, hence their integration also attracts the attention of researchers, which covers a variety of scenarios including Internet-of-Things (IoT) [4,17,41], and edge computing [15,19,28].

In the IoT scenario, Zhang et al. [41] proposed an edge intelligence and blockchain empowered IIoT framework under the 5G environment. The proposed scheme includes a cross-domain resource scheduling mechanism and a credit-differentiated edge transaction approval mechanism. It also achieves secure service management and low latency with the help of blockchain and 5G. Hewa et al. [17] presented an automatic certificate revocation scheme, where Elliptic Curve Qu Vanstone (ECQV) certificates are used to achieve lightweight authentication for the resource-restricted IoT devices, and smart contracts are used to achieve reliable and automatic certificate revocation. The proposed scheme realizes a lightweight certificate store, update, and revocation, hence it is suitable for the 5G-based wireless network that interconnects millions of IoT devices. Bera et al. [4] introduced the issues and challenges of applying blockchain in the 5G-based IoT environment. They also presented a secure framework for blockchain-based data management that can resist several potential attacks and achieve reliability. Detailed analysis shows that the proposed scheme provides less communication and computation overheads as compared to other relevant works.

In the edge computing scenario, Nkenyereye et al. [28] adopted a 5G cellular architecture of Emergency Driven Message (EDM) Protocol which provides higher scalability with lower latency. They also constructed a blockchain-based system where each node is seen as an edge node to reliably store EDM records of which the privacy is protected by a lightweight signcryption scheme. Jangirala et al. [19] designed a lightweight RFID-based authentication protocol for supply chains, named LBRAPS. Their proposed LBRAPS protocol uses several lightweight cryptographic primitives such as bitwise XOR and one-way hash functions, hence it is suitable for the 5G mobile edge computing environment. Gao et al. [15] incorporated another novel technique, software-defined networks (SDNs) to ensure effective management for blockchain-enabled fog computing in 5G networks. The article also shows that the combination of blockchain and the SDN relieves the pressure of the centralized controller.

Besides, some privacy-preserving schemes that try to leverage 5G technology in blockchain-oriented solutions have been presented [7,10,11,16,22,26]. We can conclude that more and more researchers are paying attention to solve the privacy issues in 5G-integrated blockchain networks.

2.2. Contact tracing

The current outbreak of coronavirus in the world has attracted extensive attention from both academic institutions and researchers in various fields. The work in [30] analyzed the advantages and shortcomings of several existing privacy-aware contact tracing solutions. It concludes from observations in existing solutions that: 1) the importance of location information is usually ignored, 2) the privacy concerns and trust relationship are generally missing, 3) the reliability cannot be guaranteed because large companies or malicious users can manipulate the uploaded data, and 4) deployment of the systems in the real-world

scenario is not specified.

In the contact tracing scenario, Ahmed et al. [2] summarizes existing mobile contact tracing APPs which can be divided into three architectures: *centralizing, decentralizing*, and *hybrid*. It also concludes that security and privacy issues are one of the most concerns that these APPs are still facing. Fitzsimons et al. [12] designed a privacy-preserving contact tracing mechanism by introducing secure two-party computation (2PC). More specifically, 2PC is used to securely calculate the distance between the location trajectory for a patient and a user. If the calculated distance is below the given threshold, the user will be considered as a close contact of the patient. However, the computation and communication costs of verification are relatively high because the 2PC protocol should be followed for each user who wants to perform the contact tracing operation.

Xu et al. presented BeepTrace [32], a blockchain-based privacy--preserving contact tracing scheme where pseudonyms are used to achieve the unlinkability between the on-chain data and the real-world identity, and the uploaded on-chain data are also encrypted by the corresponding user. Compared with other existing technicians, BeepTrace achieves privacy protection with a decentralized architecture. Unfortunately, the user uses Geo public key to encrypt the location information, and the location privacy cannot be well guaranteed if the Geo Solver who holds the decryption private key is malicious. Besides, it cannot actively trace the contact of a given patient.

2.3. Blockchain-based medical applications

Because of the decentralization and immutability of the blockchain, several works have introduced blockchain in medical applications to achieve reliable medical data storage, analysis, and sharing. Biswas et al. [6] present a comprehensive analysis of challenges and solutions for using blockchain effectively in e-healthcare systems. Liu at al[24]. proposed a blockchain-based data sharing scheme to address the privacy issue of Electronic Medical Record (EMR) sharing. The proposed scheme also used CP-ABE-based access control and the content extraction signature scheme. Li et al. [20] proposed a blockchain-based medical data preservation system to realize privacy-preserving and verifiable medical data storage. Shen et al. [29] presented a privacy-preserving image retrieval mechanism for medical IoT systems that used customized blockchain transaction structures to store the feature vector for each image. Smart contracts are also used to execute privacy-preserving image retrieval based on the feature vectors. Chang et al. [8] discussed how blockchain can help people in the fight against COVID-19. From their perspective, blockchain will be widely used in future medical applications.

2.4. Motivations

Based on the above analysis, we make three conclusions that form the major motivation of this work:

1. The integration of blockchain achieves reliable data storage and program execution in a decentralized manner, which also mitigates the computation & computation loads and the probability of single-point failure of centralized servers. Unfortunately, the communication delay of blockchain is relatively high because of the decentralization property.
2. The incorporation of the 5G network brings out more powerful communication ability with higher bandwidth and lower latency compared with the existing 4G-based wireless networks. However, most of the 5G devices are small IoT or fog devices such as communication base station, smartphone, or even wearable devices, has relative low computation ability and storage capacity, which results in unreliable data storage and transmission.
3. The techniques of contact tracing are just in their infancy, which means more effective mechanisms and solutions need to be developed. Besides, the decentralization property of blockchain can be widely used in medical applications to solve the issues caused by centralized architecture.

In PTBM, we use the blockchain-based 5G network and lightweight cryptographic primitives as the underlying infrastructure and higher construction respectively to achieve reliable and privacy-preserving contact tracing with high efficiency and low latency. More specifically, the reliability of blockchain and enhanced communication bandwidth with low latency of 5G network will be utilized, whereas the deficiencies bring from using either of them alone will be eliminated. The privacy of the user's identity and the patient route can be well protected, whereas the traceability can be also guaranteed.

3. Preliminaries

In this section, some basic primitives used in the proposed scheme are introduced. These include the blockchain system, public-key cryptosystem with strong key decryption (PCSD), and the bloom filter (BF).

3.1. Blockchain

The concept of blockchain originates from the Bitcoin cryptocurrency that achieves reliable transactions under decentralized and trust-less circumstances. Blockchain can be seen as a distributed and append-only ledger with immutability, hence the data stored on the blockchain cannot be deleted or tampered with.

Blockchain can be primarily categorized into two types: *permissioned* and *permissionless* blockchain. Before participating in the *permissioned* blockchain, all users must register with the Trusted Authority (TA), hence only the authorized (registered) users can get access to the data block stored on the ledger. The *permissionless* blockchain does not need access control, and anyone can participate in and query the data stored on the blockchain, however, this leads to scalability and public accountability as well as some privacy issues. For example, external attackers can perform inference attacks that use statistical analysis to shrink the data privacy and identity privacy of the blockchain users with the help of background knowledge.

For the purpose of mitigating these privacy issues, we use the hierarchical architecture of blockchain with secure cryptographic primitives to achieve privacy protection without losing the decentralization & accountability properties.

3.2. Public-key cryptosystem with strong private key decryption

The concept of PCSD derives from the Public-Key Cryptosystem with Distributed Decryption (PCDD) presented in [25]. PCSD consists of the following algorithms:

- $(msk, (pk_1, sk_1), \cdots, (pk_n, sk_n)) \leftarrow \mathsf{KeyGen}(\lambda, n)$ is a probabilistic algorithm that receives a security parameter λ and a number of key-pairs n as input, and outputs a strong private key msk and n key-pairs $(pk_1, sk_1), \cdots, (pk_n, sk_n)$. Let p, q be two large prime numbers that satisfy $|p| = |q| = \lambda$. Set $N = pq$ and $\alpha = lcm(p-1, q-1)/2$. Choose $g \in \mathbb{Z}^*_{N^2}$ with order $(p-1)(q-1)/2$, and define a function $L(x) = (x-1)/N$. For each $i \in \mathbb{Z}_n$, compute $h_i = g^{\beta_i} \mathrm{mod} N^2$ where $\beta_i \in [1, N/4]$ is randomly selected. The public key and private key for i is $pk_i = (N, g, h_i)$ and $sk_i = \beta_i$, respectively. The strong private key is $msk = \alpha$.
- $c_i \leftarrow \mathsf{Enc}(pk_i, m_i)$ is a probabilistic algorithm that receives i's public key pk_i and a message m_i, and outputs a ciphertext c_i associated with m. Given i's public key pk_i and a message $m_i \in \mathbb{Z}_N$, choose $r_i \in [1, N/4]$ randomly and compute the ciphertext $c_i = \{T_{i1}, T_{i2}\}$, where $T_{i1} = h_i^{r_i}(1 + mN) \mathrm{mod} N^2$, and $T_{i2} = g^r \mathrm{mod} N^2$.
- $m_i \leftarrow \mathsf{Dec}(sk_i, c_i)$ is a deterministic algorithm that receives i's private key sk_i and a ciphertext c_i, and outputs the message m_i. With i's

private key sk_i, the message m_i can be recovered by computing $m_i = L((T_{i1}\cdot(T_{i2}^{\beta_i})^{-1})\mathrm{mod}N^2)\mathrm{mod}N$.

- $m \leftarrow \mathrm{SDec}(msk, c)$ is a deterministic algorithm that receives a strong private key msk and a ciphertext c as input, and outputs the message m. For any ciphertext c, the corresponding message m can be recovered by computing $m = L(T_1^{\alpha}\mathrm{mod}N^2)\cdot\alpha^{-1}\mathrm{mod}N$.

Assume c_i is encrypted by i's public key pk_i, note that for all $1 \le i \le n$, the corresponding message m_i can be recovered by using msk. Hence we call msk a strong private key. Entities (other users and attackers) that do not know msk or sk_i, the cyphertext c_i cannot be decrypted. We leverage this property of PCSD to achieve privacy-preserving tracing in the proposed PTBM scheme.

3.3. Bloom filter

The BF can be considered as an indexed structure used for membership queries. The idea of BF is to choose o independent secure hash functions $H_1, \cdots, H_o$ with the same domain $D = \{a_1, \cdots, a_n\}$ and range $R = \mathbb{Z}_m$. The BF consists of three algorithms described as follows:

- **Init**: Choose an m-bit vector $\mathscr{B}$ that will be used to store the membership information. All the bits in $\mathscr{B}$ are set to 0.
- **Insert**: All the members in D will be inserted into the vector $\mathscr{B}$. More specifically, to insert a membership a_i, o hashed values $\bigcup_{k=1}^{o} H_k(a_i)$ will be computed, and each $H_k(a_i)$ position of $\mathscr{B}$ will be set to 1.
- **Query**: To query whether $a \in D$, o hashed values $\bigcup_{k=1}^{o} H_k(a)$ will be computed. If there exists an $H_k(a)$ such that the corresponding position of $\mathscr{B}$ is 0, it means $a \notin D$, otherwise $a \in D$.

Note that $\mathscr{B}$ can also be implemented using a hash table. The **Insert** algorithm inserts all the entries indexed by $H_1(a_i), \cdots, H_o(a_i)$ with value 1 (i.e., for each $H_k(a_i)$, $\mathscr{B}[H_k(a_i)] = 1$). In the **Query** algorithm if there exists an $H_k(a)$ such that $\mathscr{B}[H_k(a)] = \perp$, it means $a \notin D$. In the proposed scheme, we use this implementation to store the location state information to protect the user's location privacy as well as realizing efficient location checking operations.

4. Problem formalization

In this section, we formalize the system model, threat model, and design goals of the proposed PTBM scheme.

4.1. System model

The system consists of five entities: Medical Center (MC), Fog Nodes, Users, Medical Organization (MO), and Blockchain systems, as shown in Fig. 1.

4.1.1. Medical center

The MC can be considered as a trusted authority controlled by the government. It performs the registration operation to generate & distribute the system parameter and key-pairs for each user, MO, and fog node. MC will stay offline after registration unless it needs to trace the patient information or MO's misbehavior. In that case, it will trace the data stored on the permissioned blockchain. Hence, the introduction of MC cannot violate the decentralization property of the blockchain. Furthermore, this allows that any MC (public or private sector entity) can be easily made part of the existing healthcare infrastructure.

4.1.2. Fog nodes

The fog nodes are deployed beside the checkpoints that are also controlled by the government. These checkpoints are specially set up to check body temperature and/or other parameters for public health monitoring. Because we utilize the 5G-integrated network as the underlying infrastructure, which means all the fog nodes are connected by 5G wireless network via 5G base station. Besides, then can also connect other 5G terminals such as the user's mobile phone or other 5G-supported wireless devices. It uploads the user's encrypted location checking information and periodically uploads its current state to the permissioned blockchain.

4.1.3. Users

When a user wants to cross a checkpoint, they will use their mobile phone to upload their identity and location information encrypted by their respective public key via 5G wireless channel. Besides, they can execute location checking on the permissionless blockchain to check whether their historical route includes dangerous areas where infected patients have been found.

4.1.4. Medical organizations

The MOs can be seen as primary healthcare institutions (e.g., community clinics) that treat infectious patients. MO will maintain several nodes in both permissioned and permissionless blockchain for patient route query and location publication respectively. The patients' activity areas will be published to the permissionless blockchain so that every user can check whether they have been to these areas. If they have, then they can go to a nearby MO for examination and treatment in time.

4.1.5. Blockchain

In our proposed system, there exist two kinds of blockchain: *permissionless* and *permissioned blockchain*. Everyone can get access to the data stored on the permissionless blockchain, whereas, only the MC, MO, and Fog Nodes have the read & write permissions for the

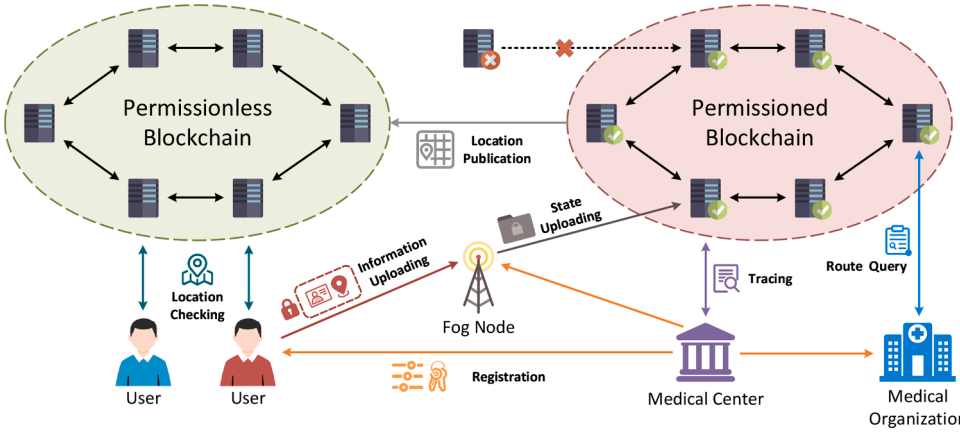

Fig. 1. System model.

permissioned blockchain. The hierarchical architecture of blockchain enables enhanced security guarantees and advanced privacy protection for both users and patients. Note that all the blockchain nodes can be also connected via 5G wireless networks which enable higher communication channel capacity with lower latency.

4.2. Threat model

In our threat model, we assume that MC cannot be compromised, and the data stored in MC cannot be leaked. Moreover, MC distributes the system parameter and key-pairs via secure channels.

Both the fog nodes and MOs are honest-but-curious, which means that they exactly perform the presented algorithms and protocols, however, they try to infer both users' and patients' private information from the data stored on the blockchain. Note that the collusion between fog nodes and MOs is not allowed because fog nodes are controlled by the government as mentioned earlier.

Most of the users are honest, however, there exist several malicious users that try to impersonate other legitimate users to upload fake information to evade supervision.

4.3. Design goals

Here we introduce the design goals of PTBM. Note that in Section 6, we prove that PTBM realizes all of these design goals.

Privacy Protection: The proposed scheme should protect every user/patient's identity privacy and route location privacy simultaneously. More specifically, both honest-but-curious MO and external adversaries cannot infer the real-world identity or recover the exact route of both users and patients.

Reliability & Authentication: The data uploaded by both users and MOs cannot be modified by both external or internal adversaries, and all the users, fog nodes, MOs, and MC can obtain the correct query/tracing result. Besides, an effective authentication mechanism should be introduced to avoid impersonation attacks by malicious users.

Traceability: Given a designated patient, his route should be traced, and all the users that might have been in close contact with the patient should also be traced. Note that this tracing operation should only be executed by MC. Besides, MC can also trace the misbehavior of MO.

Efficiency: Due to the limited computation and storage capacity of the devices in the 5G-integrated network, the computation complexity should be as low as possible, especially for users and fog nodes that make use of mobile and IoT devices, respectively. Besides, the communication costs should also below to save the channel resource and bring out low latency.

5. The proposed PTBM scheme

In this section, a detailed description of the proposed PTBM scheme is given. The notations used in this work are illustrated in Table 1.

Table 1
List of notations.

Notation	Description
λ	Security parameter
m	The number of users
n	The number of fog nodes
uid_i, nid_j	The pseudonym of user i and fog node j
(upk_i, usk_i)	Signature key-pair for user i
(npk_j, nsk_j)	Encryption key-pair for fog node j
K, msk	Secret key and strong private key for MC
F	A secure pseudo-random function.
$H, H_1, \cdots, H_o$	$o+1$ secure hash functions

5.1. Registration

In this process, MC first generates a secret key $K \leftarrow \{0,1\}^\lambda$ held by MC itself, and the strong private key & signature key-pair $(msk, \bigcup_{j=1}^{n}(npk_j, nsk_j)) \leftarrow \mathsf{PCSD.KeyGen}(\lambda, n)$, where the key-pairs will be distributed to the corresponding fog nodes.

Besides, MC randomly chooses a secure digital signature scheme DS that consists of three algorithms: KeyGen (key generation), Sig (signature), and Ver (verification). Then it chooses a secure random function $F: \{0,1\}^\lambda \times \{0,1\}^* \rightarrow \{0,1\}^\lambda$ and $o+1$ secure hash functions $H, H_1, \cdots, H_o: \{0,1\}^* \rightarrow \{0,1\}^\lambda$. These functions can be seen as system parameters that will be sent to all the users and fog nodes.

For each user i associated with the real identity u_i, MC generates i's pseudonym $uid_i = F(K, u_i)$ and signature key-pair $(upk_i, usk_i) \leftarrow \mathsf{DS.KeyGen}(\lambda)$. Then it sends (uid_i, upk_i, usk_i) to user i through secure channels, and publishes (uid_i, upk_i) to the permissioned blockchain. Besides, it will initialize a list $L[uid_i]$ on permissioned blockchain for each user i that will be used to store the encrypted route information.

For each fog node j associated with the real identity n_j, MC also generates the pseudonym $nid_j = F(K, n_j)$. Then is sends (nid_j, npk_j, nsk_j) to fog node j through secure channels. Besides, it will initialize a dictionary S on the permissioned blockchain that will be used to store the encrypted state information. Note that each nid is associated with a geographic location about the checkpoint, of which the correspondence is held by MC secretly.

For each MO M, it needs the real identity mid_M and the public key pk_M for registration. MC will generate the corresponding blockchain address $addr_M$ used on both permissioned and permissionless blockchain to invoke smart contracts of *Route Query* and *Location Publishing*, respectively. Finally, MC publishes $(mid_M, addr_M)$ to the permissioned blockchain.

5.2. Information uploading

When a user i wants to cross a checkpoint associated with fog node j, it first sends a request $\mathscr{R}_i = (uid_i, t_i, \sigma_i)$ to j, where t_i is the current timestamp and $\sigma_i = \mathsf{DS.Sig}(usk_i, H(uid_i \parallel t_i))$ is the signature generated by i's private key.

After receiving $\mathscr{R}_i$, j first check whether the timestamp t_i is obsolete. If the difference between current time t and t_i exceeds the threshold t_θ, $\mathscr{R}_i$ will be rejected. If the time checking is successful, it queries i's public key upk_i by searching the permissioned blockchain with the index uid_i, and verifies the signature σ_i by executing $\mathsf{DS.Ver}(upk_i, \sigma_i, H(uid_i \parallel t_i))$. If the verification returns *true*, it inserts $\bigcup_{k=1}^{o} H_k(uid_i)$ to the bloom filter $\mathscr{B}_{s_j}$, where $s_j \leftarrow \{0,1\}^\lambda$ is a random string that represents j's current state. If the verification returns *false*, $\mathscr{R}_i$ will also be rejected. Finally, j adds (s_j, t_j) to $L[uid]$ stored on the permissioned blockchain where t_j represents the current timestamp.

Note that s_j is periodically updated, and j will upload the current state information $(E_j, U_{s_j}, \mathscr{B}_{s_j})$ to $S[s_j]$ stored on the permissioned blockchain before the update operation, where $E_j = \mathsf{PCSD.Enc}(npk_j, nid_j)$ is the encrypted pseudonym of j, and U_{s_j} represents the users that passed-by in this time period. For each $u_i' \in U_{s_j}$, $u_i' = \mathsf{PCSD.Enc}(npk_j, uid_i)$.

5.3. Route query

When a medical organization MO receives a patient p, it uses the address $addr_M$ to execute route query contract of the corresponding uid_p given by p with the preset start timestamp t_s. More specifically, MO queries the permissioned blockchain and obtains p's recent route $L_p \subseteq L[uid_p]$ where each $(s,t) \in L_p$ satisfies $t \geq t_s$. Note that elements in $L[uid_p]$ are arranged in chronological order, hence the elements in L_p also follow a chronological order.

5.4. Location publication

During the route tracing operation, MO obtains p's recent route L_p, then it uses the address $addr_M$ to perform location publication contract. More specifically, for each $(s,t) \in L_p$, MO obtains $S[s] = (E_s, U_s, \mathscr{B}_s)$ from the permissioned blockchain. The encrypted pseudonym E_s and user's information U_s are used for MC's tracing, and the corresponding bloom filter $\mathscr{B}_s$ will be published as the activity area information to the permissionless blockchain.

In our scenario, all the patients are seen as infectious disease patients, hence their recent activity areas should be published under the premise of protecting their privacy. In that case, everyone can check whether their historical route includes these dangerous areas. If so, they can go to the medical organizations nearby for further examination.

5.5. Location checking

Each user i can use his mobile phones or other 5G-support devices to check the location information $\mathscr{B}$ published on the permissionless blockchain to check whether they have been to these dangerous areas. More specifically, i computes $\bigcup_{k=1}^{o} H_k(uid_i)$ and finds whether all the k hashed values appear in the bloom filter $\mathscr{B}$. If so, it means i should go to the MO nearby for further examination because the published area includes the patient's recent activity area.

Note that $\mathscr{B}$ is based on the time state which means i and the patient are in the same location at the same time period if all the $\bigcup_{k=1}^{o} H_k(uid_i)$ are in $\mathscr{B}$. It is obvious to conclude that the user i was in close contact with the patient with a high probability. Therefore, i should go to an MO nearby to determine whether they are infected or not.

5.6. Tracing

Note that not all patients are active in executing the location checking operation. In that case, the MC can trace the users who might have been in close contact with the patient p and inform them to get a thorough examination. More specifically, like *Route Query* and *Location Publication*, the MC finds $L_p \subseteq L[uid_p]$ and $S[s] = (E_s, U_s, \mathscr{B}_s)$ for each $(s, t) \in L_p$. Then for each $u' \in U_s$, it recovers the user's pseudonym uid by executing $\mathsf{PCSD.SDec}(msk, u')$. Because in the registration operation, each user uses their real identity to register, MC can contact them easily.

Besides, for an MO M, it uses its address $addr_M$ to invoke the contract of route query and location publication, and all the operations will be recorded to the immutable blockchain. During the *Registration* process, M uses the real-world identity mid_M to register from MC and obtains $addr_M$. Hence, each address $addr$ is associated with the corresponding MO's real-world identity, which means that the misbehavior of MO (e.g., publishing fake location information, abusing the route query operation) can be traced by MC.

6. Theoretical analysis

To show that the proposed PTBM scheme achieves the aforementioned design goals of privacy protection, reliability, authentication, and traceability, here we present a thorough analysis.

6.1. Privacy protection

In the proposed scheme, both the privacy of patients and other users should be protected, which includes identity privacy and route privacy.

6.1.1. Identity privacy

In PTBM, each user will be assigned a pseudonym generated by MC by computing $uid_i = F(K, u_i)$. If the pseudo-random function F is secure, the user i's pseudonym uid_i and the corresponding real-world identity u_i is unlinkable without knowing the secret key K held by MC.

The patient p can be considered as a special kind of user. During the *Route Query* process, their pseudonym uid_p will be used. As mentioned above, the proposed PTBM scheme achieves unlinkability between u_p and uid_p. Hence, only the query requester MO knows the real identity of p, which is inevitable because the MO is responsible for p's examination and treatment.

For external adversaries, the inference attack cannot be performed because they can only access the permissionless blockchain that only stores the published location information.

Therefore, both honest-and-curious MO and external adversaries cannot infer the real-world identity of both patients and other users, which means the proposed PTBM scheme achieves identity privacy protection.

6.1.2. Route privacy

In the permissioned blockchain, given a pseudonym uid_i, the encrypted route information $L_i = L[uid_i]$ can be obtained, where $(s,t) \in L_i$ reflects the user i's location at time t. For each state s, the state dictionary S stores the tuple $S[s] = (E_s, U_s, \mathscr{B}_s)$. Assuming s represents one of the fog node j's states, only the corresponding private key sk_j and MC's strong private key msk can recover the encrypted result. Note that E_s and U_s is encrypted by pk_j. The bloom filter $\mathscr{B}_s$ only stores an obfuscated location information which consists of several hashed values of users' pseudonym. If all the hash function $H_1, \cdots, H_o$ are secure, then all the pre-hash value (i.e., the user's pseudonym) cannot be recovered. In summary, for each state s, $S[s]$ cannot leak the location information for any user.

In the permissionless blockchain, only the bloom filter $\mathscr{B}$ associated with a patient p's activity area is published. As mentioned above, external adversaries cannot find which user has been to this area associated with $\mathscr{B}$.

Therefore, both honest-and-curious MO and external adversaries cannot recover the exact route of any user i, which means the proposed PTBM scheme achieves location privacy protection.

6.2. Reliability & authentication

Due to the reliability of blockchain which has been well established in the literature, all the data stored on the permissionless and permissioned blockchain cannot be modified or deleted. Hence, the correctness of query/tracing results on the blockchain can also be guaranteed.

In PTBM, each user is assigned a key-pair for generating digital signatures. For a malicious user, it cannot impersonate another legitimated user to upload the information without knowing the private key. Besides, we use timestamp t_i to resist replay attacks, which means the malicious users cannot use the obsolete request of others. Therefore, PTBM achieves effective user authentication.

6.3. Traceability

As mentioned above, MC can perform route tracing operations of a given pseudonym uid_p of a patient p, or tracing of all the users that might have been in close contact with p. Besides, all misbehaviors can be traced by MC with the help of access mechanisms in the permissioned blockchain and registration rules in PTBM scheme. In that case, MC can punish the misbehaving MOs by both economical and administrative mechanisms to regulate their behavior.

7. Performance evaluation

In this section, we evaluate both computation & communication complexity based on a blockchain platform to prove that the proposed PTBM scheme has high computation efficiency with low communication costs.

7.1. Experimental setup

We have implemented the proposed PTBM scheme in the Go language, which includes the implementation of PCSD scheme based on [25]. The security parameter $\lambda = 256$, and the number of shared keys in the bloom filter is set to $o = 5$. All the pseudo-random functions and hash functions are instantiated by HMAC-256 and SHA256, respectively. All programs are compiled in Go 1.14 x64 environment.

We choose the Hyperledger Fabric[2] as the underlying blockchain platform. Hyperledger Fabric provides permissioned management with flexible programmability & efficiency. Fabric is suitable for our scenario where both permissioned & permissionless blockchains are required, and its high transaction throughput as compared with Bitcoin and Ethereum makes it a practical real-world solution.

We deploy four peer nodes of Fabric as the test blockchain network, where each node is running on a virtualized server on an Intel i7-9700K CPU and 8GB RAM with a 64-bit Ubuntu 16.04 operating system. The client-side programs (by users, fog nodes, and MOs) are executed on a tablet with Intel i5-7300U CPU and 4GB RAM with a 64-bit Windows 10 operating system.

7.2. Computational costs

To evaluate the computational performance of PTBM, we set the number of users m ranging from 1000 to 10,000 with increments of 1000, the number of fog nodes $n = 100$, the number of patients $m/1000$, and the number of users that perform location checking operation to $m * 20\%$. We randomly generate the route of each user, and the patients are also uniformly & randomly selected. All the evaluations are executed 5 times, and we calculate the average execution time for each process to remove relative errors. The results are shown in Fig. 2.

7.2.1. Registration

During the *Registration* process, each user i is assigned as a pseudonym uid_i and a signature key-pair (upk_i, usk_i), each fog node j is assigned as a pseudonym nid_j and an encryption/decryption key-pair (npk_j, nsk_j). Assume $\tau(o)$ represents the average execution time of operation o, the average execution time of *Registration* is $m{\cdot}\tau(\mathsf{DS.KeyGen}) + n{\cdot}\tau(\mathsf{PCSD.KeyGen}) + (m+n){\cdot}\tau(F)$, where m and n represents the number of user and fog node, respectively. Therefore, the corresponding computation complexity is $O(m+n)$ for MC.

Because the number of fog nodes is relatively fixed, we mainly evaluate the time cost by different numbers of users. It can be seen in Fig. 2a, as the number of users increases, the time cost also increases. Note that even if the number of users raises to 10000, it only takes about 1 min for registration. Besides, the registration operation only performs once, and in the real world situation, it will be done immediately when a new user joins.

7.2.2. Information uploading

During the *Information Uploading* process, the user i generates a request $\mathscr{R}_i$ which includes i's pseudonym uid_i, a timestamp t_i, and a signature σ_i. Hence for user, it takes $\tau(\mathsf{DS.Sig})$ to generate $\mathscr{R}_i$ in the *Information Uploading* process, and the corresponding time complexity is $O(1)$. Note that we omit the calculation of negligible time consuming such as generating hash value.

For each $\mathscr{R}_i$, the fog node j checks the timestamp and verifies the signature. If the checking & verification are successful, i's state will be updated with the current state s_j of j via Update operation of smart contract. Periodically, the state information will be uploaded to the permissioned blockchain which includes several encrypted user's pseudonym passed by j in this period of time, and j's encrypted pseudonym. Assume the number of users pass by is m_j, the time cost in the *Information Uploading* process for a fog node is $m_j{\cdot}\tau(\mathsf{DS.Sig}) + (m_j+1){\cdot}\tau(\mathsf{PCSD.Enc}) + (m_j+1){\cdot}\tau(\mathsf{Update})$, and the corresponding time complexity is $O(m_j)$. However, in the real-world scenario, a fog node can handle the users' request in parallel, which means the time complexity can be decreased to $O(1)$.

As is illustrated in Fig. 2(b), the execution time is not related to the number of users pass by. We also notice that the execution time slightly increases with the number of users increases. That is because a larger number of users bring out a larger size of state information for node j that will be uploaded to the permissioned blockchain, which results in higher communication delay.

7.2.3. Route query & location publication

During the *Route Query* process, the MO queries the patient p's route $L[uid_p]$ with the help of uid_p, which only needs one Query operation of smart contract. Hence, the time cost of *Route Query* for MO is $\tau(\mathsf{Query})$ with the corresponding time complexity $O(1)$.

During the *Location Publication* process, the MO queries the permissioned blockchain to obtain p's recent activity areas, and uploads the associated bloom filter to the permissionless blockchain. Assume the number of p's recent activity area is n_p, the time cost of *Location Publication* process for MO is $\tau(\mathsf{Query}) + \tau(\mathsf{Update})$, the corresponding time complexity is $O(1)$.

As can be seen in Fig. 2(c), the execution time is not related to the number of users, and it only takes about 40ms to perform the complete route query & location publication process.

7.2.4. Location checking

During the *Location Checking* process, each user i will check the location information published by MO previously. Assume that only one bloom filter $\mathscr{B}$ is published, and in that case, i only executes the **Query** algorithm once, which is negligible. Hence, the time cost of *Location Checking* process for user is $\tau(\mathbf{Query})$, the corresponding time complexity is also $O(1)$.

As is illustrated in Fig. 2(d), although the number of users increases from 1000 to 10000, the execution time looks almost the same, which proves that the proposed PTBM scheme achieves $O(1)$ complexity during this process.

7.2.5. Patient tracing

During the *Patient Tracing* process, the MC obtains the state information related to p's recent activity as what the MO does in the *Location Publication* process. Hence, the time cost of *Patient Tracing* for MC is $\tau(\mathsf{Query})$ with the corresponding time complexity $O(1)$.

As is seen in Fig. 2(e), the execution time is irrelevant to the number of users and ranges from 35ms to 45ms, which is efficient.

7.2.6. Contact tracing

During the *Contact tracing* process, MC recovers each contact's pseudonym by executing PCDD.SDec operations for each state s obtained by *Patient Tracing* process. Hence, it takes $m_j{\cdot}n_p{\cdot}\tau(\mathsf{PCSD.SDec})$ to recover all the pseudonym for all states, and the corresponding time complexity is $O(m_j{\cdot}n_p)$.

As is seen in Fig. 2(f), the execution time is irregular, that is because, in our experimental setting, each user's route is randomly generated which results in random m_j and n_p.

7.3. Communication costs

The communication behavior mainly happens during the *Information Uploading, Location Query, Location Publication* and *Location Checking* process. For users, it is obvious that the communication complexity of *Information Uploading* and *Location Checking* processes are both $O(1)$ because he only sends one request and performs one query operation,

[2] https://www.hyperledger.org/use/fabric

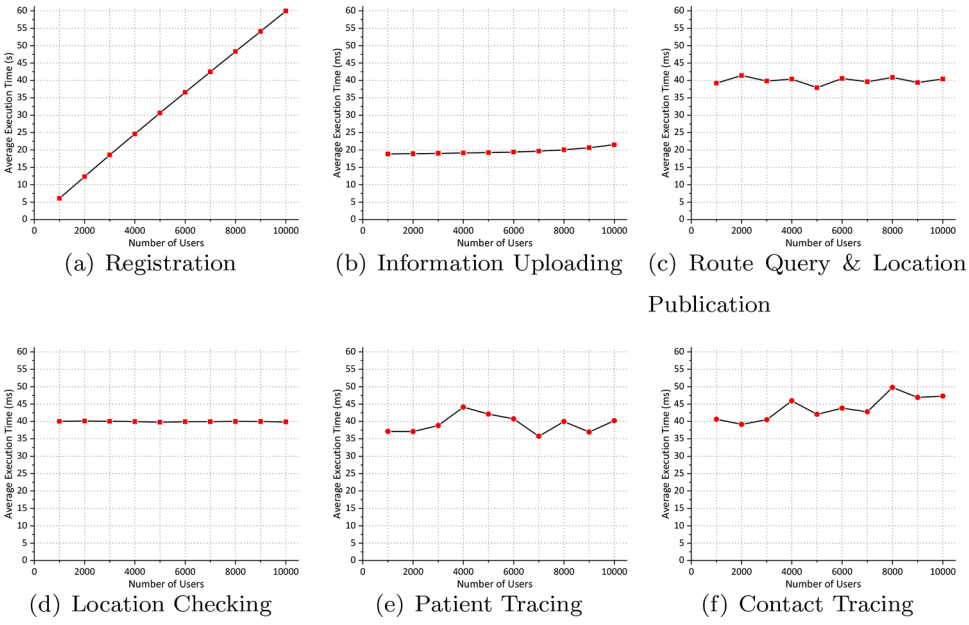

Fig. 2. Experimental evaluation of computational costs.

respectively. For fog node, the communication complexity is $O(m_j)$ because m_j encrypted pseudonyms will be uploaded to the permissioned blockchain. For MO, it takes $O(n_p)$ communication complexity for both *Location Query* and *Location Publication* processes because the information of m_j states will be obtained by querying the permissioned blockchain and uploading on the permissionless blockchain, respectively.

We evaluate the communication cost for users, fog nodes, and MOs in our experiment, as shown in Table 2, where we set the number of users $m = 1000$. It can be observed that the communication costs for users, fog nodes, and MOs are all less than 10KB, which is quite efficient. Therefore, PTBM achieves high communication efficiency and can well save the bandwidth usage and reduce the delay of the 5G-integrated infrastructure.

7.4. Summary

Table 3 shows both the time and communication complexity of the proposed PTBM. Through the experimental evaluation, it is observed that the execution time of the most aforementioned processes (except the *Registration* process that is executed only once) is not related to the number of users. More specifically, it only takes less than 40ms for each of the given operations to complete. Hence, PTBM can operate with high computation efficiency, which means that the fog nodes can handle a large number of user requests. For users and MOs, they can efficiently check the published location and query the location of a given patient, respectively. Besides, MC can quickly trace the information of patient activity or contacts uploaded by fog nodes. Besides, the empowerment of the 5G-integrated and blockchain-based network eliminates the burden of the centralized server compared to existing schemes with centralized architecture with higher communication bandwidth & lower delay.

Table 2
Communication costs.

Operation	User	Fog Node	MO
Information Uploading	<1KB	8.74KB	-
Route Query	-	-	<1KB
Location Publication	-	-	5.61KB
Location Ckecking	5.24KB	-	-

Table 3
Time and communication complexity of PRVB.

Process	Entity	Time Complexity	Communication Complexity
Registration	MC	$O(m+n)$	-
Information Uploading	User	$O(1)$	$O(1)$
	Fog Node	$O(1)$	$O(m_j)$
Route Query	MO	$O(1)$	$O(n_p)$
Location Publication	MO	$O(1)$	$O(n_p)$
Location Checking	User	$O(1)$	$O(1)$
Patient Tracing	MC	$O(1)$	-
Contact Tracing	MC	$O(m_j \cdot n_p)$	-

8. Conclusion and future work

Int his work, we propose PTBM, a privacy-preserving patient contact tracing scheme that enables tracing the current route of a patient with infectious diseases (e.g., COVID-19), and location checking of public without violating their identity & location privacy. More specifically, permissionless and permissioned blockchain is used to achieve public location checking and reliable route storage respectively. Bloom filters, PCSD cryptosystem, pseudo-random functions, and hash function also enhance the privacy-preserving property of the proposed scheme. Theoretical analysis and experimental evaluations also show that the proposed PTBM scheme achieves privacy protection, reliability, and traceability with low computation & communication complexity.

For future work, we will consider leveraging this blockchain-based solution for more comprehensive patient management, vaccination protocols, and protected information sharing with the international organizations in a global pandemic scenario. Besides, how to integrate the emerging 5G technology to other relevant medical application that demands high communication reliability and low latency is also a promising research direction.

CRediT authorship contribution statement

Can Zhang: Conceptualization, Methodology, Software, Writing - original draft. **Chang Xu:** Resources, Investigation, Formal analysis.

Kashif Sharif: Writing - review & editing. **Liehuang Zhu:** Supervision, Funding acquisition.

Declaration of Competing Interest

We declare that we have no conflicts of interest to this work. We do not have any commercial or associative interest that represents a conflict of interest in connection with the work submitted.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant Nos. 61972037, 61402037, 61872041, U1836212).

References

[1] A. Ahad, M. Tahir, M.A. Sheikh, K.I. Ahmed, A. Mughees, A. Numani, Technologies trend towards 5g network for smart health-care using iot: a review, Sensors 20 (14) (2020) 4047, https://doi.org/10.3390/s20144047.

[2] N. Ahmed, R.A. Michelin, W. Xue, S. Ruj, R.A. Malaney, S.S. Kanhere, A. Seneviratne, W. Hu, H. Janicke, S.K. Jha, A survey of COVID-19 contact tracing apps, IEEE Access 8 (2020) 134577–134601, https://doi.org/10.1109/ACCESS.2020.3010226.

[3] G. Apple, How Apple and Google are enabling COVID-19 contact-tracing, 2020, URL https://www.wired.com/story/apple-google-bluetooth-contact-tracing-covid-19/.

[4] B. Bera, S. Saha, A.K. Das, N. Kumar, P. Lorenz, M. Alazab, Blockchain-envisioned secure data delivery and collection scheme for 5g-based iot-enabled internet of drones environment, IEEE Trans. Veh. Technol. 69 (8) (2020) 9097–9111, https://doi.org/10.1109/TVT.2020.3000576.

[5] Q. Bi, Y. Wu, S. Mei, C. Ye, X. Zou, Z. Zhang, X. Liu, L. Wei, S.A. Truelove, T. Zhang, W. Gao, C. Cheng, X. Tang, X. Wu, Y. Wu, B. Sun, S. Huang, Y. Sun, J. Zhang, T. Ma, J. Lessler, T. Feng, Epidemiology and transmission of COVID-19 in 391 cases and 1286 of their close contacts in shenzhen, china: a retrospective cohort study, The Lancet Infectious Diseases (2020), https://doi.org/10.1016/S1473-3099(20)30287-5.

[6] S. Biswas, K. Sharif, F. Li, S.P. Mohanty, Blockchain for e-health-care systems: easier said than done, Computer (Long Beach Calif) 53 (7) (2020) 57–67, https://doi.org/10.1109/MC.2020.2989781.

[7] V. Chamola, V. Hassija, V. Gupta, M. Guizani, A comprehensive review of the COVID-19 pandemic and the role of iot, drones, ai, blockchain, and 5g in managing its impact, IEEE Access 8 (2020) 90225–90265, https://doi.org/10.1109/ACCESS.2020.2992341.

[8] M.C. Chang, D. Park, How can blockchain help people in the event of pandemics such as theCOVID-19? J. Medical Systems 44 (5) (2020) 102, https://doi.org/10.1007/s10916-020-01577-8.

[9] M.Z. Chowdhury, M.T. Hossan, M. Shahjalal, M.K. Hasan, Y.M. Jang, A new 5g ehealth architecture based on optical camera communication: an overview, prospects, and applications, IEEE Consum. Electron. Mag. (2020) 1.

[10] G.G. Dagher, J. Mohler, M. Milojkovic, P.B. Marella, Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology, Sustainable Cities and Society 39 (2018) 283–297, https://doi.org/10.1016/j.scs.2018.02.014.

[11] K. Fan, Y. Ren, Y. Wang, H. Li, Y. Yang, Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5g, IET Commun. 12 (5) (2018) 527–532, https://doi.org/10.1049/iet-com.2017.0619.

[12] J.K. Fitzsimons, A. Mantri, R. Pisarczyk, T. Rainforth, Z. Zhao, A note on blind contact tracing at scale with applications to the COVID-19 pandemic, in: M. Volkamer, C. Wressnegger (Eds.), ARES 2020: The 15th International Conference on Availability, Reliability and Security, Virtual Event, Ireland, August 25–28, 2020, ACM, 2020, pp. 92:1–92:6, https://doi.org/10.1145/3407023.3409204.

[13] W.E. Forum, 5g outlook series: The impact of mobile technology on the response to COVID-19, 2020, URL http://www3.weforum.org/docs/WEF_Global_Accelerator_Program_5G_Outlook_Report_2020.pdf.

[14] W.E. Forum, These are the 10 most discussed tech topics during covid-19, 2020, URL https://www.weforum.org/agenda/2020/07/0-top-tech-topics-during-covid-19-india-china-us-eu/.

[15] J. Gao, K.O.O. Agyekum, E.B. Sifah, K.N. Acheampong, Q. Xia, X. Du, M. Guizani, H. Xia, A blockchain-sdn-enabled internet of vehicles environment for fog computing and 5g networks, IEEE Internet Things J. 7 (5) (2020) 4278–4291, https://doi.org/10.1109/JIOT.2019.2956241.

[16] P. Gorla, C. Vinay, H. Vikas, K. Neeraj, Blockchain for 5g: a prelude to future telecommunication, IEEE Netw PP (99) (2020).

[17] T. Hewa, A. Bracken, M. Ylianttila, M. Liyanage, Blockchain-based automated certificate revocation for 5g iot. 2020 IEEE International Conference on Communications, ICC 2020, Dublin, Ireland, June 7–11, 2020, IEEE, 2020, pp. 1–7, https://doi.org/10.1109/ICC40277.2020.9148820.

[18] IBM, How much would a data breach cost your business?, 2019, URL https://www.ibm.com/security/data-breac.

[19] S. Jangirala, A.K. Das, A.V. Vasilakos, Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5g mobile edge computing environment, IEEE Trans. Ind. Informatics 16 (11) (2020) 7081–7093, https://doi.org/10.1109/TII.2019.2942389.

[20] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, S. Liu, Blockchain-based data preservation system for medical data, J. Medical Systems 42 (8) (2018) 141:1–141:13, https://doi.org/10.1007/s10916-018-0997-3.

[21] L. Li, Q. Zhang, X. Wang, J.J. Zhang, T. Wang, T. Gao, W. Duan, K.K. Tsoi, F. Wang, Characterizing the propagation of situational information in social media during COVID-19 epidemic: a case study on weibo, IEEE Trans. Comput. Social Systems 7 (2) (2020) 556–562, https://doi.org/10.1109/TCSS.2020.2980007.

[22] S. Linoy, H. Mahdikhani, S. Ray, R. Lu, N. Stakhanova, A.A. Ghorbani, Scalable privacy-preserving query processing over ethereum blockchain. IEEE International Conference on Blockchain, Blockchain 2019, Atlanta, GA, USA, July 14–17, 2019, IEEE, 2019, pp. 398–404, https://doi.org/10.1109/Blockchain.2019.00061.

[23] E. Liu, E.E. Effiok, J. Hitchcock, Survey on health care applications in 5g networks, IET Commun. 14 (7) (2020) 1073–1080, https://doi.org/10.1049/iet-com.2019.0813.

[24] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, M. Guizani, BPDS: A blockchain based privacy-preserving data sharing for electronic medical records. IEEE Global Communications Conference, GLOBECOM 2018, Abu Dhabi, United Arab Emirates, December 9–13, 2018, IEEE, 2018, pp. 1–6, https://doi.org/10.1109/GLOCOM.2018.8647713.

[25] X. Liu, B. Qin, R.H. Deng, R. Lu, J. Ma, A privacy-preserving outsourced functional computation framework across large-scale multiple encrypted domains, IEEE Trans. Computers 65 (12) (2016) 3567–3579, https://doi.org/10.1109/TC.2016.2543220.

[26] I. Mistry, S. Tanwar, S. Tyagi, N. Kumar, Blockchain for 5g-enabled iot for industrial automation: a systematic review, solutions, and challenges, Mech Syst Signal Process 135 (2020) 106382, https://doi.org/10.1016/j.ymssp.2019.106382.

[27] MIT, Bluetooth signals from your smartphone could automate COVID-19 contact tracing while preserving privacy, 2020, URL http://news.mit.edu/2020/bluetooth-covid-19-contact-tracing-0409.

[28] L. Nkenyereye, B.A. Tama, M.K. Shahzad, Y. Choi, Secure and blockchain-based emergency driven message protocol for 5g enabled vehicular edge computing, Sensors 20 (1) (2020) 154, https://doi.org/10.3390/s20010154.

[29] M. Shen, Y. Deng, L. Zhu, X. Du, N. Guizani, Privacy-preserving image retrieval for medical iot systems: a blockchain-based approach, IEEE Netw 33 (5) (2019) 27–33, https://doi.org/10.1109/MNET.001.1800503.

[30] Q. Tang, Privacy-preserving contact tracing: current solutions and open questions, CoRR abs/2004.06818 (2020).

[31] A.M. Wong, C. Hsu, T. Le, M. Hsieh, T. Lin, Three-factor fast authentication scheme with time bound and user anonymity for multi-server e-health systems in 5g-based wireless sensor networks, Sensors 20 (9) (2020) 2511, https://doi.org/10.3390/s20092511.

[32] H. Xu, L. Zhang, O. Onireti, Y. Fang, W.B. Buchanan, M.A. Imran, Beeptrace: blockchain-enabled privacy-preserving contact tracing for COVID-19 pandemic and beyond, CoRR abs/2005.10103 (2020).

[33] S. Xu, J. Ning, Y. Li, Y. Zhang, G. Xu, X. Huang, R.H. Deng, Match in my way: fine-grained bilateral access control for secure cloud-fog computing, IEEE Transactions on Dependable and Secure Computing. (2020), https://doi.org/10.1109/TDSC.2020.3001557.

[34] S. Xu, G. Yang, Y. Mu, Revocable attribute-based encryption with decryption key exposure resistance and ciphertext delegation, Inf. Sci. 479 (2019) 116–134, https://doi.org/10.1016/j.ins.2018.11.031.

[35] S. Xu, G. Yang, Y. Mu, X. Liu, A secure iot cloud storage system with fine-grained access control and decryption key exposure resistance, Future Gener. Comput. Syst. 97 (2019) 284–294, https://doi.org/10.1016/j.future.2019.02.051.

[36] K. Xue, B. Zhu, Q. Yang, D.S.L. Wei, M. Guizani, An efficient and robust data aggregation scheme without a trusted authority for smart grid, IEEE Internet Things J. 7 (3) (2020) 1949–1959, https://doi.org/10.1109/JIOT.2019.2961966.

[37] Y. Xue, K. Xue, N. Gai, J. Hong, D.S.L. Wei, P. Hong, An attribute-based controlled collaborative access control scheme for public cloud storage, IEEE Trans. Inf. Forensics Secur. 14 (11) (2019) 2927–2942, https://doi.org/10.1109/TIFS.2019.2911166.

[38] C. Zhang, L. Zhu, C. Xu, K. Sharif, X. Liu, PPTDS: A privacy-preserving truth discovery scheme in crowd sensing systems, Inf. Sci. 484 (2019) 183–196, https://doi.org/10.1016/j.ins.2019.01.068.

[39] C. Zhang, L. Zhu, C. Xu, K. Sharif, C. Zhang, X. Liu, PGAS: Privacy-preserving graph encryption for accurate constrained shortest distance queries, Inf. Sci. 506 (2020) 325–345, https://doi.org/10.1016/j.ins.2019.07.082.

[40] C. Zhang, L. Zhu, C. Xu, C. Zhang, K. Sharif, H. Wu, H. Westermann, BSFP: blockchain-enabled smart parking with fairness, reliability and privacy protection, IEEE Trans. Veh. Technol. 69 (6) (2020) 6578–6591, https://doi.org/10.1109/TVT.2020.2984621.

[41] K. Zhang, Y. Zhu, S. Maharjan, Y. Zhang, Edge intelligence and blockchain empowered 5g beyond for the industrial internet of things, IEEE Netw 33 (5) (2019) 12–19, https://doi.org/10.1109/MNET.001.1800526.

[42] N. Zhaolong, D. Peiran, W. Xiaojie, H. Xiping, G. Liang, H. Bin, G. Yi, Q. Tie, K. Ricky, Mobile edge computing enabled 5g health monitoring for internet of medical things: a decentralized game theoretic approach, ieee journal on selected areas in communications, 2020, IEEE J. Sel. Areas Commun. (2020).