IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 12, 2019, accepted June 25, 2019, date of publication June 28, 2019, date of current version July 18, 2019.

*Digital Object Identifier 10.1109/ACCESS.2019.2925625*

# Flexible and Efficient Blockchain-Based ABE Scheme With Multi-Authority for Medical on Demand in Telemedicine System

**RUI GUO[1,2], HUIXIAN SHI[3], DONG ZHENG[1], CHUNMING JING[1], CHAOYUAN ZHUANG[1], AND ZHENGYANG WANG[1]**

[1]National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
[2]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
[3]Department of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710069, China

Corresponding author: Rui Guo (guorui@xupt.edu.cn)

This work was supported in part by the National Key R&D Program of China under Grant 2017YFB0802000, in part by the Natural Science Foundation of China under Grant 61802303, Grant 61772418, and Grant 61602378, in part by the Key Research and Development Program of Shaanxi under Grant 2019KW-053, in part by the Innovation Ability Support Program in Shaanxi Province of China under Grant 2017KJXX-47, in part by the Natural Science Basic Research Plan in Shaanxi Province of China under Grant 2016JM6033 and Grant 2018JZ6001, in part by the Open Foundation of State key Laboratory of Networking and Switching Technology (Beijing University of Posts and Telecommunications) under Grant SKLNST-2016-2-11, in part by the Fundamental Research Funds for the Central Universities under Grant GK201903005, and in part by the New Star Team of Xi'an University of Posts and Telecommunications under Grant 2016-02.

**ABSTRACT** Telemedicine offers a medical-on-demand (MoD) service from a distance. This technology is designed to overcome distance barriers and improve the process of accessing medical services in distant rural communities. With the development of cloud computing, the MoD services in the telemedicine system are provided by the Cloud Service Provider (CSP). This CSP connects the patient and the medical staff in different places with both convenience and fidelity. Meanwhile, the outsourcing healthcare data on public cloud platforms bring some new challenges on the security. Although attribute-based encryption (ABE) algorithm realizes flexible and fine-grained access control, a large number of patients subscribe or unsubscribe the different medical services frequently in the cloud, which takes a huge cost for membership management. In this paper, an ABE scheme is presented to achieve the dynamic authentication and authorization with higher flexibility and efficiency for the MoD services in telemedicine system. On the one hand, when the patient alters his ordered service, it requires no updating on the parameters for those whose statuses remain unchanged. We construct an independent-update key policy ABE scheme in the distributed telemedicine system that aims to updates patient's keys separately, and there are multiple authorities to manage this system altogether which is more similar to the real situation. On the other hand, by using blockchain and distributed database technologies, the private healthcare data stored in public cloud is protected in integrity, which avoids the misdiagnosis accident from the inaccurate electronic health records distorted by a malicious user or authority from the inner cloud. Finally, we analyze the collusion attack in multiple authorities and formally prove the security of this protocol in a standard model. After comparing and simulating, the results of this work show a better performance.

**INDEX TERMS** Attribute-based encryption, blockchain, independent-update, multi-authority, medical on demand.

## I. INTRODUCTION

As the population grows, the requirement of medical resource increase dramatically in the healthcare system. Patients living in underdeveloped areas, where traffic is inconvenient, are extremely lack of mobility as well as access authority to high quality healthcare, especially for the aged or disabled ones. The telemedicine system enables to bridge this gap [1]. This system takes advantage of telecommunication and information technology to supply the remote healthcare resource, which overcomes the distance barriers to improve the medical services in remote rural communities, and even saves the life in the critical and emergency situation [2].

The associate editor coordinating the review of this manuscript and approving it for publication was Donghyun Kim.

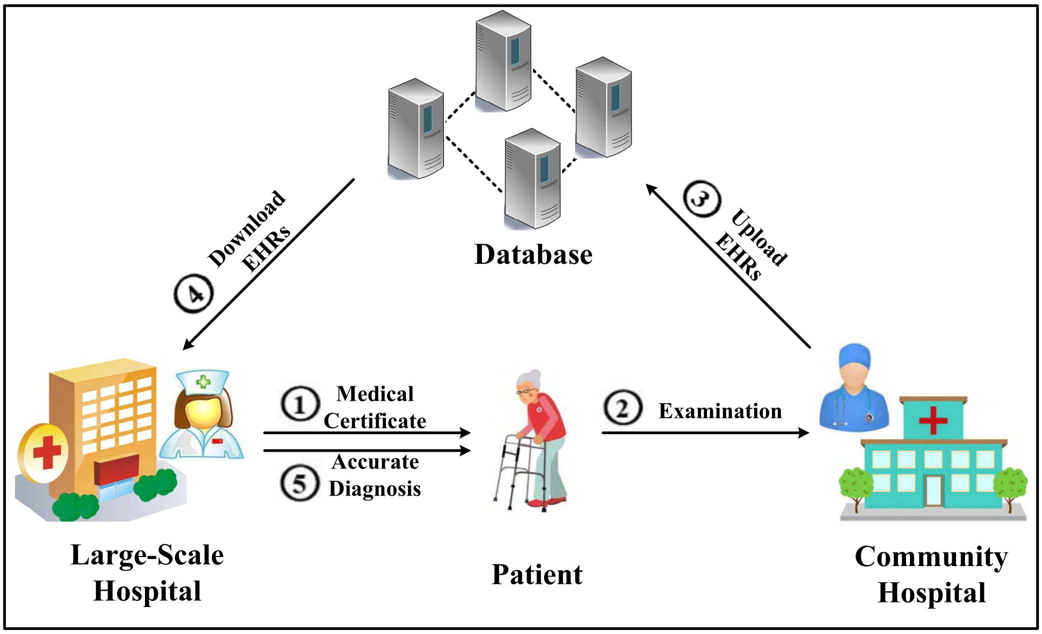



**FIGURE 1.** MoD service in the telemedicine system.

Medical on demand (MoD) is aroused with the development of telemedicine system recently. As shown in FIGURE 1, patient is permitted to communicate with the most eminent doctors or specialists in distance without visiting them face to face. According to the medical certificate from the remote specialist in the large scale hospital, patient does some laboratory tests and physical examinations on demand in local or community hospital, whose responsibility is uploading the electronic health records (EHRs) to the database (or cloud). After receiving the patient's examination reports, the remote specialist makes out the accurate diagnosis on him. In this model, the telemedicine system supports remote diagnose and prescription verification, which saves the precious medial resource and reduces the overall cost of healthcare for poverty-stricken patient. Moreover, this system allows healthcare specialist in different places to share information and discuss the diagnostic results as if they are staying in the meeting room [3], [4]. In the face of serious illness, this system can also avoid the transmission of infectious diseases or parasites between infectors and medical staffs (e.g., SARS).

Nowadays, the telemedicine system is usually established by Cloud Server Provider (CSP) who provides a virtual platform that allows doctors and patients to work together for overall wellness and health, and supports in-home care. By means of this platform, it builts up the communication links among patient, medical staff and storage server. Patient could subscribe some medical services on demand for greater access to quality care and improving his experiences. Cloud server is responsible to store EHRs and other related healthcare data. As for specialist and researcher, they access the physical data stored in the cloud to make accurate diagnosis and do some scientific researches. Cloud computing has changed the traditional model of medical care on paper into a digital one [5]–[7].

Cloud computing provides a shared pool of different types of configurable computing resources (such as networks, storage and services) to users on an on-demand basis [8]. In the cloud, users enjoy the convenient service from all the underlying cloud infrastructure maintained by the CSP. And the aim of cloud includes cutting costs and capital expenditures, improving operational efficiency, and helping the users focus on the core business instead of being impeded by IT obstacles [9], [10]. Therefore, several types of cloud computing models on health have been created in the last few years. For instance, Microsoft and Google have established Microsoft Health Vault [11] and Google Health [12] to provide the medical infrastructure as a service.

Although it shows a lot of advantages to the medical services, cloud computing also brings some security challenges [13]–[19]. In the cloud, all the sensitive data related to patient is controled by CSP, such as name, address, social security number, allergic history and so on. Normally, the service provider is a commercial enterprize (such as Amazon and IBM) that cannot be trusted completely. These enterprizes enable to access users' privacy at any time, and alter or delete data accidentally or deliberately. Consequently, it is necessary to restrict the behaviors of curious CSP and unauthorized users, and prevent the information stored in cloud from being tampered. However, the traditional cryptography paradigm adopts one-to-one mode to provide security protection, which is inconsistent with characteristics of cloud computing with flexibility, distributed management, and data sharing.

With regards to access authority and confidentiality in cloud, one of the preeminent cryptographic primitives is Attribute-Based Encryption (ABE) [20]–[22], which provides the encryption-decryption ability according to the attributes of user. In an ABE scheme, it can be executed as one-to-many mode. Anyone has capability of decrypting the protected data by using a set of data owner's attribute, if and only if the partial components of the encrypted data are matched with the components of the private key. On basis of this characteristic, the data owner could upload the data to a public cloud server without apprehension [23]. Depending on the different relationships among access structures, private keys and ciphertexts, ABE scheme is divided into Key-Policy ABE (KP-ABE) [21] and Ciphertext-Policy ABE (CP-ABE) [22] generally. In KP-ABE, the private keys of user are associated with designated policies, as well as the ciphertexts are labeled by some sets of attribute. This user enables to decrypt the ciphertext only if the access policy of private key is satisfied by the attributes embedded in this ciphertext, which reflects the user's permissions. Hence, KP-ABE is usually applied to protect the outsourced data on confidentiality [23]. As for CP-ABE, the ciphertext is attached with some policies, and the private key of user is described by a set of attribute. This user can decrypt a ciphertext with access tree if and only if the attributes attached with the private key satisfy this access structure, which reflects some requirements for the decryptor. CSP has ability to tag medical services by attributes in telemedicine system and distribute the private key under user's subscription, instead of tagging user. Consequently, KP-ABE is better for providing access authority and confidentiality for MoD services than CP-ABE.

Furthermore, CSP has stored the mutual information between doctor and patient, including diagnostic opinions, physical data and so on. Any minor changes on these information will lead to the serious consequences on patient and the whole system. Accordingly, it is crucial to provide integrity protection on the data in the telemedicine system, and the blockchain technology is an excellent choice. Blockchain was developed to serve as the public transaction distributed ledger of the bitcoin by Satoshi Nakamoto in 2008 [24], which can record transactions between two parties efficiently and in a verifiable and permanent way. The primary function of blockchain today has been expanded from a distributed ledger for cryptocurrencies to IoT and cloud computing [25]–[29]. For instance, the current telemedicine system is totally controlled by CSP, which is the main target by the hacker. Taking advantage of the blockchain, it encapsulates all transactions into the immutable distributed ledger that ensures the responsibility and transparency in the medical service [30]–[32]. Therefore, the blockchain is available for providing integrity of the medical data, helping the telemedicine system reduce the medical accidents and preserving the privacy.

### A. RELATED WORKS

ABE protocol plays an important role in the confidentiality and fine-grained access control for the medical services in cloud. Sahai and Waters adopted the attribute-based structure to design a cryptographic primitive [20]. However, in the distributed cloud system, dynamic membership is vitally important to ABE. Li *et al*. [33] put forward a KP-ABE scheme as access control in the healthcare of cloud, but it was inefficient in user/attribute revocation, which needed to update other users' private keys. Liang *et al*. [34] presented a CP-ABE protocol with efficient user revocation in single authority. However, this scheme achieved no forward security, so that a revoked entity could decrypt the previous accessed data as usual. Based on the CP-ABE framework, Fan *et al*. [35] firstly provided an efficient scheme with arbitrary-state to satisfy the feature of dynamic membership in 2014. In their protocol, every entity needed to interact with authority to update his/her attribute value. He *et al*. [23] designed an independent-update KP-ABE scheme to renew user's key separately. This protocol changed the access policy to guarantee the forward security and other users would not be influenced. Wei *et al*. [36] gave a novel CP-ABE scheme for cloud storage system with multi-authority. This scheme supported dynamic user revocation while the system public parameter remaining unchanged. But this protocol permited the server to update the ciphertext by only using of the public parameters without the help of the data owner and the authority. Therefore, everyone in this system must trust the CSP unconditionally.

Recently, there are some works making the effort to apply attribute-based cryptography to the blockchain. Guo *et al*. [37], in the EHRs system, employed an attribute-based signature scheme with multi-authority to verify the facticity of the block, in which is stored with the patient's sensitive data. In their protocol, a patient published his physical data in a block anonymously, and set the access policy for those who desired to obtain these data. Wang *et al*. [38] adopted ABE method to distribute secret key and encrypt shared data in the cloud. In this scheme, the blockchain technology ensures that the keyword search function on the ciphertext is implemented. Wang and Song [39] combined the ABE, IBE, IBS and blockchain in one cryptosystem to facilitate the management of the system. To promote the data sharing and preserve privacy, Liu *et al*. [40] proposed a blockchain-based privacy-preserving data sharing scheme for EMRs, which was stored in the cloud and the indexes were reserved in a tamper-proof consortium blockchain. Zhang *et al*. [41] presented an access control solution for exchanging blockchain-based EMRs that omitted the gateway in order to authorize users' access with block level granularity. Recently, Mohsin *et al*. [42] gave a novel verification secure framework for patient authentication between a patient enrollment device and a node database. The blockchain technique guaranteed the integrity and traceability of the medical data.

Conclusions as a result, considering the flexibility and distributed requirements of MoD services in the telemedicine system, this work concerns about constructing a KP-ABE scheme to achieve confidentiality and fine-grained access control with features of independence and multi-authority co-management. Moreover, we utilize the blockchain technology to ensure the integrity and traceability of patient sensitive data.

### B. CONTRIBUTIONS

In this paper, taking the telemedicine system in cloud computing into consideration, a blockchain-based multi-authority KP-ABE with independent-update is proposed, which is suitable for being applied in the distributed telemedicine system. Our contributions are as follows.

(a) First of all, user in this system can dynamically join and leave freely, and he/she updates or revokes access policy on-demand while other users will not be influenced, which enjoys the forward security.

(b) Secondly, we adopt the mode of multi-authority co-management for meeting the requirements of the distributed telemedicine system. Furthermore, it shares one pseudorandom function seed privately in every two authorities. Beside that, in every user's private key, it contains each authority's private key to resist ($N$-1) corrupted authorities at most in the collusion attack.

(c) Thirdly, provided that the Decisional Bilinear Diffie-Hellman (DBDH) assumption holds, the security of this scheme is proven in the standard model. Moreover, the comparisons demonstrate that our protocol has a better performance.

(d) Fourthly, this scheme employs the blockchain technology on the medical data transmitted between the doctor and the patient, which provides the integrity and traceability of those sensitive data.

### C. ORGANIZATION

The framework of this paper is designed as following. Section 2 demonstrates a overview of preliminaries, the bilinear mapping, the security assumption and some definitions. Section 3 presents the blockchain-based model of the telemedicine system while Section 4 describes the detailed construction of our proposal. In section 5, we give formal security proof and performance analysis between this protocol and other related works. Finally, the conclusions of this work is given in Section 6.

## II. PRELIMINARIES

### A. BILINEAR MAPPING

Supposing that $(G, G_T)$ are the two cyclic groups of prime order $p$. $\hat{e} : G \times G \rightarrow G_T$ is a bilinear mapping with generator $g$ of $G$ which satisfies the following properties:

(a) *Bilinearity*: For all $g, h \in G$, $a, b \in Z_p$, we have $\hat{e}(ag, bh) = \hat{e}(g, h)^{ab}$.

(b) *Non-Degeneracy*: There exists $\hat{e}(g, g) \neq 1 \in G_T$.

(c) *Computability*: There is an efficient algorithm to compute $\hat{e}(g, h)$ for all $g, h \in G$.

### B. DEFINITIONS

*Definition 1 (DBDH Problem):* Let $G$ and $G_T$ be two cyclic groups with prime order $p$, $g$ be the generator of $G$, and $\hat{e} : G \times G \rightarrow G_T$ be a bilinear mapping. The Decisional Bilinear Diffie-Hellman (DBDH) problem is that given the tuple $(g, ag, bg, cg, Z)$, where $Z \in G_T$ and $a, b, c \in Z_p^*$, decides whether $Z = \hat{e}(g, g)^{abc}$ holds or not.

*Definition 2 (DBDH Assumption):* Provided that there is a probabilistic polynomial-time (PPT) adversary $\mathcal{A}$, who can distinguish $Z$ from $\hat{e}(g, g)^{abc}$ with advantage

$$Adv_{DBDH}(\mathcal{A}) = \mid \Pr[\mathcal{A}(g, ag, bg, cg, \hat{e}(g, g)^{abc}) = 1] - \Pr[\mathcal{A}(g, ag, bg, cg, Z) = 1] \mid,$$

where the probability is over the random choice of $a, b, c \in Z_p^*$ and $Z \in G_T$. The DBDH assumption is stated if there is no PPT adversary that has non-negligible advantage in solving the DBDH problem.

*Definition 3 (Independence):* An ABE scheme with independence should satisfy the following:

(a) The private key of user could be revoked, and this revoked key is useless to those protected data after the revocation. The private key also could be renewed, and the old private key is useless after renewing.

(b) When the private key revoking or renewing occurs, the other users in the system are unnecessary to interact with authority to renew their private keys.

*Definition 4 (Correctness):* An ABE scheme is correct, provided that for $CT \leftarrow$ **Encrypt**$(PK, \tilde{A}, M)$, $D_i \leftarrow$ **KeyGen**$(\mathbb{A}, PK)$, the equation **Decrypt**$(CT, D_i) = M$ holds for any user $i$ whose access policy $\mathbb{A}$ satisfies that $\mathbb{A}(\tilde{A}) = TRUE$, where $\tilde{A}$ is an attribute set.

*Definition 5 (Scheme Model):* This ABE scheme contains the following algorithms:

**Global Setup** $(1^\delta) \rightarrow params$: Taking a security parameter $1^\delta$ as input, this algorithm generates the public parameters $params$ of system.

**Authority Setup** $(1^\delta) \rightarrow (PK_k, SK_k)$: For every $k \in \{1, 2, \cdots, N\}$, every authority $A_k$ outputs his public key $PK_k$ and private key $SK_k$, where $N$ is the number of authority.

**KeyGen** $(SK_k, \mathsf{GID}, \mathbb{A}) \rightarrow SK_U$: Each authority $A_k$ and data consumer $U$ execute this algorithm altogether to output the private key $SK_U$ of $U$. It inputs the tuple $(SK_k, \mathsf{GID}, \mathbb{A})$, where $SK_k$ is the private key of $A_k$, $\mathbb{A}$ is an access policy corresponding to the data consumer and GID is its global identifier. And then, this algorithm outputs the private key $SK_U$ of $U$.

**Revoke** $(i)$: When user $i$ is revoked, this algorithm will be executed and the corresponding public key $PK_i$ will be updated.

**Encrypt** $(params, PK_k, \tilde{A}, M) \rightarrow CT$: This algorithm inputs the parameters $params$, the public key $PK_k$ of each authority $A_k$, a set of attribute $\tilde{A}$ and a message $M$. It will return the ciphertext $CT$.

**ReEncrypt** $(params, CT) \rightarrow CT^*$: This algorithm takes the public parameters *params*, an exist ciphertext $CT$, after revocation, it returns the updated ciphertext $CT^*$.

**Decrypt** $(PK_k, SK_U, CT) \rightarrow M$: This algorithm takes the ciphertext $CT$ and the private key $SK_U$ of $U$ as inputs, if the access policy $\mathbb{A}$ of $U$ satisfies $\mathbb{A}(\tilde{A}) = TRUE$, it decrypts the ciphertext and outputs the message $M$ successfully. Otherwise, $\perp$ is returned.

*Definition 6 (Security Model):* Let $\mathcal{A}$ be an PPT adversary and $\prod$ be an ABE scheme with multiple authorities. The adversary $\mathcal{A}$ interacts with a challenger $\mathcal{C}$ as follows.

*Global Setup*: Challenger $\mathcal{C}$ executes **Global Setup** and outputs the parameters *params* to $\mathcal{A}$. Adversary $\mathcal{A}$ submits a list of corrupted authorities $L_A$ to $\mathcal{C}$, and the challenging access structure is $\mathbb{A}^*$.

*Authority Setup*: If the authority is corrupted, the challenger $\mathcal{C}$ sends the public and private keys ($PK_k$,$SK_k$) to adversary $\mathcal{A}$. On the contrary, for the honest authority, the challenger $\mathcal{C}$ only transmits the public key $PK_k$ to $\mathcal{A}$.

*Phase 1*: The adversary $\mathcal{A}$ makes query on the following four algorithms:

*KeyGen*($\mathbb{A}$): This algorithm is aimed to extract user $i$'s private key $SK_i$, where $\mathbb{A}$ is the access structure belonging to $i$. Then, $SK_i$ is recorded in a list $L_{SK}$.

*Revoke*($i$): This algorithm is aimed to revoke the private key of user $i$. After revocation, $PK_i$ is updated while $SK_i$ is deleted from $L_{SK}$.

*Update*($i$, $\mathbb{A}'$): This algorithm is aimed to modify the access policy of $i$ into $\mathbb{A}'$. After updating, this updated private key is delivered to adversary $\mathcal{A}$. Accordingly, both $PK_i$ and $L_{SK}$ will also be renewed.

*Decrypt*($CT$): This algorithm is aimed to decrypt a given ciphertext $CT$ and outputs the corresponding plaintext $M$. If $CT$ is not correctly protected, this algorithm outputs $\perp$ as a result.

*Challenge*: The adversary $\mathcal{A}$ submits $(M_0, M_1, \tilde{A})$ to the challenger, where $M_0$ and $M_1$ are two messages with equal-length and $\tilde{A}$ is a set of attribute. $\mathcal{C}$ flips a random coin $\theta \in \{0, 1\}$ and encrypt $M_\theta$ with $\tilde{A}$. The protected data $CT^*$ is transmitted to adversary $\mathcal{A}$. Provided that there exist $SK \in L_{SK}$ which can decrypt $CT^*$, this query will be aborted.

*Phase 2*: In this phase, $\mathcal{A}$ executes those algorithms in *Phase 1* repeatly with restriction that $\mathcal{A}$ cannot make queries on *Decrypt*($CT^*$) and *KeyGen*($\mathbb{A}$), where $\mathbb{A}(\tilde{A}) = TRUE$ holds.

*Guess*: Adversary $\mathcal{A}$ outputs his guess $\theta' \in \{0, 1\}$ on $\theta$, it wins this game if $\theta' = \theta$. The advantage of adversary $\mathcal{A}$ in this model is defined as

$$Adv_{\prod}^{CCA-DM}(\mathcal{A}) = \mid \Pr[\theta' = \theta] - \frac{1}{2} \mid .$$

*Definition 7 (CCA-DM Secure:)* A multi-authority ABE protocol $\prod$ with dynamic membership is considered as CCA-DM secure, provided that, for any adversary $\mathcal{A}$, $Adv_{\prod}^{CCA-DM}(\mathcal{A})$ is negligible in polynomial time.

## III. BLOCKCHAIN-BASED MOD SERVICE IN THE TELEMEDICINE SYSTEM

Telemedicine takes advantage of information and communication technologies to overcome geographical barriers, and increases access to healthcare services. Implementation of telemedicine has been considered to be particularly beneficial in improving the user experience and saving the limited medical resource and cost. Combining the cloud computing technology, sharing of healthcare data in the telemedicine system helps doctors make accurate diagnosis in time and provide better quality care for patients.

Healthcare data in the telemedicine system contains personal and sensitive information that may be attractive to cybercriminals. Therefore, a big challenge for telemedicine system is how to store, share and utilize healthcare data without divulging the privacy. Moreover, the privacy and integrity of healthcare data must be protected not only from external attacker, but also from unauthorized access attempt from inside of the telemedicine system (e.g., authority and CSP).

How to construct the secure telemedicine system to guarantee the privacy and integrity of the healthcare data is an attractive research hotspot. As for privacy, we adopt KP-ABE protocol to regulate the limit access to the medical resource and ensure the confidentiality of data. As FIGURE 2 shown, a protected medical service is labeled with a set of attribute in the form of tags, such as electrocardiographic examination is tagged with coronary heart disease, angina pectoris, sinus arrhythmia and item price etc. The multiple authorities of the telemedicine system collaborate together to distribute keys with various access policies to the distinct patients. For instance, these authorities, who are responsible for user registration, healthcare subsidies, e-cash payment and so on, generate a key for Alice to decrypt the protected MoD service that her attributes satisfy ((Department of Cardiology) AND (( Coronary Heart Disease) OR (Angina Pectoris) OR (Sinus Arrhythmia)) AND (10 Dollars)). Hence, KP-ABE scheme can provide access control and data confidentiality in this telemedicine system.

As for integrity, we employ consortium blockchain that is managed by these multiple authorities in FIGURE 3. Specifically, after accessing the private key, Alice makes electrocardiographic examination with either the wearable medical device by herself in the house or the sophisticated professional equipment in the nearest community hospital. After that, these examination results, such as Electrocardiograph (ECG), Colour Doppler Ultrasound (CDU) and Physical Status Video (PSV), are uploaded to the database provided by CSP, and the indexes of these data containing the abstracts and keywords of results are stored in one block. For doctor and specialist, they download the examination results from cloud and return the medical certificate back to Alice by CSP. And for MoD services in the different days, it will generate only one block chronologically to store the

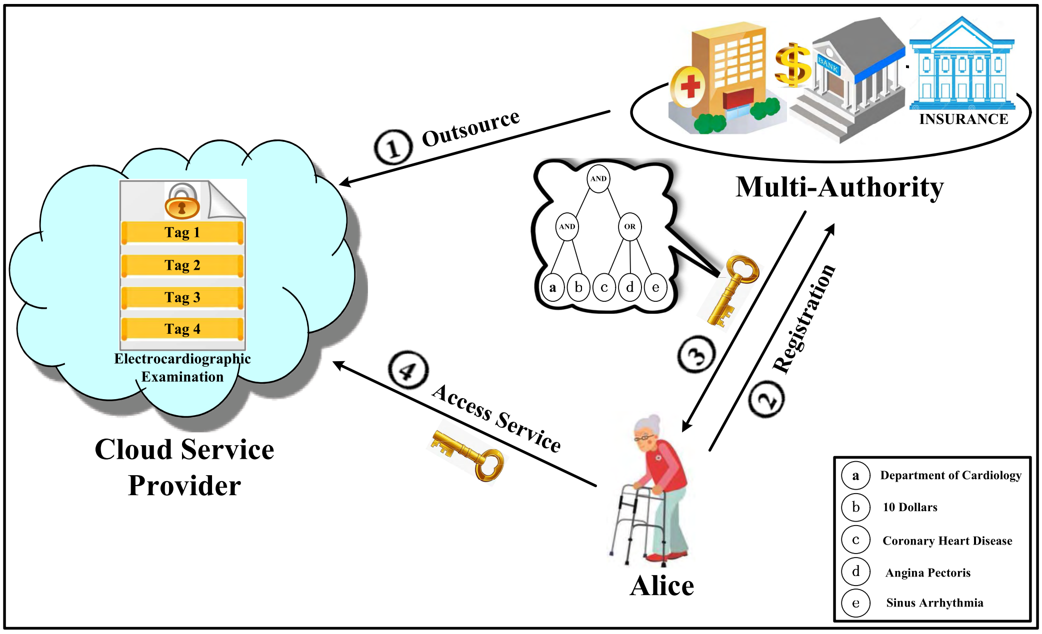



FIGURE 2. An example of access medical service based on KP-ABE.

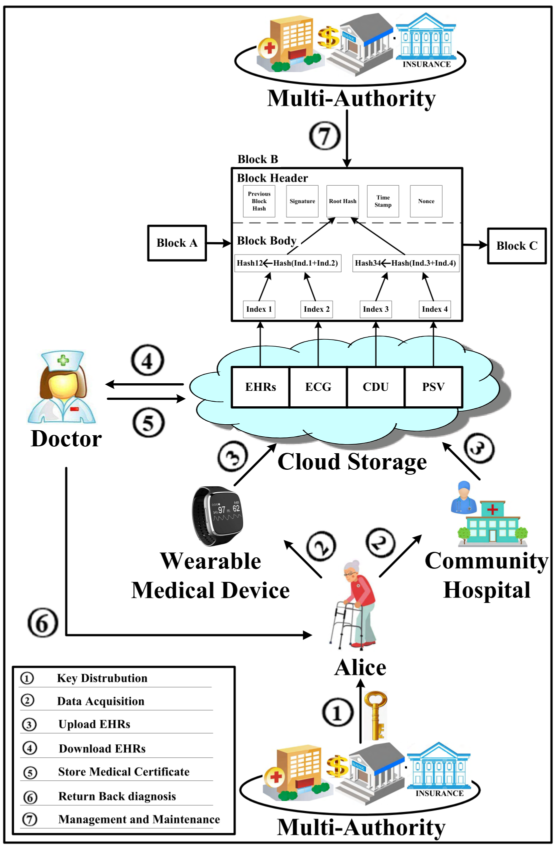



FIGURE 3. Blockchain-based MoD service in the telemedicine system.

indexes of the related healthcare data while the corresponding original data is stored in the cloud. These blocks on MoD services are connected in series into a blockchain that belonged to Alice. Because of the small size of index, it does not exceed the limitation of the storage space in every block. According to this model, any changes about the original healthcare data in cloud would cause that the corresponding index in the blockchain is altered, and each entity including Alice and all authorities will discover these variations. This technique achieves a global view of Alice's medical history in an efficient, verifiable and permanent method. Hence, the blockchain technique is benefit to providing the integrity protection on the healthcare data in cloud.

## IV. OUR CONSTRUCTION

### A. RELATIONSHIP BETWEEN THE PARTICIPANTS

This MoD service in the telemedicine system consists of four participants as shown in FIGURE 4, namely Multi-Authority (MA), Cloud Service Provider (CSP), Doctor and Patient. Specifically, the Multi-Authority in this system is the different organizations, such as Hospital, Bank, Medical Insurance Center, etc. They are responsible for managing the Doctor and Patient, including registration and revocation, key and parameters distribution. Moreover, these authorities outsource the MoD services to the CSP. As a storage platform, CSP is responsible for operating the various MoD services, storing the EHRs, diagnosis and other related healthcare data. Doctor accesses the patient's EHRs from CSP, and makes accurate diagnosis depending on these data. After that, it uploads the diagnosis into CSP for Patient's consideration.

In the following part, the KP-ABE scheme is designed to protect a symmetric data encryption key (DEK) between Patient and Doctor, which is used to access the medical service by Patient.

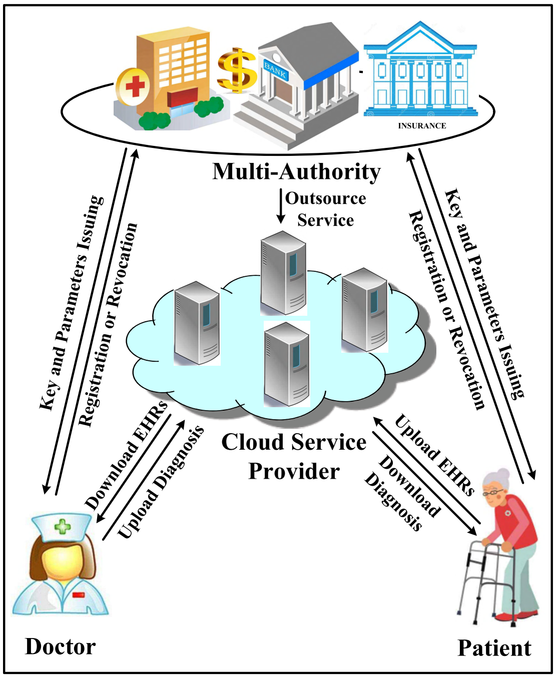



**FIGURE 4.** Relationship between the participants.

**TABLE 1.** Notation meaning.

| Notation | Meaning |
|---|---|
| $U$ | the set of registered patients |
| GID | the global identity of patient |
| $H$ | the strong collision-resistant hash function |
| $\mathbb{A}$ | the access policy |
| Ver | the version number of parameter |
| DEK | the symmetric data encryption key between doctor and patient |
| $\tilde{A}$ | the set of all provided attribute |
| $N$ | the number of authority |
| PRF | the pseudorandom function |
| $\lvert\tilde{A}\rvert$ | the number of elements in set $\tilde{A}$ |
| $n_q$ | the number of elements in attribute set of the $q$th authority |

## B. PROPOSED SCHEME

In this subsection, some notations are defined in TABLE 1 firstly. To satisfy the requirements of independent-update ABE scheme with multi-authority, we construct seven algorithms that are provided in detailed as follows.

**Global Setup**: This algorithm consists of three steps.

Step 1. Given the security parameter $1^\delta$, the telemedicine system generates a bilinear mapping $\hat{e} : G \times G \rightarrow G_T$ with generators $g, h$ of $G$, where $G$ and $G_T$ are additive cyclic group and multiplicative cyclic group respectively whose orders are the same prime value $p$.

Step 2. Generating two default patients with global identity $\{\mathsf{GID}_0, \mathsf{GID}_1\}$. Supposing that there is a strong collision-resistant hash function $H : \{0,1\}^* \rightarrow Z_p^*$, computing two default patients $U = \{u_0 = H(\mathsf{GID}_0), u_1 = H(\mathsf{GID}_1)\}$. Randomly choosing $2(|\tilde{A}|+1)$ elements $\{v_{i,j}\}_{\forall i \in U, j\in\{1,2,\ldots,|\tilde{A}|\}}$, and $\{t_i\}_{\forall i\in U}$ in $Z_p^*$, computing

$$\{V_j = (\prod_{\forall i\in U} v_{i,j})g\}_{j\in\{1,2,\ldots,|\tilde{A}|\}},$$

$$\{\overline{v_{i,j}} = \prod_{k\neq i, k\in U} v_{k,j}^{-1} + t_i v_{i,j}\}_{\forall i\in U, j\in\{1,2,\ldots,|\tilde{A}|\}}.$$

Step 3. The public parameters are the tuple of $params = (\hat{e}, G, G_T, p, g, h, H, \{V_j, \{\overline{v_{i,j}}\}_{\forall i\in U}\}_{\forall j\in\{1,2,\ldots,|\tilde{A}|\}}, \mathsf{Ver})$, where Ver is a version number of these parameters.

**Authority Setup**: This algorithm consists of four steps.

Step 1. Generating $N$ authorities $A_1, A_2, \cdots, A_N$. For each authority $A_q$, it manages its attribute set $\tilde{A}_q = \{\tilde{a}_{q,1}, \tilde{a}_{q,2} \ldots \tilde{a}_{q,n_q}\}_{q\in[1,N]}$, and picks $\alpha_q \in Z_p^*$ randomly, computes $w_q = \hat{e}(g,g)^{\alpha_q}$. For each attribute $\tilde{a}_{q,m} \in \tilde{A}_q$, where $m \in [1, n_q]$, selects $\gamma_{q,m} \in Z_p^*$ randomly and computes $T_{q,m} = \gamma_{q,m} g$, $T'_{q,m} = \gamma_{q,m} h$.

Step 2. Two authorities $A_q$ and $A_l$ share a value $s_{ql} \in Z_p^*$ between themselves as a pseudorandom function (PRF) seed which is transmitted in the two-party key exchange channel secretly, and it can be found that $s_{ql} = s_{lq}$ obviously.

Step 3. $A_q$ and $A_l$ choose $x_q, x_l \in Z_p^*$ respectively, and take a secure key agreement protocol to define a PRF for two patients as

$$\mathrm{PRF}_{q,l}(u_{\{0,1\}}) = \frac{x_q x_l}{s_{ql} + u_{\{0,1\}}} h,$$

where $u_{\{0,1\}}$ represents a hash value of $\mathsf{GID}_0$ or $\mathsf{GID}_1$.

Step 4. Authority $A_q$ outputs his public key as

$$PK_q = (w_q, \{T_{q,m}, T'_{q,m}\}_{m\in[1,n_q]}),$$

while its private key is

$$SK_q = (\alpha_q, x_q, \{s_{ql}\}_{l\in\{1,2,\ldots,N\}\setminus\{q\}}, \{\gamma_{q,m}\}_{m\in[1,n_q]}).$$

**KeyGen**: Based on the tuple of *params*, a new Patient $i$ takes part in the telemedicine system. Let $\mathbb{A}$ be an access policy of Patient $i$, this algorithm returns a tuple of private keys that enables this new Patient $i$ to obtain the cipertext $CT$ only if the attribute of $CT$ satisfies this access policy $\mathbb{A}$. This algorithm consists of four steps.

Step 1. The authority randomly picks $(|\tilde{A}| + 1)$ elements $\{t_i, \{v_{i,j}\}_{\forall j\in\{1,2,\ldots,|\tilde{A}|\}}\}$ in $Z_p^*$.

Step 2. Setting $U = U \cup \{i\}$, authority $A_q$ chooses $r_q \in Z_p^*$.

Step 3. Patient $i$ interacts with every authority $A_q$ in $N-1$ times to achieve the anonymous key issuing. Then, it computes

$$D_{ql} = \alpha_q g + r_q h + \mathrm{PRF}_{ql}(i) \;\; for \;\; q > l,$$

$$D_{ql} = \alpha_q g + r_q h - \mathrm{PRF}_{ql}(i) \;\; for \;\; q < l,$$

and

$$D_i = \sum_{(q,l)\in\{1,2,\ldots N\}\times(\{1,2,\ldots N\}\setminus\{q\})} D_{ql} = \sum_{q=1}^{N}(N-1)\alpha_q g + \sum_{q=1}^{N}(N-1) r_q h,$$

$$\{V_j = v_{i,j}V_j\}_{\forall j\in\{1,2,\ldots,|\tilde{A}|\}},$$
$$\{\overline{v_{i,j}} = \prod_{k\neq i,k\in U} v_{k,j}^{-1} + t_i v_{i,j}\}_{\forall j\in\{1,2,\ldots,|\tilde{A}|\}},$$
$$\{\overline{v_{k,j}} = (\overline{v_{k,j}} - t_k v_{k,j})v_{i,j}^{-1} + t_k v_{k,j}\}_{\forall k\neq i,k\in U,j\in\{1,2,\ldots,|\tilde{A}|\}}.$$

Step 4. Let $\mathbb{A}$ be an access policy over the set of attributes $\tilde{A}$. By using of the linear secret sharing scheme, we can obtain the share $\{\beta_j\}$ of the secret $s \in Z_p^*$. It denotes the element corresponding to the share $\beta_j$ as $\tilde{a}_j \in \tilde{A}$, where $a_j$ is the attribute underlying $\tilde{a}_j$. Note that $\tilde{a}_j$ may be negated or non-negated attribute.

For every $j$ such that $\tilde{a}_j$ is non-negated attribute,

$$D_{i,j}^{(1)} = \{v_{i,j}^{-1}\beta_j\alpha_q g\}_{q\in\{1,2,\ldots,N\}},$$
$$D_{i,j}^{(2)} = \{\frac{v_{i,j}^{-1}\beta_j r_q}{1+t_i(\prod_{i\in U} v_{i,j})}h\}_{q\in\{1,2,\ldots,N\}},$$
$$D_{i,j}^{(3)} = \{t_i\beta_j\alpha_q g\}_{q\in\{1,2,\ldots,N\}},\quad D_j^{(4)} = \{\beta_j r_q h\}_{q\in\{1,2,\ldots,N\}}.$$

For every $j$ such that $\tilde{a}_j$ is negated attribute,

$$D_{i,j}^{(5)} = \{\frac{\beta_j}{\sum_{m=1}^{n_q}\gamma_{q,m}}(D_i)\}_{q\in\{1,2,\ldots,N\}},\quad D_j^{(6)} = \frac{\beta_j}{\sum_{m=1}^{n_q}\gamma_{q,m}} r_q g.$$

The private key of patient $i$ consists of the above group elements that

$$SK_i = (D_{i,j}^{(1)}, D_{i,j}^{(2)}, D_{i,j}^{(3)}, D_j^{(4)}, D_{i,j}^{(5)}, D_j^{(6)}).$$

**Revoke**: This algorithm is aimed to revoke the private key of some registered patient $u$, the authority increases the version number Ver and updates $\{V_j, \{\overline{v_{i,j}}\}_{\forall i\in U}\}_{\forall j\in\{1,2,\ldots,|\tilde{A}|\}}$ in *params* in the following,

$$\{V_j = v_{u,j}^{-1}V_j\}_{\forall j\in\{1,2,\ldots,|\tilde{A}|\}},$$
$$\{\overline{v_{k,j}} = (\overline{v_{k,j}} - t_k v_{k,j})v_{u,j} + t_k v_{k,j}\}_{\forall k\neq u,k\in U,j\in\{1,2,\ldots,|\tilde{A}|\}}.$$

Then, the authority deletes $\{\overline{v_{u,j}}\}_{\forall j\in\{1,2,\ldots,|\tilde{A}|\}}$.

**Encrypt**: This algorithm takes $(\mathsf{DEK}, \tilde{A}, Params, s)$ as inputs, where $\tilde{A}$ is a set of attribute for the medical service, and encrypts this service under the DEK. A set of values $\{s_j\}_{j\in\{1,2,\ldots,|\tilde{A}|\}}$ is randomly selected, which satisfies the equation $\sum_{j=1}^{|\tilde{A}|} s_j\beta_j = s$. Then, it outputs the ciphertext of the DEK as follows.

$$CT = (\tilde{A}, c^{(0)} = \mathsf{DEK}\cdot(\prod_{q=1}^{N} w_q)^s,$$
$$\{c_j^{(1)} = s_j V_j\}_{j\in\{1,2,\ldots,|\tilde{A}|\}},$$
$$\{c_j^{(2)} = s_j g\}_{j\in\{1,2,\ldots,|\tilde{A}|\}},$$
$$\{c_j^{(3)} = \sum_{m=1}^{n_q} s_j T_{q,m}\}_{j\in\{1,2,\ldots,|\tilde{A}|\},q\in\{1,2,\ldots,N\}},$$
$$\{c_j^{(4)} = \sum_{m=1}^{n_q} s_j T'_{q,m}\}_{j\in\{1,2,\ldots,|\tilde{A}|\},q\in\{1,2,\ldots,N\}}, \mathsf{Ver}).$$

**ReEncrypt**: This algorithm inputs the current parameters *params*, an exist ciphertext $CT$, and the corresponding $s$, it outputs the updated ciphertext $CT^*$ which is accessed by replacing $\{c_j^{(1)}\}_{\forall j\in\{1,2,\ldots,|\tilde{A}|\}}$ of $CT$ with $\{c_j^{(1)*} = s_j V_j^*\}_{\forall j\in\{1,2,\ldots,|\tilde{A}|\}}$, where $V_j^*$ is the current public parameter.

**Decrypt**: Patient checks whether $\mathbb{A}(\tilde{A}) = TRUE$ holds or not. If not, outputs $\perp$. Otherwise, executes the following.

For each non-negated attribute $\tilde{a}_j \in \tilde{A}$, patient computes

$$F_j = \frac{\prod_{q=1}^{N}[\hat{e}(\overline{v_{i,j}}(D_{i,j}^{(1)} + D_{i,j}^{(2)}) - D_{i,j}^{(3)}, c_j^{(1)})]}{\prod_{q=1}^{N}[\hat{e}(c_j^{(2)}, D_j^{(4)})]} = \hat{e}(g,g)^{s_j\beta_j\sum_{q=1}^{N}\alpha_q}.$$

For each negated attribute $\tilde{a}_j \notin \tilde{A}$, patient computes

$$F_j = \frac{\hat{e}(D_{i,j}^{(5)}, \frac{c_j^{(3)}}{N-1})}{\prod_{q=1}^{N}[\hat{e}(c_j^{(4)}, D_j^{(6)})]} = \hat{e}(g,g)^{s_j\beta_j\sum_{q=1}^{N}\alpha_q}.$$

Then, patient computes

$$F = \prod_{j=1}^{|\tilde{A}|}(F_j) = \hat{e}(g,g)^{s\sum_{q=1}^{N}\alpha_q}.$$

Finally, patient obtains DEK that is uses to access the medical services by computing

$$\mathsf{DEK} = \frac{c^{(0)}}{F}.$$

## V. SECURITY ANALYSIS AND COMPARISONS

### A. SECURITY ANALYSIS

A valid protocol must satisfy the property of correctness and security. In this subsection, it proves that this protocol is correct and secure in the CCA-DM model.

*Theorem 1 (Correctness):* Provided that the authority and patient are honest in the process of executing the specified algorithms, no matter that the attribute $\tilde{a}_j$ is negated or not, the patient can obtain the valid symmetric data encryption key DEK only if $\mathbb{A}(\tilde{A}) = TRUE$.

*Proof:* The correctness of this protocol comes from the following derivation:

For every non-negated attribute $\tilde{a}_j \in \tilde{A}$,

$$F_j = \frac{\prod_{q=1}^{N}[\hat{e}(\overline{v_{i,j}}(D_{i,j}^{(1)} + D_{i,j}^{(2)}) - D_{i,j}^{(3)}, c_j^{(1)})]}{\prod_{q=1}^{N}[\hat{e}(c_j^{(2)}, D_j^{(4)})]}$$

$$= \{\prod_{q=1}^{N}[\hat{e}((\prod_{k\neq i,k\in U} v_{k,j}^{-1} + t_i v_{i,j})(v_{i,j}^{-1}\beta_j\alpha_q g + \frac{v_{i,j}^{-1}\beta_j r_q}{1+t_i(\prod_{i\in U} v_{i,j})}h) - t_i\beta_j\alpha_q g,$$
$$s_j(\prod_{i\in U} v_{i,j})g)]\}/\{\prod_{q=1}^{N}[\hat{e}(s_j g, \beta_j r_q h)]\}$$
$$= \{\prod_{q=1}^{N}[\hat{e}((\prod_{i\in U} v_{i,j})^{-1}\beta_j\alpha_q g + \frac{(\prod_{i\in U} v_{i,j})^{-1}\beta_j r_q}{1+t_i(\prod_{i\in U} v_{i,j})}h + t_i\beta_j\alpha_q g + \frac{t_i\beta_j r_q}{1+t_i(\prod_{i\in U} v_{i,j})}h - t_i\beta_j\alpha_q g,$$
$$s_j(\prod_{i\in U} v_{i,j})g)]\}/\{\prod_{q=1}^{N}[\hat{e}(g,h)^{s_j\beta_j r_q}]\}$$
$$= \frac{\prod_{q=1}^{N}[\hat{e}(g,g)^{s_j\beta_j\alpha_q}\cdot \hat{e}(h,g)^{\frac{s_j\beta_j r_q}{1+t_i(\prod_{i\in U} v_{i,j})}}\cdot \hat{e}(h,g)^{\frac{t_i s_j\beta_j r_q(\prod_{i\in U} v_{i,j})}{1+t_i(\prod_{i\in U} v_{i,j})}}]}{\prod_{q=1}^{N}[\hat{e}(g,h)^{s_j\beta_j r_q}]}$$
$$= \frac{\prod_{q=1}^{N}[\hat{e}(g,g)^{s_j\beta_j\alpha_q}\cdot \hat{e}(h,g)^{s_j\beta_j r_q}]}{\prod_{q=1}^{N}[\hat{e}(g,h)^{s_j\beta_j r_q}]}$$
$$= \prod_{q=1}^{N}[\hat{e}(g,g)^{s_j\beta_j\alpha_q}] = \hat{e}(g,g)^{s_j\beta_j\sum_{q=1}^{N}\alpha_q}.$$

For every negated attribute $\tilde{a}_j \notin \tilde{A}$,

$$F_j = \frac{\hat{e}(D_{i,j}^{(5)}, \frac{c_j^{(3)}}{N-1})}{\prod_{q=1}^{N}[\hat{e}(c_j^{(4)}, D_j^{(6)})]}$$
$$= \frac{\hat{e}(\frac{\beta_j(N-1)}{\sum_{m=1}^{n_q}\gamma_{q,m}}(\sum_{q=1}^{N}\alpha_q g + \sum_{q=1}^{N} r_q h), \frac{\sum_{m=1}^{n_q} s_j\gamma_{q,m} g}{N-1})}{\prod_{q=1}^{N}[\hat{e}(\sum_{m=1}^{n_q} s_j\gamma_{q,m} h, \frac{\beta_j}{\sum_{m=1}^{n_q}\gamma_{q,m}} r_q g)]}$$
$$= \frac{\hat{e}(\frac{\beta_j}{\sum_{m=1}^{n_q}\gamma_{q,m}}\cdot\sum_{q=1}^{N}\alpha_q g + \frac{\beta_j}{\sum_{m=1}^{n_q}\gamma_{q,m}}\cdot\sum_{q=1}^{N} r_q h, \sum_{m=1}^{n_q} s_j\gamma_{q,m} g)}{\prod_{q=1}^{N}[\hat{e}(h,g)^{(\sum_{m=1}^{n_q} s_j\gamma_{q,m})\cdot(\frac{\beta_j}{\sum_{m=1}^{n_q}\gamma_{q,m}} r_q)}]}$$
$$= \frac{\hat{e}(g,g)^{s_j\beta_j\sum_{q=1}^{N}\alpha_q}\cdot\hat{e}(h,g)^{s_j\beta_j\sum_{q=1}^{N} r_q}}{\prod_{q=1}^{N}[\hat{e}(h,g)^{s_j\beta_j r_q}]}$$
$$= \frac{\hat{e}(g,g)^{s_j\beta_j\sum_{q=1}^{N}\alpha_q}\cdot\hat{e}(h,g)^{s_j\beta_j\sum_{q=1}^{N} r_q}}{\hat{e}(h,g)^{s_j\beta_j\sum_{q=1}^{N} r_q}} = \hat{e}(g,g)^{s_j\beta_j\sum_{q=1}^{N}\alpha_q}.$$

Therefore,

$$F = \prod_{j=1}^{|\tilde{A}|}(F_j) = \prod_{j=1}^{|\tilde{A}|}(\hat{e}(g,g)^{s_j\beta_j\sum_{q=1}^{N}\alpha_q})$$
$$= \hat{e}(g,g)^{(\sum_{q=1}^{N}\alpha_q)\cdot(\sum_{j=1}^{|\tilde{A}|} s_j\beta_j)} = \hat{e}(g,g)^{s\sum_{q=1}^{N}\alpha_q}.$$

The symmetric encryption key DEK is achieved by

$$\frac{c^{(0)}}{F} = \frac{\mathsf{DEK}\cdot(\prod_{q=1}^{N}\hat{e}(g,g)^{\alpha_q})^s}{\hat{e}(g,g)^{s\sum_{q=1}^{N}\alpha_q}}$$
$$= \frac{\mathsf{DEK}\cdot\hat{e}(g,g)^{s\sum_{q=1}^{N}\alpha_q}}{\hat{e}(g,g)^{s\sum_{q=1}^{N}\alpha_q}} = \mathsf{DEK}.$$

When the authority and patient honestly perform this proposed protocol, the above proof process shows that the symmetric data encryption key DEK is valid. The patient will take use of this key to access the medical service successfully. Thus, the correctness is proved.

*Theorem 2 (Collusion Resistance):* This protocol enables to resist $(N-1)$ corrupted authorities collusion attack at most.

*Proof:* For any two authorities $A_q$ and $A_l$, they share a PRF seed $s_{ql}$ between themselves and keep this seed secretly. Therefore, even if there are $(N-2)$ corrupted authorities in the system, it still has one seed that is not accessed by the malicious authority at least. Moreover, in the algorithm **KeyGen**, the private key $SK$ of patient contains the private key $\alpha_q$ of every authority. Even if only one authority is honest, the other $(N-1)$ malicious authorities still have nothing yet about $SK$, which indicates that only all $N$ malicious authorities could execute the collusion attack successfully in this system. In order to protecting the patient's privacy, taking advantage of the anonymous key issuing protocol, this private key is generated securely and the identity of patient GID is not revealed by these authorities directly. Hence, the corrupted authorities cannot trace GID and eavesdrop the privacy of patient.

*Theorem 3 (CCA-DM Secure):* Provided that an adversary enables to break out this protocol under the advantage $\epsilon$ in CCA-DM model, there is a simulator to solve the DBDH problem with advantage at least $\frac{1}{2}(\epsilon - \sigma)$, where $\sigma$ is negligible.

*Proof:* Assuming that $\mathcal{C}$ is a challenger to simulate the CCA-DM model for solving the DBDH problem.

*Global Setup*: Given $< G, G_T, \hat{e}, g, ag, bg, cg, Z >$ as a DBDH instance, the challenger $\mathcal{C}$ depends on Step 2 in the algorithm **Global Setup** in Section 4.2 to generate a patient set $U = \{u_0 = H(\mathsf{GID}_0), u_1 = H(\mathsf{GID}_1)\}$ and $\{V_j, \{\overline{v_{i,j}}\}_{\forall i \in U}\}_{\forall j \in \{1,2,\ldots,|\tilde{A}|\}}$. After that, $\mathcal{C}$ chooses $\lambda \in Z_p^*$ randomly, outputs $h = (a + \lambda)g$ and publishes the parameters $params = (\hat{e}, G, G_T, p, g, h, H, \{V_j, \{\overline{v_{i,j}}\}_{\forall i \in U}\}_{\forall j \in \{1,2,\ldots,|\tilde{A}|\}}, \mathsf{Ver})$. Adversary $\mathcal{A}$ delivered a group of corrupted authorities list $L_A$ to challenger $\mathcal{C}$, where $|L_A| < N$. The challenging access structure is $\mathbb{A}^*$.

*Authority Setup*: $\mathcal{C}$ selects $A_q^* \in \{A_1, A_2, \ldots, A_N\} \backslash L_A$ at random.

(a) For $A_q \in L_A$, $\mathcal{C}$ chooses $w_q, y_{q,m} \in Z_p^*$ at random, computes $T_{q,m} = y_{q,m} g$ for $\tilde{a}_{q,m} \in \tilde{A}_q$. Then, $\mathcal{C}$ picks $x_q \in Z_p^*$, a PRF seed $s_{ql} \in Z_p^*$ from two corrupted authorities $A_q$ and $A_l$. It gives $< w_q, y_{q,m}, x_q, s_{ql} >$ and $< W_q, T_{q,m} >$ to $\mathcal{A}$, where $W_q = \hat{e}(g, g)^{w_q}$.

(b) For $A_q \notin L_A$, $\mathcal{C}$ chooses $w_q, y_{q,m} \in Z_p^*$ at random and computes $T_{q,m} = y_{q,m} g$ for $\tilde{a}_{q,m} \in \mathbb{A}^*$, and $T_{q,m} = y_{q,m} h = \lambda y_{q,m} g$ for $\tilde{a}_{q,m} \notin \mathbb{A}^*$. If $A_q \neq A_q^*$, sets $W_q = \hat{e}(g, g)^{b w_q}$. Otherwise, $W_q = \hat{e}(g, g)^{ab} \cdot \prod_{A_q \in L_A} \hat{e}(g, g)^{-w_q} \cdot \prod_{A_q \notin L_A, A_q \neq A_q^*} \hat{e}(g, g)^{-b w_q}$. Challenger $\mathcal{C}$ selects a PRF seed $s_{ql} \in Z_p^*$ randomly for two honest authorities $A_q$ and $A_l$, and gives $< W_q, T_{q,m} >$ to adversary $\mathcal{A}$.

After that, $\mathcal{C}$ generates a list $L_{SK}$, and simulates the oracles in *Phase 1* of the CCA-DM model as follows.

*Phase 1*: $\mathcal{A}$ queries on the following four algorithms for the private keys,

*KeyGen*: Inputting the access structure $\mathbb{A}$,

(a) For $A_q \in L_A$, $\mathcal{C}$ generates the private keys by using of $< w_q, y_{q,m}, x_q, s_{ql} >$ for the corresponding access structure.

(b) For $A_q \notin L_A$, $\mathcal{C}$ chooses $r_q \in Z_p^*$ and computes $D_{ql}$ in two distinct situations as below:

i) $A_q \neq A_q^*$: For $q > l$, sets $D_{ql} = w_q(bg) + r_q h + \mathrm{PRF}_{ql}(i)$. Otherwise, sets $D_{ql} = w_q(bg) + r_q h - \mathrm{PRF}_{ql}(i)$.

ii) $A_q = A_q^*$: For $q > l$, sets $D_{ql} = (-\lambda)(bg) + \sum_{A_q \in L_A} (-w_q)g + \sum_{A_q \notin L_A, A_q \neq A_q^*} (-w_q)bg + r_q h + \mathrm{PRF}_{ql}(i)$. Otherwise, sets $D_{ql} = (-\lambda)(bg) + \sum_{A_q \in L_A} (-w_q)g + \sum_{A_q \notin L_A, A_q \neq A_q^*} (-w_q)bg + r_q h - \mathrm{PRF}_{ql}(i)$.

For the reason that $D_{ql}$ is distributed uniformly and the condition of $q > l$ is similar to $q < l$, this proof just describes the $q > l$ as follows.

$$\begin{aligned} D_{ql} &= (-\lambda)(bg) + \sum_{A_q \in L_A} (-w_q)g \\ &\quad + \sum_{A_q \notin L_A, A_q \neq A_q^*} (-w_q)bg + r_q h + \mathrm{PRF}_{ql}(i) \\ &= abg + (a+\lambda)(r_q - b)g \\ &\quad -\Big(\sum_{A_q \in L_A} w_q + \sum_{A_q \notin L_A, A_q \neq A_q^*} b w_q\Big)g + \mathrm{PRF}_{ql}(i) \\ &= abg + (r_q - b)h \\ &\quad -\Big(\sum_{A_q \in L_A} w_q + \sum_{A_q \notin L_A, A_q \neq A_q^*} b w_q\Big)g + \mathrm{PRF}_{ql}(i). \end{aligned}$$

Let $r_q' = r_q - b$, we have

$$D_{ql} = abg + r_q' h - \Big(\sum_{A_q \in L_A} w_q + \sum_{A_q \notin L_A, A_q \neq A_q^*} b w_q\Big)g + \mathrm{PRF}_{ql}(i).$$

Considering that $a$ is a secret value unknown to $\mathcal{C}$, $\{\beta_j\}_{j \in \{1,2,\ldots,n_q\}}$ are valid shares of $a$. Then, $\mathcal{C}$ gives the following tuples to adversary $\mathcal{A}$ as the private keys.

For every $j$ such that $\tilde{a}_j$ is not-negated attribute, we have

$$D_{i,j}^{(1)} = \{v_{i,j}^{-1} \beta_j w_q g\}_{q \in \{1,2,\ldots,N\}},$$

$$D_{i,j}^{(2)} = \Big\{\frac{v_{i,j}^{-1} \beta_j r_q}{1 + t_i(\prod_{i \in U} v_{i,j})} h\Big\}_{q \in \{1,2,\ldots,N\}},$$

$$D_{i,j}^{(3)} = \{t_i \beta_j w_q g\}_{q \in \{1,2,\ldots,N\}}, \quad D_j^{(4)} = \{\beta_j r_q h\}_{q \in \{1,2,\ldots,N\}}.$$

For every $j$ such that $\tilde{a}_j$ is negated attribute, we have

$$D_{i,j}^{(5)} = \Big\{\frac{\beta_j}{\sum_{m=1}^{n_q} y_{q,m}} (D_i)\Big\}_{q \in \{1,2,\ldots,N\}}, \quad D_j^{(6)} = \frac{\beta_j}{\sum_{m=1}^{n_q} y_{q,m}} r_q g.$$

At last, all these elements are stored in $L_{SK}$.

*Revoke*: $\mathcal{C}$ follows the **Revoke** algorithm and removes the corresponding private key $SK_i$ from $L_{SK}$.

*Update*: $\mathcal{C}$ runs the above *Revoke*$(i)$ algorithm and *KeyGen*$(\mathbb{A}')$ algorithm in sequence defined in this part.

*Decrypt*: On receiving the ciphertext $CT$, $\mathcal{C}$ checks whether that a private key $SK_i$ existes in $L_{SK}$ or not, which is used to decrypt $CT$ correctly. If it does, $\mathcal{C}$ decrypts $CT$ depending on $SK_i$ to excute **Decrypt** algorithm and outputs the result to the adversary $\mathcal{A}$. Otherwise, $\mathcal{C}$ executes the algorithms as follows to generate a pseudo patient $i'$ whose access policy $\mathbb{A}'$ satisfies $\mathbb{A}'(\tilde{A}) = TRUE$, and then $\mathcal{C}$ utilizes the private key of $i'$ to decrypt $CT$.

(a) Randomly picks $(|\tilde{A}| + 1)$ elements

$$\{t_{i'}, \{v_{i',j}\}_{j \in \{1,2,\ldots,|\tilde{A}|\}}\}$$

from $Z_p^*$.

(b) Computing $c_j^{(1)} = v_{i',j} c_j^{(1)}, \overline{v_{i',j}} = \prod_{k \in U} v_{k,j}^{-1} + t_{i'} v_{i',j}$.

(c) Creating the private key $SK_{i'}$ of pseudo user $i'$ according to the algorithm presented in the *KeyGen*.

(d) Using $SK_{i'}$ to decrypt $CT$ by running the algorithm of **Decrypt** in Section 4.2, it returns the results to adversary $\mathcal{A}$.

*Challenge*: On receiving $(M_0, M_1, \tilde{A})$, $\mathcal{C}$ chooses a set of $|\tilde{A}|$ value $\{s_j'\}_{j \in \{1,2,\ldots,|\tilde{A}|\}}$ such that $c = \sum_{j \in \{1,2,\ldots,|\tilde{A}|\}} s_j'$. And then, $\mathcal{C}$

**TABLE 2. Feature comparisons.**

| Schemes | Independent-Update | | Multi-Authority | Special Feature |
|---|---|---|---|---|
| | Updating | Revoking | | |
| [17] | No | No | No | Attribute Hidden |
| [22] | No | No | No | Key Delegation |
| [23] | Yes | Yes | No | Independence |
| [33] | Yes | Yes | No | - |
| [35] | Yes | Yes | No | Independence |
| [36] | Yes | Yes | Yes | - |
| [38] | No | No | No | Keyword Search, Traceability, Integrity |
| Ours | Yes | Yes | Yes | Independence, Traceability, Integrity |

**TABLE 3. Notations for performance comparisons.**

| Notation | Meaning |
|---|---|
| $n$ | the number of the members in the system |
| $N$ | the number of the authorities in the system |
| $m$ | the number of the attributes provided in the system |
| $m_C$ | the number of the attributes associated to a ciphertext |
| $m_U$ | the number of a user's attributes |

randomly selects $\theta \in \{0, 1\}$ and prepares

$$CT' = (\tilde{A}, c^{(0)} = M_\theta \cdot Z,$$
$$\{c_j^{(1)} = \prod_{i \in U} v_{i,j} cg\}_{j \in \{1,2,\ldots,|\tilde{A}|\}},$$
$$\{c_j^{(2)} = s'_j g\}_{j \in \{1,2,\ldots,|\tilde{A}|\}},$$
$$\{c_j^{(3)} = \sum_{m=1}^{n_q} s'_j T_{q,m}\}_{j \in \{1,2,\ldots,|\tilde{A}|\}, q \in \{1,2,\ldots,N\}},$$
$$\{c_j^{(4)} = \sum_{m=1}^{n_q} s'_j T'_{q,m}\}_{j \in \{1,2,\ldots,|\tilde{A}|\}, q \in \{1,2,\ldots,N\}}, \mathsf{Ver}).$$

Provided that there exists $SK \in (L_{SK} - SK_{i'})$ which is used to decrypt $CT'$ correctly, the challenge will abort. At last, $\mathcal{C}$ outputs the ciphertext $CT'$ to adversary $\mathcal{A}$.

*Phase 2*: In this phase, some oracles are simulated as those in *Phase 1*. However, the adversary $\mathcal{A}$ is not allowed to make some queries on $Decrypt(CT')$ or $KeyGen(\mathbb{A}')$, where $\mathbb{A}'(\tilde{A}) = TRUE$ holds.

*Guess*: $\mathcal{A}$ outputs its guess $\theta' \in \{0, 1\}$ on $\theta$. If $\theta' = \theta$, $\mathcal{C}$ returns 1 as a result. Otherwise, returns 0.

In probabilistic polynomial time, if the adversary $\mathcal{A}$ wins the CCA-DM game with non-negligible advantage at least $\epsilon$, $\mathcal{C}$ solves the DBDH problem under the non-negligible advantage $\epsilon'$, where $\epsilon' > \frac{1}{2}(\epsilon - \sigma)$. This advantage analysis is given as following.

We define that the event $\mathcal{C}(g, ag, bg, cg, Z) = 1$ as $\mathsf{E}_1$, $\mathcal{C}(g, ag, bg, cg, Z) = 0$ as $\mathsf{E}_0$, $Z = \hat{e}(g, g)^{abc}$ as $\mathsf{Z}_1$, the element $Z$ is selected from $G_T \backslash \{\hat{e}(g, g)^{abc}\}$ randomly as $\mathsf{Z}_0$. When $Z = \hat{e}(g, g)^{abc}$, $\Pr[\mathsf{E}_1|\mathsf{Z}_1] = \Pr[\theta' = \theta|\mathsf{Z}_1]$ holds, where $\Pr[\theta' = \theta|\mathsf{Z}_1] - \frac{1}{2} \geq \epsilon$. Otherwise, we get $\Pr[\mathsf{E}_1|\mathsf{Z}_0] = \Pr[\theta' = \theta|\mathsf{Z}_0]$. For the reason of randomness, $|\Pr[\theta' = \theta|\mathsf{Z}_0] - \frac{1}{2}| \leq \sigma$, where $\sigma$ is negligible. Therefore, the advantage of the simulator in solving the DBDH problem is

$$\epsilon' = |\frac{1}{2}\Pr[\mathsf{E}_1|\mathsf{Z}_1] - \frac{1}{2}\Pr[\mathsf{E}_1|\mathsf{Z}_0]| \geq \frac{1}{2}(\epsilon - \sigma).$$

### B. COMPARISONS

In this subsection, some significant features are analyzed, which affects the flexibility and practicability of this scheme in the telemedicine system. Additionally, the performance on computation, storage and communication are also analyzed.

(a) *Independent-Update*: This property includes updating and revoking that have been defined in ***Definition 3***. An ABE scheme with independent-update should permit users to update or revoke their access policies. Moreover, when the access policy updating or revoking occurs, the other users in system should not be affected. In the algorithm of **Revoke**, when the user leaving or joining in the system, the authority increases the version number $\mathsf{Ver}$ and updates parameter $\{V_j, \{\overline{v_{i,j}}\}_{\forall i \in U}\}_{\forall j \in \{1,2,\ldots,|\tilde{A}|\}}$. At last, it will delete $\{\overline{v_{u,j}}\}_{\forall j \in \{1,2,\ldots,|\tilde{A}|\}}$ of patient $u$. According to this model, the revoked patient cannot access the service any more and other patients are not affected. Therefore, this protocol meets these two requirements.

(b) *Multiple Authorities*: Every different authority is responsible for managing the different type data in MoD services, which supports both of the features of distributed network structure and non-concentrated power. Our scheme provides mechanism to handle multi-authority management.

(c) *Traceability and Integrity*: In this protocol, it combines the technologies of blockchain and cloud storage. The original medical data is stored in the cloud while the index of it is encapsulated in the blockchain. According to this storage model, it prevents the medical data (including diagnosis) from being distorted, which reduces the medical accident and medical dispute.

We make a comparison on the supported feature between this work and other related schemes [17], [22], [23], [33], [35], [36], [38], and the results are demonstrated in TABLE 2. From this table, it can be concluded that only this protocol satisfies independent-update including updating and revoking, traceability and integrity of data, and multi-authority co-management.

In TABLE 4 and 5, it also compares the computation, storage and communication cost, where the big $\mathcal{O}$ notation

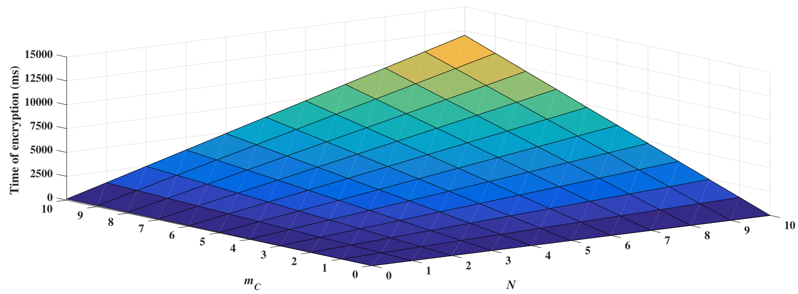



**FIGURE 5.** The computation cost in encrypt.

**TABLE 4.** Performance comparisons: Computation cost.

| Schemes | Encryption Cost | Decryption Cost | The Computation Cost of the Authority | | |
|---|---|---|---|---|---|
| | | | Registering | Updating | Revoking |
| [17] | $\mathcal{O}(m_C)$ | $\mathcal{O}(m_C)$ | $\mathcal{O}(m)$ | $\mathcal{O}(n \times m)$ | $\mathcal{O}(n \times m)$ |
| [22] | $\mathcal{O}(m_C)$ | $\mathcal{O}(m_C)$ | $\mathcal{O}(m)$ | $\mathcal{O}(n \times m)$ | $\mathcal{O}(n \times m)$ |
| [23] | $\mathcal{O}(m_C)$ | $\mathcal{O}(m_U)$ | $\mathcal{O}(m + m_U + n)$ | $\mathcal{O}(m + m_U + n)$ | $\mathcal{O}(m)$ |
| [33] | $\mathcal{O}(m_C)$ | $\mathcal{O}(m_U)$ | $\mathcal{O}(m_U)$ | $\mathcal{O}(n \times m_U)$ | $\mathcal{O}(n \times m_U)$ |
| [35] | $\mathcal{O}(m_C)$ | $\mathcal{O}(m_C)$ | $\mathcal{O}(m + m_U + n)$ | $\mathcal{O}(m + m_U + n)$ | $\mathcal{O}(m)$ |
| [36] | $\mathcal{O}(N \times m_C)$ | $\mathcal{O}(N \times m_C)$ | $\mathcal{O}(N \times m)$ | $\mathcal{O}(N \times m)$ | $\mathcal{O}(N \times m)$ |
| [38] | $\mathcal{O}(m_C)$ | $\mathcal{O}(m_C)$ | $\mathcal{O}(m)$ | $\mathcal{O}(n \times m)$ | $\mathcal{O}(n \times m)$ |
| Ours | $\mathcal{O}(N \times m_C)$ | $\mathcal{O}(N \times m_U)$ | $\mathcal{O}(N \times (m + m_U + n))$ | $\mathcal{O}(m + m_U + n)$ | $\mathcal{O}(m)$ |

**TABLE 5.** Performance comparisons: Storage and communication cost.

| Schemes | Size of Private Key | Size of Ciphertext | Size of Public Parameters | The Communication Cost between the Authority and a User | | |
|---|---|---|---|---|---|---|
| | | | | Registering | Updating | Revoking |
| [17] | $\mathcal{O}(m)$ | $\mathcal{O}(m_C)$ | $\mathcal{O}(1)$ | $\mathcal{O}(m)$ | $\mathcal{O}(n \times m)$ | $\mathcal{O}(n \times m)$ |
| [22] | $\mathcal{O}(m)$ | $\mathcal{O}(m_C)$ | $\mathcal{O}(1)$ | $\mathcal{O}(m)$ | $\mathcal{O}(n \times m)$ | $\mathcal{O}(n \times m)$ |
| [23] | $\mathcal{O}(m_U)$ | $\mathcal{O}(m_C)$ | $\mathcal{O}(n \times m)$ | $\mathcal{O}(m_U)$ | $\mathcal{O}(m_U)$ | $\mathcal{O}(1)$ |
| [33] | $\mathcal{O}(m_U)$ | $\mathcal{O}(m_C)$ | $\mathcal{O}(m)$ | $\mathcal{O}(m_U)$ | $\mathcal{O}(n \times m_U)$ | $\mathcal{O}(n \times m_U)$ |
| [35] | $\mathcal{O}(m_U)$ | $\mathcal{O}(m_C)$ | $\mathcal{O}(n \times m)$ | $\mathcal{O}(m_U)$ | $\mathcal{O}(m_U)$ | $\mathcal{O}(1)$ |
| [36] | $\mathcal{O}(n + N \times m + m)$ | $\mathcal{O}(N \times m_C)$ | $\mathcal{O}(n)$ | $\mathcal{O}(n + N \times m + m)$ | $\mathcal{O}(N \times n)$ | $\mathcal{O}(1)$ |
| [38] | $\mathcal{O}(m \times m_U)$ | $\mathcal{O}(m \times m_U)$ | $\mathcal{O}(m \times m_U)$ | $\mathcal{O}(m)$ | $\mathcal{O}(n \times m)$ | $\mathcal{O}(n \times m)$ |
| Ours | $\mathcal{O}(N \times m_U)$ | $\mathcal{O}(N \times m_C)$ | $\mathcal{O}(n \times m)$ | $\mathcal{O}(N \times m_U)$ | $\mathcal{O}(N \times m_U)$ | $\mathcal{O}(1)$ |

means the computation and communication cost, and the other used symbols are defined in TABLE 3. Specifically, in TABLE 4, we evaluate the computation cost of encryption and decryption. The cost of the proposal increases with the number of authority linearly. In TABLE 5, it demonstrates the size of private key, ciphertext and system public parameters. Furthermore, we investigate the necessary computation and communication cost of the authority in dealing with dynamic membership. Considering the management of dynamic membership, there are multiple authorities to generate the corresponding private key for a registered patient. When the patient unsubscribes or updates his access policy, these authorities must revoke this patient's existing private key by updating the public parameters. In other schemes, which has no algorithm aiming to deal with patient's revoking and access policy updating by interacting with multiple authorities, all of the unrevoked patients are necessary to connect the multi-authority and renew their private keys except the references [23] and [35]. In this system, when revoking and updating occurs, the unrevoked patients need not to update their private keys. Moreover, in the background of multi-authority co-management, only our system provides the traceability and integrity of all the medical data stored in cloud by the blockchain technology.

At last, in order to evaluate the costs of this proposal in encryption and decryption, we simulate our scheme with Pairing-Based Cryptography (PBC) library in C language (pbc-0.5.14) [43]. The elliptic curve parameter is chosen in Type-A, and the order of group is 160 bits. Our experiments are implemented on a laptop with 64-bit Windows 10 operation system, 2.20GHz Intel Core i5-5200U CPU, with 4 GB RAM. Supposing that every authority has 10 attributes (i.e., $n_q = 10$), FIGURE 5 and FIGURE 6 demonstrate the costs of encryption and decryption algorithms spent in this scheme

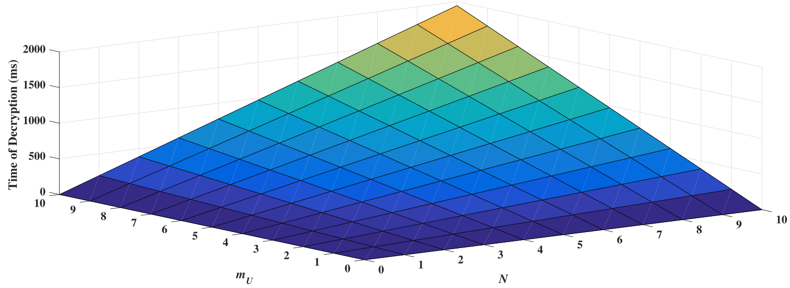



**FIGURE 6.** The computation cost in decrypt.

respectively, where $m_C$, $m_U$ and $N$ are listed in TABLE 3. We can conclude that the running time is increased linearly with the number of authority and attribute involved in this system.

## VI. CONCLUSIONS

In this paper, based on blockchain technology, we put forward an independent-update ABE scheme with multiple authorities, which is applied in the MoD service of the telemedicine system. The patient in this protocol is allowed to enroll and leave freely, and he/she can also change their access policies on-demand, while any other unrelated patients are unnecessary to renew his private key in registration and updating. In addition, by employing the blockchain technique, the EHRs of the patient are stored in the chain to avoid being tampered by unauthorized user or authority. All the advantages make this proposal more efficient and flexible for MoD services in telemedicine system. Finally, we have concluded that this scheme enables to resist collusion attack in $(N - 1)$ malicious authorities and also is given the formally proof on the security of this scheme in the CCA-DM model. In the comparisons, it analyzes the performance with other related works in different phases and simulates the cost of encryption and decryption.

## REFERENCES

[1] J. Matusitz and J. M. Breen, "Telemedicine: Its effects on health communication," *Health Commun.*, vol. 21, no. 1, pp. 73–83, Dec. 2007.

[2] World Health Organization. (2010). *Telemedicine: Opportunities and Developments in Member States: Report on the Second Global Survey on eHealth*. [Online]. Available: http://www.who.int/iris/handle/10665/44497

[3] M. Berman and A. Fenaughty, "Technology and managed care: Patient benefits of telemedicine in a rural health care network," *Health Econ.*, vol. 14, no. 6, pp. 559–573, 2005.

[4] N. M. Hjelm, "Benefits and drawbacks of telemedicine," *J. Telemed. Telecare*, vol. 11, no. 2, pp. 60–70, Mar. 2005.

[5] A. Benharref and M. A. Serhani, "Novel cloud and SOA-based framework for e-health monitoring using wireless biosensors," *IEEE J. Biomed. Health Informat.*, vol. 18, no. 1, pp. 46–55, Jan. 2014.

[6] O. Ali, A. Shrestha, J. Soar, and S. F. Wamba, "Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review," *Int. J. Inf. Manage.*, vol. 43, pp. 146–158, Dec. 2018.

[7] Y. Karaca, M. Moonis, Y.-D. Zhang, and C. Gezgez, "Mobile cloud computing based stroke healthcare system," *Int. J. Inf. Manage.*, vol. 45, pp. 250–261, Apr. 2019.

[8] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST, Gaithersburg, MD, USA, Tech. Rep. SP-800-145, 2011. doi: 10.6028/NIST.SP.800-145.

[9] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Kaz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[10] M. Hamdaqa and L. Tahvildari, "Cloud computing uncovered: A research landscape," *Adv. Comput.*, vol. 86, pp. 41–85, Jan. 2012.

[11] *Microsoft Healthvault*. Accessed: Oct. 2007. [Online]. Available: http://www.healthvault.com

[12] *Google Health*. Accessed: May 2008. [Online]. Available: http://www.healthgoogle.com

[13] V. Casola, A. Castiglione, K. K. Choo, and C. Esposito, "Healthcare-related data in the cloud: Challenges and opportunities," *IEEE Cloud Comput.*, vol. 3, no. 6, pp. 10–14, Apr. 2016.

[14] D. He, S. Zeadally, and L. Wu, "Certificateless public auditing scheme for cloud-assisted wireless body area networks," *IEEE Syst. J.*, vol. 12, no. 1, pp. 64–73, Mar. 2018.

[15] L.-Y. Yeh, P.-Y. Chiang, Y.-L. Tsai, and J.-L. Huang, "Cloud-based fine-grained health information access control framework for lightweight IoT devices with dynamic auditing and attribute revocation," *IEEE Trans. Cloud Comput.*, vol. 6, no. 2, pp. 532–544, Apr./Jun. 2018.

[16] S. H. Lee, J. H. Song, and I. K. Kim, "CDA generation and integration for health information exchange based on cloud computing system," *IEEE Trans. Services Comput.*, vol. 9, no. 2, pp. 241–249, Mar. 2016.

[17] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2130–2145, Jun. 2018.

[18] S. Sharma, K. Chen, and A. Sheth, "Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems," *IEEE Internet Comput.*, vol. 22, no. 2, pp. 42–51, Mar. 2018.

[19] A. Abbas and S. U. Khan, "A review on the state-of-the-art privacy-preserving approaches in the e-Health clouds," *IEEE J. Biomed. Health Inform.*, vol. 18, no. 4, pp. 1431–1441, Jul. 2014.

[20] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, Aarhus, Denmark, 2005, pp. 457–473.

[21] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Secur.*, Alexandria, VA, USA, Oct./Nov. 2006, pp. 89–98.

[22] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Secur. Privacy*, Berkeley, CA, USA, May 2007, pp. 321–334.

[23] K. He, J. Chen, Y. Zhang, R. Du, Y. Xiang, M. M. Hassan, and A. Alelaiwi, "Secure independent-update concise-expression access control for video on demand in cloud," *Inf. Sci.*, vol. 387, pp. 75–89, May 2017.

[24] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[25] M. Pilkington, *Blockchain Technology: Principles and Applications*. Northampton, MA, U.K.: Edward Elger, 2016, pp. 35–54.

[26] J. Garay, A. Kiayias, and N. Leonardos, "The Bitcoin backbone protocol: Analysis and applications," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, Sofia, Bulgaria, 2015, pp. 281–310.

[27] B. Huang, Z. Liu, J. Chen, A. Liu, Q. Liu, and Q. He, "Behavior pattern clustering in blockchain networks," *Multimedia Tools Appl.*, vol. 76, no. 19, pp. 20099–20110, Oct. 2017.

[28] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the Internet of Things," *Peer Peer Netw. Appl.*, vol. 10, no. 4, pp. 983–994, Jul. 2017.
[29] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan./Feb. 2018.
[30] IBM Institute for Business Value, IBM Corporation. (2016). *Healthcare Rallies for Blockchains: Keeping Patients at the Center*. [Online]. Available: http://www.ibm.biz/blockchainhealth
[31] P. Taylor, *Applying Blockchain Technology to Medicine Traceability*. [Online]. Available: https://www.securingindustry.com/pharmaceuticals/applying-blockchaintechnology-to-medicine-traceability/s40/a2766/#.V5mxL-mLTIV
[32] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *J. Med. Syst.*, vol. 40, no. 10, p. 218, 2016.
[33] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013.
[34] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, "An efficient and secure user revocation scheme in mobile social networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Kathmandu, Nepal, Dec. 2011, pp. 1–5.
[35] C.-I. Fan, V. S.-M. Huang, and H.-M. Ruan, "Arbitrary-state attribute-based encryption with dynamic membership," *IEEE Trans. Comput.*, vol. 63, no. 8, pp. 1951–1961, Aug. 2014.
[36] J. Wei, W. Liu, and X. Hu, "Secure and efficient attribute-based access control for multiauthority cloud storage," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1731–1742, Jun. 2018.
[37] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018.
[38] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38437–38450, 2018.
[39] H. Wang and Y. Song, "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain," *J. Med. Syst.*, vol. 42, no. 8, p. 152, 2018.
[40] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, "BPDS: A blockchain based privacy-preserving data sharing for electronic medical records," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 1–6. doi: 10.1109/GLOCOM.2018.8647713.
[41] X. Zhang, S. Poslad, and Z. Ma, "Block-based access control for Blockchain-based electronic medical records (EMRs) query in eHealth," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 1–7. doi: 10.1109/GLOCOM.2018.8647433.
[42] A. H. Mohsin, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, A. S. Albahri, M. A. Alsalem, and K. I. Mohammed, "Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient authentication," *Comput. Standards Interfaces*, to be published. doi: 10.1016/j.csi.2019.04.002.
[43] B. Lynn. (2012). *PBC (Pairing-Based Cryptography) Library*. [Online]. Available: http://crypto.stanford.edu/pbc/

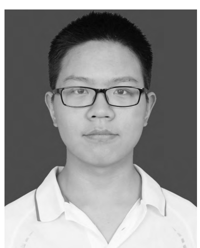
**RUI GUO** received the Ph.D. degree from the Department of State Key Laboratory of Networking and Switch Technology, Beijing University of Posts and Telecommunications, in 2014. He is currently a Lecturer with the National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications. His current research interests include attribute-based cryptograph, cloud computing, and blockchain technology.

**HUIXIAN SHI** received the B.S. and Ph.D. degrees from the Department of Mathematics and Information Science, Shaanxi Normal University, Xi'an, China, in 2007 and 2013, respectively, where she is currently an Associate Professor with the Department of Mathematics and Information Science. Her current research interests include information security and blockchain technology.

**DONG ZHENG** received the Ph.D. degree from Xidian University, in 1999. He then joined the School of Information Security Engineering, Shanghai Jiao Tong University. He is currently a Professor with the Xi'an University of Post and Telecommunications, China. His research interests include information theory, cryptography, and information security. He is a Senior Member of the Chinese Association for Cryptologic Research and a member of the Chinese Communication Society.

**CHUNMING JING** received the bachelor's degree from the Xi'an University of Posts and Telecommunications. He is currently pursuing the master's degree with the National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications. His research interests include security and privacy in the Internet of Thing, and blockchain technology.

**CHAOYUAN ZHUANG** received the bachelor's degree from the Xi'an University of Posts and Telecommunications, where he is currently pursuing the master's degree with the National Engineering Laboratory for Wireless Security. His research interests include security and privacy in cloud, and blockchain technology.



**ZHENGYANG WANG** is currently pursuing the bachelor's degree with the Department of Information and Communication Engineering, Xi'an University of Posts and Telecommunications. His primary research interests are in the area of information science, data security, and blockchain technology.