Flexible and Fine-Grained Access Control for EHR in Blockchain-Assisted E-Healthcare Systems

Dajiang Chen, *Member, IEEE*, Li Zhang, Zeyu Liao, Hong-Ning Dai, *Senior Member, IEEE*, Ning Zhang, *Senior Member, IEEE*, Xuemin Shen, *Fellow, IEEE*, and Minghui Pang

***Abstract*—It is of the utmost importance to achieve flexible and fine-grained access control of electronic health records (EHRs) in smart elderly healthcare (SEH) for providing high-quality healthcare services for the elderly and protecting their privacy simultaneously. In this article, a flexible, fine-grained, and elderly centric access control scheme is presented for EHR data in SEH. In the proposed scheme, ciphertext policy attribute-based encryption (CP-ABE), permission token, dual-key regression, and blockchain techniques are leveraged to realize multidimensional access control of EHR data in terms of data generation time, data user properties, access times, and access period. Moreover, a novel token segmentation algorithm is designed to transfer access rights between doctors efficiently for multiparty diagnosis and treatment. Since the elderly can define the attributes of users accessing his/her EHR data, the access number, the access time, and the access range of data from the time dimension of data generation with the cooperation of the SEH institution, the privacy of EHR data of the elderly is well protected. The security analysis demonstrates that our scheme can achieve EHR ciphertext indistinguishability under chosen-plaintext attacks and token unlinkability and unforgeability under data users' collusion attacks. The experimental results show that our scheme performs well in terms of time cost and computational overhead.**

***Index Terms*—Access control, blockchain, ciphertext policy attribute-based encryption (CP-ABE), electronic health records (EHR), permission delegation, smart elderly healthcare (SEH).**

Manuscript received 26 January 2023; revised 27 July 2023 and 21 September 2023; accepted 25 October 2023. Date of publication 30 October 2023; date of current version 7 March 2024. This work was supported in part by the National Natural Science Foundation of China under Grant 62002047 and Grant 61872059; in part by the International Scientific and Technological Innovation Cooperation Project in Sichuan Province under Grant 2020YFH0062; and in part by the Demonstration of Scientific and Technology Achievements Transform in Sichuan Province under Grant 2022ZHCG0036. *(Corresponding author: Minghui Pang.)*

Dajiang Chen, Li Zhang, and Zeyu Liao are with the Network and Data Security Key Laboratory of Sichuan Province, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: djchen@uestc.edu.cn).

Hong-Ning Dai is with the Department of Computer Science, Hong Kong Baptist University, Hong Kong (e-mail: hndai@ieee.org).

Ning Zhang is with the Department of Electrical and Computer Engineering, University of Windsor, ON N9B 3P4, Canada (e-mail: ning.zhang@uwindsor.ca).

Xuemin Shen is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: sshen@uwaterloo.ca).

Minghui Pang is with the Department of Geriatric Surgery, Sichuan Provincial People's Hospital, University of Electronic Science and Technology of China, Chengdu 610072, Sichuan, China (e-mail: mhpang@uestc.edu.cn).

Digital Object Identifier 10.1109/JIOT.2023.3328382

I. Introduction

With the aggravation of aging, the traditional elderly healthcare is facing increasingly severe challenges, e.g., nursing staff shortage, and difficulty in obtaining the health status of the elderly in time. As one of emerging smart technologies, the Internet of Things (IoT) revolutionizes the way how people live and work, with the help of artificial intelligence (AI) [1], [2], [3], the new generation of wireless communications (e.g., 5G and 6G) [4], [5], [6], and the information security [7], [8], [9]. When IoT meets elderly healthcare, smart elderly healthcare (SEH) system has emerged to provide the elderly people with healthcare services in a revolutionary way, thereby making elderly centric healthcare environment be a reality [10], [11], [12].

In SEH system, electronic health records (EHR) include historical electronic medical records, regular physical health examination data, and daily physical data, which play a critical role in health condition prediction, clinical diagnosis, and treatment. Generally, EHR data is continuously generated in the form of data stream in SEH system. For instance, elderly's physical data is measured by the nursing workers and/or recorded by the smart wearable devices every day. If EHR data is leaked, the privacy of the elderly will be threatened. Therefore, it is of great importance to realize flexible and fine-grained access control of EHR data [13], [14], [15], [16].

Recently, blockchain-based schemes have brought new directions to realize data access control, privacy protection and data sharing in healthcare system [17], [18], [19], [20]. However, these schemes are not suitable for the elderly centric smart healthcare system due to the following reasons.

1) EHR data at different times are usually encrypted with the same key. To prevent privacy leakage, it is necessary to update the key and re-encrypt the ciphertext after each access, causing a huge workload.
2) In the case of multiparty consultation or diagnostic assistance, each doctor needs the permission from SEH institutions. This process is cumbersome, inefficient and unable to respond to emergencies, and also increases the load on SEH institutions.
3) The data owners (i.e., the elderly and their families) cannot fully control their own EHR data, and they are completely unclear about the access of EHR data.

The attribute-based encryption (ABE) techniques can be used to realize fine-gained access control to solve the issues above partially [21]. However, when ABE-based methods meet

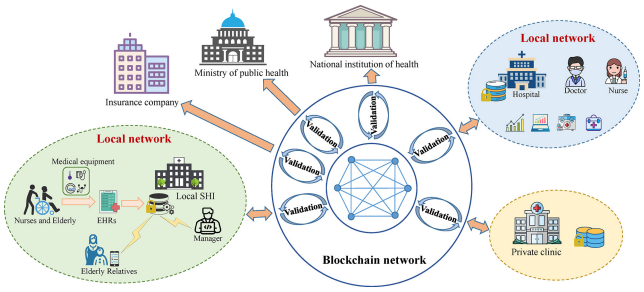

Fig. 1. Application scenario.

SEH, it still faces several challenges as follows. 1) How to realize access control in terms of the generation time of EHR data. The diagnosis of different diseases has different accessing requirements in terms of the generation time of EHR data, while, in ABE-based methods, the access content of EHR data is fixed, and it cannot be changed flexibly according to the generation time of EHR data for each access. 2) How to realize access control of EHR data for joint consultation efficiently. If an elderly person urgently needs a joint consultation, it should define an appropriate access structure to ensure that all the doctors participating in such a joint consultation have the right to access elderly's EHR data. However, in ABE-based methods, the access structure is defined before the access is made. To redefine the access structure, the EHR data must also be re-encrypted, which is a time-consuming task.

Accordingly, a flexible and fine-grained access control scheme in a SEH system should include the following properties. *Elderly-centric*: the access policy definer should be the elderly or his/her guardian; *Data Secure Sharing*: the EHR can be secure shared form data center to legitimate data user; *Authorization Traceability*: the history of data authorization and access can be traceable; *Time-dimension Access*: the access control of data can be realized according to the generation time of data. and *Efficient Multiparty Diagnosis*: access control scheme should support efficient multiparty diagnosis.

In this article, a flexible and fine-grained access control scheme is proposed for sharing EHR data in SEH to realize the shift from the institution-centered system to the elderly centric system. The application scenario is shown in Fig. 1, in which the blockchain network connects various distributed institutions and entities. The EHR data is stored in distributed database, such as database of SEH institutions, hospitals, and private clinics. After a doctor satisfies the access control permission and obtains the data access token, he/she can have a chance to provide diagnostic services for the elderly. If necessary, government agencies and insurance companies can also apply for permission to access data.

Several entities involved in the system are described as follows. There is a global certificate authority (CA) to generate system parameters and corresponding keys to each entity. There are several smart healthcare institutions (SHIs), in which a lot of health care data of the elderly is periodically measured and recorded by the nursing workers as well as the intelligent wearable medical devices. The EHR data of the elderly is stored in distributed databases. There is a database server of the distributed databases to store owners' EHR data and provide users with data-access services according to the authority token submitted by the data users. A large number of data owners exist in this system, who are the elderly in a SHI and can formulate access control policies for their own EHR data. There are a number of data users, who are the doctors in different hospitals to diagnose the elderly in a SHI. Only when the doctor's attributes satisfy the access control policy of the data owner, he/she can have a chance to decrypt the encrypted permission token generated from SHI. Since it can cause huge burdens at the blockchain if the EHR data is stored at the blockchain, the blockchain platform only stores the metadata of the EHR data (e.g., the storage location and the digest of EHR), the access control information and logs.

For intelligently and scientifically monitoring the health condition of the elderly living in the SHI, a healthcare data analysis system is deployed at SHI with data mining techniques. When some abnormal events occur, the healthcare data analysis system will automatically recognize the elderly with abnormal system data and push them to the doctors who are working in the SHI, being usually referred to as general practitioners (GPs). The GP may need to request access to the elderly's health care data and electronic medical records for further diagnosis. In case GP is unable to deal with the diseases of an elderly, the GP will recommend a suitable specialist physician for the elderly while complying with the requirements of the elderly and/or their guardians for the doctor's professional title, hospital grade, etc. Moreover, the specialist physician will ask for a consultation from another specialist physician if necessary. Thus, the GP and the specialist physicians have the potential to be daily users to access health care data and electronic medical records of elderly. The main objective of the proposed scheme is to realize efficient storage and flexible access control of EHR data to meet the above business logic.

In the proposed scheme, the EHR data is encrypted with different symmetric keys according to time sequence and then stored in a distributed server, so that the access control permissions can be divided in a time dimension with dual-key regression techniques. Based on the dual-key regression techniques, a permission token of an elderly can be issued by the corresponding SHI by utilizing the ciphertext policy ABE (CP-ABE) encryption algorithm to realize flexible access control according to the data generation time, the properties of the data user, and access times and access period of token. Moreover, it is allowed the authorized data users (e.g., doctors) to delegate part of their authority to other doctors without the authorization of SHI, so as to get the assistance from other doctors to realize the rapid, convenient and reliable diagnosis of elderly. The security semantic model is formally defined to describe the EHR data security and Token security. The corresponding security proof demonstrates that the proposed scheme is ciphertext indistinguishability under chosen-plaintext attacks, and token unlinkable and unforgeable under data users' collusion attack. The results of

extensive experiments show that our scheme performs well in terms of time cost and computational overhead.

The main contributions of this article are summarized below.

1) A novel flexible, fine-grained, and elderly centric access control model is proposed to achieve multidimensional access control (e.g., data generation time, data user properties, access times, and access period).
2) In the proposed scheme, a token segmentation algorithm is presented to realize the transfer of access rights between doctors, such that a doctor can invite the assistance of other doctors without the complex and cumbersome authorization of the SHI for faster, convenient and reliable multiparty diagnosis and treatment.
3) It is proved that our scheme can achieve EHR ciphertext indistinguishability under chosen-plaintext attacks and token unlinkable and unforgeable under data users' collusion attack. Moreover, the experimental results demonstrate that the proposed scheme has low time overhead consumption and computation overhead.

The remainder of this article is structured as below. The related work and the preliminaries are introduced in Sections II and III, respectively. Section IV shows the system model and describes the system procedure. In Section V, the details of the proposed scheme are presented. Security analysis is discussed in Section VI. The experimental results are presented in Section VII. Finally, Section VIII concludes the whole paper.

II. Related Work

Blockchain technology is a combination innovation based on a series of technologies, such as peer to peer (P2P) networks, block-chain data structure, and cryptography [22]. The use of hash functions and consensus protocols in blockchain not only ensures the unforgeability of data stored therein but also ensures traceability [23]. As a representative of the second generation blockchain, Ethereum has adopted some features of bitcoin and introduced Turing-complete smart contract, making it a popular distributed application platform [24].

ABE, as one of the important public-key algorithms, was first introduced in [25], which can be used in fine-grained access control to determine the access authority of users according to their attributes. ABE has developed into two directions, namely, KP-ABE and CP-ABE. In KP-ABE, the user's private key is related to the access-control structure, while the ciphertext is related to the attribute set [26]. Differently, in CP-ABE, the user's private key is associated with the attribute set, while the ciphertext is associated with the access-control structure [27]. In [28], combining linear secret sharing schemes (LSSSs), a general construction of CP-ABE was presented by using a matrix $\mathbf{M}$ and a corresponding function ρ to represent the access-control structure. Narayan [29] employed Attribute-based Cryptography to realize privacy protection on EHR.

Fine-grained access has become an emerging technique for the data security and privacy protection of IoT ecosystems. In [30], a data access control scheme for cloud-assisted industrial IoT by using CP-ABE techniques to achieve item-level data protection for IoT data. In [31], a fine-grained access control scheme is proposed with the attribute update enabled in a blockchain-enabled IoT systems. In [32], a privacy-preserving scheme for bilateral access control is proposed with fine granularity in cloud-enabled industrial IoT healthcare. In [33], an efficient, flexible, secure fine-grained access control mechanism is proposed with data verification in a healthcare IoT system. Xu et al. [45] employed KP-ABE to implement access control and data sharing. Other related work also includes [50], in which, a scalable access control method was proposed for privacy-preserving media sharing in mobile cloud computing.

Recently, a number of access-control schemes based on blockchain for EHR data have been introduced. In particular, Azaria et al. [36] proposed the MedRec system to manage the access control permissions with blockchain for EHR data sharing. Then, Yang and Yang [37] proposed advance-MedRec to guarantee the secure sharing of EHR. Later, an Ethereum-based framework, namely, Ancile, that pays more attention to operability, access efficiency and privacy protection were designed in [38]. Ancile creatively employs smart contracts to strengthen access control and data fuzzy processing. To further improve EHR data security, Wang and Song [39] designed an EHR access control protocol by combining identity-based encryption and identity-based signatures. Hirtan et al. [40] designed mainchains and sidechains to enhance the data security and user privacy. In their work, the nodes of the blockchain network contain trusted nodes and untrusted nodes, where trusted nodes include the approved healthcare providers and medical institutions, which have higher permissions and are in charge of validating the transactions. It is worth mentioning that this work can be used to ensure the traceability of EHR data. Guo et al. [41] presented a blockchain-based method to support secure access control, by using ABE technology and employing a tamper-proof log of access events. In [41], a blockchain-based method was presented to provide a tamper-proof log of access events while storing EHRs on edge nodes (offchain) and using ABE to support secure access control. In [34], a system named Healthchain was designed for key management and privacy protection of large-scale health data. To realize data secure sharing, Zhang et al. [42] employed a large universe CP-ABE with access policies partially hidden, but this scheme lacks flexibility and has high computational overhead. Huang et al. [43] proposed MedBloc, a secure EHR sharing system based on blockchain, in which smart contracts are used for access control. Later, Liu et al. [44] presented a system, namely, BC-SABE, to store encrypted EHR data in cloud servers. In BC-SABE, a search token is generated for the user who meets the access-control structure, and the cloud server returns the predecrypted ciphertext according to the search token. Egala et al. [18] proposed a new medical architecture model Fortified-Chain, in which the selective ring-based access control, patient anonymity, and device authentication algorithms are employed to realize privacy protection of EHR data. Li et al. [19] designed EHRChain to realize access control by utilizing CP-ABE, and protect users' privacy by utilizing homomorphic encryption

technology. Wang et al. [20] proposed MedShare, a trusted platform with smart contracts. In MedShare, ABE is used to implement access control, and the EHR data access track is provided.

III. Preliminaries

A. Hash Function and Pseudorandom Function

Definition 1: A hash function $H : \{0,1\}^* \rightarrow \{0,1\}^l$ is collision resistant, if the following two properties are satisfied.

1) *Second-Preimage Resistance:* Given a uniform x, it is infeasible for a probabilistic polynomial-time (PPT) adversary to find a value $x' \neq x$ with $H(x') = H(x)$.
2) *Preimage Resistance:* Given a uniform y, it is infeasible for a PPT adversary to find a value x such that $H(x) = y$.

Definition 2: An efficient function $F : \{0,1\}^{l'} \rightarrow \{0,1\}^{l''}$ is a pseudorandom function, if there exists a negligible function negl$(\cdot)$ such that

$$\left|\Pr\left[\mathcal{A}^{F(\cdot)}\left(1^n\right) = 1\right] - \Pr\left[\mathcal{A}^{f(\cdot)}\left(1^n\right) = 1\right]\right| \leq \text{negl}(n) \quad (1)$$

for all PPT algorithm $\mathcal{A}$, where f is selected from $\mathcal{F}_n = \{\text{func} : \{0,1\}^{l'} \rightarrow \{0,1\}^{l''}\}$ uniformly at random.

B. CP-ABE

CP-ABE is a public-key encryption algorithm according to user's attributes. CP-ABE was introduced in [27], which encrypts message according to access structure. Significantly, in [28], a LSSS matrix $\mathbf{M}$ was used in CP-ABE scheme, in which $(\mathbf{M}, \rho)$ is utilized to represent access control policy, where $\mathbf{M}$ is an $l \times n$ matrix and ρ is a function associated with rows of $\mathbf{M}$ to attributes. In our system, CP-ABE presented in [28] is utilized to realize fine-grained access control of EHR data. The four algorithms of CP-ABE are introduced as follows.

Setup$(u) \rightarrow (pk, mk)$: The Setup algorithm outputs the public key pk and the master key mk by taking the number of attributes u as input.

KeyGen$(mk, \mathcal{S}) \rightarrow sk$: In the KeyGen algorithm, by taking the master key mk and attributes set $\mathcal{S}$ as input, it outputs a secret key sk.

Encrypt$(pk, M, \mathbb{A}) \rightarrow C$: The Encrypt algorithm takes the public key pk, a message M and the access structure $\mathbb{A}$ as input, and outputs the ciphertext C.

Decrypt$(pk, sk, C) \rightarrow M$: The Decrypt algorithm takes the public key pk, the secret key sk and the ciphertext C as input. If the attributes set $\mathcal{S}$ satisfies the access structure $\mathbb{A}$, the Decrypt algorithm outputs the message M.

C. Dual-Key Regression

The dual-key regression scheme that was first proposed in [46], which can be used to share a massive number of keys by only sharing two hash tokens of the start time and the end time and employing two hash chains in the reverse order. As shown in hash chain 1 of Fig. 2, by taking s_1 as a random seed and N as length of hash chains, hash tokens are generated by hash function H sequentially to form the hash chain as follows: $h_1 = H(s_1), h_2 = H(h_1) = H^2(s_1), \ldots, h_i = H(h_{i-1}) = H^i(s_1)$. Given a hash token h_i, it is easy and efficient to compute the hash token after h_i. With the significant preimage resistance nature of hash functions, it is computationally hard to compute hash tokens before h_i. Hash chain 2 is similar to hash chain 1, except that it is generated in the reverse order. The hash chain 2 is generated as follows: $h'_N = H(s_2), h'_{N-1} = H(h'_N) = H^2(s_2), \ldots, h'_i = H(h'_{i+1}) = H^{N-i+1}(s_2)$. Through two opposite hash chains, the start time and the end time are defined to limit the range of data. For instance, given time interval (t_3, t_5) and two corresponding hash tokens h_3 and h'_5, it is easy to compute hash tokens between time t_3 and time t_5, but it is extremely difficult to compute other hash tokens outside (t_3, t_5). For each time interval t_i, SEK$_i$ is calculated as SEK$_i$ = KDF$(h_i \| h'_i)$, where *KDF* is a key derivation function. With the hash tokens (h_i, h'_j) corresponding to time t_i and time t_j, all hash tokens and *SEK*s from time t_i to time t_j can be easily calculated.

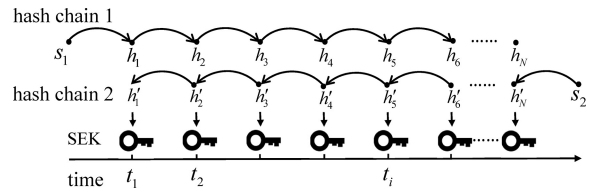

Fig. 2. Dual-key regression.

D. Blockchian

Blockchain is a P2P, unforgeable and tamper-proof distributed ledger [22]. Blockchain stores data in blocks, and connects blocks to each other in chronological order. In blockchain, each block contains the hash values of the previous block. Therefore, if any block changes, the hash values of all subsequent blocks will change. In addition, each node in the blockchain network is independent and has the same status, and stores complete data according to the block structure. In other words, each node maintains the same complete data ledger. The above design enables blockchain to have many excellent features, such as tamper-proof, unforgeable, and traceable. These properties are eligible for secure storage and reliable sharing of medical data among medical institutions.

IV. System Overview

A. System Model

As shown in Fig. 3, there exist several kinds of entities in the system, including a global CA, SHIs, data owners, data users, blockchain, and database server.

CA: The CA is a global trusted CA, which generates system public parameters, global public key, master key, a public-private key pair for each SHI and legal user, and a secret key according to the data user's attributes.

SHI: SHIs provide the elderly with healthcare services. SHIs are responsible for measuring the physical data (e.g., the heart rate, body temperature, body weight, and blood pressure) of the elderly every day, as well as managing the elderly's EHR data including the electronic medical record, regular physical health examination data and daily physical data.

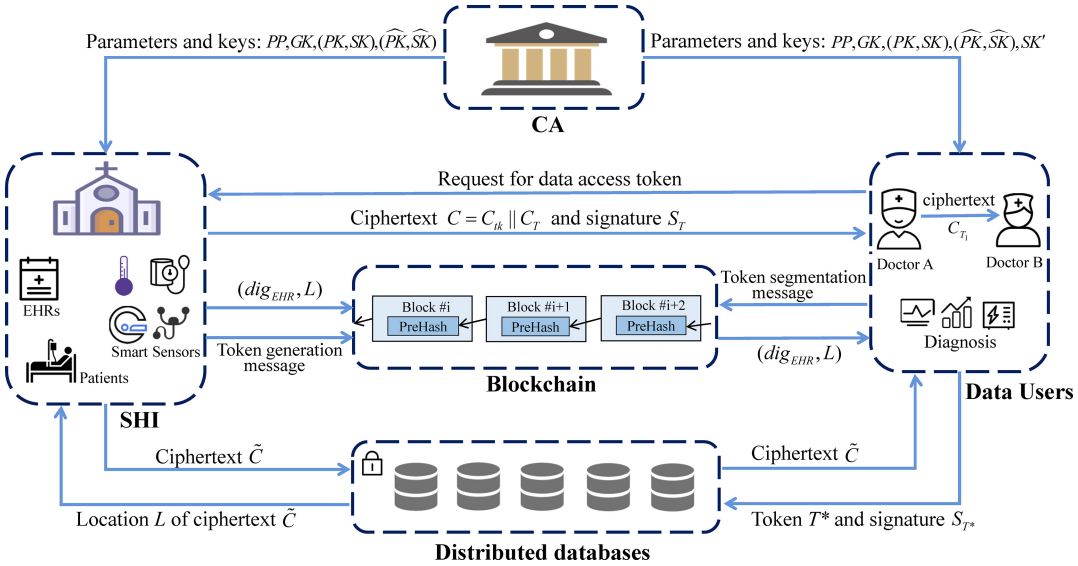

Fig. 3. System model.

Data Owner: The data owners are the elderly in a SHI. When the elderly registers in a SHI, he/she will authorize the SHI to manage his/her EHR data by default. Therefore, the data owner just needs to define access control policies over attributes. Only when the data user's attributes satisfy the corresponding access policy, he/she has the chance to access the elderly's EHR data.

Data User: Data users can be the doctors who need to access the EHR data of an elderly in a SHI for diagnosing the elderly, the employees in an insurance company who help the elderly in a SHI with insurance approval and reimbursement, and the staff in ministry of public health, etc. For convenience, we only consider access control for doctors in this article, and the access control for other types of data users, e.g., the employees in an insurance company, is similar. Only when the doctor's attributes satisfy the corresponding access control policy can he/she have a chance to decrypt the encrypted permission token generated from SHI. When doctor A needs other doctors to assist him/her in diagnosis, doctor A can delegate the corresponding part of his/her token to other doctors.

Blockchain: Blockchain is the platform that stores the hash digest of EHR data, the access address of the encrypted EHR data and the token list to record the token segmentation message. Due to the huge cost of uploading all the original EHR data, the blockchain just stores the digest of EHR.

Database Server: The database server is one of the distributed databases of medical institutions. It stores owners' EHR data and provides data users with data-access services. Whenever a ciphertext is successfully stored, it returns the storage address to SHI. Then, SHI transmits the digest of the EHR data and the storage address on blockchain. When a data user requests to access EHR data over a period of time, he/she should submit a token to the server. The server will send the EHR ciphertext to the data user after the token is verified successfully.

B. System Procedure

1) System Initialization: In the system initialization phase, the CA runs the $\text{Setup}(u) \rightarrow (PP, GK, MK)$ algorithm, which takes the number of attributes universe u, to generate system public parameter PP, global public key GK, and master secret key MK.

2) Key Generation: In this phase, the CA runs three algorithms, e.g., $\text{PSkeyGen}(1^\lambda) \rightarrow (PK, SK)$ algorithm, $\text{SignKeyGen}(1^\lambda, PP) \rightarrow (\widehat{PK}, \widehat{SK})$ algorithm and $\text{SKGen}(MK, S) \rightarrow SK'$ algorithm. The PSkeyGen algorithm generates the pair of public/private keys (PK, SK) for SHIs and users with implicit security parameter λ as input. Similarly, the SignKeyGen algorithm generates the pair of public/private keys $(\widehat{PK}, \widehat{SK})$ of signature for SHIs and users with implicit parameter λ and public parameter PP as input. The SKGen algorithm generates SK' according to $\mathcal{S}$ by taking the master secret key MK and the attributes set $\mathcal{S}$ as input.

3) Data Storage: In data storage phase, the SHI first runs the algorithm $\text{DataEnc}(1^\lambda, \text{EHR}, PP, \mathcal{T}) \rightarrow (C_{\text{EHR}}, \text{dig}_{\text{EHR}}, \mathcal{K})$ to encrypt the EHR data and computes the digest of EHR. By inputting the security parameter λ, the EHR data, the system public parameter PP and the time tuple $\mathcal{T}$, this algorithm outputs the ciphertext C_{EHR}, digest dig_{EHR} and symmetric key $\mathcal{K}$, where time tuple $\mathcal{T}$ contains the start time t_{start}, end time t_{end} and unit time interval t_{unit}. Then SHI runs algorithm $\text{KeyEncap}(\mathcal{T}, \mathcal{K}, PP) \rightarrow (C_{\mathcal{K}}, \gamma, \mathcal{HL})$ to encapsulate symmetric key. The algorithm takes the time tuple $\mathcal{T}$, the public parameter PP and symmetric key $\mathcal{K}$ as input, then outputs the ciphertext $C_{\mathcal{K}}$, a secret random γ and hash-token list $\mathcal{HL}$. In the proposed scheme, data storage is carried out according to time sequence, in the form of data sequence. Then, the SHI sends the digest of EHR, location of encrypted EHR to the blockchain, and sends ciphertext $\tilde{C} = C_{\mathcal{K}} \| C_{\text{EHR}}$ to database.

4) Token Generation: When a data user requests access to an elderly's EHR data over a period of time, the SHI runs $\text{TokenGen}(\gamma, \widehat{SK}, R, \mathcal{HL}) \rightarrow T$ algorithm to generate data

TABLE I
NOTATIONS

Notations	Definition
$\mathbb{G}$	The multiplicative cyclic group of prime order p
e	The bilinear map
u	The number of attributes in the system
α, β	The random exponents in $\mathbb{Z}_p$
λ	The security parameter.
PP	The system public parameter
GK	The global public key
MK	The master key
(PK, SK)	The pair of public/private keys
$(\widehat{PK}, \widehat{SK})$	The pair of public/private keys for signature
SK'	The secret key related to users' attributes
dig_M	The hash digest of message M
C_M	The ciphertext of message M
$(\mathbf{M}, \rho)$	The LSSS access structure
N	The maximum number of EHR files for a data owner
t_{unit}	The unit interval length for data to be stored
t_{start}	The start time of the data to be stored
t_{end}	The end time of the data to be stored
T	The data access token
S_T	The signature of token T
$k, \mathcal{K}$	The symmetric key to encrypt EHR and its sequence
SEK	The key to encrypt symmetric key k
$\mathcal{HL}$	The hash token list
R	The request message
F	The pseudorandom function
s_1, s_2	The secret random seeds

access token T for him/her, where the R is the request message of data access. Then, the SHI computes the signature S_T of the token. Next, the SHI runs $\mathrm{TokenEnc}(PP, GK, (\mathbf{M}, \rho), T) \rightarrow C$ algorithm to encrypt the token T, where $(\mathbf{M}, \rho)$ is the access structure. If the data user's attributes meet the access policy, he/she can run $\mathrm{TokenDec}(C, SK') \rightarrow T$ algorithm to obtain the token T.

5) Token Segmentation: Sometimes, doctor A needs another doctor B_i to assist him/her to complete the medical diagnosis. Doctor A first runs $\mathrm{TokenSeg}(T, S_T, PP, uid_i) \rightarrow (T, T_i)$ algorithm to separate subtoken T_i from his/her token, where the uid_i is the identity of the target data user. Then, he/she runs $\mathrm{TokenDel}(T_i, PK_{B_i}, \widehat{SK}_A) \rightarrow C_{T_i}$ algorithm to delegate a subtoken T_i to the doctor B_i. All token segmentation and delegation information will be sent to the blockchain.

6) Data Access: After passing the token verification, the data user can obtain the location of the EHR data from the blockchain, and downloads the ciphertext $\tilde{C}$ from the database server if the token verification is successful. Then, the data user runs the $\mathrm{DataDec}(T, PP, \tilde{C}) \rightarrow$ EHR algorithm to obtain the EHR data. When the legitimate data users completed the diagnosis by accessing the EHR data between time t_i and time t_j, the key-update procedure is performed to get new keys in order to withdraw the data users' access authority.

V. PROPOSED SCHEME

In this section, we introduce the detailed construction of our scheme. Before that, we first list the notations and definitions used in our scheme in Table I.

A. System Initialization

First, the CA performs global settings to generate system public parameters PP, the global public key GK, as well as the master key MK by using algorithm $\mathrm{Setup}(u) \rightarrow (PP, GK, MK)$, where u is the number of attributes universe.

1) Select two multiplicative cyclic groups $\mathbb{G}$ and $\mathbb{G}_T$ of prime order p, in which the generator of $\mathbb{G}$ is g. Choose a bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$.
2) Select three hash functions as follows: $H_0 : \{0,1\}^* \rightarrow \mathbb{Z}_p$, $H_1 : \{0,1\}^* \rightarrow \{0,1\}^l$, and $H_2 : \{0,1\}^* \rightarrow \{0,1\}^{l^*}$, and a pseudorandom function $F : \{0,1\}^{2l} \rightarrow \{0,1\}^{l^*}$, where H_1 is a collision resistant hash function, and l and l^* are two integers.
3) Choose u group elements $h_1, h_2, \ldots, h_u \in \mathbb{G}$ uniformly at random, which are related with the u attributes.
4) Select $\alpha, \beta \in \mathbb{Z}_p$ uniformly at random.
5) Compute the system public parameters PP, the global public key GK and the master key MK as

$$PP = \left(\mathbb{G}, H_0, H_1, H_2, F, g, p, g^{\beta}, e(g,g)^{\alpha}\right) \quad (2)$$

$$GK = \{h_x | x \in [1, u]\} \quad (3)$$

$$MK = \left(\beta, g^{\alpha}\right). \quad (4)$$

B. Key Generation

This phase consists of three parts: 1) public and private keys generation (*PSkeyGen* for short); 2) public and private keys of signature generation (SignKeyGen for short); and 3) secret key generation (SKGen for short).

Part 1 PSKeyGen*:* CA generates public-private key pairs for each SHI and user as follows.

1) Choose two large prime numbers q_1 and q_2 with similar size, and computes $n = q_1 q_2$ and $\varphi(n) = (q_1 - 1)(q_2 - 1)$.
2) Select an integer b from $[2, \varphi(n) - 1]$ uniformly at random so that $(b, \varphi(n)) = 1$, and computes $a \equiv b^{-1} (\mathrm{mod} \varphi(n))$.
3) Transmit (PK, SK) to SHI as the public/private key, in which $PK = (n, b)$ and $SK = (n, a)$.

The public/private keys for data users can be obtained from the same processes.

Part 2 SignKeyGen*:* CA generates the public key and private key of signature for each SHI and user as follows. CA chooses a uniform $x \in \mathbb{Z}_p$, and computes g^x. Then, CA transmits $(\widehat{PK}, \widehat{SK})$ to SHI as the public/private key, where $\widehat{PK} = g^x$ and $\widehat{SK} = x$. The CA performs the same processes to distribute public/private key for each user.

Part 3: SKGen*:* CA generates the secret key SK' for data user according to the attributes of data user, where the secret key of each data user is related to his/her attributes.

1) Verifie the legitimacy of the identity of the data user, and distributes an attributes set S for him/her.
2) Choose an element $t \in \mathbb{Z}_p$ uniformly at random.
3) Compute

$$K = g^{\alpha + \beta t}, \quad L = g^t, \quad K_x = h_x^t \quad (\forall x \in S). \quad (5)$$

4) Output the secret key of data user as follows:

$$SK' = (K, L, \{K_x\}_{x \in S}). \quad (6)$$

$C_{k_1} \| C_{EHR_1}$	$C_{k_2} \| C_{EHR_2}$	···	$C_{k_i} \| C_{EHR_i}$	···	$C_{k_N} \| C_{EHR_N}$

Fig. 4. Data format on database server.

C. Data Storage

After the elderly is registered in a SHI, the elderly first authorizes the SHI to manage his/her EHR data. At the beginning, the SHI negotiates with the elderly for unit interval t_{unit}, such as one week, one month, one year, etc. Then, the SHI sets the start time t_{start}, and selects an enough large t_{end} as the end time. Let $\mathcal{T}$ represents time tuple $(t_{\text{start}}, t_{\text{end}}, t_{\text{unit}})$ and N represents the number of time interval, which satisfies the equation $t_{\text{end}} = t_{\text{start}} + N \cdot t_{\text{unit}}$.

The EHR data storage phase is performed by SHI, which includes DataEnc algorithm and KeyEncap algorithm.

Part 1 (Data Encryption): By taking the security parameter λ, the time tuple $\mathcal{T}$, the system public parameter PP and EHR data as input, the DataEnc algorithm is described as follows.

First, for each time interval t_i, the algorithm chooses $k_i \in \{0,1\}^{l^*}$ uniformly at random as encryption key for EHR data of an elderly generated in time interval t_i. The key sequence constitutes the symmetric key $\mathcal{K} = \{k_1, k_2, \ldots, k_N\}$. Naturally, EHR data is also packaged EHR_i according to each time interval t_i $(i = 1, 2, \ldots, N)$. Then, for each time interval t_i, it computes the digest of the EHR data by

$$\text{dig}_{\text{EHR}i} = H_1(\text{EHR}_i), \quad i \in \{1, 2, \ldots, N\}. \tag{7}$$

The EHR data is encrypted by AES algorithm with symmetric key k_i as

$$C_{\text{EHR}_i} = \text{Enc}_{k_i}(\text{EHR}_i), \ \ i \in \{1, 2, \ldots, N\}. \tag{8}$$

Part 2 (Symmetric Key Encapsulation): By inputting the time tuple $\mathcal{T}$, the key $\mathcal{K}$ and system public parameter PP, and outputs the ciphertext $C_{\mathcal{K}}$, the secret random γ and the hash-token list $\mathcal{HL}$, the algorithm $\text{KeyEncap}(\mathcal{T}, \mathcal{K}, PP) \rightarrow (C_{\mathcal{K}}, \gamma, \mathcal{HL})$ is described as follows.

The algorithm chooses $s_1, s_2 \in \{0,1\}^{2l}$ uniformly at random, in which s_1 and s_2 are two different secret seeds to generate two hash-chains in opposite directions. Then, the algorithm chooses $\gamma \in \{0,1\}^{2l}$ uniformly at random. For each time t_i, hash tokens h_i and h'_i are generated with collision resistant hash function H_1 in two chains, respectively. All hash tokens are recorded in hash-token list $\mathcal{HL}$. Then, the algorithm employs the pseudorandom function F to compute the SEK_i with

$$\text{SEK}_i = F\big((h_i \| h'_i) \oplus \gamma\big). \tag{9}$$

The algorithm encapsulates symmetric key with SEK_i as

$$C_{k_i} = \text{Enc}_{\text{SEK}_i}(k_i) \ \forall i \in \{1, \ldots, N\} \tag{10}$$

where the encryption algorithm is AES. The SHI sends the ciphertext $\tilde{C} = C_{k_i} \| C_{\text{EHR}i}$ of EHR data of elderly to database server in the format as described in Fig. 4. After the database server successfully stores the ciphertext, the server returns the ciphertext location L_i (such as URL) to the SHI. Finally, the SHI sends $(\text{dig}_{\text{EHR}i}, L_i)$ to the blockchain.

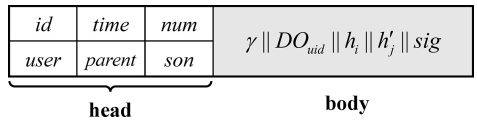

Fig. 5. Token structure.

D. Token Generation

If a data user requests to access EHR data generated from time t_i to t_j, he/she first sends the request message $R = (\text{uid}, \text{DO}_{\text{uid}}, (t_i, t_j))$ to the SHI, where *uid* is the identify of data user, DO_{uid} is the identify of the data owner, (t_i, t_j) is the interval of generated time of the accessing EHR data. Then, the SHI runs $\text{TokenGen}(\gamma, \widehat{SK}, R, \mathcal{HL}) \rightarrow T$ algorithm to generate a data access token T. The structure of the token is shown in Fig. 5, which includes two parts: head and body. The head of token comprises *id*, time, num, user, parent and son fields, where *id* is a unique identity number for each token, time represents the effective time of the token, num represents the times the token can be used, user represents the owner of the token, parent represents the *id* of its parent token and son represents the *id* of its son token. The content of the token body consists of a secret random number γ, the identify of the data owner DO_{uid} and hash tokens h_i and h'_j. SHI runs the digital signature algorithm Sign as in [35] and [47] to sign the contents of the token body as follows.

1) Choose a uniform $\pi \in \mathbb{Z}_p$.
2) Compute $r' = H_0(g^{\pi}, \gamma \| \text{DO}_{\text{uid}} \| h_i \| h'_j)$.
3) Calculate $\sigma' = (r' \cdot \widehat{SK}_{\text{SHI}} + \pi)(\mod p)$.
4) Output the signature $\text{sig} = (r', \sigma')$.

Accordingly, the data access token is shown as follows:

$$T = \Big(\textbf{head}, (\gamma, DO_{\text{uid}}, h_i, h'_j, \text{sig})\Big). \tag{11}$$

Similarly, the SHI runs the $\text{Sign}(T, \widehat{SK}_{\text{SHI}}, PP) \rightarrow S_T$ algorithm to sign the whole token, where $S_T = (r, \sigma)$.

The elderly can set access control policy with the help of SHI to decide who can access his/her EHR data. In our system, the access control policy can be represented as an access structure $(\mathbf{M}, \rho)$, where $\mathbf{M}$ is a $\theta_1 \times \theta_2$ matrix, θ_1 denotes the total number of attributes in terms of the access control policy of the EHR data, and ρ is a function which maps each row $\mathbf{M}_i$ of $\mathbf{M}$ with each attribute.

Then, the SHI runs the TokenEnc algorithm to encrypt the data access token as follows.

1) Choose an element $tk \in \mathbb{G}_T$ uniformly at random.
2) Encrypt the token T with symmetric key $H_2(tk)$ to get ciphertext $C_T = \text{Enc}_{H_2(tk)}(T)$.
3) Choose $s, y_2, \ldots, y_{\theta_2} \in \mathbb{Z}_p$ randomly, and denotes $\vec{v} = (s, y_2, \ldots, y_{\theta_2})$.
4) For $i = 1$ to θ_1, computes $\varphi_i = \vec{v} \cdot \mathbf{M}_i$, where $\mathbf{M}_i$ is the ith row of $\mathbf{M}$.
5) Choose $r_1, r_2, \ldots, r_{\theta_1} \in \mathbb{Z}_p$ uniformly at random.
6) Compute

$$C' = tk \cdot e(g, g)^{\alpha s}, \quad C'' = g^s \tag{12}$$

$$C_i = g^{\beta \varphi_i} h_{\rho(i)}^{-r_i}, \ \ D_i = g^{r_i} \ \forall i \in \{1, 2, \ldots, \theta_1\}. \tag{13}$$

7) Output the ciphertext of tk

$$C_{tk} = \left(C', C'', \{C_i, D_i\}_{i=1}^{\theta_1}\right). \tag{14}$$

Finally, SHI sends $C = C_{tk} \| C_T$ to the data user.

If the data user's attributes set $\mathcal{S}$ satisfies the access control policy, he/she can run the TokenDec algorithm to decrypt the ciphertext C_{tk} with the private key SK' to obtain tk as follows.

Define index set $\mathcal{I} = \{i : \rho(i) \in \mathcal{S}\}$ and matrix

$$\mathbf{M}_{\mathcal{I}} = \left[M_{i_1}; M_{i_2}; \ldots; M_{i_{|\mathcal{I}|}}\right] \tag{15}$$

where $|\mathcal{I}|$ is the cardinality of $\mathcal{I}$. Defining $\theta_2 \times 1$ matrix $\Xi_0 = [1, 0, \ldots, 0]^T$, the data user finds a root of a linear system of equations

$$\mathbf{M}_{\mathcal{I}}^T \mathbf{X} = \Xi_0 \tag{16}$$

and denotes the root as $\Omega_{\mathcal{I}} = [\omega_{i_1}, \ldots, \omega_{i_{|\mathcal{I}|}}]^T$, where $\mathbf{X} = [x_1, x_2, \ldots, x_{|\mathcal{I}|}]$. Then, he/she can obtain s by computing

$$s = \Psi_{\mathcal{I}} \Omega_{\mathcal{I}} \tag{17}$$

where $\Psi_{\mathcal{I}} = [\varphi_{i_1}, \ldots, \varphi_{i_{|\mathcal{I}|}}]$. Then, the data user computes

$$\begin{aligned} &\frac{e\left(C'', K\right)}{\prod_{i \in I}\left(e(C_i, L) e(D_i, K_{\rho(i)})\right)^{\omega_i}} \\ &= \frac{e\left(g^s, g^{\alpha+\beta t}\right)}{\prod_{i \in I}\left(e(g^{\beta\varphi_i} h_{\rho(i)}^{-r_i}, g^t) e(g^{r_i}, h_{\rho(i)}^t)\right)^{\omega_i}} \\ &= \frac{e(g^s, g^\alpha) e\left(g^s, g^{\beta t}\right)}{\prod_{i \in I} e(g, g)^{\beta t \omega_i \varphi_i}} = \frac{e(g^s, g^\alpha) e\left(g^s, g^{\beta t}\right)}{e\left(g^s, g^{\beta t}\right)} \\ &= e(g, g)^{\alpha s}. \end{aligned} \tag{18}$$

The data user can obtain tk as follows:

$$tk = C' \big/ e(g, g)^{\alpha s}. \tag{19}$$

Finally, the data user obtains token T by decrypting C_T with symmetric key $H_2(tk)$.

E. Token Segmentation

When doctor A (as a data user) encounters difficulties in diagnosing the elderly, he/she needs to apply for assistance from doctor B_1, doctor B_2, etc. However, it would take a lot of time for SHI to generate a new token for each doctor, accompanied by a series of request and confirmation communications. For the sake of improving the diagnosis efficiency and diminish the burden of the SHI and the centralization of the system, doctor A can delegate his/her authority to other doctors. Accordingly, token segmentation algorithm is presented in the proposed system to realize more fine-grained and flexible permission management as follows.

Part 1 (Token Segmentation): Doctor A (whose id is denoted by uid_0) first verifies the signature of the token. If the token is valid, then he/she segments the token into several subtokens as follows. Let $uid_1, uid_2, \ldots, uid_\tau$ be the id of the permission delegate objects. First, for any i in $\{1, 2, \ldots, \tau\}$, the algorithm creates a copy T_i of token T, revises the value of the corresponding field of T_i and reduces the corresponding value of T. After the user field of T_i is set as uid_i of doctor B_i, the algorithm sets parent field of T_i as id of token T, while the algorithm adds id of token T_i to the son field of T.

Algorithm 1 Token Segmentation Algorithm: TokenSegm

Input: Current token T, public parameter PP, token signature $S_T = (r, \sigma)$, SHI's public key for signing $\widehat{PK}_{SHI}$, and permission delegate objects $uid_1, uid_2, \cdots, uid_\tau$.
Output: $T_0, T_1, T_2, \ldots, T_\tau$

```
verify ← 0
if H_0(g^σ · PK̂_SHI^{-r}, T) = r then
    verify ← 1
end if
if verify = 1 then
    for i = 1 to τ do
        Chooses time_i and num_i with time_i ≤ T.time and
        num_i ≤ T.num
        T_i ← copy(T)
        T_i.time ← time_i
        T_i.num ← num_i
        T.num ← T.num − num_i
        T_i.parent ← T
        [T.son]+ = T_i
        T_i.user ← uid_i
    end for
    rename T as T_0
    return T_0, T_1, T_2, ..., T_τ
end if
```

After the token segmentation, doctor A signs the new tokens with his/her private key and gets the set of signatures $\{S_{T_i}\}_{i=0}^{\tau}$. Note that, as doctor A needs the assistance of doctor B_i to complete the diagnosis at the same time, we allow token T and T_i to have the same time period in our system. For details of token segmentation algorithm TokenSegm, please refer to Algorithm 1.

Part 2 (Token Delegation): After token segmentation, doctor A can run TokenDel algorithm to delegate subtoken T_i to doctor B_i as follows. The algorithm chooses a random number $r_i \in \{0, 1\}^{l^*}$, and encrypts subtoken T_i as

$$C_{T_i} = E_{PK_{B_i}}(r_i) \| \mathrm{Enc}_{r_i}\left(T_i \| S_{T_i}\right) \tag{20}$$

where S_{T_i} is the signature of T_i by doctor A, $E_{PK_{B_i}}(\cdot)$ is the encryption algorithm of RSA-OAEP scheme [49] with public key PK_{B_i} of doctor B_i, and $\mathrm{Enc}_{r_i}(\cdot)$ is the encryption algorithm of AES with key r_i. Then, doctor A transmits the ciphertext C_{T_i} to doctor B_i, and publishes the information $\mathrm{TSM} = \{\mathrm{uid}_i, C_{T_i}\}_i$ to the blockchain.

F. Data Access

When a data user doctor B obtains a token T (suppose his/her token is a subtoken obtained from doctor A), he/she can send the request message $R = (\mathrm{uid}, \mathrm{DO}_{\mathrm{uid}}, (t_i, t_j))$ to the blockchain for data access. After receiving the request, blockchain returns the pair of the digest and location of the EHR data $(\mathrm{dig}_{\mathrm{EHR}_\iota}, L_\iota)$ to data user, where $\iota = i, , \ldots, j$. According to the location L, the doctor submits his/her token T and the token signature S_T to the corresponding database

Algorithm 2 Token Verification Algorithm: TokenVeri

Input: Token T, token signature S_T, public parameter PP, SHI's public key for signing $\widehat{PK}_{SHI}$ and doctor B's public key for signing $\widehat{PK}_B$.
Output: verify
verify $\leftarrow 0$
if $(H_0(g^{\sigma} \cdot PK_B^{-r}, T) = r) \wedge (H_0(g^{\sigma'} \cdot PK_{SHI}^{-r'}, \gamma \| DO_{uid} \| h_i \| h'_j) = r')$ **then**
  verify $\leftarrow 1$
  return verify
end if

server for EHR data. As shown in Algorithm 2, the database server verifies the token by running the token verification algorithm TokenVeri.

If the token verification is successful, the server sends ciphertext stream $\tilde{C} = \{C_{k_\iota} \| C_{\mathrm{EHR}_\iota}\}_{\iota=i}^{j}$ between time t_i and t_j to doctor B. After receiving ciphertext $\tilde{C}$, the doctor runs the algorithm $\mathrm{DataDec}(T, PP, \tilde{C}) \rightarrow \mathrm{EHR}$ to obtain the EHR data as follows.

1) Extract h_i, h'_j, and γ from token T. $\forall \iota \in [i, j]$, compute the symmetric key k_ι between time t_i and t_j by
$$k_\iota = \mathrm{Dec}_{SEK_\iota}\left(C_{k_\iota}\right) \tag{21}$$
where $\mathrm{SEK}_\iota = F((h_\iota \| h'_\iota) \oplus \gamma)$, $h_\iota = H_1^{(\iota-i)}(h_i)$ and $h'_\iota = H_1^{(j-\iota)}(h'_j)$.
2) $\forall \iota \in [i, j]$, the EHR data can be obtained by decrypting the ciphertex C_{EHR_ι}
$$\mathrm{EHR}_\iota = \mathrm{Dec}_{k_\iota}\left(C_{\mathrm{EHR}_\iota}\right). \tag{22}$$

The doctor computes $\mathrm{dig}'_{\mathrm{EHR}} = H_1(\mathrm{EHR})$. If $\mathrm{dig}_{\mathrm{EHR}}$ and $\mathrm{dig}'_{\mathrm{EHR}}$ are equal, it demonstrates that the EHR data has not been tampered with, and doctors can provide diagnostic services for the elderly.

When the doctors completed the diagnosis by accessing the EHR data between time t_i and time t_j, the key-update procedure should be performed to withdraw the data users' access authority as below.

1) For each $\iota \in \{i, \ldots, j\}$, SHI chooses $k'_\iota \in \{0, 1\}^{l^*}$ uniformly at random. Then the key sequence is $\mathcal{K}' = \{k_1, \ldots, k_{i-1}, k'_i, \ldots, k'_j, k_{j+1}, \ldots, k_N\}$.
2) SHI computes the cipertext C'_{EHR} as follows:
$$C'_{\mathrm{EHR}_\iota} = \mathrm{Enc}_{k'_\iota}(\mathrm{EHR}_l),\ \iota \in \{i, \ldots, j\}. \tag{23}$$
3) SHI runs the $\mathrm{KeyEncap}(\mathcal{T}, \mathcal{K}', PP) \rightarrow (C_{\mathcal{K}}, \gamma', \mathcal{HL}')$ algorithm again. To reduce the system cost, the EHR data without being accessed, does not require to be encrypted again.

VI. Security Analysis

A. Security Model

In the proposed system, both the CA and SHI are assumed to be trusted. The database server is assumed to be semi-trusted (i.e., curious but honest). Data users are dishonest and may collude to obtain unauthorized access to data. The security model is described as the following games.

Let us first discuss the security model of EHR data. Considering the game between a challenger and a PPT adversary $\mathcal{A}$ as follows.

Setup: The challenger sends the system public parameters PP to the adversary by running the Setup algorithm.

Phase 1: The adversary queries the following oracles adaptively.

1) *DataEnc Oracle:* The adversary sends a message m to the challenger in order to obtain the corresponding ciphertext. Then, the challenger runs the $\mathrm{DataEnc}(1^\lambda, m, PP, \mathcal{T}) \rightarrow (C_m, \mathrm{dig}_m, \mathcal{K})$ algorithm and sends C_m to the adversary.
2) *KeyEncap Oracle:* When the adversary queries the oracle, the challenger runs the $\mathrm{KeyEncap}(\mathcal{T}, k, PP) \rightarrow (C_k, \gamma, \mathcal{HL})$ algorithm and sends C_k to the adversary.

Phase 2: The adversary can query as in Phase 1 with polynomial time in λ. Then, the adversary can get the set of triples $\{m'_i, C_{m'_i}, C_{k'_i}\}_{i=1}^{\ell}$.

Challenge: The adversary submits two messages m_0 and m_1 of the same length to the challenger, in which, m_0 and m_1 are not in $\{m'_i\}_{i=1}^{\ell}$. The challenger randomly chooses a bit $b \in \{0, 1\}$ and runs the DataEnc algorithm and KeyEncap algorithm. Finally, the challenger sends the $C_k \| C_{m_b}$ to the adversary.

Guess: The adversary guesses b' for b. The advantage of the adversary for winning this confidentiality game is defined as $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{cpa}} = |\Pr[b = b'] - 1/2|$.

Definition 3: The proposed scheme is ciphertext indistinguishability under chosen-plaintext attacks (i.e., *IND-CPA secure*), if the advantage of any PPT adversary $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{cpa}}$ defined above is negligible, i.e.,
$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{cpa}} = \left|\Pr\left[b = b'\right] - 1/2\right| \leq \mathrm{negl}(\lambda).$$

Then, we discuss the security model of token. To prevent that adversary obtains the privacy of the elderly by inferring the relationship (such as father-child relationship, sibling relationship) between tokens through the ciphertext of the segmented tokens, the property of token unlinkability should also be satisfied. To this end, we consider the following game between a challenger C and a PPT adversary $\mathcal{A}$.

Setup: The challenger sends the system public parameters PP and public/private key pair of adversary $(PK_{\mathrm{adv}}, SK_{\mathrm{adv}})$ to the adversary by running the Setup algorithm.

Case I (Unlinkability of Between the Parent and Child Tokens):

Phase 1: The adversary selects two tokens T_0 and T_1 of the same size adaptively, and then sends them to the challenger.

1) *Challenge:* The challenger chooses a bit b from $\{0, 1\}$ uniformly at random, and then runs the $\mathrm{TokenSeg}(T_b, S_{T_b}, PP, \mathrm{uid}_C) \rightarrow (T_b, T'_b)$ algorithm and $\mathrm{TokenDel}(T'_b, PK_{B_i}, \widehat{SK}_C) \rightarrow C_{T'_b}$, where $\widehat{SK}_C$ is the private key of signature of challenger, and the public key of adversary PK_{adv} is not equal to PK_{B_i}. Finally, the challenger returns $C^*_{T'_b}$ to the adversary.
2) *Phase 2:* After obtaining the challenger returns for the pair of T_1 and T_2, the adversary can further make queries as in Phase I in order to get more information about b.

Case II (Unlinkability of Between Subtokens):

Phase 1: The adversary selects a token T, and separates it into two subtokens T_1 and T_2 of the same size adaptively; then he selects a token T_0 with the same size adaptively; finally, he sends $\{T_0, T_1, T_2\}$ to the challenger.

1) *Challenge:* The challenger first runs algorithm $\text{TokenDel}(T_2, PK_{B_i}, \widehat{SK}_C) \rightarrow C_{T_2}$. Then, the challenger chooses a random bit $b \in \{0, 1\}$, and runs algorithm $\text{TokenDel}(T_b, PK_{B_i}, \widehat{SK}_C) \rightarrow C_{T_b}$. Finally, he returns C_{T_2} and C_{T_b} to the adversary.
2) *Phase 2:* After obtaining the challenger returns for the pair of T_1 and T_2, the adversary can further make queries as in Phase I in order to get more information about b.

Guess: The adversary guesses b' for b. The advantage of the adversary for winning this confidentiality game is defined as $\text{Adv}_{\mathcal{A}}^{\text{unlink}} = |\Pr[b = b'] - 1/2|$.

Definition 4: The proposed scheme satisfies the property of *token unlinkability*, if the advantage $\text{Adv}_{\mathcal{A}}^{\text{unlink}}$ defined above for any PPT adversary is negligible, i.e.,

$$\text{Adv}_{\mathcal{A}}^{\text{unlink}} = \left|\Pr\left[b = b'\right] - 1/2\right| \leq \text{negl}(\lambda).$$

B. Security Analysis

Suppose that F is a pseudorandom function and encryption algorithm AES is a random permutation when the key of AES is chosen from key space uniformly at random, the following theorem shows that the EHR data is ciphertext indistinguishability under chosen-plaintext attacks.

Theorem 1: Suppose that F is a pseudorandom function, and encryption algorithm AES is a random permutation when the key is selected for key space uniformly at random, then the proposed scheme is IND-CPA secure.

Proof: Let $\Pi = (\text{DataEnc}, \text{KeyEncap})$: $\widetilde{\Pi}$ is defined the same as Π except that a truly random function f is utilized in place of pseudorandom function F. In other words, $\widetilde{\Pi}$ uses a truly random function f to compute the *SEK*. Let $\mathcal{A}$ be a PPT adversary. The CPA indistinguishability experiment $\text{Priv}K_{\mathcal{A},\widetilde{\Pi}}^{\text{cpa}}(PP)$ is described as follows.

1) Run Setup to generate PP.
2) $\mathcal{A}$ is given PP and oracles access to DataEnc$(\cdot)$ and KeyEncap$(\cdot)$, and outputs two messages m_0 and m_1 of the same length.
3) Choose a random bit $b \in \{0, 1\}$ and run the DataEnc algorithm and KeyEncap algorithm to generate C_{m_b} and C_k. Then give $C_k \| C_{m_b}$ to $\mathcal{A}$.
4) $\mathcal{A}$ has oracle access to DataEnc$(\cdot)$ and KeyEncap$(\cdot)$ before outputs a bit b'.
5) If $b' = b$, the experiment outputs 1, otherwise 0.

A distinguisher D for the pseudorandom function F is constructed by using $\mathcal{A}$ to determine whether this function is pseudorandom or not as follows. D is given input PP and access to oracles DataEnc$(\cdot)$ and KeyEncap$(\cdot)$.

Distinguisher D:

1) *Run $\mathcal{A}(PP)$:* When $\mathcal{A}$ queries the oracle on a message m, answer this query in the following way:
   a) Runs the DataEnc algorithm to generate C_m.
   b) Runs the KeyEncap algorithm to generate C_k.
   c) Returns $C_k \| C_m$ to $\mathcal{A}$.
2) When $\mathcal{A}$ output two messages m_0 and m_1 of the same length, chooses a uniform bit $b \in \{0, 1\}$ and then as follows.
   a) Runs the DataEnc algorithm to gennerate C_{m_b}.
   b) Runs the KeyEncap algorithm to gennerate C_k.
   c) Returns $C_k \| C_{m_b}$ to $\mathcal{A}$.
3) Continue answering oracle queries of $\mathcal{A}$ until $\mathcal{A}$ outputs a bit b'. If $b' = b$, output 1, otherwise 0.

Since F is a pseudorandom function, there is a negligible function $\text{negl}(n)$ such that

$$\left|\Pr\left[D^{F(\cdot)}(PP) = 1\right] - \Pr\left[D^{f(\cdot)}(PP) = 1\right]\right| \leq \text{negl}(\lambda). \quad (24)$$

According to the scheme Π and $\widetilde{\Pi}$, the following conclusions can be drawn.

1) If the function $\mathcal{F}$ in D is a pseudorandom function F, then for $\mathcal{A}$, it is equivalent to an experiment $\text{Priv}K_{\mathcal{A},\Pi}^{\text{cpa}}(PP)$. According distinguisher D, we know that
$$\Pr\left[D^{F(\cdot)}(PP) = 1\right] = \Pr\left[\text{Priv}K_{\mathcal{A},\Pi}^{\text{cpa}}(PP) = 1\right]. \quad (25)$$
2) If the function $\mathcal{F}$ in D is a random function f, then for $\mathcal{A}$, it is equivalent to an experiment $\text{Priv}K_{\mathcal{A},\widetilde{\Pi}}^{\text{cpa}}(PP)$. According distinguisher D we know that
$$\Pr\left[D^{f(\cdot)}(PP) = 1\right] = \Pr\left[\text{Priv}K_{\mathcal{A},\widetilde{\Pi}}^{\text{cpa}}(PP) = 1\right]. \quad (26)$$

From, (24), we can get

$$\left|\Pr\left[\text{Priv}K_{\mathcal{A},\Pi}^{\text{cpa}}(PP) = 1\right] - \Pr\left[\text{Priv}K_{\mathcal{A},\widetilde{\Pi}}^{\text{cpa}}(PP) = 1\right]\right| \leq \text{negl}(\lambda). \quad (27)$$

Now let us consider experiment $\text{Priv}K_{\mathcal{A},\widetilde{\Pi}}^{\text{cpa}}$. Note that, $C_k = \text{Enc}_{SEK_i}(k)$ and $\text{SEK}_i = f((h_i \| h_i') \oplus \gamma)$. Since γ and f are selected from $\{0, 1\}^{2l}$ and $\mathcal{F}_n = \{\text{func} : \{0, 1\}^{2l} \rightarrow \{0, 1\}^{l^*}\}$ uniformly at random, respectively. We have SEK_i is from $\{0, 1\}^{l^*}$ uniformly at random. Therefore, the key of AES is chosen for key space $\{0, 1\}^{l^*}$ uniformly at random. From the assumption of this theorem, we have AES is a random permutation. Accordingly, we have

$$\left|\Pr\left[\text{Priv}K_{\mathcal{A},\widetilde{\Pi}}^{\text{cpa}}(PP) = 1\right] - \frac{1}{2}\right| \leq \text{negl}'(\lambda). \quad (28)$$

From (29), we have

$$\begin{aligned}
&\left|\Pr\left[\text{Priv}K_{\mathcal{A},\Pi}^{\text{cpa}}(PP) = 1\right] - \frac{1}{2}\right| \\
&\qquad - \left|\Pr\left[\text{Priv}K_{\mathcal{A},\widetilde{\Pi}}^{\text{cpa}}(PP) = 1\right] - \frac{1}{2}\right| \\
&\leq \left|\left(\Pr\left[\text{Priv}K_{\mathcal{A},\Pi}^{\text{cpa}}(PP) = 1\right] - \frac{1}{2}\right)\right. \\
&\qquad \left. - \left(\Pr\left[\text{Priv}K_{\mathcal{A},\widetilde{\Pi}}^{\text{cpa}}(PP) = 1\right] - \frac{1}{2}\right)\right| \\
&\leq \text{negl}(\lambda). \quad (29)
\end{aligned}$$

Therefore, the following inequality holds:

$$\begin{aligned}
&\left|\Pr\left[\text{Priv}K_{\mathcal{A},\Pi}^{\text{cpa}}(PP) = 1\right] - \frac{1}{2}\right| \\
&\leq \left|\Pr\left[\text{Priv}K_{\mathcal{A},\widetilde{\Pi}}^{\text{cpa}}(PP) = 1\right] - \frac{1}{2}\right| \\
&\qquad + \text{negl}(\lambda) \leq \text{negl}'(\lambda) + \text{negl}(\lambda).
\end{aligned}$$

Since the sum of two negligible functions is negligible, there exists a negligible function $\text{negl}''(\lambda) = \text{negl}'(\lambda) + \text{negl}(\lambda)$, such that

$$\text{Adv}_{\mathcal{A}}^{\text{cpa}} = \left|\Pr\left[\text{Priv}K_{\mathcal{A},\Pi}^{\text{cpa}}(PP) = 1\right] - \frac{1}{2}\right| \leq \text{negl}''(\lambda). \quad (30)$$

Accordingly, the advantage of the PPT adversary breaks the proposed scheme is negligible and the ciphertext of EHR data achieves IND-CPA security. ■

The next, we consider the unlinkability of tokens in the proposed scheme. The following theorem shows that token unlinkability is based on the security of the CP-ABE scheme and the RSA-OAEP scheme, as well as the encryption algorithm AES.

Theorem 2: Suppose that the RSA-OAEP scheme is secure and the encryption algorithm AES is a random permutation when the key of AES is chosen from key space uniformly at random, then the proposed scheme is token unlinkable.

Proof: Note that, for any subtoken T_i, we have that, $C_{T_i} = E_{PK_{B_i}}(r_i)\|\text{Enc}_{r_i}(T_i\|S_{T_i})$, where r_i is be encrypted with RSA-OAEP scheme [49], and $T_i\|S_{T_i}$ is encrypted by AES with key r_i. From the security analysis in [49], RSA-OAEP scheme can resist adaptive chosen ciphertext attack (and also adaptive chosen plaintext attack). Therefore, we can assume that no PPT adversary can obtain r_i from $E_{PK_{B_i}}(r_i)$.

The unlinkability of the tokens can be discussed in two cases: (I) unlinkability between the parent token and the child token; and (II) unlinkability among subtokens. For case I, let T_0' and T_1' be the subtokens of T_0 and T_1, respectively. Note that, r_i is chosen from $\{0,1\}^{l^*}$ uniformly at randomly. Accordingly, the encryption algorithm AES is a random permutation. Thus, when PPT adversary obtains $C_{T_b'}$ from the challenger, the advantage of the adversary for winning the game is negligible. That is to say, when a token is separated as several subtokens for delegating them to other data users, no PPT adversary can link any parent token and subtoken given ciphertext. Similarly, we can conclude that the subtokens are also unlinkable. Therefore, no adversary can obtain any information by linking the tokens. ■

Finally, we consider the token unforgeability of the proposed scheme under data users' collusion attack. A critical part of the token structure for token unforgeability is the signature of the token body. If a user loose access of the data owner, he/she may collude with other users to get the valid secret γ or exchange the hash tokens. Once the body of the token is changed, the verification of token signature will be failed.

Theorem 3: The tokens in the proposed scheme are unforgeable under data users' collusion attack if the signature scheme in [35] is secure.

Proof: The body of the token (which includes a secret γ, DO_{uid} of data owner and hash token h_i and h_j') has been signed by the SHI with the signature scheme presented in [35]. If data users collude to modify and forge the contents of the token, such as, modifying h_i or h_j' to get the access permissions for more EHR data, the signature verification for contents will be failed. Accordingly, data users cannot collude to obtain a forged token in order to realize an unauthorized access. ■

TABLE II
NOTIONS USED IN THE EXPERIMENTS

Notation	Meaning
l_m	The size of plaintext in bytes
l_r	The length of key of RSA
d	The size of the digest of EHR data
N	The length of hash chain
n	The number of EHRs accessed by users
n_a	The number of attributes owned by the user
$\|p\|$	The size of elements in $\mathbb{Z}_p$
$\|g\|$	The size of elements in $\mathbb{G}$
$\|k\|$	The length of the symmetric key k
$\|L\|$	The size of the URL of the location of the EHR
$\|T\|$	The size of token
$\|M\|$	The size of TSM

TABLE III
LENGTH OF PARAMETERS OF CRYPT. ALGORITHMS

Algorithm	Key	Output
H_1: $SHA256$	–	256bits
H_2: $MD5$	–	128bits
F: $MD5$	–	128bits
AES	128bits	$\lceil l_m/16 \rceil \times 8$bits
RSA-OAEP	2048bits	2048bits

VII. IMPLEMENTATION AND EVALUATION

In this section, we conduct several experiments to evaluate the performance of the proposed scheme. The parameters and environment of the experiments will be introduced. Then, the communication cost of the system will be comprehensively analyzed. Finally, the computation efficiency of the system will be evaluated. Notations used in this section are induced in Table II.

A. Experimental Settings

Our experiment is conducted on a desktop computer with Ubuntu 18.04 operation system, Intel Core i7-7700T CPU, 8GB of RAM. All experimental evaluations are conducted with the libraries of Python. Specifically, the CP-ABE scheme is implemented mainly on the python library *charm*, which optimizes exponential operation and bilinear pairing operation. We employ SHA-256 as hash function H_1 and MD5 as hash function H_2 and function F. For AES and RSA-OAEP, the key length is 128 bits and 1024 bits, respectively. Note that, the blockchain platform is used in our system to store digest and address of EHR data (for integrity checking and file resource addressing of EHR data), and token segmentation messages (for evidence preservation of the transfer of access control permission). To this end, a blockchain storage platform is implemented by using Go-version Ethereum client (i.e., Geth), in which, the Geth Version is 1.10.26-stable, the Version of Go programming language is go1.18.5, and Operating System is linux. It is shown that, the time cost of per transaction is about 1.916 s for 100 blockchain nodes. In Table III, we list the length of the key and output of some cryptography algorithms.

TABLE IV
COMMUNICATION COST OF THE PROPOSED SYSTEM

Communication Cost	Our Scheme
CA &SHI	$\|p\|+u\|g\|$
CA & Data User	$l_r+2\|p\|+n_a\|g\|+u\|g\|$
SHI & Blockchain	$d+\|L\|+\|M\|$
SHI &Database Server	$N\|k\|+\|L\|$
SHI & Data User	$\|T\|+\|p\|+\|g\|$
Data User & Blockchain	$d+\|L\|+\|M\|$
Between Data Users	$\|g\|+l_r+\|T\|+\|p\|$
Data User & Database Server	$\|T\|+\|p\|+n\|k\|$

B. Communication Cost of the Proposed Scheme

In order to evaluate the proposed scheme comprehensively, we analyze the communication overhead of our system. The communication cost between each entity is shown in Table IV, in which we have the following.

1) The communication cost between the CA and SHI originates from global public key GK, RSA-OAEP keys and signature keys.
2) The communication cost between the CA and data user includes global public key GK, secret key SK', RSA-OAEP keys and signature keys.
3) The communication cost between the SHI and Blockchain comes from the EHR digest, EHR location and token segmentation message TSM.
4) The communication cost between the SHI and database server is the ciphertext of the symmetric key $\mathcal{K}$ and location of the EHR data.
5) The communication cost between the SHI and data user is the ciphertext of token and signature of the token.
6) The communication cost between data user and blockchain comes from TSM, the digest and location of the EHR data.
7) The communication cost between users is ciphertext generated in token delegation.
8) The communication cost between user and database server consists of token, signature of token and the ciphertext of part of the symmetric key $\mathcal{K}$.

C. Computation Efficiency of the Proposed Scheme

In order to test the computation efficiency of the system, an experiments is conducted to get the time cost of several stages of the system and important algorithms, in which each final result is the average value of experimental results over 20 experiments. In our experiment, we set the length of the hash-chains in the stage of data storage to 1000. Note that, the time cost of AES for encrypting EHR data and the efficiency of RSA algorithm are not the focus of our investigation in this work, although AES and RSA are efficient algorithms.

The experimental results are shown in Fig. 6, in which the first two columns represent the time cost of system initialization and secret key generation, respectively. In our system, the system initialization occurs only once. Similarly, secret key generation occurs only once for a user, unless the access control policy changes. The next two columns

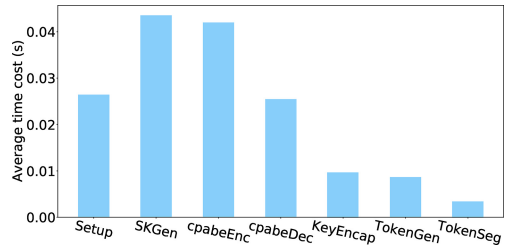

Fig. 6. Time cost of stages of our system.

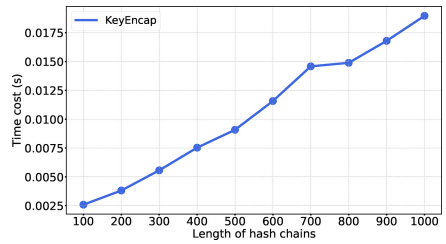

Fig. 7. Time cost of KeyEncap.

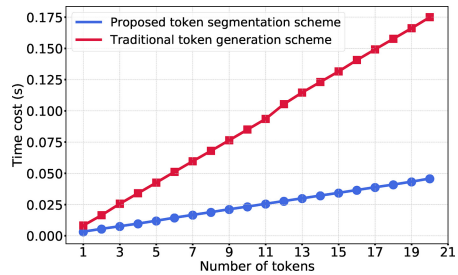

Fig. 8. Comparison of proposed token segmentation time and traditional token generation time.

represent the time cost of CP-ABE encryption and decryption, respectively. Since the message space encrypted by CP-ABE is a group $\mathbb{G}_T$, text-messages cannot be encrypted directly. In practice, we randomly select an element tk from $\mathbb{G}_T$ and employ the hash function H_2 to convert the group element tk into a symmetric key. In this way, we can avoid the trouble of encoding messages into group elements, and each user only performs the encryption or decryption of CP-ABE once (unless the access control policy changes), and users can directly use the symmetric encryption algorithm with $H_2(tk)$ in subsequent encryption and decryption processes.

Another experiment is conducted to further measure the time overhead of key encapsulation with different length of hash chains. From Fig. 7, we can see that the time cost increases linearly with the increase of hash-chain length. Moreover, when the length of hash-chains is 1000, the time cost of KeyEncap is less than 0.02 s. It is worth noting that KeyEncap occurs only once in a system, until the system updates the keys.

As shown in Fig. 8, we compare time cost of the proposed scheme with the traditional token generation scheme. In our proposed scheme, SHI generates a token for doctor A, and then doctor A segments and delegates the subtokens according to the number of doctors to be invited. In the traditional token generation scheme, SHI generates a token for each doctor

TABLE V
FUNCTION COMPARISON

Scheme	Fine-Grained Control	Policy Definer	Data Secure Sharing	Authorization Traceability	Time-dimension Access	Efficient Multi-party Diagnosis
[19]	CP-ABE	Patient	✓	✗	✗	✗
[20]	ABE	Trusted Institutions	✓	✗	✗	✗
[29]	CP-ABE	Patient	✓	✗	✗	✗
[41]	Attribute-based Access	Patient	✗	✗	✗	✗
[34]	Blockchain	–	✗	✓	✗	✗
[45]	KP-ABE	–	✓	✗	✗	✗
Ours	CP-ABE+Token Segmentation	Elderly	✓	✓	✓	✓

participating in the diagnosis, and sends the token to each doctor, respectively. In this experiment, we repeatedly measure the time cost of token generation and transmission a total of 20 times, and calculate the average as the final time cost. Moreover, we assumed that each data user has performed CP-ABE encryption or decryption, so they have obtained $H_2(tk)$.

In Fig. 8, the red line represents the time cost of the traditional token generation scheme (e.g., SHI runs TokenGen algorithm and TokenEnc algorithm to generate tokens and send them to doctors), and the blue line represents the cost of the proposed scheme (e.g., SHI runs TokenGen algorithm and TokenEnc algorithm to generate a token and send it to doctor A, doctor A runs TokenSeg algorithm to segment his/her token into some subtokens, and runs TokenDel algorithm to delegate subtokens to other doctors). It can be seen that, as the number of tokens increases, the time cost of the traditional token generation scheme is more than three times that of the proposed scheme. In practice, the traditional permission concentration mode will produce a long request and response communication process between SHI and each data user (such as doctor). Accordingly, the proposed token segmentation scheme can improve the efficiency of the system so that doctors can provide diagnostic services for patients quickly.

D. Comparison With Existing Schemes

Most of existing studies only achieve partial find-grained control and cannot fulfill the flexibility of data sharing, authorization traceability, policy definer, time dimension access and privacy protection. We summarize the function comparison of our proposed scheme with existing studies in Table V. It can be shown that, only the proposed scheme can achieve time-dimension access and support efficient multiparty diagnostics.

As a result, a performance comparison of the proposed scheme and several existing works (i.e., the access control schemes presented in [19], [20], and [29]) is discussed with two experiments.

First of all, we compare the communication overhead of the proposed scheme with that of three existing works mentioned above through experiments. Note that, the related schemes also have other security-related functions besides access control. To make a fair comparison, we only consider the communication overhead of the existing works in access control. Fig. 9 plots the communication overhead of the proposed scheme and the existing works with the increase of the number of the accessed

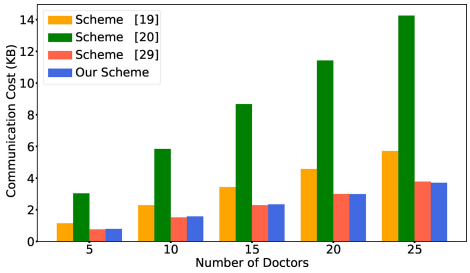

Fig. 9. Comparison of communication cost between the proposed scheme and related works.

users. It can be seen that, the communication cost of the proposed scheme is less than that of the schemes in [19] and [20], and is similar to that of the scheme in [29].

Then, another experiment is conducted to compare the time cost of the proposed scheme with the three existing works in access control of joint consultation of doctors. In this experiment, two cases are considered as follows. Case I: the invited doctors satisfy the preset access control attributes by the elderly or his/her guardian; and Case II: the invited doctors do not meet the preset access control attributes. Fig. 10(a) and (b) plots the time consumption of Case I and Case II under different number of doctors in a joint consultation, respectively. Note that, a joint consultation is happened only when the number of doctors is larger than 1 in Fig. 10. The results show that: (1) in Case I, the time consumption of the proposed scheme is less than that of the schemes in [19] and [20], and is also similar to that of the scheme in [29]; and (2) in Case II, the proposed scheme significantly outperforms existing three schemes in terms of time cost with the increasing of the number of doctors in a joint consultation. The reason is that, it is required to reset the access control properties by the elderly or his/her guardian when schemes in [19], [20], and [29] meet Case II, while, in the proposed scheme, it is only required that the doctor in charge splits the token and encapsulates the subtokens, and then distributes them to the invited doctors.

VIII. CONCLUSION

In order to achieve a flexible and fine-grained access control for EHR data, we have proposed the scheme by leveraging attribute-based encryption, token segmentation,

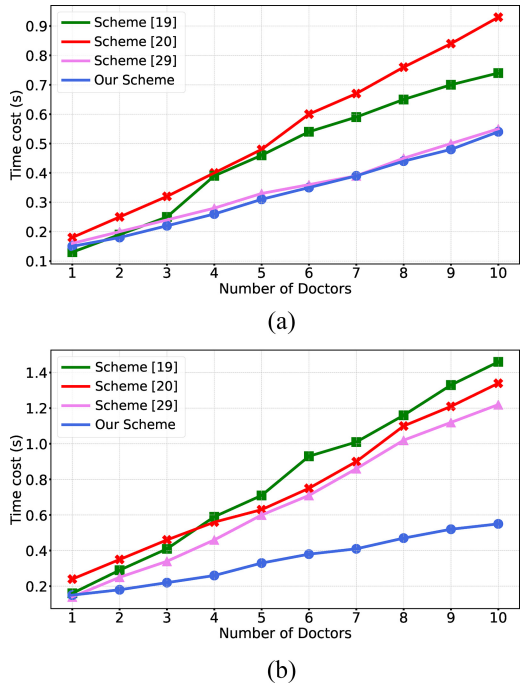

Fig. 10. Comparison of time cost between the proposed scheme and related works. (a) Invited doctors' attributes satisfy the access control policy. (b) Invited doctors' attributes do not satisfy the access control policy.

dual-key regression, and blockchain. In our scheme, EHR data is encrypted and stored according to time with dual-key regression, and the access permission of EHR data is granted according to on the user's attributes and the permission token issued by SHI. Moreover, a token segmentation algorithm has been designed to transfer the access rights between doctors to achieve convenient and efficient multiparty consultation. Therefore, the proposed scheme not only protects users' privacy, but also reduces system costs by avoiding re-encryption of all ciphertext. We have provided security analysis to illustrate that the proposed scheme can achieve EHR data security and token security. Finally, the experimental results have demonstrated that the proposed scheme is considerably efficient in terms of computation and communication overhead. In the proposed model, it is assumed that there is a globally trusted CA authority, which will limit the application of this scheme, and we will investigate how to remove this limitation in the future.

REFERENCES

[1] L. Ale, N. Zhang, H. Wu, D. Chen, and T. Han, "Online proactive caching in mobile edge computing using bidirectional deep recurrent neural network," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5520–5530, Jun. 2019.

[2] D. Chen et al., "MAGLeak: A learning-based side-channel attack for password recognition with multiple sensors in IIoT environment," *IEEE Trans. Ind. Informat.*, vol. 18, no. 1, pp. 467–476, Jan. 2022.

[3] W. Wu et al., "AI-native network slicing for 6G networks," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 96–103, Feb. 2022.

[4] P. Liu, Y. Ding, and T. Fu, "Optimal ThrowBoxes assignment for big data multicast in VDTNs," *Wireless Netw.*, vol. 28, no. 3, pp. 1229–1239, 2022.

[5] N. Zhang, P. Yang, J. Ren, D. Chen, L. Yu, and X. Shen, "Synergy of big data and 5G wireless networks: opportunities, approaches, and challenges," *IEEE Wireless Commun.*, vol. 25, no. 1, pp. 12–18, Feb. 2018.

[6] X. Shen, J. Gao, W. Wu, M. Li, C. Zhou, and W. Zhuang, "Holistic network virtualization and pervasive network intelligence for 6G," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 1–30, 1st Quart., 2022.

[7] X. Yang, S. Yang, J. Liu, C. Wang, Y. Chen, and N. Saxena, "Enabling finger-touch-based mobile user authentication via physical vibrations on IoT devices," *IEEE Trans. Mobile Comput.*, vol. 21, no. 10, pp. 3565–3580, Oct. 2022.

[8] W. Tong, W. Chen, B. Jiang, F. Xu, Q. Li, and S. Zhong, "Privacy-preserving data integrity verification for secure mobile edge storage," *IEEE Trans. Mobile Computing*, vol. 22, no. 9, pp. 5463–5478, Sep. 2023, doi: 10.1109/TMC.2022.3174867.

[9] D. Chen, N. Zhang, N. Cheng, K. Zhang, Z. Qin, and X. Shen, "Physical layer based message authentication with secure channel codes," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 5, pp. 1079–1093, Sep./Oct. 2020.

[10] W. Y. B. Lim et al.,"Dynamic contract design for federated learning in smart healthcare applications," *IEEE Internet Things J.*, vol. 8, no. 23, pp. 16853–16862, Dec. 2021.

[11] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *J. Inf. Security Appl.*, vol. 50, Feb. 2020, Art. no. 102407.

[12] D. Chen et al., "Privacy-preserving encrypted traffic inspection with symmetric cryptographic techniques in IoT," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17265–17279, Sep. 2022.

[13] N. Wei and A. A. Sani, "SchrodinText: Strong protection of sensitive textual content of mobile applications," *IEEE Trans. Mobile Comput.*, vol. 21, no. 4, pp. 1402–1419, Apr. 2022.

[14] W. Zhang, Y. Lin, J. Wu, and T. Zhou, "Inference attack-resistant E-healthcare cloud system with fine-grained access control," *IEEE Trans. Services Comput.*, vol. 14, no. 1, pp. 167–178, Jan./Feb. 2021.

[15] A. Ndikumana et al., "Joint communication, computation, caching, and control in big data multi-access edge computing," *IEEE Trans. Mobile Comput.*, vol. 19, no. 6, pp. 1359–1374, Jun. 2020.

[16] W. Tang, K. Zhang, J. Ren, Y. Zhang, and X. Shen, "Flexible and efficient authenticated key agreement scheme for BANs based on physiological features," *IEEE Trans. Mobile Comput.*, vol. 18, no. 4, pp. 845–856, Apr. 2019.

[17] P. P. Ray, B. Chowhan, N. Kumar, and A. Almogren, "BIoTHR: Electronic health record servicing scheme in IoT-blockchain ecosystem," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10857–10872, Jul. 2021.

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

[19] F. Li, K. Liu, L. Zhang, S. Huang, and Q. Wu, "EHRChain: A blockchain-based EHR system using attribute-based and homomorphic cryptosystem," *IEEE Trans. Services Comput.*, vol. 15, no. 5, pp. 2755–2765, Sep./Oct. 2022, doi: 10.1109/TSC.2021.3078119.

[20] M. Wang, Y. Guo, C. Zhang, C. Wang, H. Huang, and X. Jia, "MedShare: A privacy-preserving medical data sharing system by using blockchain," *IEEE Trans. Services Comput.*, vol. 16, no. 1, pp. 438–451, Jan./Feb. 2023, doi: 10.1109/TSC.2021.3114719.

[21] D. Han, N. Pan, and K.-C. Li, "A traceable and revocable ciphertext-policy attribute-based encryption scheme based on privacy protection," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 1, pp. 316–327, Jan./Feb. 2022.

[22] S. Nakamoto (Bitcoin, Las Vegas, NV, USA). *Bitcoin: A Peer-to-Peer Electronic Cash System.* (2008). [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[23] J. Li, J. Wu, L. Chen, J. Li, and S.-K. Lam, "Blockchain-based secure key management for mobile edge computing," *IEEE Trans. Mobile Comput.*, vol. 22, no. 1, pp. 100–114, Jan. 2023, doi: 10.1109/TMC.2021.3068717.

[24] V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum, Zug, Switzerland, White Paper, 2014.

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

[26] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM CCS*, Alexandria, VA, USA, 2006, pp. 89–98.

[27] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE SP*, Berkeley, CA, USA, 2007, pp. 321–334.
[28] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proc. Int. Workshop Public Key Cryptogr.*, 2011, pp. 53–70.
[29] S. Narayan, "Privacy preserving EHR system using attribute-based infrastructure," in *Proc. ACM CCS*, 2010, pp. 47–52.
[30] S. Qi, Y. Lu, W. Wei, and X. Chen, "Efficient data access control with fine-grained data protection in cloud-assisted IIoT," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2886–2899, Feb. 2021.
[31] G. Yu et al., "Enabling attribute revocation for fine-grained access control in blockchain-IoT systems," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1213–1230, Nov. 2020.
[32] J. Sun, Y. Yuan, M. Tang, X. Cheng, X. Nie, and M. U. Aftab, "Privacy-preserving bilateral fine-grained access control for cloud-enabled industrial IoT healthcare," *IEEE Trans. Ind. Informat.*, vol. 18, no. 9, pp. 6483–6493, Sep. 2022.
[33] S. Xu, Y. Li, R. H. Deng, Y. Zhang, X. Luo, and X. Liu, "Lightweight and expressive fine-grained access control for healthcare Internet-of-Things," *IEEE Trans. Cloud Comput.*, vol. 10, no. 1, pp. 474–490, Jan.–Mar. 2022.
[34] J. Xu et al., "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8770–8781, Oct. 2019.
[35] C.-P. Schnorr, "Efficient signature generation by smart cards," *J. Cryptol.*, vol. 4, no. 3, pp. 161–174, 1991.
[36] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. IEEE OBD*, Vienna, Austria, 2016, pp. 25–30.
[37] H. Yang and B. Yang, "A blockchain-based approach to the secure sharing of healthcare data," in *Proc. Norwegian Inf. Security Conf.*, 2017, pp. 100–111.
[38] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc.*, vol. 39, pp. 283–297, May 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, pp. 1–9, 2018.
[40] L. Hirtan, P. Krawiec, C. Dobre, and J. M. Batalla, "Blockchain-based approach for e-health data access management with privacy protection," in *Proc. IEEE CAMAD*, Limassol, Cyprus, 2019, pp. 1–7.
[41] H. Guo, W. Li, M. Nejad, and C.-C. Shen, "Access control for electronic health records with hybrid blockchain-edge architecture," in *Proc. IEEE Blockchain*, Atlanta, GA, USA, 2019, pp. 44–51.
[42] 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.
[43] J. Huang, Y. W. Qi, M. R. Asghar, A. Meads, and Y.-C. Tu, "MedBloc: A blockchain-based secure EHR system for sharing and accessing medical data," in *Proc. IEEE TrustCom/BigDataSE*, Rotorua, New Zealand, 2019, pp. 594–601.
[44] S. Liu, J. Yu, Y. Xiao, Z. Wan, S. Wang, and B. Yan, "BC-SABE: blockchain-aided searchable attribute-based encryption for cloud-IoT," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 7851–7867, Sep. 2020.
[45] S. Xu, J. Ning, X. Huang, Y. Li, and G. Xu, "Untouchable once revoking: A practical and secure dynamic EHR sharing system via cloud," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 6, pp. 3759–3773, Nov./Dec. 2022, doi: 10.1109/TDSC.2021.3106393.
[46] H. Shafagh, L. Burkhalter, S. Ratnasamy, and A. Hithnawi, "Droplet: Decentralized authorization and access control for encrypted data streams," in *Proc. USENIX Security*, Boston, MA, USA, 2020, pp. 2469–2486.
[47] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. Boca Raton, FL, USA: CRC Press, 2020, pp. 456–458.
[48] J. Shi and R. Li, "Permission token segmentation scheme based on blockchain access control," in *Proc. IEEE TrustCom*, Guangzhou, China, 2020, pp. 1956–1964.
[49] M. Bellare and P. Rogaway, "Optimal asymmetric encryption padding-how to encrypt with RSA," in *Proc. EUROCRYPT*, 1994, pp. 92–111.
[50] Q. Huang, Z. Zhang, and Y. Yang, "Privacy-preserving media sharing with scalable access control and secure deduplication in mobile cloud computing," *IEEE Trans. Mobile Comput.*, vol. 20, no. 5, pp. 1951–1964, May 2021.

Dajiang Chen (Member, IEEE) received the Ph.D. degree in information and communication engineering from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2014.

He is currently an Associate Professor with the School of Information and Software Engineering, UESTC. He was a Post Doctoral Fellow with the Broadband Communications Research group, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, from 2015 to 2017. He was also a Post Doctoral Fellow with the School of information and software Engineering, UESTC, from 2014 to 2017. His current research interest includes physical layer security, secure channel coding, and machine learning and its applications in wireless security.

Dr. Chen served as the Workshop Chair for IEEE BDEC-SmartCity2019, EAI-CollaborateCom2020 (IoT Track), and INFCOM2023 (PerAI-6G).

Li Zhang received the B.S. degree in software engineering from the School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing, China, in 2020. She is currently pursuing the M.S. degree with the School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China.

Her research interests include security and privacy protection in E-healthcare systems.

Zeyu Liao received the B.S. degree in software engineering from the School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China, in 2021, where he is currently pursuing the M.S. degree.

His research interests include security and privacy protection in wireless networks.

Hong-Ning Dai (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from the Department of Computer Science and Engineering, The Chinese University of Hong Kong, Hong Kong, in 2008.

He is currently with the Department of Computer Science, Hong Kong Baptist University, Hong Kong, as an Associate Professor. His current research interests include the Internet of Things, big data, and blockchain technology.

Dr. Dai has served as an Associate Editors/Editors for IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, *Ad Hoc Networks*, and *Connection Science*. He is also a Senior Member of Association for Computing Machinery.

Ning Zhang (Senior Member, IEEE) received the B.E. degree from Beijing Jiaotong University, Beijing, China, in 2007, the M.S. degree from Beijing University of Posts and Telecommunications, Beijing, in 2010, and the Ph.D degree from the University of Waterloo, Waterloo, ON, Canada, in 2015.

He is an Associate Professor with the Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON, Canada. He was a Postdoctoral Research Fellow with the University of Waterloo and the University of Toronto, Toronto, ON, Canada. His current research interests include next generation mobile networks, physical layer security, machine learning, and mobile edge computing.

Dr. Zhang serves/served as an Associate Editor for IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, IEEE ACCESS and *IET Communications*, and an Area Editor of *Encyclopedia of Wireless Networks* (Springer) and Cambridge Scholars.

Xuemin (Sherman) Shen (Fellow, IEEE) received the B.Sc. degree in electrical engineering from Dalian Maritime University, Dalian, China, in 1982, and the M.Sc. and Ph.D. degrees in electrical engineering from Rutgers University, New Brunswick, NJ, USA, in 1987 and 1990, respectively.

He is a University Professor and the Associate Chair with the Graduate Studies, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. His research focuses on wireless resource management, wireless network security, social networks, smart grid, and vehicular ad hoc and sensor networks.

Dr. Shen received the IEEE ComSoc Education Award, the Joseph LoCicero Award for Exemplary Service to Publications, the Excellent Graduate Supervision Award in 2006, and the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada. He is the elected IEEE ComSoc VP Publication, was a member of IEEE ComSoc Board of Governor, and the Chair of Distinguished Lecturers Selection Committee. He served as the Editor-in-Chief for IEEE INTERNET OF THINGS JOURNAL, IEEE NETWORK, *Peer-to-Peer Networking and Application*, and *IET Communications*; a Founding Area Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS; and an Associate Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and IEEE WIRELESS COMMUNICATIONS, etc. He is a registered Professional Engineer of Ontario, Canada, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, and a Distinguished Lecturer of IEEE Vehicular Technology Society and Communications Society.

Minghui Pang received the Ph.D. degree in clinical medicine from Southern Medical University, Guangzhou, China, in 2012.

He is a Professor and a Chief Surgeon with Sichuan Academy of Medical Sciences, Sichuan Provincial People's Hospital, which is also the affiliated hospital of University of Electronic Science and Technology of China, Chengdu, China. He is the Chief of Geriatric Surgery Department, the Chief Professor of undergraduate teaching and the Head with the Department of Clinical College of Medicine, University of Electronic Science and Technology. He is also the Visiting Scholar with the Medicine College of Harvard University, Boston, MA, USA. His research interests include basic and clinical research of gastrointestinal tumor and peritoneal metastases tumor, and the research on artificial intelligence for the risk of recurrence and metastasis of gastrointestinal tumors and the prediction of curative effect.