Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Medical blockchain: Data sharing and privacy preserving of EHR based on smart contract

Jung-San Lee [*], Chit-Jie Chew, Jo-Yun Liu, Ying-Chin Chen, Kuo-Yu Tsai

Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724, Taiwan

ARTICLE INFO

Keywords:
Electronic health record
Data sharing
Blockchain
Smart contract
HIPAA

ABSTRACT

No doubt that medical data sharing is very crucial but important in realizing cross-hospital diagnosis and improving research development. In traditional mechanisms, there always exists a tradeoff between correctness of medical data and patient privacy. Here we are going to introduce the concept of blockchain and smart contract to build up an electronic medical record sharing mechanism: medical blockchain. Specifically, we have implemented the medical record sharing through cryptography design. Simulations have demonstrated that the correctness of medical data and privacy of patient can be guaranteed through the adoption of blockchain, while the integrity of a specific patient can be achieved via the smart contract control. Furthermore, the proposed medical blockchain can resist the potential Internet attack simulated by the formal verification. Thus, no leakage of patient identity occurs, and the tradeoff could be eliminated effectively without the modification of current hospital devices according to the simulation results.

1. Introduction

With the explosive development of technology and the Internet communication, the electronic health record (EHR) is widely applied in medical field [1, 2]. This can help each hospital effectively sharing the medical data, such as evidence-based medicine (EBM). EBM is a procedure to systematically review the clinic research findings and patient knowledge for assisting the optimum clinic care to patient. Basically, the clinical decision support system (CDSS) is used to implement EBM which is a program-based artificial intelligence in medical data system. When the system acquires more patient knowledge, it is able to offer the better predict accuracy for medical diagnosis. Accordingly, we learn that the EHR is important in both EBM and CDSS fields [34]. The exchange data directly transmitted via the Internet, however, is insecure. Therefore, the United States Congress has passed the Health Insurance Portability and Accountability Acts (HIPAA) since 1996, which is the most significant and integrated standard for EHR [3]. The EHR contains the entire health message of an individual, such as medical record, medical image, and health examination [4, 5]. All of medical information relating to electronic process have to comply with HIPAA, including healthcare organizations and healthcare clearinghouses. There are two main ideas of HIPAA, privacy and security regulations, which describe how to avoid improper violation and unauthenticated disclosure of EHR. First, the privacy regulation depicts that a patient owns right to manage and understand the usage of his/her medical information [6, 7]. In other words, each EHR content shall not be disclosed to the public without permission of the patient. Furthermore, privacy regulation determines the baseline of de-identification [8, 9]. No one has the ability to learn the true status of the patient from EHR, especially for a medical researcher. Second, the security regulation has three safeguards: administrative, physical, and technical, in which it is used for ensuring the confidentiality (C), integrity (I), and availability (A) of EHR during the processes of storage, access, and transmission.

Undoubtedly, the adoption of EHR has brought feasible solutions for physical health record, i.e. preservation and messy handwriting. Moreover, it has strengthened the medical data sharing platform to improve the quality of cross-hospital diagnosis and effectiveness of corresponding research. Based on the circumstance of cross-hospital diagnosis with EHR, a patient can reduce the time cost and retain the effective diagnosis since he/she needs not to examine the duplicate medical checkup. In the aspect to the doctor, he/she has the ability to offer reliable diagnosis due to learning the previous prescription of the patient. For medical research development, the researcher is able to explore the specific disease through analyzing the rich EHRs. Consequently, the patient can obtain a better treatment.

Nevertheless, there always exists a tradeoff between correctness of

[*] Corresponding author.
E-mail addresses: leejs@fcu.edu.tw (J.-S. Lee), d0030577@mail.fcu.edu.tw (J.-Y. Liu), kytsai@fcu.edu.tw (K.-Y. Tsai).

https://doi.org/10.1016/j.jisa.2022.103117

Available online 20 January 2022

medical data and patient privacy through the traditional mechanisms [10–15]. In 2001, Ausanka-crues has investigated multiple access control of cloud data sharing mechanism [10]. In contrast, the function of discretionary access control allows user to elevate privilege of anyone. This might increase the probability of embedding Trojan by hacker. Thus, the secure verification is hard to be implemented. After that, Liu et al. have proposed a multi-owner data sharing play, which is able to manage the data according to the different authorities of owners [11]. The owner category is divided into two types, the original data owner and the person who is able to use data, the so-called user. Unfortunately, the valid data will be disclosed once a malicious cloud server launches collusion attack with revoked user. Therefore, the method of Liu et al. cannot preserve the essential of confidentiality. Later on, Muthukumar and Nandhini have tried to transfer medical data to user in cipher based on polynomial interpolation function. However, the transferred data might suffer from the tampering attack during sharing procedure [12]. That is, a legal user cannot reveal the correct data to satisfy the verification of integrity. Subsequently, Zhu and Jiang have introduced an anti-collusion attack data sharing scheme based on Delov-Yao model and asymmetric cryptosystem [13], in which a revoked user cannot store any data for reaching confidentiality. However, Ganesh et al. have found that Zhu and Jiang method cannot resist the man-in-the-middle attack and data tampering attack since the server does not verify the registration message from user [14].

Aside from researches, the reality of Healthcare IT News exists medical data leakage [15]. The leakage data include name, social security number (SSN), address, and license plate. It is due to BJC HealthCare, which is a non-profit organization, misses correct configuration on cloud server. The despiteful attacker has the ability to access the information of valid user. That is, the feature of confidentiality cannot be confirmed. The willingness of sharing EHR might be reduced since the patient may suffer from the massive loss of finance and life. Hence, preserving privacy and security of EHR in data sharing platform is an important and emergent mission.

For summarizing, there exist above issues of anonymity, privacy, confidentiality, availability, and integrity in current EHR data sharing schemes. Therefore, we are going to introduce the concept of blockchain and smart contract to build up an electronic medical record sharing mechanism: medical blockchain. The architecture is displayed in Fig. 1. The group of peer includes patient, hospital, and researcher institute. A patient uploads the de-identification EHR to medical blockchain, then hospital and research institute can access EHR. The correctness of medical data can be guaranteed through the adoption of blockchain [16, 17], while the integrity of a specific patient can be achieved via the smart contract control [18]. Also, the proposed medical blockchain complies with HIPAA. The EHR in medical blockchain have to acquire the authority of the patient. In particular, the privacy of patient is inherited from the anonymity of blockchain. Thus, no leakage of patient identity occurs, and the tradeoff could be eliminated effectively without the modification of current hospital devices according to the simulation results, including analysis of potential attacks and property achievements. Following, we conclude the fundamental properties of a security data sharing platform, which shall be confirmed for medical scenario.

- Anonymity: This property is to enable a patient to share medical data on the blockchain via an anonymous identity. Namely, the true identity needs not to be public or verified.
- Confidentiality: This essential is to ensure that only an authorized user can access data.
- Availability: The availability is to examine the functionality of the system.
- Privacy: This is for confirming the privacy regulation of HIPAA.
- Immutability: This issue is to guarantee that no one can tamper the data content.
- Unforgeability: This property is to confirm that a pair of data and corresponding signature cannot be forged.
- Integrity: This feature indicates that the stored data is unable to be tampered. Besides, the malicious attacker cannot forge the real transferred data.

The rest of this article is organized as follows. The details of preliminary are depicted in Section 2. The proposed scheme and performance analysis are explained in Sections 3 and 4, respectively. We make conclusions in Section 5.

2. Preliminaries

Before explaining the details of the new mechanism, we first introduce the complied HIPAA regulations in Section 2.1. Next, we briefly describe the core concepts of blockchain and smart contract in Sections 2.2 and 2.3, respectively.

2.1. Health insurance portability and accountability acts

HIPAA regulations are defined for integrating the medical data, which all medical institutions, data exchange centers, and staffs must

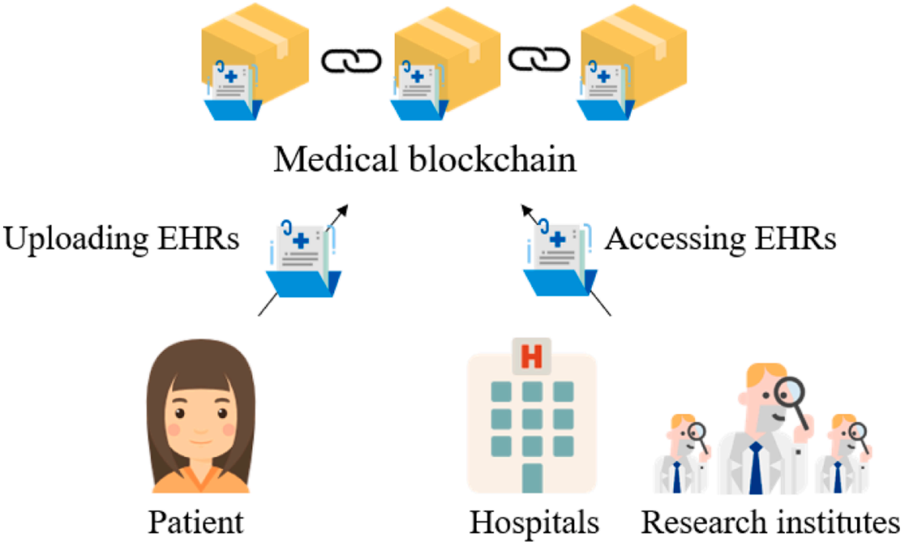


Fig. 1. The architecture of medical blockchain.

comply with. Among regulations, privacy and security rules have been concerned in the medical blockchain environment as they are relevant to personal health management. Furthermore, NIST has released the cybersecurity framework for improving critical infrastructure [31], which is a common language for organization communication. Then, the Office for Civil Rights (OCR) has announced a crosswalk document to identify the mappings between the cybersecurity framework and HIPAA security rule [31]. Note that the entities regulated by HIPAA must comply with the HIPAA security rule in the healthcare space.

2.1.1. Privacy rule

This regulation has declared the right of a patient to learn how to disclose and use the personal medical information [4, 5]. More precisely, the patient shall be able to determine and understand the usage of personal treatment data. In case that an institution has released a patient record without commission, it has violated the privacy rule. In particular, the standard of de-identification has also been included in the rule [6, 7]. Even a patient has agreed to release corresponding EHRs for specific usage, no one shall be able to link these data to the original owner [8, 9].

2.1.2. Security rule

The security regulation has determined how to store, access, and transfer EHRs to guarantee if these records have been well-protected. It applies three strategies to achieve the confidentiality, integrity, and availability of EHRs, including administrative safeguards, physical safeguards, and technical safeguards.

Administrative safeguards: It contains the political policy, deployment procedure, and the training program of medical staffs. All members have to follow the defined procedure to mitigate the risk from man-made mistakes.

Physical safeguards: It concerns the hardware maintenance and equipment protection. Thus, physical damage and unauthorised access can be prevented to secure EHR.

Technical safeguards: It refers to the design of electronic health record mechanism. The system shall be able to preserve the confidentiality, integrity, and availability of EHR [38].

2.2. Blockchain

The blockchain has played an important role to confirm the privacy of patient and immutability of EHR in the new medical system, which is a distributed system for data storage [16, 17]. The blockchain is applied in distinct fields, such as smart grid [19], double auction [20], and agricultural supply chain [21]. Each participant in blockchain network is named as a node. Once a transaction between nodes has been launched, the hash value of transaction data will be broadcasted to the network [35]. Concerning to the efficiency and data protection, we have applied the consortium blockchain to the new mechanism, consisting of patient, hospital, and medical research institution. A patient uploads EHR to the blockchain, while hospitals and medical centers can access the data and have to provide the computation power to maintain the chain. A brief block structure is depicted in Fig. 2, while the parameters used in block are defined in Table 1.

The account creation in blockchain network relies on elliptic curve digital signature algorithm [22]. It is considered as the node identity in transactions and consists of a pair of public and private keys. A node employs the private key to encrypt the transaction content for confirmation, while others can apply the public key to verify the transaction. The main characteristics of blockchain are highlighted as follows.

De-centralized: The transaction data have been verified and recorded in blocks. All nodes share the responsibility for maintaining the block content; thus, it is unnecessary to introduce a trusted third party or centralized node to deal with transactions.

Immutability: Each block contains the hash value of previous block contents. In case that an attacker tries to tamper the data, this attempt must be detected soon as other nodes will learn the inequivalent hash results of the subsequent transactions.

Unforgeability: Without the legal private key, an attacker is unable to make up a pair of message and corresponding signature.

Anonymity: The public and private key pair has been used to

Table 1
The parameters defined in a block.

Name	Definition
Block header	The hash value of Previous hash, Timestamp, Nonce, and Merkle root calculated by SHA256.
Previous hash	The previous Block header value.
Timestamp	The time of block establishment.
Nonce	The difficulty of PoW.
TX *n*	The *n*th transaction.
Hash *x*	It is the hash value of TX *n*.
Merkle root	The hash value from two adjacent Hash *x* using the Merkle tree algorithm, which contains a summary of all transactions in a block. For example, the hash values Hash 1 and Hash 2 are combined to create Hash 12.

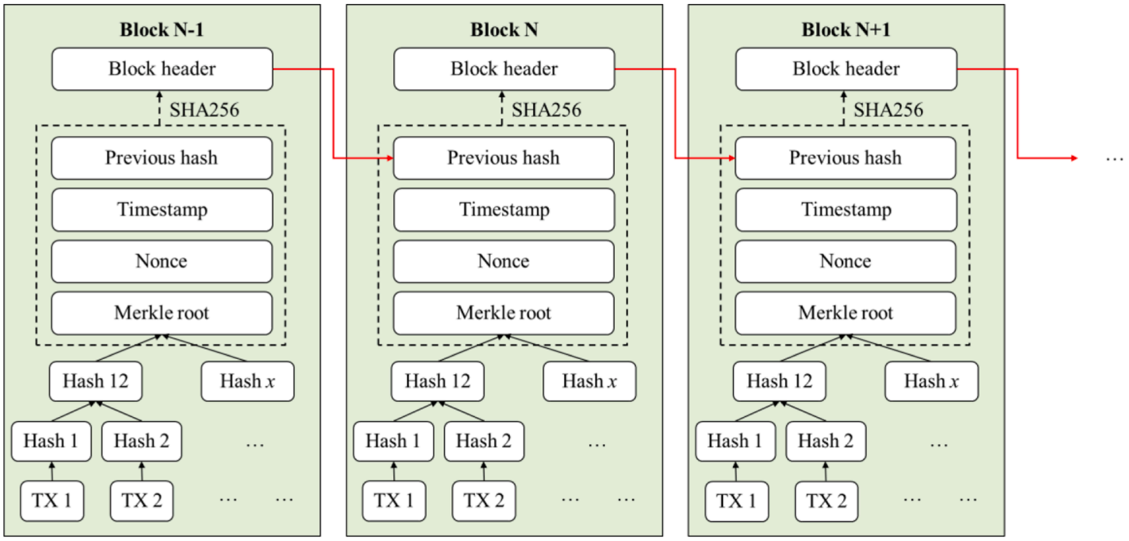


Fig. 2. The structure of a block.

validate a node so that no one can trace the real identity.

Transparency: All nodes have shared the block contents so that the data are transparent to consortium members.

2.3. Smart contract

The smart contract used in the new mechanism is to aggregate medical information of an individual patient. This can help researchers obtaining a continuous observation of the patient. The concept has been first proposed by Szabo in 1997 [18]. Szabo encouraged people to define the transaction content in a program language, and it is performed automatically by a computer. Integrating the smart contract with blockchain [23], the code defined in the contract cannot been illegally tampered to achieve the fairness of a transaction. The flowchart of smart contract is shown in Fig. 3, and the parameters used in contract are listed in Table 2. The content of current smart contract is written in solidity language. The certified content is kept in blockchain. A user employs Externally Owned Account (EOA) to be the node identity. A contract is triggered via the address and specific regulations, such as value and state. There are two types of contract execution. The first one is a trigger event, including property transfer or data deposition, while the second one is to call other contract to achieve specific goal. Without loss of generality, a smart contract can be applied to more complicated brand-new scenarios, such as copyright grant [24], crowdfunding [25], and lottery game [26]. Taking the scenario of vending machine for instance, a program has been written to determine the output product. Then the results shall be pushed to the public. People who agree with the price can put the money in and push the button. When the conditions of the contract are reached, the program will automatically output the corresponding beverage; otherwise, it returns money to user. This has illustrated the fact that a transaction can be well-handled through a smart contract voluntarily, as shown in Algorithm 1.

3. Proposed scheme

In this section, we describe the medical blockchain with data sharing and privacy preserving of EHR using a scenario instance. The proposed scheme consists of two phases: registration and diagnosis in Sections 3.1 and 3.2, respectively. In the beginning, a patient (Alice) has to register a smart card with the Health Care Authority (HCA) which is the health information administration department under the Ministry of Health and Welfare [27]. HCA is in charge of the smart card registration and distribution. Each smart card records the corresponding health information of a patient. After that, the medical officer is able to identify the patient by his/her smart card in a hospital. Notations used in the proposed scheme are defined in Table 3.

Table 2
The parameter of smart contract.

Name	Definition
Value	The number of virtual currency.
State	The current state of the smart contract, which is updated by executing a transaction.
Functions	The executions for different purposes.
Address	An address on the blockchain network for identifying a particular place.

Algorithm 1
Vending machine instance.

```
Input: Coin, button
Output: Beverage
Begin
contract vendor_machine
    beverage_price = 1
    received_money = 0
    button = False

    function buying(coin, button)
        IF coin == beverage_price and button == True
            release_beverage()
end
```

Table 3
Notations.

Notations	Description
$\boldsymbol{x}$	User x.
$\boldsymbol{SSN_x}$	Social security number (SSN) of x.
$\boldsymbol{PI_x}$	Personal identifiers of x, such as name, SSN, telephone number, and address.
$\boldsymbol{QI_x}$	Quasi-identifiers of x, such as gender, age, blood group, and allergy.
$\boldsymbol{PW_x}$	The password of x.
$\boldsymbol{P_1{}^x, P_2{}^x, P_3{}^x, P_4{}^x}$	The registration parameters of x computed by HCA, where $P_1{}^x = h(PW_x) \oplus (PI_x \Vert QI_x)$, $P_2{}^x = h(PW_x) \oplus SSN_x$, $P_3{}^x = h(PW_x) \oplus SK_x$, and $P_4{}^x = h(PI_x \Vert QI_x)$.
$\boldsymbol{EHR_x}$	Electronic health record of x, where $EHR_x = PI_x \Vert QI_x \Vert DC \Vert t$.
EHRde Alice	De-identification electronic health record of x, where $EHRde\ x = QI_x \Vert DC \Vert t$.
$\boldsymbol{DC}$	Diagnosis content.
$\boldsymbol{t}$	Timestamp.
$\boldsymbol{h()}$	One-way hash function of SHA256.
$\oplus$	The exclusive-or operation.
$\Vert$	The concatenation operation.
$\boldsymbol{SK_x/PK_x}$	The private/public key of x.
$\boldsymbol{E_{SK_x}(m)/E_{PK_x}(m)}$	The asymmetric encryption and decryption of message m with SK_x and PK_x, respectively.
$\boldsymbol{address_x}$	Blockchain address of x.

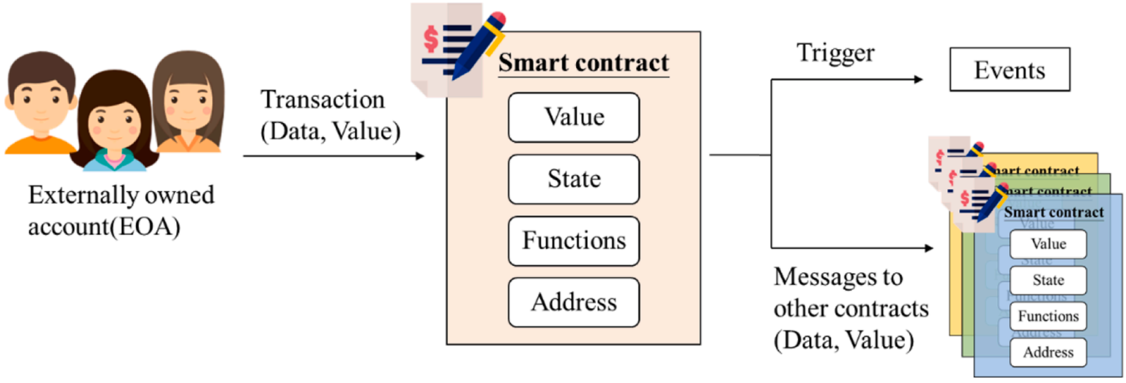

Externally owned account(EOA)
Transaction (Data, Value)
Smart contract
Value
State
Functions
Address
Trigger
Events
Messages to other contracts (Data, Value)
Smart contract
Value
State
Functions
Address

Fig. 3. The flowchart of smart contract.

3.1. Registration phase

Alice goes to HCA for acquiring a smart card. The flowchart is shown in Fig. 4.

Step 1. Alice provides SSN_{Alice}, PI_{Alice}, QI_{Alice}, and PW_{Alice} to register with HCA.

Step 2. If yes, HCA accepts the registration request, it creates a new smart contract account for her, including SK_{Alice}, PK_{Alice}, and $address_{Alice}$. Next, HCA computes and embeds P_1^{Alice}, P_2^{Alice}, P_3^{Alice}, P_4^{Alice}, PK_{Alice}, and $address_{Alice}$ into the corresponding smart card. The computed parameters are also stored in HCA database. Finally, HCA issues the smart card to Alice.

3.2. Diagnosis phase

The diagnosis phase has three stages, the first consultation, the follow-up consultation, and emergency situation, as explained in Sections 3.2.1, 3.2.2, and 3.2.3. The flowchart of the diagnosis phase is shown in the Fig. 5.

3.2.1. The first consultation

The first consultation means that a patient goes to the hospital for the first time. After completing the registration phase, Alice can go to the hospital with her smart card. The flowchart of the first consultation is shown in Fig. 5, which consists of four steps, login, diagnosis, authorization, and verification.

Step 1. Alice inserts her smart card into the device and enters PW_{Alice}. Then, the diagnosis system computes the following parameters, $PI_{Alice}'||QI_{Alice}' = h(PW_{Alice})\oplus P_1^{Alice}$ and $P_4^{Alice'}$. If $P_4^{Alice'} = P_4^{Alice}$ holds, the identity of Alice is successfully authenticated. Later, the system filters and displays PI_{Alice} and QI_{Alice} to the doctor's computer.

Step 2. After the diagnosis, the doctor generates EHR_{Alice} and signs it $E_{SK_{Doctor}}(EHR_{Alice})$. Subsequently, the doctor obtains SSN_{Alice} from PI_{Alice}, and stores SSN_{Alice}, EHR_{Alice}, and $E_{SK_{Doctor}}(EHR_{Alice})$ into the hospital database as a record for this consultation. Note that the doctor can provide the advanced cure from learning PI_{Alice} and QI_{Alice} to avoid allergic reaction in prescribing the medicine.

Step 3. If Alice is willing to share record of the first consultation to research institutions, she needs to store EHR in her contract account. Alice must insert the smart card into the device and key in PW_{Alice}. The hospital system reveals $PI_{Alice}'||QI_{Alice}' = h(PW_{Alice})\oplus P_1^{Alice}$ and $P_4^{Alice'}$. Then, the system verifies whether $P_4^{Alice'} = P_4^{Alice}$. If it holds, the system obtains SSN_{Alice} and further searches for EHR_{Alice} through SSN_{Alice} in its database. Next, the system calculates $EHRde\ Alice$ for de-identification and sign the signature $E_{SK_{Hospital}}(EHRde\ Alice)$. Also, Alice signs and stores $E_{SK_{Alice}}(EHRde\ Alice||E_{SK_{Hospital}}(EHRde\ Alice))$ with the corresponding certificate, which includes PK_{Alice}, to medical blockchain according to $address_{Alice}$.

Step 4. The other peers of medical blockchain, hospitals and research institutions, verify whether the $D_{PK_{Alice}}(E_{SK_{Alice}}(EHRde\ Alice||E_{SK_{Hospital}}(EHRde\ Alice)))$?= $EHRde\ Alice||E_{SK_{Hospital}}(EHRde\ Alice)$ and $D_{PK_{Hospital}}(E_{SK_{Hospital}}(EHRde\ Alice))$?= $EHRde\ Alice$ via relevant certificate once they receive the broadcast information. If both equations hold, the sharing of $EHRde\ Alice$ is confirmed.

3.2.2. The follow-up consultation

The follow-up consultation represents that a patient needs healthcare service again, such as returning visit examination, making an appointment in different outpatient departments, and going to another hospital. The procedure of the follow-up consultation is similar to Section 3.2.1. Only steps of login and authentication are minor different, as described in the following, while the diagnosis and verification steps keep the same. Also, the diagram is similar to Fig. 5.

Step of login: Alice inserts her smart card into the device and enters PW_{Alice}. Then, the diagnosis system computes the following parameters, $PI_{Alice}'||QI_{Alice}' = h(PW_{Alice})\oplus P_1^{Alice}$ and $P_4^{Alice'}$. If $P_4^{Alice'} = P_4^{Alice}$ is valid, the identity of Alice is successfully authenticated. The system applies SSN_{Alice} to search whether EHR_{Alice} exists in its database or not. Also, the system seeks whether $EHRde\ Alice$ is in medical blockchain using $address_{Alice}$. If both conditions are true, the system will show all information of Alice; otherwise, it only filters and displays PI_{Alice} and QI_{Alice} to doctor's computer.

Step of authentication: If Alice is willing to share current consultation to research institutions, she needs to store EHR in her contract account using the hospital computer Alice must insert the smart card into the device and key in PW_{Alice}. The system reveals $PI_{Alice}'||QI_{Alice}' = h(PW_{Alice})\oplus P_1^{Alice}$ and $P_4^{Alice'}$. Subsequently, the system verifies whether $P_4^{Alice'} = P_4^{Alice}$. If it holds, the system obtains SSN_{Alice} and further uses it to search for EHR_{Alice} in its database. Next, the system calculates $EHRde\ Alice$ for de-identification and sign the signature $E_{SK_{Hospital}}(EHRde\ Alice)$. Also, Alice signs and stores $E_{SK_{Alice}}(EHRde\ Alice||E_{SK_{Hospital}}(Ede\ Alice))$ with the corresponding certificate, which includes PK_{Alice}, to medical blockchain on the basis of $address_{Alice}$.

3.2.3. Emergency situation

Emergency situation expresses that a patient requires an emergent treat without login procedure by himself/herself, such as a comatose state happens. Hence, the healthcare worker is able to search the previous EHR of the patient. The detail steps are shown in the following. Note that only the authorized emergency healthcare worker has the ability to acquire the data.

Step of login: The healthcare worker inserts Alice's smart card into the hospital device. Next, the diagnosis system obtains P_4^{Alice} from the smart card. Consequently, the healthcare worker is able to search EHR_{Alice} through the index P_4^{Alice} from database. If the search outcomes are positive, the system will send PI_{Alice}, QI_{Alice}, and EHR_{Alice} to doctor computer; otherwise, it shows fail message, which means that the patient Alice is determined as the first consultation.

After that, the emergency patient can obtain a cure which is the same procedure as the step 2 of Section 3.2.1. Note that the steps 3 and 4 of Section 3.2.1 do not be conducted since the sharing willingness of the patient is considered as negative under comatose status.

4. Performance analysis

In this section, we evaluate the achievement and privacy of medical blockchain. We first introduce the application scenario in Section 4.1.

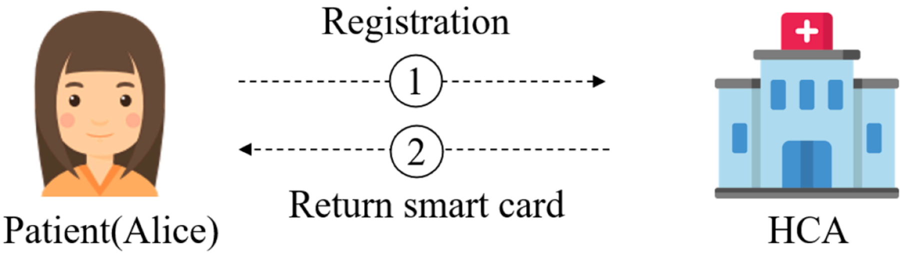


Fig. 4. Flowchart of registration phase.

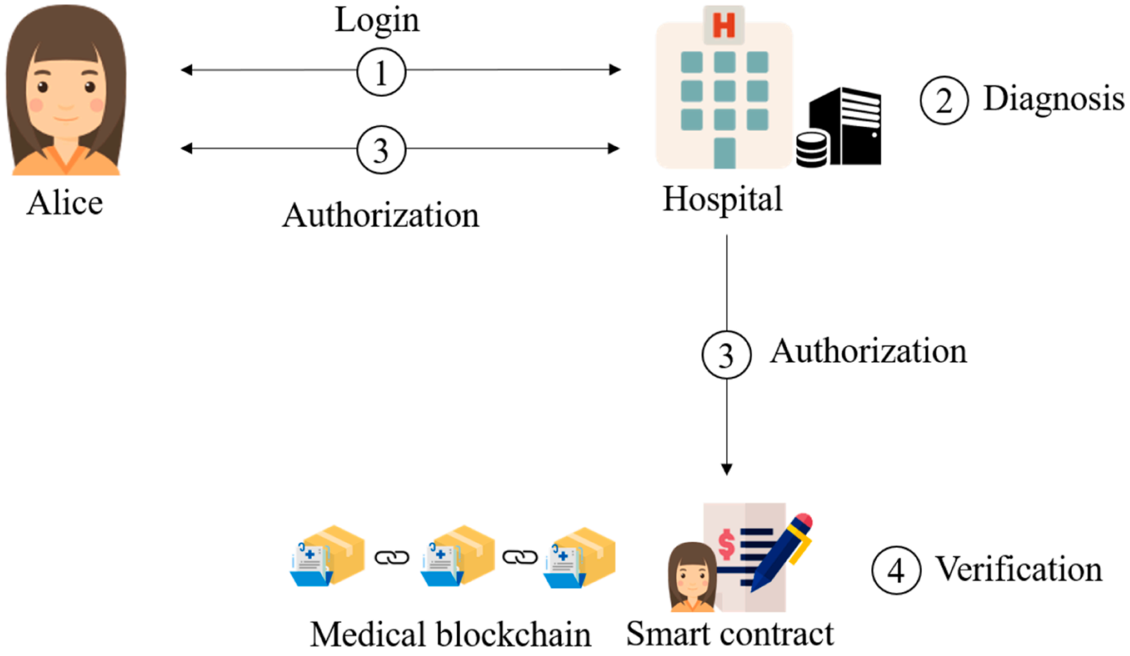


Fig. 5. The flowchart of the diagnosis phase.

According to the following assumptions of one-way hash function and asymmetric elliptic curve cryptosystem, we then explain how to resist malicious attacks and confirm the achievements in Sections 4.2 and 4.3, respectively. Efficiency discussions are given in Section 4.4. Lastly, the formal proof is given in Section 4.5.

Assumption of one-way hash function [28]

Input an arbitrarily size message m into $h(.)$, it is easy to obtain a fixed size of output $y = h(m)$. The security of one-way hash function depends on the following properties.

(1) The preimage resistance: Given an output $y = h(m)$, it is impossible to derive m from y.
(2) The second preimage resistance: Given m, it is computational infeasible to find $h(m) = h(m')$, where $m \neq m'$.
(3) Collision resistance: Given m and $h(m)$, it is computational infeasible to find m' such that $h(m) = h(m')$.

Assumption of asymmetric elliptic curve cryptosystem [22]

An elliptic curve based asymmetric cryptosystem is used to secure the digital signature used in the new mechanism. The security of the new method is inherited from that of current blockchain network, which relies on the difficulty of compromising elliptic curve discrete logarithm problem.

4.1. Application scenario

In this subsection, we introduce an application scenario to show how the new method can enable Alice to protect EHR_{Alice} and share *EHRde Alice* to the medical blockchain. For the first time Alice heads to a hospital, she has to insert the smart card and corresponding password determined in the registration phase. A legal password string can lay out a hash value of personal information which is the same as that kept in the smart card. According to the identical comparison result, Alice could be verified by the hospital. The smart contract pseudo code of registration phase is shown in Algorithm 2.

After the diagnosis, Alice can decide to release the grant of sharing EHR_{Alice}. If it is positive, Alice has to enter her password so that the hospital can further remove her relevant data to obtain *EHRde Alice*; thus, achieving the de-identification in accordance with HIPAA. *EHRde Alice* is then uploaded to her smart contract and broadcasted to the medical blockchain. The corresponding pseudo code of diagnosis is displayed in Algorithm 3.

Algorithm 2
Registration phase.

```
Input: $SSN_{Alice}$, $PI_{Alice}$, $QI_{Alice}$, and $PW_{Alice}$
Output: Smart card
Begin
1. HCA computes the following values and embeds into the smart card.
2. $P_1^{Alice}$
3. $P_2^{Alic}$
4. $P_3^{Alice}$
5. $PK_{Alice}$
6. $address_{Alice}$
7. $P_4^{Alice}$
8. Return smart card.
End
```

As all the information related to Alice have been eliminated from *EHRde Alice*, the privacy of Alice can be firmly guaranteed. That is, authorized researchers can freely access the data through the medical blockchain without contacting the hospital. Moreover, the anonymity of blockchain can ensure that no one can link the data to a specific patient, while the immutability can confirm the correctness of medical data.

In case that Alice has to see a doctor in another hospital, the doctor can apply $address_{Alice}$ to find *EHRde Alice* to learn the medical information without persistent checking. This can help Alice saving time and cost to obtain a complete diagnosis.

4.2. Analysis of potential attacks

Here we analyze how to resist impersonation and replay attacks in Sections 4.2.1 and 4.2.2, respectively.

4.2.1. Impersonation attack

Assume that a malicious attacker Eve has stolen the smart card of Alice and tried to impersonate Alice to obtain a diagnosis. In login step of the diagnosis phase, Eve has to offer a password string to generate $h(PI_{Alice}'||QI_{Alice}')$. Without the correct password, however, it is computationally infeasible for Eve to achieve $h(PI_{Alice}'||QI_{Alice}') = h(PI_{Alice}||$

Algorithm 3
Diagnosis phase.

```
Input: Smart card
begin
Alice inserts her smart card into the device and enters $PW_{Alice}$.
Hospital receives smart card and computes the following value.
$PI_{Alice}'||QI_{Alice}' = h(PW_{Alice}) \oplus (P_1^{Alice})$
IF $P_4^{Alice}{}' = P_4^{Alice}$
System displays $PI_{Alice}$ and $QI_{Alice}$ to the doctor's computer.
The doctor generates following values.
$EHR_{Alice} = PI_{Alice}||QI_{Alice}||DC||t$
$E_{SK_{Doctor}}(EHR_{Alice})$
The doctor stores the following values into the hospital database.
$SSN_{Alice}$
$EHR_{Alice}$
$E_{SK_{Doctor}}(EHR_{Alice})$
IF Alice is willing to share record
Alice inserts her smart card into the device and enters $PW_{Alice}$ .
IF $PI_{Alice}'||QI_{Alice}' = h(PW_{Alice}) \oplus (P_1^{Alice})$
System calculates following values.
$EHRde\ Alice = QI_{Alice}||DC||t$
$E_{SK_{Hospital}}(EHRde\ Alice)$
$E_{SK_{Alice}}(EHRde\ Alice||E_{SK_{Hospital}}(EHRde\ Alice))$
IF $D_{PK_{Alice}}(E_{SK_{Alice}}(EHRde\ Alice||E_{SK_{Hospital}}(EHRde\ Alice))) == EHRde\ Alice||E_{SK_{Hospital}}(EHRde\ Alice)$
and $D_{PK_{Hospital}}(E_{SK_{Hospital}}(EHRde\ Alice)) ?= EHRde\ Alic$
The sharing of $EHRde\ Alic$ is confirmed.
End
```

QI_{Alice}) under the assumption of one-way hash function. Thus, Eve cannot succeed in pretending Alice to have treatment in the hospital.

4.2.2. Replay attack

Suppose that Eve is able to intercept the data Alice uploaded to the medical blockchain in authentication step of diagnosis phase. In case that she wants to replay the data uploading to blockchain for disturbing the correctness of medical data, she has to solve the problem of an overdue timestamp. It is due to that the replayed transaction has to pass the validness checking. To renew a current timestamp in the transaction, nevertheless, it is computational infeasible without the private key of Alice based on the assumption of asymmetric elliptic curve cryptosystem. Consequently, we can confirm that Eve must fail in replaying a transaction uploading.

4.3. Achievement evaluation and comparisons

In Section 4.3.1, we explain the achievements of the new method in terms of data privacy complying with HIPAA regulation [29]. Next, the comparisons with related works are discussed in Section 4.3.2 [11–13].

4.3.1. Data privacy discussion complying with HIPAA regulation

To confirm the data privacy of patient, we have designed the new method according to HIPAA regulations. As defined in the regulation, a patient is able to grant personal EHRs to specific entity. In authentication step of diagnosis phase, Alice can upload and share her *EHRde Alice* to medical blockchain indeed. Furthermore, the de-identification standard is defined in HIPAA regulation. That is, researchers shall not be able to learn the real identity of an EHR even they can freely access data from medical blockchain. Here we first follow the anonymity of blockchain to incise the relationship of transaction and real identity of uploader. As to the health data shared on medical blockchain, we have eliminated PI_{Alice} from EHR_{Alice}. to form *EHRde Alice*. No doubt that *EHRde Alice* is the final data uploaded to the blockchain. More precisely, it contains no information about true status of Alice. Compared with traditional de-identification mechanism [29], enlarging the scale of medical item or removing specific attribute are no longer necessary in the new mechanism. All important information can be kept to contribute to the medical researches.

Here we focus on four technical safeguards of HIPAA and explain each protection mechanism for EHR.

Access control: The access control is to manage the authority of EHR. Only the valid user has the ability to ask for EHR data. This control has three essential security specifications, as mentioned in Section 2.1.2.

(1) Unique user identification: This specification means that each identity of patient shall be unique. During the registration phase of the proposed scheme, *SSN* of each patient has the feature of matchless so that the applied smart card is unique, as shown in the Section 3.1. The duplicated identities shall not exist in the system.
(2) Emergency access procedure: This procedure represents that the hospital member is able to access patient's EHR even during emergency, as explained in the Section 3.2.3.
(3) Encryption and decryption: This specification indicates that the data of EHR shall be protected by secure encryption and decryption method. During the proposed scheme, the doctor will sign the patient's EHR by his/her private key in the step of Section 3.2, $E_{SK_{Doctor}}(EHR_{Alice})$.

Hence, our scheme has complied the property of access control in HIPAA.

- Integrity: This feature is to ensure that an EHR cannot be tampered through executing the policy and procedure. In the proposed scheme, the record transmitted to medical block has to be verified by public key, the $D_{PK_{Alice}}(E_{SK_{Alice}}(EHRde\ Alice||E_{SK_{Hospital}}(EHRde\ Alice))) ?= EHRde\ Alice||E_{SK_{Hospital}}(EHRde\ Alice)$ and $D_{PK_{Hospital}}(E_{SK_{Hospital}}(EHRde\ Alice)) ?= EHRde\ Alice$, as shown in the step 4 of Section 3.2.1 and the authentication step of Section 3.2.2. Consequently, we can reach the feature of integrity in HIPAA.
- Person or entity authentication: This rule implies that the person or entity who applies to access EHR data must be authenticated via the corresponding identification. As to our scheme, the patient Alice need to insert the smart card and enter password. Later, she is able to access her EHR after successfully verification, which is mentioned in the step 1 of Section 3.2.1 and the authentication step of Section 3.2.2
- Transmission security: This rule is to protect EHR during transmission procedure for preventing unauthorised user accessing. In the step 3 of Section 3.2.1 and authentication step of Section 3.2.2, the record transferred to medical blockchain has to be encrypted by private keys of patient Alice or hospital, $E_{SK_{Alice}}(EHRde\ Alice||E_{SK_{Hospital}}(EHRde\ Alice))$ and $E_{SK_{Hospital}}(EHRde\ Alice)$. Therefore, we have achieved the requirement of transmission security in HIPAA.

4.3.2. Achievement comparison analysis

To highlight the performance of the medical blockchain, we subsequently compare achievements of related works [11-13, 37] with those of ours in Table 4, including anonymity, confidentiality, availability, privacy, immutability, unforgeability, and integrity [32–33].

Anonymity: This property is to enable a patient to share medical data on the blockchain via an anonymous identity. Namely, the true

Table 4
Achievement comparisons, Y: Yes, N: No, N/A: No mention.

	[11]	[12]	[13]	[37]	Ours
Anonymity	Y	N/A	Y	Y	Y
Confidentiality	N	Y	N	Y	Y
Availability	Y	Y	Y	Y	Y
Privacy	N/A	N/A	N/A	N/A	Y
Immutability	Y	N	N	Y	Y
Unforgeability	Y	N	N	Y	Y
Integrity	Y	N	N	Y	Y
Blockchain-based	N	N	N	N	Y

identity needs not to be public or verified. In [11, 13, 37], the authors have employed digital signature algorithms to authenticate the user, but the private key cannot be connected with the true identity. Thus, these two methods can preserve the anonymity requirement. As to [12], the anonymity is not concerned in designing the system so that it is improper to check this. Regarding to the new method, we have adopted the private key of elliptic curve asymmetric cryptosystem to verify user. Note that the private key is irrelevant to the true identity of Alice. Researchers are able to obtain the medical data from the blockchain, but they cannot learn the relationship between *EHRde Alice* and Alice under the assumption of elliptic curve cryptosystem. As shown in Table 4, the anonymity can only be confirmed in [11, 13] and the new method.

Confidentiality: This essential is to ensure that only an authorized user can access data. In [11], it is unable to resist a collusion attack launched by a set of cloud users; thus, leading to the leakage of personal information [30]. Concerning to [12], the polynomial interpolating strategy is applied to achieve that only granted users can access information. Thus, medical data could be secure to confirm the confidentiality. Nevertheless, it has been pointed in [14] that a man-in-the-middle attack might be successfully mounted in [13]. That is, an attacker may be able to violate the confidentiality to illegally learn personal data. In [37], the MedGreen Communication authentication algorithm is applied to achieve that only authorized users can access the information. Thus, medical data can be secured to confirm the feature of confidentiality. As to the medical blockchain used in the new mechanism, it belongs to the type of consortium blockchain, in which the members only include patient, hospital, and research center. More precisely, only these consortium members are allowed to access *EHRde Alice* on the blockchain. We thus conclude that the confidentiality can be ensured in the new mechanism, as listed in Table 4.

Availability: The availability is to examine the functionality of the system. In [11, 12, 13, 37], all the methods rely on the cloud storage to keep data. Moreover, the backup strategy is employed to enhance the data availability. Regarding this issue, the new method has uploaded all data to medical blockchain, which is a distributed environment and each node has a copy of whole data. In case that a computer has been out of function, the system is still alive, and so is the medical record. As displayed in Table 4, we have derived that related works and the new mechanism are able to confirm this property.

Privacy: This is for confirming the privacy regulation of HIPAA. The patient has right to understand the usage of his/her EHR, and each EHR shall follow the de-identification standard. In [11-13, 37], all research data are transmitted in cipher text during the sharing procedure. However, the de-identification of privacy regulation is not considered in these methods. As to the proposed scheme, the patient is endowed with the right of EHR management during the authorization of diagnosis in Sections 3.2.1 and 3.2.2. Also, the researcher is unable to learn the true identity of a specific patient based on the de-identification process and the feature of anonymity. Thus, the new method can reach the property of privacy, as displayed in Table 4.

Immutability: This issue is to guarantee that no one can tamper the data content. In [11], a user can apply the public key to verify the received message. Unless an attacker is able to compromise the asymmetric cryptosystem, it is computationally infeasible to tamper the data signed by the corresponding private key. For [12], the authors have employed the polynomial interpolating algorithm to encrypt and share the message on the cloud. Once an attacker has tampered the cipher text, the user still might be able to extract a meaningful plain text. Consequently, the immutability cannot be ensured in [12]. On the other hand, researchers have shown that the method of [13] is vulnerable to the message tampering attack [14]; thus, leading to violating this essential. In [37], the authentication algorithm depends on elliptic curve construction method and HMAC technique. Unless an attacker can compromise the elliptic curve algorithm, it is computationally infeasible to tamper the data signed by the corresponding private key. As to the data on medical blockchain, the immutability has been inherited from the original blockchain network. That is, an attacker Eve must fail to disturb the correctness of medical data via tampering *EHRde Alice* unless she is able to modify the same data block stored in 51% blockchain nodes, which has offered the evidence that the new method is able to guarantee the immutability, as shown in Table 4.

Unforgeability: This property is to confirm that a pair of data and corresponding signature cannot be forged. In [12], a malicious attacker Eve is able to make up and encrypt a message through the polynomial interpolating algorithm. Since the receiver is unable to check the message validity, this essential cannot be preserved. This situation also happens in [13] as attacker Eve can generate a pair of content and corresponding signature. As to [11, 37] and the new method, Eve is unable to construct the valid signature of data without the private key under the assumption of asymmetric elliptic curve cryptosystem. This has demonstrated that the essential can be realized in these two methods.

Integrity: This feature indicates that the stored data is unable to be tampered. Besides, the malicious attacker cannot forge the real transferred data. In [12], the transferred data may suffer from the tampering attack during data sharing phase. As to [13], the method has been pointed out that it might encounter the man-in-the-middle attack and data tampering attack [14]. The reason is that the server does not check the registration data from user in [13]. Hence, [12–13] cannot ensure the property of data integrity. Conversely, [11, 37] and the proposed scheme carefully verify the transferred message. When the record transmitted to medical blockchain, it must to be authenticated by the public key, the $D_{PK_{Alice}}(E_{SK_{Alice}}(EHRde\ Alice||E_{SK_{Hospital}}(EHRde\ Alice)))\ ?= EHRde\ Alice||E_{SK_{Hospital}}(EHRde\ Alice)$ and $D_{PK_{Hospital}}(E_{SK_{Hospital}}(EHRde\ Alice))\ ?= EHRde\ Alice$, as shown in the step 4 of Section 3.2.1 and the authentication step of Section 3.2.2. Therefore, we can accomplish the integrity both in the situations of storing data and transferring data.

Blockchain-based: This feature presents the implementation of medical record sharing platform maintained by point to point (P2P) architecture, blockchain network. In [11-13, 37], all of these researches are based on the centralized server in the cloud environment. The centralization server might result in potential security issues and efficiency bottleneck. On the contrary, we build up a distributed mechanism using blockchain. The medical blockchain is maintained by all participants. It is hard for malicious attacker to modify the medical record until he/she can change 51% of blockchain points.

4.4. *Efficiency discussions*

In the following, we demonstrate the practicability of medical blockchain. Here we evaluate the computational overheads of registration and diagnosis phases to prove that the new mechanism can be realized in current environment of hospital. Simulations are conducted in Python with a personal computer running Windows 10 64-bit. It is equipped with an Intel Core i5–650 3.2-GHz with 4 G RAM, which is a common device used in a hospital.

All the operations and time overheads are listed in Table 5, where notations are defined as follows. T_{XOR} is the time cost of an exclusive-or operation, T_h denotes the overhead of a one-way hash function, $T_{E_{ECC}}$ represents the time spent for an elliptic curve encryption, and $T_{D_{ECC}}$ means the time required in performing an elliptic curve decryption. Meanwhile, we compare the overall spending time cost with related works [11, 13] in Table 6.

As to [11], it executes one time T_h and four times T_h in user registration and user revocation, which cost 0.0025 ms and 0.01 ms,

Table 5
Execution time.

T_{XOR}	T_h	$T_{E_{ECC}}$	$T_{D_{ECC}}$
0.0002ms	0.0025ms	49.1621ms	0.0099ms

Table 6
Execution time.

Related works	[11]	[13]	Ours
Time	196.7033ms	442.5574ms	147.4969ms

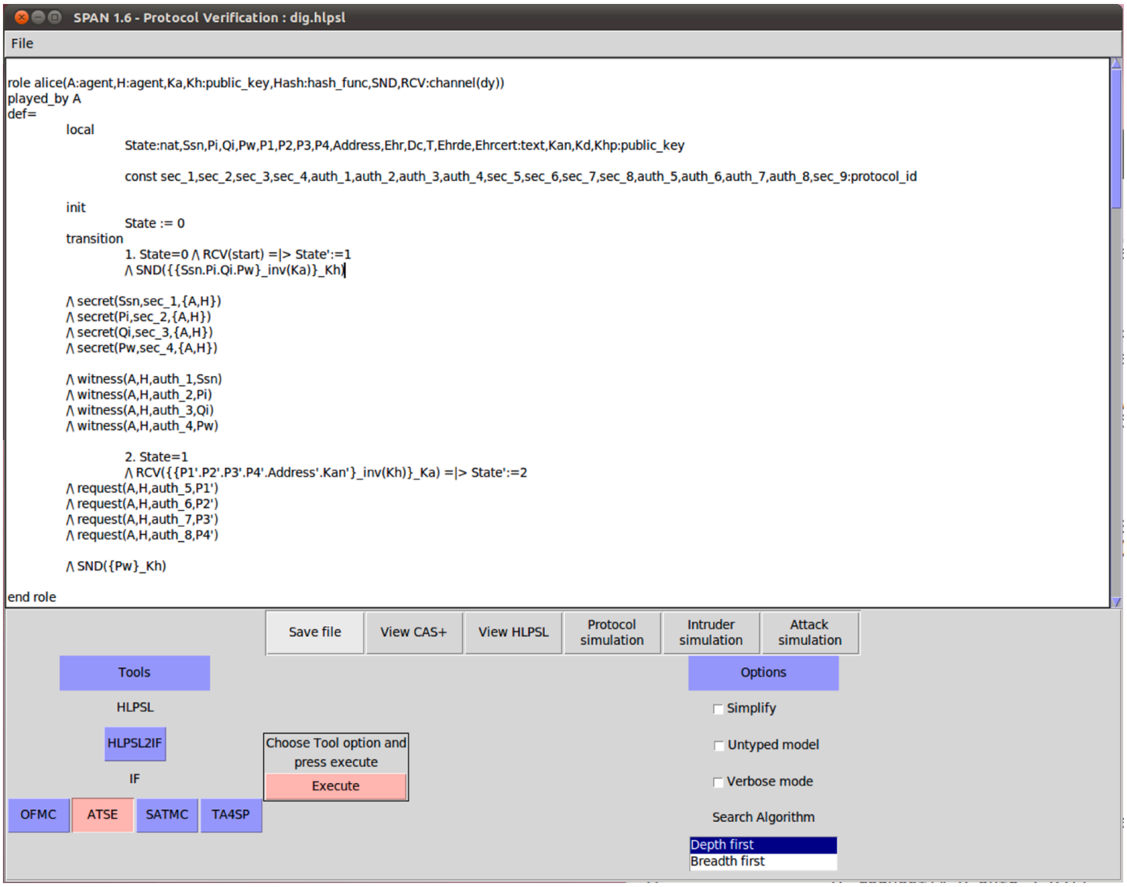
respectively. Following it spends $2T_{E_{ECC}} + 4T_h = 98.3342$ ms in file generation stage and takes $T_{E_{ECC}} + 9T_h = 49.1846$ ms in file deletion phase. Next, [11] performs the file access stage by spending $T_{E_{ECC}} + T_{D_{ECC}} = 49.1721$ ms. Therefore, it totally requires 196.7033 ms. Regarding to [13], it contains registration, file upload, and file download phases. Each of phase takes $3T_{E_{ECC}} + 2T_h + 2T_{D_{ECC}} = 147.5501$ ms, $5T_{E_{ECC}} + 3T_h + 1T_{D_{ECC}} = 245.8254$ ms, and $T_{E_{ECC}} + 2T_{D_{ECC}} = 49.1819$ ms, respectively.

To accomplish a user registration of our proposed scheme, it requires three exclusive-or operations and two one-way hash functions. Thus, HCA has to spend $3T_{XOR} + 2T_h = 0.0056$ ms. As to the diagnosis stage, the hospital has to perform one exclusive-or operation and two hash functions to confirm the login of Alice in Step 1. It needs $T_{XOR} + 2T_h = 0.0052$ ms in total. After the diagnosis, the doctor has to execute one elliptic curve encryption in Step 2, which costs $T_{E_{ECC}} = 49.1621$ ms. In case that Alice is willing to share her medical data *EHRde Alice* to the blockchain, the hospital device has to perform two exclusive-or operations, two hash functions, and two elliptic curve encryptions, which resulting in spending $2T_{XOR} + 2T_h + 2T_{E_{ECC}} = 98.3296$ ms. Totally, it requires $0.0052 + 49.1621 + 98.3296 = 147.4969$ ms in completing a diagnosis. Aside from that, a miner only needs to perform two elliptic curve decryption to verify the transaction uploaded by Alice, where $2T_{D_{ECC}} = 0.0198$ ms. Through these simulation results, it is not difficult to learn the fact that it needs no more than 147.5 ms for hospital device with i5–650 processor to finish a patient diagnosis. This has offered the evidence that the new mechanism can be applied to current hospital environment without device upgrading. Also, the effectiveness feature is obviously superior to that of [11, 13].

4.5. Formal proof analysis

We have adopted the Automated Validation of Internet Security Protocols and Applications (AVISPA) to prove the security of our proposed medical blockchain, which is widely used to verify the properties of robustness and authentication for a protocol [36]. The version of AVISPA for simulation is the Security Protocol Animator version 1.6 (SPAN 1.6) installed on Ubuntu10.10-light workstation with an Intel-Core-i5 CPU running at 2 GHz with 2GB of RAM, as shown in Fig. 6.

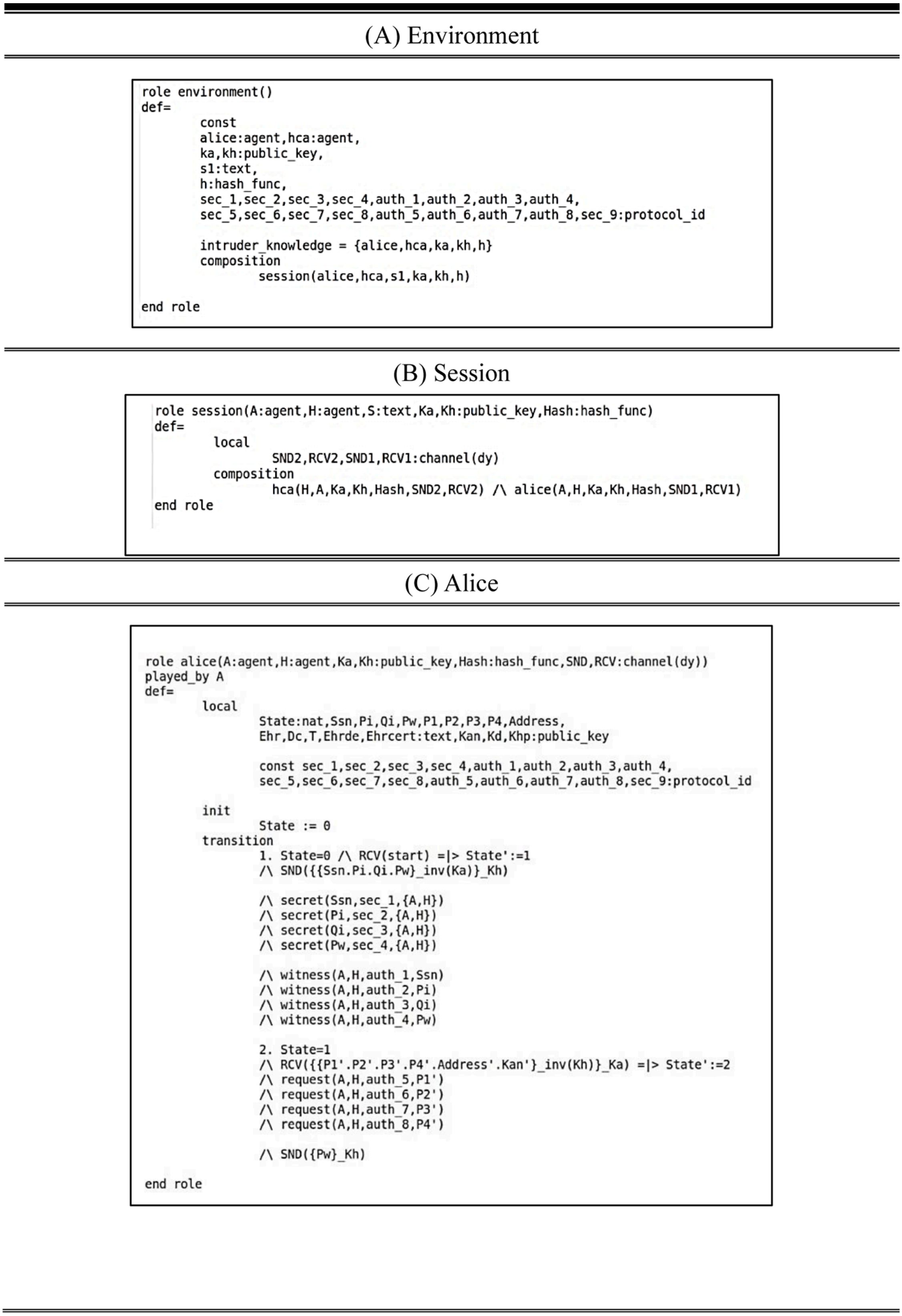
AVISPA uses High Level Protocol Specification Language (HLPSL) to explain the environment, session, two roles, and goal of our mechanism, as shown in **Figs. 7(A)-(E)**. During the simulation, the replay attack, impersonation attack, and server spoofing attack are used to examine the strong authentication features in each transmitted message. In Fig. 9 (E), we verified the confidential properties of generated data, including step 1 of Sections 3.1, sec_1 ~ sec_4, steps 2–3 of Section 3.2, sec_5 ~ sec_9. At the same time, the transferred data are checked, consisting of step 1 of Section 3.1, auth_1 ~ auth_4, and step 2 of Section 3.1, auth_5 ~ auth_8. The Constraint-Logic-based Attack Searcher (CL-ATSE) and On-the-Fly-Model-Checker (OFMC) are used to analyze whether the proposed mechanism is secure or not. There are two models and one mode adopted in CL-ATSE, where typed model contains the whole types of parameters, un-typed model has only generic-kind parameters, and verbose mode depicts the attacking trace once the protocol is insecure. On the other hand, OFMC processes the protocol by modularization. Consequently, the outcomes of CL-ATSE and OFMC are safe and secure against the Internet attack, as shown in **Figs. 8(A)-(C)** and 9.



```
role alice(A:agent,H:agent,Ka,Kh:public_key,Hash:hash_func,SND,RCV:channel(dy))
played_by A
def=
        local
                State:nat,Ssn,Pi,Qi,Pw,P1,P2,P3,P4,Address,Ehr,Dc,T,Ehrde,Ehrcert:text,Kan,Kd,Khp:public_key

                const sec_1,sec_2,sec_3,sec_4,auth_1,auth_2,auth_3,auth_4,sec_5,sec_6,sec_7,sec_8,auth_5,auth_6,auth_7,auth_8,sec_9:protocol_id

        init
                State := 0
        transition
                1. State=0 /\ RCV(start) =|> State':=1
                /\ SND({{Ssn.Pi.Qi.Pw}_inv(Ka)}_Kh)

        /\ secret(Ssn,sec_1,{A,H})
        /\ secret(Pi,sec_2,{A,H})
        /\ secret(Qi,sec_3,{A,H})
        /\ secret(Pw,sec_4,{A,H})

        /\ witness(A,H,auth_1,Ssn)
        /\ witness(A,H,auth_2,Pi)
        /\ witness(A,H,auth_3,Qi)
        /\ witness(A,H,auth_4,Pw)

                2. State=1
                /\ RCV({{P1'.P2'.P3'.P4'.Address'.Kan'}_inv(Kh)}_Ka) =|> State':=2
        /\ request(A,H,auth_5,P1')
        /\ request(A,H,auth_6,P2')
        /\ request(A,H,auth_7,P3')
        /\ request(A,H,auth_8,P4')

        /\ SND({Pw}_Kh)

end role
```

□ Simplify
□ Untyped model
□ Verbose mode
Search Algorithm
Depth first (selected)
Breadth first

Fig. 6. AVISPA SPAN 1.6 simulation.



(A) Environment

```
role environment()
def=
        const
        alice:agent,hca:agent,
        ka,kh:public_key,
        s1:text,
        h:hash_func,
        sec_1,sec_2,sec_3,sec_4,auth_1,auth_2,auth_3,auth_4,
        sec_5,sec_6,sec_7,sec_8,auth_5,auth_6,auth_7,auth_8,sec_9:protocol_id

        intruder_knowledge = {alice,hca,ka,kh,h}
        composition
                session(alice,hca,s1,ka,kh,h)

end role
```

(B) Session

```
role session(A:agent,H:agent,S:text,Ka,Kh:public_key,Hash:hash_func)
def=
        local
                SND2,RCV2,SND1,RCV1:channel(dy)
        composition
                hca(H,A,Ka,Kh,Hash,SND2,RCV2) /\ alice(A,H,Ka,Kh,Hash,SND1,RCV1)
end role
```

(C) Alice

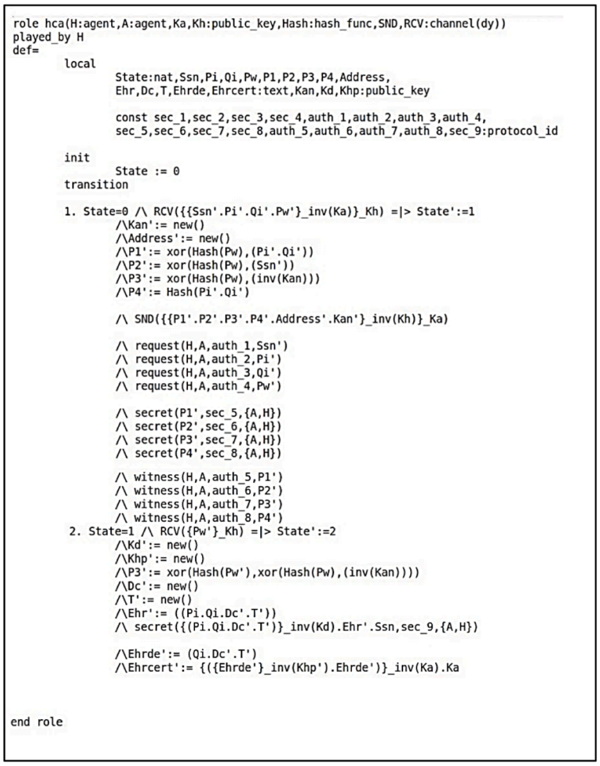
```
role alice(A:agent,H:agent,Ka,Kh:public_key,Hash:hash_func,SND,RCV:channel(dy))
played_by A
def=
        local
                State:nat,Ssn,Pi,Qi,Pw,P1,P2,P3,P4,Address,
                Ehr,Dc,T,Ehrde,Ehrcert:text,Kan,Kd,Khp:public_key

                const sec_1,sec_2,sec_3,sec_4,auth_1,auth_2,auth_3,auth_4,
                sec_5,sec_6,sec_7,sec_8,auth_5,auth_6,auth_7,auth_8,sec_9:protocol_id

        init
                State := 0
        transition
                1. State=0 /\ RCV(start) =|> State':=1
                /\ SND({{Ssn.Pi.Qi.Pw}_inv(Ka)}_Kh)

                /\ secret(Ssn,sec_1,{A,H})
                /\ secret(Pi,sec_2,{A,H})
                /\ secret(Qi,sec_3,{A,H})
                /\ secret(Pw,sec_4,{A,H})

                /\ witness(A,H,auth_1,Ssn)
                /\ witness(A,H,auth_2,Pi)
                /\ witness(A,H,auth_3,Qi)
                /\ witness(A,H,auth_4,Pw)

                2. State=1
                /\ RCV({{P1'.P2'.P3'.P4'.Address'.Kan'}_inv(Kh)}_Ka) =|> State':=2
                /\ request(A,H,auth_5,P1')
                /\ request(A,H,auth_6,P2')
                /\ request(A,H,auth_7,P3')
                /\ request(A,H,auth_8,P4')

                /\ SND({Pw}_Kh)

end role
```

Fig. 7. HLPSL code.

5. Conclusion

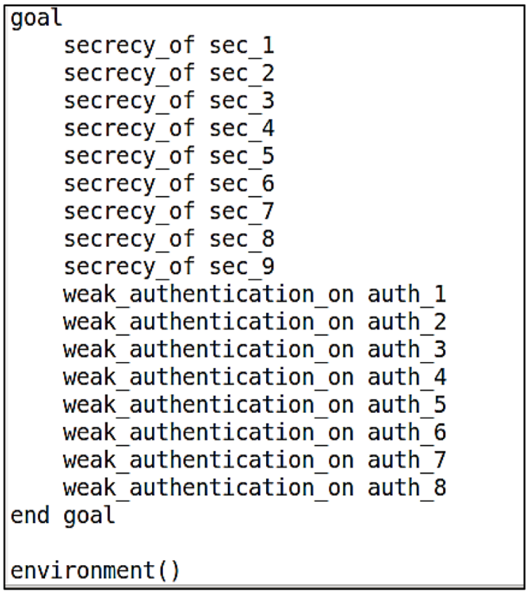
In this article, the blockchain and smart contract have been adopted to design a medical data sharing mechanism, which can accomplish seven fundamental properties of a secure medical data sharing platform. The leakage problem of patient data on the cloud platform can be firmly avoided. The anonymity and immutability of blockchain are used to preserve the patient privacy and keep the correctness of health data,

(D) HCA



```
role hca(H:agent,A:agent,Ka,Kh:public_key,Hash:hash_func,SND,RCV:channel(dy))
played_by H
def=
        local
                State:nat,Ssn,Pi,Qi,Pw,P1,P2,P3,P4,Address,
                Ehr,Dc,T,Ehrde,Ehrcert:text,Kan,Kd,Khp:public_key

                const sec_1,sec_2,sec_3,sec_4,auth_1,auth_2,auth_3,auth_4,
                sec_5,sec_6,sec_7,sec_8,auth_5,auth_6,auth_7,auth_8,sec_9:protocol_id

        init
                State := 0
        transition

        1. State=0 /\ RCV({{Ssn'.Pi'.Qi'.Pw'}_inv(Ka)}_Kh) =|> State':=1
                /\Kan':= new()
                /\Address':= new()
                /\P1':= xor(Hash(Pw),(Pi'.Qi'))
                /\P2':= xor(Hash(Pw),(Ssn'))
                /\P3':= xor(Hash(Pw),(inv(Kan)))
                /\P4':= Hash(Pi'.Qi')

                /\ SND({{P1'.P2'.P3'.P4'.Address'.Kan'}_inv(Kh)}_Ka)

                /\ request(H,A,auth_1,Ssn')
                /\ request(H,A,auth_2,Pi')
                /\ request(H,A,auth_3,Qi')
                /\ request(H,A,auth_4,Pw')

                /\ secret(P1',sec_5,{A,H})
                /\ secret(P2',sec_6,{A,H})
                /\ secret(P3',sec_7,{A,H})
                /\ secret(P4',sec_8,{A,H})

                /\ witness(H,A,auth_5,P1')
                /\ witness(H,A,auth_6,P2')
                /\ witness(H,A,auth_7,P3')
                /\ witness(H,A,auth_8,P4')
         2. State=1 /\ RCV({Pw'}_Kh) =|> State':=2
                /\Kd':= new()
                /\Khp':= new()
                /\P3':= xor(Hash(Pw'),xor(Hash(Pw),(inv(Kan))))
                /\Dc':= new()
                /\T':= new()
                /\Ehr':= ((Pi.Qi.Dc'.T'))
                /\ secret({(Pi.Qi.Dc'.T')}_inv(Kd).Ehr'.Ssn,sec_9,{A,H})

                /\Ehrde':= (Qi.Dc'.T')
                /\Ehrcert':= {({Ehrde'}_inv(Khp').Ehrde')}_inv(Ka).Ka


end role
```

(E) Goal



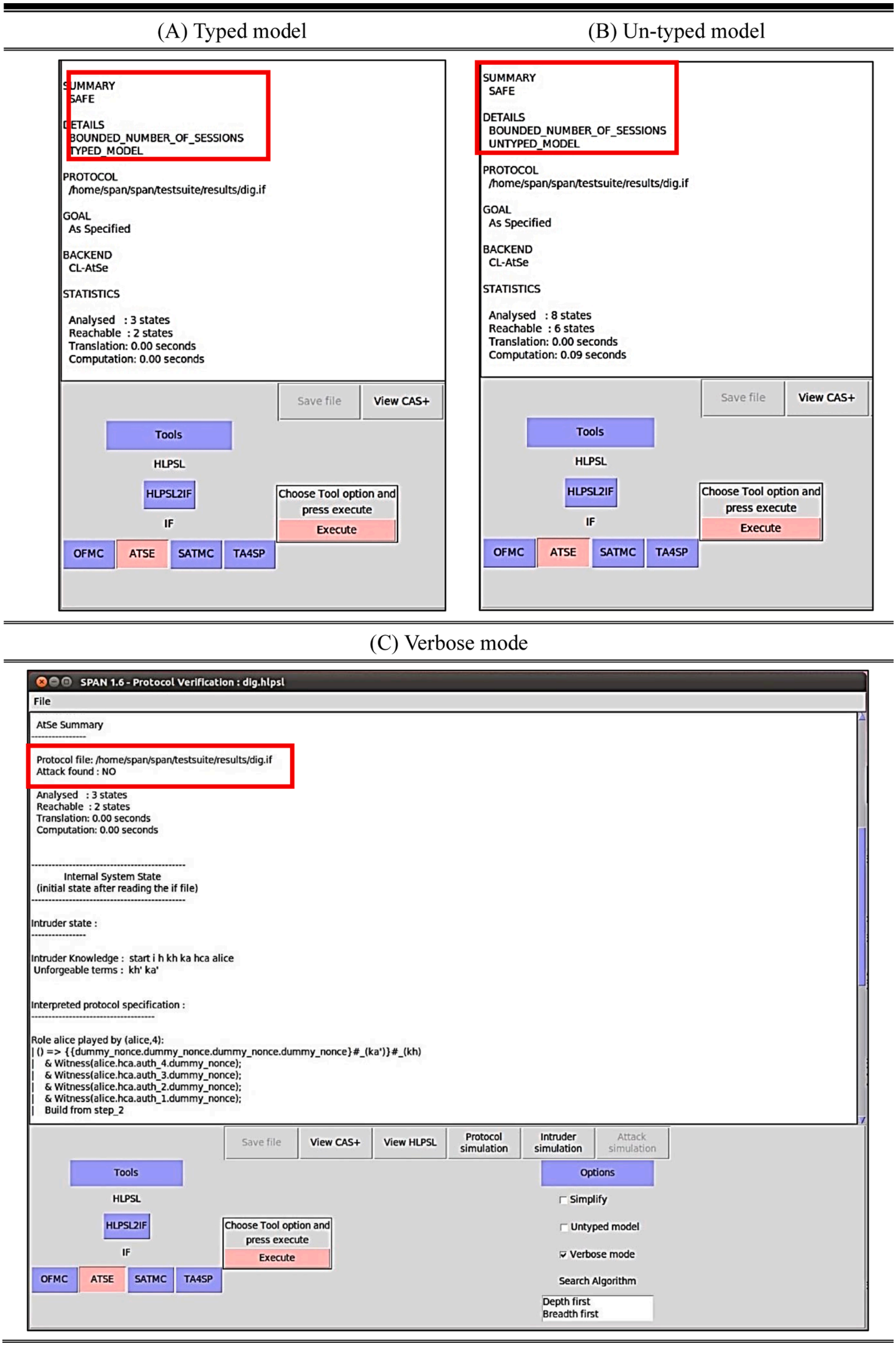
```
goal
    secrecy_of sec_1
    secrecy_of sec_2
    secrecy_of sec_3
    secrecy_of sec_4
    secrecy_of sec_5
    secrecy_of sec_6
    secrecy_of sec_7
    secrecy_of sec_8
    secrecy_of sec_9
    weak_authentication_on auth_1
    weak_authentication_on auth_2
    weak_authentication_on auth_3
    weak_authentication_on auth_4
    weak_authentication_on auth_5
    weak_authentication_on auth_6
    weak_authentication_on auth_7
    weak_authentication_on auth_8
end goal

environment()
```

Fig. 7. (*continued*).

respectively; thus, leading to integrating cross-hospital diagnosis and enhancing research precision. Even the patient occurs the emergency situation, the first responder is able to access the his/her EHR smoothly. Aside from complying with HIPAA regulations and cybersecurity framework to share medical data, simulation results have demonstrated that medical blockchain can be implemented in current hospital devices to achieve the practicability. Moreover, we simulate the formal verification tool, AVISPA, to prove the robustness of our proposed mechanism. In the future work, we focus on access control of EHRs to achieve a more feasible data management, including partial-grant, full-grant, and proxy-grant of medical data.

CRediT authorship contribution statement

Jung-San Lee: Conceptualization, Data curation. **Chit-Jie Chew:** Formal analysis, Investigation. **Jo-Yun Liu:** Visualization. **Ying-Chin**



(A) Typed model

```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/dig.if

GOAL
 As Specified

BACKEND
 CL-AtSe

STATISTICS

 Analysed   : 3 states
 Reachable  : 2 states
 Translation: 0.00 seconds
 Computation: 0.00 seconds
```

(B) Un-typed model

```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 UNTYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/dig.if

GOAL
 As Specified

BACKEND
 CL-AtSe

STATISTICS

 Analysed   : 8 states
 Reachable  : 6 states
 Translation: 0.00 seconds
 Computation: 0.09 seconds
```

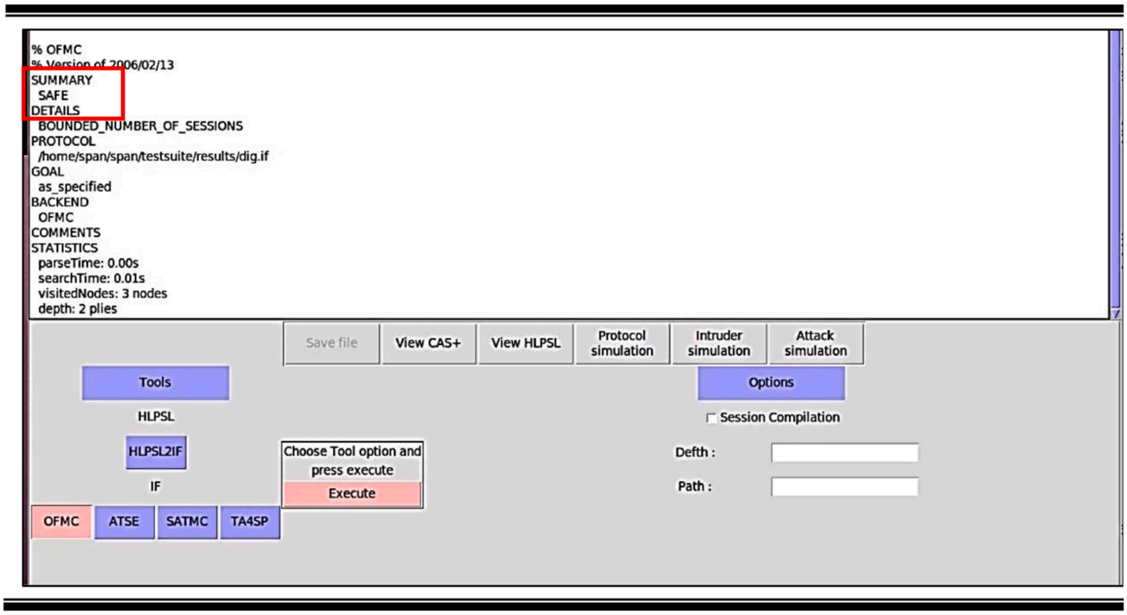
(C) Verbose mode

```
 AtSe Summary
----------------

 Protocol file: /home/span/span/testsuite/results/dig.if
 Attack found : NO
 Analysed   : 3 states
 Reachable  : 2 states
 Translation: 0.00 seconds
 Computation: 0.00 seconds


-------------------------------------------
        Internal System State
 (initial state after reading the if file)
-------------------------------------------

Intruder state :
----------------

Intruder Knowledge :  start i h kh ka hca alice
 Unforgeable terms :  kh' ka'


Interpreted protocol specification :
------------------------------------

Role alice played by (alice,4):
| () => {{dummy_nonce.dummy_nonce.dummy_nonce.dummy_nonce}#_(ka')}#_(kh)
|   & Witness(alice.hca.auth_4.dummy_nonce);
|   & Witness(alice.hca.auth_3.dummy_nonce);
|   & Witness(alice.hca.auth_2.dummy_nonce);
|   & Witness(alice.hca.auth_1.dummy_nonce);
|   Build from step_2
```

□ Simplify
□ Untyped model
☑ Verbose mode

Search Algorithm
Depth first
Breadth first

Fig. 8. The effect of CL-ATSE.



```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/dig.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.01s
  visitedNodes: 3 nodes
  depth: 2 plies
```

Fig. 9. The effect of OFMC.

Chen: Writing – original draft. **Kuo-Yu Tsai:** Writing – review & editing.

Declaration of Competing Interest

The authors declare no conflicts of interest.

References

[1] Pan LJ, Fu XT, Cai FF, Meng Y, Zhang CJ. Design a novel electronic medical record system for regional clinics and health centers in China. In: 2016 2nd IEEE International conference on computer and communications; Oct. 2016. p. 38–41.

[2] Zhang XY, Zhang PY. Recent perspectives of electronic medical record systems. Experim Therap Med Apr. 2016:2083–5.

[3] Health insurance portability and accountability act of 1996. 104th Congress, Public Law; 1996. p. 104–91.

[4] Ngxabane M, Cilliers L. A framework for addressing young adults' trust issues concerning mobile access to electronic health records. In: 2020 Conference on information communications technology and society; Mar. 2020. p. 1–6.

[5] Bernardini M, Romeo L, Misericordia P, Frontoni E. Discovering the type 2 diabetes in electronic health records using the sparse balanced support vector machine. IEEE J Biomed Health Inform Jan. 2020;24:235–46.

[6] Lee CD, Ho IJ, Lee WB. A novel key management solution for reinforcing compliance with HIPAA privacy/security regulations. IEEE Trans Inf Technol Biomed Jul. 2011;15:550–6.

[7] Lee WB, Lee CD. A cryptographic key management solution for HIPAA privacy/security regulations. IEEE Trans Inf Technol Biomed Jan. 2008;12(1):34–41.

[8] Ruan HM, Tsai MH, Huang YN, Liao YH, Lei CL. Discovery of de-identification policies considering Re-identification risks and information loss. In: 2015 10th Asia joint conference on information security; May 2015. p. 69–76.

[9] Benitez K, Loukides G, Malin B. Beyond safe harbor: automatic discovery of health information de-identification policy alternatives. In: ACM International health informatics symposium; Jan. 2010. p. 163–72.

[10] Ausanka-crues R. Methods for access control: aAdvances and limitations. 2001. Technical Report of Harvey Mudd CollegeAvailable Online: https://www.cs.hmc.edu/~mike/public_html/courses/security/s06/projects/ryan.pdf.

[11] Liu XF, Zhang YQ, Wang BY, Yan JB. Mona: secure multi-owner data sharing for dynamic groups in the cloud. IEEE Trans Parallel Distrib Syst Jan. 2013;24:1182–91.

[12] Muthukumar KA, Nandhini M. Modified secret sharing algorithm for secured medical data sharing in cloud environment. In: 2016 S International conference on science technology engineering and management; Mar. 2016. p. 67–71.

[13] Zhu ZM, Jiang R. A secure anti-collusion data sharing scheme for dynamic groups in the public cloud. IEEE Trans Parallel Distrib Syst Jan. 2016;27:40–50.

[14] Ganesh SM, Pandi V, Deborah LJ, Bhuiyan MZA. Attacks on the anti-collusion data sharing scheme for dynamic groups in the cloud. In: International conference on security, privacy and anonymity in computation, communication and storage. 10658; Jan. 2017. p. 457–67.

[15] Davis J. Medical data of 33,000 BJC HealthCare patients exposed online for 8 months. Priv Secur Healthc IT News Mar. 2018. Available Online, https://www.healthcareitnews.com/news/medical-data-33000-bjc-healthcare-patients-exposed-online-8-months.

[16] Zheng WL, Zheng ZB, Chen XP, Dai KM, Li PS, Chen RF. NutBaaS: a blockchain-as-a-service platform. IEEE Access Sep. 2019;7:134422–33.

[17] Dinh TTA, Liu R, Zhang MH, Chen G, Ooi BC, Wang J. Untangling blockchain: a data processing view of blockchain systems. IEEE Trans Knowl Data Eng Jan. 2018;30:1366–85.

[18] Szabo N. Formalizing and securing relationships on public networks. First Monday Sep. 1997;2(9).

[19] Fan MC, Zhang XH. Consortium blockchain based data aggregation and regulation mechanism for smart grid. IEEE Access Mar. 2019;7:35929–40.

[20] Khan AS, Rahulamathavan Y, Basutli B, Zheng G, Assadhan B, Lambotharan S. Blockchain-based distributive auction for relay-assisted secure communications. IEEE Access Jul. 2019;7:95555–68.

[21] Salah K, Nizamuddin N, Jayaraman R, Omar M. Blockchain-based soybean traceability in agricultural supply chain. IEEE Access May 2019;7:73295–305.

[22] Bai QH, Zhang WB, Jiang P, Lu X. Research on design principles of elliptic curve public key cryptography and its implementation. In: 2012 International conference on computer science and service system; Aug. 2012. p. 1224–7.

[23] Wutthikarn R, Yan GH. Prototype of blockchain in dental care service application based on hyperledger composer in hyperledger fabric framework. In: 2018 22nd International computer science and engineering conference; Nov. 2018. p. 1–4.

[24] Mehta R, Kapoor N, Sourav S, Shorey R. Decentralised image sharing and copyright protection using blockchain and perceptual hashes. In: 2019 11th International conference on communication systems & networks; Jan. 2019. p. 1–6.

[25] Zichichi M, Contu M, Ferretti S, D'Angelo G. LikeStarter: a smart-contract based social DAO for crowdfunding. In: IEEE INFOCOM 2019 - IEEE conference on computer communications workshops; Apr. 2019. p. 313–8.

[26] Liao DY, Wang XH. Design of a blockchain-based lottery system for smart cities. In: 2017 IEEE 3rd International conference on collaboration and internet computing; Oct. 2017. p. 275–82.

[27] Li B, Lee JS. A cryptographic alternative for preserving PHI in compliance with HIPAA privacy/security regulations. J Comput Apr. 2007:27–36.

[28] Suhaili SB, Watanabe T. Design of high-throughput SHA-256 hash function based on FPGA. In: 2017 6th International conference on electrical engineering and informatics; Nov. 2017. p. 1–6.

[29] Prasser F, Kohlmayer F, Spengler H, Kuhn KA. Scalable and pragmatic method for the safe sharing of high-quality health data. IEEE J Biomed Health Inform Mar. 2018;22(2):611–22.

[30] Zhu ZM, Jiang ZM, Jiang R. The attack on mona: secure multi-owner data sharing for dynamic groups in the cloud. In: 2013 International conference on information science and cloud computing companion; Dec. 2013. p. 213–8.

[31] U.S. Department of Health & Human Services. HIPAA security rule crosswalk to NIST cybersecurity framework. HealthCare.gov; Feb. 2014. Available Online: https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf.

[32] Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for secure EHRs sharing of mobile cloud based e-health systems. IEEE Access May 2019;7:66792–806.

[33] Yang XD, Li T, Xi WT, Chen AJ, Wang CF. A blockchain-assisted verifiable outsourced attribute-based signcryption scheme for EHRs sharing in the cloud. IEEE Access Sep. 2020;8:170713–31.

[34] National Center for Chronic Disease Prevention and Health Promotion. Implementing clinical decision support systems. Center for Disease Control and Prevention; Jun. 2020. Available Online: https://www.cdc.gov/dhdsp/pubs/guid

es/best-practices/clinical-decision-support.htm?fbclid=IwAR05C3iUdlSdOlGvaL0bcLBCirgSw3aL3jBBdxhoMOcqNw-A7l0uL0Lv8BE.

[35] Castro M, Liskov B. Practical Byzantine Fault Tolerance. Proceedings of the third symposium on operating systems design and implementation. New Orleans, USA; Feb. 1999.

[36] European Community under the Information Society Technologies Proframme. Deliverable D2.1: the high level protocol specification language. Automated validation of internet security protocols and applications. Aug. 2003. Available Online: http://www.avispa-project.org/.

[37] Zhang J, Liu H, Ni L. A secure energy-saving communication and encrypted storage model based on RC4 for EHR. IEEE Access Feb. 2020;8:38995–9012.

[38] "45 CFR § 164.312 – Technical safeguards," Legal Information Institute, Available Online: https://www.law.cornell.edu/cfr/text/45/164.312.