Research Article

A Traceable Blockchain-Based Vaccination Record Storage and Sharing System

Jingshou Chen,1 Xiaofeng Chen,2 and Chin-Ling Chen3,4,5

1Department of Infectious Diseases, The First Affiliated Hospital of Xiamen University, Xiamen 361003, China
2School of Electronic Information Science, Fujian Jiangxia University, Fuzhou 35010, China
3School of Information Engineering, Changchun Sci-Tech University, Changchun 130600, China
4School of Computer and Information Engineering, Xiamen University of Technology, Xiamen 361024, China
5Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung 41349, Taiwan

Correspondence should be addressed to Chin-Ling Chen; clc@cyut.edu.tw

Received 3 October 2021; Revised 30 January 2022; Accepted 14 February 2022; Published 9 March 2022

Academic Editor: Ikram Ud Din

Copyright © 2022 Jingshou Chen et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Blockchain technology is essentially a decentralized database maintained by relevant parties and has been widely used in various scenarios such as logistics and finance. In terms of applications in the medical field, it is becoming more and more important because the patient’s symptoms may be related to a certain vaccine. Whether the patient has been vaccinated with this vaccine will lead to different diagnostic results by the doctor. However, in the current vaccination environment of many regions, the vaccination record (VR) can only be kept in the patient’s vaccination booklet, which is easy to lose or destroy. Therefore, the doctor needs to retrieve the patient’s VR through a centralized database maintained by the government, which is time-consuming and will increase the medical risk. This study proposes a traceable blockchain-based vaccination record storage and sharing system. In the proposed system, the patient gets the vaccination at any legal clinic and the VR can be saved accompanied by the signature into the blockchain center, which ensures traceability. When the patient visits the hospital for treatment, the doctor can obtain the detail of the VR from the blockchain center and then make a diagnosis. The security of the proposed system will be protected by the programmed smart contracts. Through mutual authentication, our system can also provide and guarantee data integrity and nonrepudiation. Moreover, the proposed system has resistance to replay and man-in-the-middle attacks, and the performance is good.

1. Introduction

The rapid evolution of information technology is giving more convenience to our daily lives. Electronic health records (EHRs), including medical payment records, medical treatment records, and medical history, are gathered and stored in the private servers of the hospitals [1–5] and now is drawing increasing attention as it contains personal privacy information. For multiple reasons including to improve the quality of services, the traditional paper-based systems have been replaced by the electronic health system for storing and processing EHRs based on a more flexible, more efficient, and more convenient platform.

It should be noticed that nowadays in many regions, vaccination recording is still in a traditional way that is not keeping up with developing technologies. The patient can only be vaccinated in a clinic nearby with a vaccine booklet that records the vaccination. The detail of the vaccination record (VR) is stored in the clinic and will be uploaded into a centralized database maintained by the government. Without the vaccine booklet, the patient cannot tell what vaccine he/she has gotten, not to mention the vaccination time and the detailed information of the vaccination phase. Unfortunately, the vaccine booklet has vulnerability to forgery, alteration, and loss. Furthermore, under the current vaccination system, the patient’s VR is not directly shared between the clinic and the hospital. When the patient visits
the hospital for treatment of a symptom without the vaccine booklet, and the symptom is related to a certain vaccine (for example, varicella-zoster virus), the hospital cannot directly gain the VR from the clinic but needs to retrieve it through the centralized database. The retrieving phase is very time-consuming and will increase the medical risk [6–10]. Therefore, allowing the patients and the doctors to track and retrieve the VR at any time is an important issue that needs to be resolved in the current stage of research.

Meanwhile, the vaccination records (VRs) need to be carefully protected as important privacy information. The centralized database provides a controlled and easy-access solution for maintaining the VRs. However, the security of VRs is bound to be threatened when the failure occurs in the centralized database. Besides, decentralized databases offer another solution for data protection. Compared with the centralized database, the data in the decentralized database are scattered and stored in different places. The collapse of one database will not lead to the failure of all the decentralized databases, so the decentralized databases have better security than the centralized database.

How to provide flexible data sharing is another concern in VRs. Centralized databases store the VRs in one place. Although this is convenient for data management, it virtually imposes a heavy burden on the server. As a result, it is not conducive to rapidly sharing the VRs via centralized databases. Decentralized databases can access its different separated databases through different channels, so they can provide efficient VR sharing.

Blockchain technology is essentially a decentralized database collectively maintained and has been widely employed in various fields [11–15]. As there is no need for third-party trust endorsements, blockchain can create a fully trusted environment between unfamiliar involved parties. Furthermore, it can ensure traceability, irreparable modification, nonrepudiation, and privacy protection through cryptography technology. Therefore, blockchain technology has been seen as a powerful tool to address the above problems in current vaccination recording systems through its attractive features.

Based on the foregoing overview, a blockchain-based vaccination record storage and sharing system is proposed, to provide traceable VRs and support the data sharing of confidential VRs. In our proposed system, the detail of the VR with the signature will be permanently stored in the blockchain center after the vaccination, thereby ensuring the integrity of the data.

In detail, the contributions of our study are listed below.

1. Each role in our blockchain-based vaccination record storage and sharing system is specifically defined. In our method, the traceability and the integrity of VR are guaranteed by blockchain technology.
2. BAN logic is used to identify the identity to provide communication security between two parties.
3. Through the characteristics of the blockchain, our system can resist a variety of attacks, i.e., replay attack and man-in-the-middle attack. Meanwhile, the performance of our system is elaborated by the computation cost, communication cost analysis, and functionality comparison.

The rest of this study is organized as follows. Section 2 reviews related work. In Section 3, the preliminary and security requirements of the proposed system will be briefly introduced. The proposed vaccination record storage and sharing system is described in a detailed way in Section 4. Section 5 and Section 6 show the security and performance analysis of the proposed system, respectively. Section 7 presents our conclusions.

2. Related Works

The massive growth of medical data impels traditional medical data management schemes to expose the defects. To overcome the drawbacks and improve the medical services, some medical systems have been proposed [16–24]. The medical systems applying cloud computing have already shown good performance in storing and processing the EHRs between different medical institutions [16, 17]. However, on the one hand, the current cloud-based systems have no superiority in privacy protection for the EHRs; on the other hand, these systems have not achieved a satisfactory data sharing mechanism. Thus, Xia et al. [18] proposed a blockchain-based system for the effective management and protection of medical records in 2017. The security of the storage data is guaranteed by authenticating user identities and using encryption mechanisms. However, the system had the risk of data leakage during the data sharing process, making the system unsuitable for real-world applications. Zheng et al. [19] designed a medical data sharing scheme that combines blockchain and cloud computing. Their scheme realized the sharing of medical data between participating parties. However, the data receiver does not know the correctness of the received data since the integrity of the received medical data cannot be verified. Xia et al. [20] introduced an electronic medical record sharing scheme based on blockchain. The tamper-resistant feature of the blockchain technology is used in their method to ensure the security of the medical records. However, the patient cannot track their EHRs in real time. Later, Yang et al. [21] suggested a blockchain-based EHR system. Although their system has good compatibility with some existing systems, their system is not efficient because the creation and verification of new blocks are all handled by a single party.

Although some secure medical systems based on electronic medical records (EMRs) have been proposed in the past, there is not much research on the medical system based on VRs [25–28]. In 2021, Hofstetter et al. [25] introduced a strategy to offer vaccinations in nonprimary care settings such as schools, hospitals, and pharmacies. However, their method can only be used to solve the restriction in the specific clinic. An electronic vaccination certificate (EVC) is developed to replace traditional vaccination record booklets. Yet, EVC is mainly used to record COVID-19 vaccination. Eisenstadt et al. [26] used the EVC as “Immunity Passport” for COVID-19. They designed a smartphone app that
connects to a centralized database that can store patients’ vaccination status. Based on that record, the app generates a token or QR (“quick response”) code signifying the vaccination status, which can then be verified by authorized parties. The EVC faces two significant challenges: interoperability and privacy [28]. Since the EVC standards established in different places are not uniform, how to realize cross-regional EVC recognition is important for the broad and easy usability of digital vaccination certificates. Data privacy is important for user trust and legal compliance making it the de facto crucial challenge than interoperability.

Based on the existing analysis of research scholars, it is foreseeable that the service quality of the medical systems can be further facilitated with the combination of blockchain technology. On the other side, it cannot be ignored that blockchain-based medical systems still have flaws in the privacy protection of data storage and sharing. Particularly, the electrification of VRs is still under development. How to allow patients to track and grasp their VRs meanwhile realizing the sharing of vaccine records between different institutions is an urgent problem to be solved. These issues are exactly the concerns of this study. In our proposed traceable blockchain-based vaccination record storage and sharing system, every VR is stored in the blockchain through the smart contract and granted secure data sharing in the future. It is visible that our scheme shows the way to fill the gaps of existing research.

3. Preliminary and Security Requirements

In this section, the preliminary requirements, including the BAN logic, ECDSA, and the smart contract, are elaborated in subsection 3.1. Subsection 3.2 shows the security requirements of the proposed scheme.

3.1. Preliminary

3.1.1. BAN Logic. The Burrows-Abadi-Needham (BAN) logic proof model [29] is widely applied in security-related scholars for proving whether the mutual authentication has been achieved of a protocol or scheme.

3.1.2. ECDSA. To guarantee the security of the transmitted and exchanged message in the digital network, several encryption systems have been proposed by scholars. The elliptic curve digital signature algorithm (ECDSA), derived from the digital signature algorithm (DSA) [30], involves the concept of elliptic curve cryptography (ECC) [31]. While compared to DSA, the ECC reduces the key size in the algorithm and also provides a faster calculation speed.

3.1.3. Smart Contract. The smart contract [32] is a computer protocol designed to spread, verify, and execute a contract in a digital form. The promised agreement between each contract participant can be executed on it. The collaboration and trust between each contract participant can be achieved in blockchain through smart contracts, which can expand the cooperation between each party.

With the development of medical technology, a large amount of information about patients’ vaccination records, medical histories, and medical payment records needs to be reserved. These records are not only stored in the local server but also permanently conserved in the blockchain by the smart contracts. When a patient visits different medical institutions, he/she can authorize medical staff to retrieve the history VR from the BC through the smart contract. Thus, the medical staff can provide better health services with the help of historical medical records.

3.2. Security Requirements. The security requirements of our vaccination record storage and sharing system are listed as follows.

(1) Mutual authentication: in a proposed system, each party must confirm the legal identity of other parties in every phase. If any two parties can confirm one another’s legal identity, then mutual authentication is achieved.

(2) Data integrity: in an insecure network environment, the message delivered from the sender may be modified by a malicious attacker. Thus, the integrity of the transferred message must be maintained and should be ensured that it can defend against tampering during the transmission.

(3) Nonrepudiation: in each information exchange phase, the sender cannot refuse to acknowledge that the message he has been sent. A secure system must achieve nonrepudiation requirements.

(4) Resisting replay attacks: the communication between two parties may be intervened by malicious attackers. The malicious attackers will pretend to be a legitimate sender and send identical information to the intended receiver. This situation will lead to the leak of personal data security and, therefore, must be prevented.

(5) Resisting man-in-the-middle attacks: the attacker may intercept the message communicated between the sender and the receiver, and then, he/she can obtain the content of the message in the middle. This situation must be prevented too.

4. Proposed Scheme

In this section, we introduce the construction and workflow of our system in detail. The system framework is shown first. Then, the meaning of some notations is elaborated as follows.

4.1. System Framework. This study proposes a blockchain-based vaccination record storage and sharing system. Figure 1 shows the main architecture of the proposed system, which is composed of four parties, including the blockchain center, the patient, the clinic, and the hospital. The detail of each party is described below.
Blockchain center (BC): The blockchain center is owned by the government. It manages all relevant data and operations on personal mobile devices and medical devices of the clinics and the hospitals. All mobile devices and medical devices need to be registered in the BC, and then, the three parties can mutually authenticate each other.

Patient: Each patient carries a personal mobile device with them. The device stores a verification message that can uniquely identify the patient. Moreover, the primary message of the VR will be reserved in the personal mobile device and will be provided to the hospital in the future to diagnose.

Clinic: The patient will be vaccinated at the clinic. The doctor of the clinic uses a medical device that can uniquely identify the clinic. When the patient goes to the clinic for vaccination, the doctor of the clinic can execute the vaccination for the patient and store the VR into the BC. Also, the patient will store the primary message of the VR on his/her mobile device.

Hospital: The patient will be diagnosed in the hospital. The doctor of the hospital uses a medical device that can uniquely identify the hospital’s identification. When the patient goes to the hospital seeking treatment for a symptom, the doctor of the hospital can retrieve the VRs through the primary message of the VR stored in the patient mobile device and further provide the diagnosis for the patient.

The following is a description of our method. It should be noticed that all parties must register their corresponding devices in the BC and retrieve a unique ID and a private and public key pair from BC, respectively.

Step 1: The patient goes to the clinic with his/her mobile device for vaccination, and the clinic and the patient must authenticate one another’s identity first. After mutual authentication, the doctor of the clinic will carry out the vaccination for the patient.

Step 2: The doctor of the clinic will save the VR in the local server of the clinic and store VR into the BC through the smart contract technology.

Step 3: The BC feedbacks the storage result to the clinic.

Step 4: The doctor of the clinic returns the primary message of the VR to the patient, and the patient saves the message on his/her mobile device.

Step 5: The patient visits the hospital with his/her mobile device for treatment of a symptom, and the patient must also authenticate each other identity first. After mutual authentication, the patient provides the VR history in his mobile device to the doctor.

Step 6: The doctor of the hospital retrieves the VRs from the BC according to the information acquired from the patient.

Step 7: The BC feedbacks the details of VRs to the hospital.

Step 8: The doctor of the hospital provides the diagnostic results for the patient based on the VRs.

4.2. Notations. The notations used in the study are listed in Table 1.

4.3. Initialization Phase. The fundamental chaincode structure of the proposed scheme is elaborated in this section. Figure 2 shows the information structure of the access parties (APs) and the enumeration of the role type. Figure 3 shows the structure to store the vaccination record in the BC.
struct APInfo{
    string ID;
    string name;
    string detail;
    Roles roleType;
}
string const Roles{
    Patient
    Clinic
    Hospital
}

Step 1. The access party (AP) provides the primary information (i.e., name and role) and sends a registration request to the BC.

Step 2. The BC generates an ECDSA private key \( d_X \) and calculates public key \( Q_X \) by the following:

\[
Q_X = d_X G.
\] (1)

The information provided by the AP needs to be validated by the BC. If it is valid, the algorithm “Registration” will be executed, as shown in Algorithm 1. Then, BC sends \((ID_X,d_X,Q_X)\) to AP.

Step 3. AP stores \((ID_X,d_X,Q_X)\) for signing the signature message.

4.5. Authentication Phase. In this phase, we define the “Sign” and “Verify” functions that implement the ECDSA to achieve identity authentication between User A and User B. The definitions of these two functions are shown in Algorithm 2 and Algorithm 3. When User A and User B exchange messages, the sender generates a signature with a “Sign” function to the receiver. When the receiver receives the message, they execute a “Verify” function to verify. The flowchart of the authentication phase is shown in Figure 5.

Step 4. User A selects a random number \( R_1 \) and calculates \( M_A \) by equation (2). Then, User A calculates \( h_A \) by equation (3).

\[
M_A = (ID_A||ID_B||T_1),
\] (2)

\[
h_A = H(M_A).
\] (3)

The signatures are generated by executing the function “Sign” in Algorithm 2. In detail, User A calculates the parameters of ECDSA by equation (4) and generates the signatures by equations (5) and (6). Then, User A encrypted \( M_A \) with User B’s public key by equation (7) and sends \((ID_A,ID_B,C_A,(r_A,s_A))\) to User B.

\[
(x_A,y_A) = R_1 G,
\] (4)

\[
r_A = x_A \mod n,
\] (5)

\[
s_A = x_A^{-1} (h_A + r_A d_A) \mod n,
\] (6)

\[
C_A = EPKB(M_A).
\] (7)

Step 5. User B receives the message at \( T_2 \) and decrypts \( C_A \) with its private key by the following:

\[
M_A = D_{SK_B}(C_A).
\] (8)

Then, User B validates the timestamp by

\[
(T_2 - T_1) \leq \tau?.
\] (9)

If it is valid, User B executes the function “Verify” in Algorithm 3 to validate the signature of User A. In detail, User B calculates the parameters by equations (10)–(13) and validates the signatures by equation (14).
\[ h'_A = H(M_A), \] (10) 
\[ u_1 = h'_A s_A^{-1} \mod n, \] (11) 
\[ u_2 = r_A s_A^{-1} \mod n, \] (12) 
\[ (x'_B, y'_B) = u_1 G + u_2 Q_A, \] (13) 
\[ x_B = r_A \mod n. \] (14) 

If it is valid, User B selects a random number \( R_2 \) and calculates \( M_B \) by equation (15). Then, User B calculates \( h_B \) by equation (16).

\[ M_B = (ID_A||ID_A||T_3), \] (15) 
\[ h_B = H(M_B). \] (16) 

The signatures are generated by executing the function “Sign” in Algorithm 2. In detail, User B calculates the parameters of ECDSA by equation (17) and generates the signatures by equations (18) and (19). Then, User B encrypted \( M_B \) with User A’s public key by equation (20) and sends \( (ID_B, ID_A, C_B, (r_B, s_B)) \) to User A.

\[ (x'_B, y'_B) = R_2 G, \] (17) 
\[ r_B = x_A \mod n, \] (18) 
\[ s_B = x_B^{-1} (h_B + r_B d_B) \mod n, \] (19) 
\[ C_B = E_{PK_A}(M_B). \] (20) 

Step 6. User A receives the message at \( T_4 \) and decrypts \( C_B \) with its private key by the following:

\[ M_B = D_{SK_A}(C_B). \] (21) 

Then, User A validates the timestamp by the following:

\[ T_4 - T_3 < \tau? \] (22) 

If it is valid, User A executes the function “Verify” in Algorithm 3 to validate the signature of User B. In detail, User A calculates the parameters by equations (23)–(26) and validates the signatures by equation (27).

\[ h'_B = H(M_B), \] (23) 
\[ u_1 = h'_B s_B^{-1} \mod n, \] (24) 
\[ u_2 = r_B s_B^{-1} \mod n, \] (25) 
\[ (x'_B, y'_B) = u_1 G + u_2 Q_B, \] (26) 
\[ x_B = r_B \mod n. \] (27) 

4.6. Patient Vaccination Phase. The patient can visit any clinic that has registered in BC for vaccination. After the mutual authentication, the patient issues the clinic the name
of the vaccination and gets the vaccination. The vaccine record will be saved in the mobile device of the patient and the local server of the clinic. Meanwhile, the signature of the patient and the clinic, and the hash value of the record accompanied by the identities of the patient, clinic, and vaccine will be stored in BC.

**Figure 5:** The flowchart of the authentication phase.

**Algorithm 2:** The smart contract Sign

```plaintext
function Sign (string h, string R, Roles d) public returns (string r, string s)
(x, y) = R * G
r = x % n
s = (h + r * d)/x%n
return r, s
```

**Step 7.** The patient selects a random number \( R_3 \) and calculates \( M_P \) with the name of the vaccination, \( V \), by equation (28). Then, the patient calculates \( h_P \) by equation (29).

\[
M_P = (ID_A || ID_B || ID_C || V || T_3),
\]  
\[
h_P = H(M_P).
\]
The signatures \((r_{p}, s_{p})\) are generated by executing the function “Sign” in Algorithm 2, as shown in the following:

\[
(r_{p}, s_{p}) = \text{Sign}(h_{p}, R_{3}, d_{p}).
\]  

(30)

Then, the patient encrypted \(M_{p}\) with the public key of the clinic by equation (31) and sends \((ID_{P}, ID_{C}, C_{p}, (r_{p}, s_{p}))\) to the clinic.

\[
C_{p} = E_{PK_{C}}(M_{p}).
\]  

(31)

**Step 8.** The clinic receives the message at \(T_{6}\) and decrypts \(C_{p}\) with its private key by the following:

\[
M_{p} = D_{SK_{p}}(C_{p}).
\]  

(32)

Then, the clinic validates the timestamp by the following:

\[
(T_{6} - T_{5}) \leq \tau?.
\]  

(33)

If it is valid, the clinic calculates \(h'_{c}\) and executes the function “Verify” in Algorithm 3 to validate the signature of the patient by equations (34) and (35).

\[
h'_{c} = H(M_{p})
\]  

(34)

\[
\text{Verify}(h'_{c}, r_{p}, s_{p}).
\]  

(35)

If the signature is valid, the clinic executes the vaccination for the patient and generates the vaccination record, \(VR\), including \(ID_{P}, ID_{V}\) (the identity of the vaccination \(V\)), \(ID_{C}\), the time of the vaccination, and other detailed information. At the same time, the primary message of \(VR\), denoted as \(K_{VR}\), is generated and delivered to the patient.
Next, the clinic selects a random number $R_4$ and calculates $M_C$ with VR by equation (36). Then, the clinic calculates $h_C$ by equation (37):

$$M_C = (ID_C||ID_P||K_{VR}||T_7), \quad (36)$$
$$h_C = H(M_C). \quad (37)$$

The signatures $(r_C, s_C)$ are generated by executing the function “Sign” in Algorithm 2, as shown in the following:

$$(r_C, s_C) = \text{Sign}(h_C, R_4, d_C). \quad (38)$$

The algorithm “RIns” is triggered to create a record stored in BC, the algorithm of which is shown in Algorithm 4. The record includes the signature of the patient and the clinic.

Finally, the clinic encrypted $M_C$ by the public key of the patient by equation (39) and sends $(ID_C, ID_P, C_C, (r_C, s_C))$ to the patient.

$$C_C = E_{PK_P}(M_C). \quad (39)$$

**Step 9.** The patient receives the message at $T_8$ and decrypts $C_C$ with its private key by the following:

$$M_C = D_{SK_P}(C_C). \quad (40)$$

Then, the patient validates the timestamp by the following:

$$(T_8 - T_7) \leq \tau? \quad (41)$$

If it is valid, the patient calculates and executes the function "Verify" in Algorithm 3 to validate the signature of the clinic by equations (42) and (43).

$$h_C' = H(M_C), \quad (42)$$
$$\text{Verify}(h_C', r_C, s_C). \quad (43)$$

If the signature is valid, the patient stores the $K_{VR}$ on his/her mobile device.

**Step 10.** The patient selects a random number $R_5$ and calculates $M_{P2}$ with the symptom, $S$, by equation (44). Then, the patient calculates $h_{P2}$ by equation (45).

$$M_{P2} = (ID_P||ID_H||S||K_{VR}||T_9), \quad (44)$$
$$h_{P2} = H(M_{P2}). \quad (45)$$

The signatures $(r_{P2}, s_{P2})$ are generated by executing the function “Sign” in Algorithm 2, as shown in the following:

$$(r_{P2}, s_{P2}) = \text{Sign}(h_{P2}, R_5, d_P). \quad (46)$$

Then, the patient encrypted $M_{P2}$ with the public key of the hospital by equation (47) and sends $(ID_P, ID_H, C_{P2}, (r_{P2}, s_{P2}))$ to the hospital.

$$C_{P2} = E_{PK_H}(M_{P2}). \quad (47)$$

**Step 11.** The hospital receives the message at $T_{10}$ and decrypts $C_{P2}$ with its private key by the following:

$$M_{P2} = D_{SK_H}(C_{P2}). \quad (48)$$

Then, the hospital validates the timestamp by the following:

$$(T_{10} - T_9) \leq \tau? \quad (49)$$

If it is valid, the hospital calculates and executes the function “Verify” in Algorithm 3 to validate the signature of the patient by equations (50) and (51).

$$h_{P2}' = H(M_{P2}), \quad (50)$$
$$\text{Verify}(h_{P2}', r_{P2}, s_{P2}). \quad (51)$$

If the signature is valid, the algorithm “RGet” is triggered to retrieve the VR. The definition of “RGet” is shown in Algorithm 5. Since the records contain the signatures of the patients and the clinics, it is convenient to track the validation of the record.

Next, the hospital selects a random number $R_6$ and calculates $M_H$ with the diagnostic result of the patient, $D$, by equation (52). Then, the hospital calculates $h_H$ by equation (53).

$$M_H = (ID_H||ID_P||D||T_{11}), \quad (52)$$
$$h_H = H(M_H). \quad (53)$$

The signatures $(r_{H}, s_{H})$ are generated by executing the function “Sign” in Algorithm 2, as shown in the following:

$$(r_{H}, s_{H}) = \text{Sign}(h_H, R_6, d_H). \quad (54)$$

Finally, the hospital encrypted $M_H$ by the public key of the patient by equation (55) and sends $(ID_H, ID_P, C_H, (r_{H}, s_{H}))$ to the patient.

$$C_H = E_{PK_P}(M_H). \quad (55)$$

**Step 12.** The patient receives the message at $T_{12}$ and decrypts $C_H$ with its private key by the following:
function RIns (string pID, string cID, string vID, string time, string p_Signature, string c_Signature) public {
    Record record = new Record()
    record.patientId = pID
    record.clinicId = cID
    record.vaccineId = vID
    record.time = time
    record.p_Signature = p_Signature
    record.c_Signature = c_Signature
    records.append(record)
}

function RGet (string pID, string vID) public return Record record {
    for (Record record in records) {
        if (record.patientId == pID && record.vaccineId == vID) {
            return record
        }
    }
    return null
}

Algorithm 4: The algorithm RIns

Algorithm 5: The algorithm RGet.
Journal of Healthcare Engineering

\[ M_H = D_{SK_p}(C_H). \]

Then, the patient validates the timestamp by the following:

\[ (T_{12} - T_{11}) < \tau'. \]

If it is valid, the patient calculates and executes the function "Verify" in Algorithm 3 to validate the signature of the hospital by equations (58) and (59).

\[ h_{11}^H = H(M_H), \] \hspace{1cm} (58)

\[ \text{Verify}(h_{11}^H, r_{11}, s_{11}). \] \hspace{1cm} (59)

If the signature is valid, the patient stores the D in his/her mobile device.

5. Security Analysis

We will analyze the security of our system in terms of the following aspects.

5.1. Mutual Authentication. In this section, we use the BAN logic proof model to prove that mutual authentication in the authentication phase is guaranteed in our proposed system. The common notations used in the BAN logic are described in Table 2.

To achieve mutual authentication, the following goals should be satisfied, as shown in Table 3.

The messages delivered between User A and User B are listed in Table 4.

To achieve the goals, the assumptions are made as shown in Table 5.

Based on the rules of BAN logic and these assumptions, the proof of the patient vaccination phase is as follows:

(a) User B authenticates User A.

Statement S1 can be derived from M1 and the seeing rule.

\[ S1. \quad \text{B} \otimes (ID_A, ID_B, T_1, PK_A, r_A, s_A) \]

Statement S2 can be derived from A2 and the freshness rule.

\[ S2. \quad B \equiv A \otimes (ID_A, ID_B, T_1, PK_A, r_A, s_A) \]

Statement S3 can be derived from S1, A4, and the message meaning rule.

\[ S3. \quad B \equiv A \otimes (ID_A, ID_B, T_1, PK_A, r_A, s_A) \]

Statement S4 can be derived from S2, S3, and the nonce verification rule.

\[ S4. \quad B \equiv A \otimes (ID_A, ID_B, T_1, PK_A, r_A, s_A) \]

Statement S5 can be derived from S4 and the belief rule.

\[ S5 \quad (G4) \quad B \equiv A \equiv A \xrightarrow{x_B} B \]

Statement S6 can be derived from S5, A6, and the jurisdiction rule.

\[ S6 \quad (G3) \quad B \equiv A \xrightarrow{s_B} B \]

Statement S7 can be derived from S3 and the belief rule.

\[ S7 \quad (G8) \quad B \equiv A \equiv ID_A \]

(b) User A authenticates User B.

Statement S8 can be derived from S7, A8, and the jurisdiction rule.

\[ S8 \quad (G7) \quad B \equiv ID_A \]

5.2. Nonrepudiation. To ensure the nonrepudiation in our proposed scheme, the message sent by the sender must be signed with the secret key of the sender. The receiver can verify the received message with the public key of the sender; therefore, the sender cannot deny sending the message. Table 6 shows the verification equations that need to be verified by the receiver in every phase of the proposed scheme.

5.3. Data Integrity. To ensure the integrity of the message transmitted in each phase, this study applies the ECDSA to generate the signature value with the hash value. As shown in Algorithm 2, the signature s is generated by hash value h. Table 7 lists the signatures in each phase. All the signatures need to be verified by the receiver, as shown in Table 6.
5.4. Resisting Replay Attack. The messages transmitted from the sender have added a sending timestamp and verified whether the timespan is valid in the receiver. The timestamp is added in each phase to resist the replay attack. For example, in the authentication phase, User A adds a timestamp to resist the replay attack will fail. Therefore, the replay attack cannot succeed in our proposed scheme.

5.5. Resisting Man-in-the-Middle Attack. In our method, the message sent by the sender is encrypted by the public key of the receiver. The receiver can decrypt the cipher message with its private key. When a malicious attacker intercepts the cipher message, he/she cannot decrypt without the relevant private key. Therefore, our proposed system can resist the man-in-the-middle attack.

6. Performance Analysis

We analyze the performance of our system in terms of the following aspects.

6.1. Computation Cost. The computation cost is also an important aspect to evaluate the performance of a system. Table 8 elaborates the computation costs of our proposed scheme in each phase for BC, the hospital, the clinic, and the patient. It can be seen from Table 8 that each role has equal computation costs. For example, in the authentication phase, User A needs two symmetric encryption/decryption operations \((T_E)\), two hash function operations \((T_H)\), one subtraction operation \((T_S)\), five multiplication operations \((T_M)\), and three division operations \((T_D)\).

6.2. Communication Cost. Assumed that an ID message required 128 bits, a cipher message required at least 512 bits, a signature message required 1024 bits, and other messages, like timestamp, requires 64 bits. As shown in the patient treatment phase, the patient encrypts the message, which contains 2 IDs, 1 timestamp, and a symptom described by the patient. The length of the symptom is set as 3 other messages, so the length of the cipher message is \(2 \times 128 + 1 \times 64 + 3 \times 64 = 512\) bits.

Taking the patient treatment phase into account, the patient and the hospital will exchange 2 messages, which require 2 IDs, 1 cipher message, and 1 signature operation message. Thus, it requires \((1282 + 5121 + 10241) 2 = 1792\) bits in total. The maximum transmission speed is 14 Mbps, 100 Mbps, and 20 Gbps in a 3.5 G, 4G, and 5 G environment. Thus, the transmission time is only 0.015 ms, 0.002 ms, and 0.01 ms, which reveals that our system can be utilized in various real-time applications. Table 9 lists the communication costs of the proposed scheme in each phase.

6.3. Functionality Comparison. Table 10 shows the functionality comparison of previous schemes and the proposed
scheme. Our proposed scheme has the advantage of providing theoretical proof, solving the nonrepudiation issue, and providing the man-in-the-middle attack resistance.

### 6.4. Limitations

There are some limitations in our system. First, every party must register in the blockchain center (BC) before joining the system. During the registration process, each participant needs to obtain the public key and private key pair of the elliptic curve signature from the BC. Second, the proposed scheme relies on stable power and network for normal operations. Thus, a backup power supply and a secure local network system can be established for the proposed system to prevent system failure.

Overall, the proposed scheme in this study is focused on applying blockchain technology to solve the storage and

---

**Table 6: Nonrepudiation of the proposed scheme.**

<table>
<thead>
<tr>
<th>Phases</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication phase</td>
<td>User A: User B:</td>
</tr>
<tr>
<td>Patient vaccination</td>
<td>Patient: Clinic:</td>
</tr>
<tr>
<td>Patient treatment</td>
<td>Hospital: Patient:</td>
</tr>
</tbody>
</table>

**Table 7: Data integrity of the proposed scheme.**

<table>
<thead>
<tr>
<th>Phases</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication phase</td>
<td>User A: User B:</td>
</tr>
<tr>
<td>Patient vaccination</td>
<td>Patient: Clinic:</td>
</tr>
<tr>
<td>Patient treatment</td>
<td>Hospital: Patient:</td>
</tr>
</tbody>
</table>

**Table 8: The computation costs of the proposed scheme.**

<table>
<thead>
<tr>
<th>Phase</th>
<th>Role 1</th>
<th>Role 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>User A:</td>
<td>User B:</td>
</tr>
<tr>
<td>Patient vaccination</td>
<td>Clinic:</td>
<td>Patient:</td>
</tr>
<tr>
<td>Patient treatment</td>
<td>Hospital:</td>
<td>Patient:</td>
</tr>
</tbody>
</table>

**Table 9: The communication costs of the proposed scheme.**

<table>
<thead>
<tr>
<th>Phase</th>
<th>Message length (bits)</th>
<th>3.5 G (ms)</th>
<th>4 G (ms)</th>
<th>5 G (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>1792</td>
<td>0.015</td>
<td>0.002</td>
<td>0.01 us</td>
</tr>
<tr>
<td>Patient vaccination</td>
<td>1792</td>
<td>0.015</td>
<td>0.002</td>
<td>0.01 us</td>
</tr>
<tr>
<td>Patient treatment</td>
<td>1792</td>
<td>0.015</td>
<td>0.002</td>
<td>0.01 us</td>
</tr>
</tbody>
</table>

**Table 10: The functionality comparison of previous schemes and the proposed scheme.**

<table>
<thead>
<tr>
<th>Scheme functionality</th>
<th>Xu et al. [17]</th>
<th>Liu et al. [22]</th>
<th>Xu et al. [23]</th>
<th>Our scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet of things (IoTs)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Blockchain architecture</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mutual authentication</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Data integrity</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Resistance to replay attack</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Resistance to man-in-the-middle attack</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Nonrepudiation</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Theoretical proof</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
sharing for VR. Some potential problems are not comprehensively considered, for example, the unpopularity or slow speed of the internet environment.

7. Conclusions

This study discusses the problems that occurred in the application of the vaccination record (VR) in reality and proposes a blockchain-based vaccination record storage and sharing system. The integrity of the VR and the privacy protection problems are solved by using blockchain technologies. The security of our system was analyzed such as mutual authentication, nonrepudiation, and data integrity. Moreover, our method can resist replay attacks and man-in-the-middle attacks. In particular, we use BAN logic to prove identity legality such that communication security is guaranteed between two parties. Not merely the computational and communication costs are quite low, the proposed method can save time and avoid medical risks than the current medical system.

In the next work, we hope to improve the proposed system using artificial intelligence (AI) and deep learning techniques, which will be used to store VR in different formats and enable efficient VR search.

Data Availability

The data supporting this study are available within the article.

Conflicts of Interest

The authors declare no conflicts of interest.

References


