An Efficient Anonymous Authentication Scheme for Medical Services Based on Blockchain

Shu Wu, Guangyu Peng, Ya Gao and Jindou Chen
An Efficient Anonymous Authentication Scheme for Medical Services Based on Blockchain

Shu Wu · Guangyu Peng · Ya Gao · Jindou Chen

Abstract Telemedicine is one of the most rapidly developing areas of health care in recent years. Telemedicine Information Systems (TMIS) enable physicians to provide remote care over the Internet to registered patients anywhere. In this work, we propose an efficient anonymous authentication scheme between patients and medical servers. We combine blockchain technology with biometric technology to form a shared session secret key to protect the privacy of patients through mutual authentication between patients and servers. Comprehensive comparative measurement shows that our proposed scheme achieves a better experimental performance in both computation and communication efficiencies.

Keywords Mutual authentication · privacy protection · shared secret key · consortium blockchain

1 Introduction

With the development of the Internet, electronic medical service has been integrated into people’s daily life [1], bringing great convenience to medical treatment. In the mobile wireless network, patients can complete various medical services such as registration via smart terminals, instead of going to the hospital. It greatly saves patient’s time and money. However, due to massive devices in the Internet of Things and the openness of mobile networks, patients are facing privacy leakage and network attacks while enjoying the convenience of electronic medical services [2].

Accordingly, how to protect privacy has become a major issue in the medical internet of things. Wang [3] demonstrates that authentication technology is usually used to achieve a high-level privacy protection scheme. However, it is often believed that servers are centralized, honest, and curious [4]. Although the centralized “client-server” model can fulfill the patient’s identity authentication, centralization brings various privacy and security challenges [5, 6]. How to achieve effective authentication between patients and medical servers while protecting privacy is a worthwhile studying question.

In recent years, the research of blockchain has attracted more and more attentions. Blockchain technology offers a potential approach to privacy protection, especially in medical field, the internet of vehicles, and smart grid, etc. [11, 12]. Unfortunately, there are little researches on efficient authentication scheme for medical field based on blockchain currently. Therefore, we propose an efficient anonymous authentication scheme based on consortium blockchain. The main contributions of this article are as follows:

– We propose a framework for anonymous mutual authentication protocol with security and privacy preservation based on consortium blockchain to improve patient diagnostic services in e-Health system.
– We design the concrete implementation steps for authentication protocol. We combine blockchain and fuzzy extraction technology for our certification scheme. The secret key can be shared between the patient and the server when mutual authentication is completed.
– We present an efficient key agreement with anonymous certification. Anonymous authentication of pa-
patients can protect the privacy of patients well. What’s more, the authentication scheme is lightweight and does not take up too much computing resource.

The remaining part of this paper is organized as follows: An overview about existing works related to our research is described in section 2. Preliminaries are presented in section 3. Section 4 describes the system model. Afterwards, section 5 describes the details of the protocol. In addition, we do security analysis in section 6. Furthermore, we compare the computational overhead and communication overhead with comparative approaches in section 7. Finally, section 8 concludes this work.

2 Related Work

The blockchain is a shared distributed ledger that records network transaction information of peer-to-peer devices. The ledger in the network will keep a copy between the member nodes. The transaction between peer nodes will be permanently recorded in the block. Therefore, blockchain technology can ensure the confidentiality, integrity and non-tampering of data.

Recently, Ekblaw[13] proposed an electronic medical record management system, which uses blockchain to ensure the accuracy of medical records. However, the protocol does not specify the access control strategy for data access. It may lead to the exposure of medical record information. In [14], Wang et al. gave an authentication protocol based blockchain for user identity management, but [15] pointed out that the computation cost of [14] is more higher. Siyal[16] analyzed the challenges faced by blockchain in the medical field, they believed that electronic medical records could be verified when using blockchain without third-party verification, but [16] could not guarantee the reliability of data. It would lead to the decline of data availability.

In addition, Yaz [18] proposed a novel decentralized authentication of patients in a distributed hospital network. However, the approach of [18] is decentralized. It was designed for IoT devices with limited computational, memory and energy capabilities. Nevertheless, [18] did not involve that how to implement a prototype of the proposed approach in a real-world setting. In[19], Fan et al. proposed a verifiable scheme to achieve one-to-many data sharing via blockchain. The blockchain data is maintained by users, but it is difficult to determine the consortium blockchain members. Recently, Zhang et al. in [20] proposed a transaction processing scheme for IoT consortium blockchain adaptively with IoT applications, which is proved to achieve anonymous, traceability, and non-frameability.

The existing works provided a variety of frameworks for patient and medical server authentication. In fact, most of them only achieved a compromise between data security and computational complexity. In addition, these authentication schemes rarely used blockchain technology to ensure the privacy of data. In this work, we design an efficient anonymous authentication scheme based on the consortium blockchain, in which the secret key is shared between the patient and the server.

3 Preliminaries

3.1 Blockchain technology

Blockchain is a collection of data elements. Elements in the collection are called blocks. All the blocks form a chain in order. Blockchain has the characteristics of distribution, decentralization, and trustiness. The blockchain system can be divided into three subtypes: public blockchain, private blockchain, and consortium blockchain.

Our scheme is mainly related to a consortium blockchain, which is composed of a registry and multiple servers in a medical organization. It is important to note that not every entity can participate in the consensus process of the consortium blockchain. Only the members of the consortium blockchain can access the data on the blockchain. So it is confidential except for consortium blockchain members.

3.2 Fuzzy extraction technique

Fuzzy extraction technology consists of two algorithms: Key generation algorithm and Key recovery algorithm.

Definition 1. Key generation algorithm.

\[ Gen(): (SP, PP) = Gen(BIO_i), \]

The output is the patient’s biometrics \( BIO_i \). The input is a random string \( SP \in \{0, 1\}^n \) and auxiliary string \( PP \in \{0, 1\}^* \).

Definition 2. Key recovery algorithm.

\[ Rep(): (SP) = Rep(BIO'_i, PP), \]

The input is the patient’s biometrics \( BIO'_i \) and auxiliary string \( PP \in \{0, 1\}^* \). The output is a random string \( SP \in \{0, 1\}^n \) when the difference between the biometric and the reinput is less than the threshold.

4 System model and Security requirements

In this section, we describe system architecture and security requirements of the system model. The system architecture is shown in Fig.1.
Table 1 Symbols And Description

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gen():</td>
<td>Key generation algorithm</td>
<td>Rep():</td>
<td>Key recovery algorithm</td>
</tr>
<tr>
<td>SP :</td>
<td>Random string</td>
<td>A_i :</td>
<td>Hash mapping of user’s personal information</td>
</tr>
<tr>
<td></td>
<td>Biometric information of the patient i</td>
<td>G :</td>
<td>The set of points on the additive</td>
</tr>
<tr>
<td>PP :</td>
<td>Auxiliary string</td>
<td>m :</td>
<td>A nonce selected by RC</td>
</tr>
<tr>
<td>ID_i :</td>
<td>The identity of the patient i</td>
<td>V_u :</td>
<td>A intermediate parameters</td>
</tr>
<tr>
<td>PW_i :</td>
<td>The key entered by the patient i</td>
<td>AID_i :</td>
<td>The anonymous identity of patient i</td>
</tr>
<tr>
<td>m_i :</td>
<td>A secret number selected by patient i</td>
<td>k_{ij}, k_{ji} :</td>
<td>A shared key between patient i and server j</td>
</tr>
</tbody>
</table>

Fig. 1 System Model.

4.1 System architecture

**Patient:** A patient provides identity information, personal password, and biometric information (e.g. face image information collected through smart terminals). Whereafter, the patient registers at the RC and servers respectively.

**Smart terminal:** The smart terminal can collect the patient’s password, biometric information, and identity information. They are sent to RC subsequently. It’s worth noting that the smart terminal only can be authenticated by the server after being registered with the RC.

**Registration center (RC):** The RC receives request information from a smart terminal. It invokes a smart contract to check whether the user is legitimate or not. RC grants the user registration when the user’s identity meets the registration criteria.

**Servers:** The server needs to complete the authentication for users. This is a two-way authentication process. After the two-way authentication of the server and the smart terminal is completed, a session key will be formed between the two sides.

**Blockchain:** Blockchain can guarantee the immutability and integrity of data. In details, patients upload their anonymous and real identities to the blockchain. The server compares that whether the user’s real identity is tampered with by the attacker. Members of the consortium blockchain include RC and servers.

4.2 Security requirements

In this subsection, security requirements are described as follows:

- **Data confidentiality and integrity.** Attacker cannot recover the shared key from the intercepted message. The key can guarantee the confidentiality of the patient’s data. What’s more, blockchain can ensure that the data uploaded to the ledger will not be tampered with, which could protect the integrity of the data.

- **Effective anonymous privacy protection.** Attacker cannot deduce the patient’s identity information from the anonymous information. In addition, blockchain can protect the privacy of data well.

5 Proposed protocol and Security analysis

5.1 Protocol description

The proposed protocol contains three process: System setup phase, Registration phase, and Authentication phase. Table 1 shows some of the parameters used in our protocol.

**Phase1: System setup phase**

*Step1:* $G_1$ is an additive cyclic group of points on an elliptic curve. The order of the cyclic group $G_1$ is prime $q$. $Z_q^*$ is a reduced residue systems modulo $q$ and $a, b \in Z_q^*$.

*Step2:* RC selects four secure hash functions $h_1 : \{0, 1\}^* \rightarrow Z_q^*$, $h_2 : G_1 \rightarrow \{0, 1\}^*$, $h_3 : \{0, 1\}^* \rightarrow Z_q^*$, $h_4 : \{0, 1\}^* \rightarrow Z_q^*$. Then RC announces initialization public parameters as $\{G_1, a, b, q, h_1, h_2, h_3, h_4\}$.

**Phase2: Registration phase**
**Step 1:** The patient $i$ enters personal information such as $ID_i$, $PW_i$, $BIO_i$ on the smart terminal. Smart terminal sends $Me_1 = \{ID_i, PW_i, BIO_i\}$ to RC via a secure channel. If the user’s $ID_i$ is valid, RC will authorize the patient’s identity.

**Step 2:** RC calculates the following parameters, where $BIO_i$ is the input of the fuzzy extraction function and $(PP, SP)$ is the output of the fuzzy extraction function.

$$(SP, PP) = Gen(BIO_i)$$

$A_i = h_1 (ID_i \| PW_i \| m\rangle)

$B_i = h_1 (A_i)

$AID_i = B_i \oplus PP$

$V_u = h_1 ((ID_i \| PW_i) \oplus BIO_i)$

**Step 3:** RC invokes the smart contract to query whether $AID_i$ is on the blockchain. If $AID_i$ doesn’t exist on the blockchain, RC will do three operations in parallel as follows.

First, RC invokes the smart contract. The smart contract adds $AID_i$ to a registerable list and uploads $(ID_i, AID_i)$ to the consortium blockchain. Second, RC sends $Me_3 = \{AID_i \| SP \| PP \| V_u\}$ to the patient $i$ via a secure channel. Third, RC keeps the mapping table of $(ID_i, A_i, AID_i)$ in its own database.

Otherwise it can directly enter the authentication phase.

**Phase 3: Authentication phase**

**Step 1:** The patient enters identity $ID_i'$, password $PW_i'$, and biological characteristics $BIO_i'$ on the smart terminal. Meanwhile, the smart terminal calculates the following equation:

$V_u' = h((ID_i' \| PW_i') \oplus BIO_i')$

Subsequently, it checks the following equation:

$h((ID_i) \oplus V_u \oplus V_u') = h((ID_i') \oplus V_u \oplus V_u')$

If the equation is not valid, the smart terminal refuses the patient. Otherwise it proceeds to the next step.

**Step 2:** The patient selects a random number $m_i \in Z_q^*$ by the smart terminal and keeps the nonce $m_i$ secretly. The smart terminal calculates $M_1, M_2$ as follow:

$M_1 = SP \oplus m_i P$

$M_2 = h_2(m_i P \| ID_i \| T_i)$

Then it sends $Me_5 = \{AID_i', M_1, M_2, PP, BIO_i', T_i\}$ as authentication information requested for the server.

**Step 3:** Once the server receives the patient’s authentication message. Firstly it checks $|T_1 - T_2| < \Delta T$, where $T_2$ is the current timestamp. If it does not hold, it will be terminated. Otherwise, the server uses $BIO_i'$ and $PP$ to recover a random string $SP$, where $BIO_i'$ is entered by the patient $i$. The server can obtain $m_i P$ as follow:

$SP = RCrypt(BIO_i', PP)$

$m_i P = M_1 \oplus SP$

Secondly, the server invokes the smart contract to download $ID_i$ according to $AID_i'$ from the blockchain. Afterwards, the server checks the following equation:

$M_2 = h_2(m_i P \| ID_i \| T_1)$

If the equation does not hold, it will stop. Otherwise it continues to proceed to the next step of the protocol.

**Step 4:** The server chooses a nonce $m_j \in Z_q^*$ secretly and calculates $m_j P$. Afterwards, the server calculates the following parameters:

$m_3 = SP \oplus m_j P$

$m_4 = h_3(K_{ji} \| m_j P \| T_3)$

The server can calculate the shared session key $K_{ji} = m_j P \cdot m_j P = m_j m_j P$. Server replies to the patient with a message $Me_7 = \{M_3, M_4, T_3\}$.

**Step 5:** When the smart terminal receives a reply message from the server. It decides the following equation $|T_3 - T_4| < \Delta T$ holds or not, where $T_4$ is the current timestamp. If it does not established, the smart terminal can calculate the shared session key $K_{ij} = m_i m_j P = m_i m_j P$, where $m_j P$ is calculate as follow: $m_j P = M_3 \oplus SP$

Finally, when the server and user both get the shared session key $K_{ij}$, the server sends the authentication result to the accounting node. The node writes it on the consortium blockchain through the PBFT algorithm and publishes the authentication result on the blockchain.

5.2 Security analysis

In this section, we describe how the protocol effectively achieves security goals.

*The proposed protocol can achieve data confidentiality and integrity. Blockchain can ensure that the data uploaded to the ledger will not be tampered with. So it could protect confidentiality and integrity of the data.*

*The proposed protocol can achieve anonymity and privacy protection of information. Patients use anonymity $AID_i$ for registration and authentication without revealing their real identity $ID_i$, which could protect personal privacy. In addition, attackers fail to obtain the patient’s real $ID_i$ from the anonymous $AID_i$ due to the one-way nature of the hash function.*

6 Implementation and performance evaluation

6.1 Comparisons of communication overhead

In this subsection, we compare the communication overhead of our scheme with other schemes. We use the Type A curves defined within the PBC library. Specifically, the packet sizes in our experiment are as follows:

$|G| = 1024\text{bits}, \ |Q| = 160\text{bits} \ |AID_i| = 160\text{bits}, \ |SP|$
Table 2: Communication overhead of the proposed protocol.

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Registration phase</th>
<th>Authentication phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>The proposed</td>
<td>$5</td>
<td>Q</td>
</tr>
<tr>
<td>Kumar[22]</td>
<td>$</td>
<td>G</td>
</tr>
<tr>
<td>Tsai[23]</td>
<td>$</td>
<td>G</td>
</tr>
<tr>
<td>Lwamo[24]</td>
<td>$3</td>
<td>Q</td>
</tr>
</tbody>
</table>

Table 3: Computational overhead of cryptographic algorithms.

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Registration phase</th>
<th>Authentication phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>The proposed</td>
<td>$3T_h + 3T_{xor}$</td>
<td>$7T_h + 2T_{xor} + 4T_{mul}$</td>
</tr>
<tr>
<td>Kumar[22]</td>
<td>$T_{mtp} + 3T_{mul} + 3T_{exp} + 2T_{pa} + 4T_h$</td>
<td>$2T_{bp} + T_{pa} + 3T_{exp} + 2T_{mul} + 5T_h + T_{mtp}$</td>
</tr>
<tr>
<td>Tsai[23]</td>
<td>$T_{mtp} + 5T_{mul} + T_{exp} + 4T_h$</td>
<td>$2T_{bp} + 2T_{mul} + 2T_{pa} + 2T_{exp} + 4T_h$</td>
</tr>
<tr>
<td>Lwamo[24]</td>
<td>$5T_h + T_{xor} + T_{dec}$</td>
<td>$9T_h + T_{xor} + 3T_{enc} + 3T_{dec}$</td>
</tr>
</tbody>
</table>

Fig. 2: Comparison of computational cost of experiment.

- $E_{RS} = 160\text{bits}$, $|V_a| = 160\text{bits}$, $|PW_a| = 32\text{bits}$ and $|ID_i| = 32\text{bits}$. As mentioned above, the communication overhead of uploading and downloading to blockchain was ignored in order to unify the benchmark.

We mainly compare cryptography communication overhead with [22–24] in Table 2. In registration phase of our scheme, the content of communication overhead mainly includes $Me1, Me3$. The total communication overhead is $5|Q| + 64 = 864\text{bits}$. Meanwhile, the communication overhead of Kumar[22] is $|G| + 32 = 1056\text{bits}$.

The communication overhead of Tsai et al.[23] is $|G| + 32 = 1056\text{bits}$. The communication overhead of Lwamo[24] is $3|Q| + 32 = 512\text{bits}$. In authentication phase, the communication overhead in our scheme contains $Me5, Me7,$ and $Me9$. Communication overhead of $Me5$ is $1696\text{bits}$. Communication overhead of $Me7$ is $1216\text{bits}$. So the total communication overhead is $1696\text{bits} + 1216\text{bits} = 2|G| + 5|Q| + 32 + 2 = 2912\text{bits}$.

As a contrast, the communication overhead of [22] is $2|G| + 2|Q| + 32 = 2400\text{bits}$. The communication overhead of [23] and [24] are $3|G| + |Q| + 32 = 3264\text{bits}$ and $10|Q| + 32 = 1632\text{bits}$. It should be pointed out that there are litter higher communication overhead in our scheme contrasted to [22,24]. The main reason is that we get a lower computational complexity and a more robust safety features at the expense of some communication overhead.

6.2 Comparisons of computational overhead

In this subsection, we conduct extensive experiments and performance evaluations in order to compare the computer overhead. The calculation time benchmark refers to Yanik[21]. The average computational time for hash functions ($T_h$), Point multiplication ($T_{mul}$), Pairing operation ($T_{bp}$) are 0.0023ms, 2.226ms, and 5.811ms respectively. Point addition ($T_{pa}$) is 0.0288ms, Modular exponentiation ($T_{exp}$) is 3.85ms. String to point hash ($T_{mtp}$) is 12.418ms, public key encryption ($T_{enc}$) is 3.85ms, decryption($T_{dec}$) is 3.85ms and XOR operation time is disregarded.

We compared computational cost of our scheme with comparative schemes. In Registration phase, the computational cost of our scheme is $3T_h + 3T_{xor} = 0.0069\text{ms}$. As a contrast, the cost of [22–24] is $31.23\text{ms}, 27.41\text{ms}$, and $3.86\text{ms}$ respectively. In authentication phase, the
computational cost of [22–24] is 25.44ms, 16.14ms, and 23.13ms, but our scheme is only \( T_{\text{TH}} + 2 T_{\text{tor}} + 4 T_{\text{mal}} = 8.92\text{ms} \), as shown in Table 3. Furthermore, Fig.2 more intuitively shows the comparison of calculation time at different scenario between our scheme and the candidate schemes. It can be seen that our scheme performs best in terms of computational complexity on overall process.

7 Conclusion

In the work, we have proposed a efficient anonymous authentication scheme based on the consortium blockchain to achieve mutual authentication between patients and medical servers. Specific protocols were proposed during the registration and authentication phases. In addition, blockchain technology is used to ensure the confidentiality and integrity of patient’s private data. Furthermore, comparative experiment shows that our scheme achieves a better performance in computation and communication overhead. It is an efficient mutual authentication protocol in a medical environment.

For future work, we will develop a specific algorithm on Hyperledger Fabric to improve the efficiency of our scheme in details.

Acknowledgements

This work is partly supported by the National Natural Science Foundation of China (Grants No. 62072005, 62001246), Natural Science Foundation of Anhui Province (No. 1808085MF164), Scientific Research Staring Foundation of Anhui Normal University (Grant No. 2018XJ40, 2108085LY22), and Anhui Provincial Engineering Laboratory on Information Fusion and Control of Intelligent Robot(Grant No. IFCIR2020008).

References


