

Received August 6, 2020, accepted August 26, 2020, date of publication September 7, 2020,
date of current version September 30, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3022429

A Permissioned Blockchain-Based Identity Management and User Authentication Scheme for E-Health Systems

XINYIN XIANG^{1,2}, (Member, IEEE), MINGYU WANG^{1,2},
AND WEIGUO FAN³, (Senior Member, IEEE)

¹School of Information, Xi'an University of Finance and Economics, Xi'an 710100, China

²China (Xi'an) Institute for Silk Road Research, Xi'an University of Finance and Economics, Xi'an 710100, China

³Department of Business Analytics, University of Iowa, Iowa, IA 52242-1994, USA

Corresponding author: Xinyin Xiang (xiangxinyin@163.com)

This work was supported in part by Natural Science Basic Research Program of Shaanxi Province of China under Grant 2019JM261, in part by the Ministry of Education (MOE) Layout Foundation of Humanities and Social Sciences of China under Grant 20XJA870001, in part by the Foundation of China (Xi'an) Institute for Silk Road Research under Grant 2016SY19, and in part by the Support Research Foundation of Xi'an University of Finance and Economics under Grant 18FCZD01.

ABSTRACT The growth of electronic healthcare (e-health) systems is promoted by the evolution of Internet of Things (IoT) technology, as this new environment provides a variety of alternatives for medical data collection. Traditional authentication models in e-health systems cannot be applied directly to scenarios requiring low-latency, real-time services. Providing a variety of means for data transmission is considered an important method to achieve effective control in e-health systems. However, this new approach also leads to security and privacy concerns as increasingly flexible communication services are introduced. Achieving effective authentication of medical data for different users while providing security guarantees in e-health systems is an interesting problem. In this paper, we present a permissioned blockchain-based identity management and user authentication (PBBIMUA) scheme for the e-health environment. Our scheme satisfies the extensive security requirements of medical data. An evaluation and security analysis show that performance, in terms of lightweight construction and lower network latency with high security standards, is improved in comparison to known methods. The experimental results show that the system has good efficiency.

INDEX TERMS Blockchain, authentication, biometric, e-health.

I. INTRODUCTION

Internet of Things (IoT) has won wide attention because of its effects on society and the economy, and it is changing our lifestyle through greater convenience in actual application fields, such as smart healthcare [1]. IoT can provide optimum quality of service (QoS) for end users. In an IoT environment, plenty of devices are connected to each other through the Internet to sense, share and process data. The terminals in the IoT consist of a wide range of devices, such as sensors and laptops. Its goals are to exchange information through wired or wireless communication channels. With the development of wearable biomedical sensors, the emergence of the IoT

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

has brought revolutionary changes in electronic healthcare (e-health). The IoT in medical care has been used to achieve remote health monitoring, study the impact of drug use, and use intelligent medical care to provide more thoughtful care.

In one e-health scenario, sensors are mounted on the patient's side and continuously sense parameters related to the health of the patient like stomach, blood pressure, heart rate and temperature. These health data collected from the terminal sensors are then transferred to the medical server (MS) and stored in the database repository. Doctors can monitor patients' health conditions in real time, even if treatment is being provided in remote areas. Medical treatment based on the IoT reduces medical costs and improves quality of life. Furthermore, patients' medical data are an important information resource containing a wealth of information, which

can be in the form of signals, text, voice data, images and so on. This information needs to be protected effectively. However, due to the vulnerability to network attacks of the medical system, sharing the sensitive information of patients in an IoT environment may result in a series of serious security and privacy issues. For example, disclosure of such information to any third party may cause misuse of health data. To provide secure data transmission and storage in an intelligent medical environment, cryptographic mechanisms must be used to protect privacy and avoid network attacks. Moreover, sensors in patients and doctors produce massive amounts of health data in real-time medical treatment, exceeding the processing power of the terminal. Because the storage capacity of the terminal is quite limited, it is not feasible to employ known key management and user authentication methods in the medical system. More precisely, the existing methods mainly rely on centralised management to perform authentication, which brings the burden of key management and the risk of health data leakage. A natural problem is how to transfer these health data more efficiently, which becomes a challenging task.

The traditional medical data management methods mainly adopt centralised management. In such a model, medical data are usually stored in the database of the medical server. An attacker can delete or modify the data after obtaining the access permissions of the database. What is more serious is that medical servers can directly apply to the database administrator to replace these data. This method not only increases the burden of data management but also makes it difficult to provide effective security guarantees for medical data. Recently, blockchain has arisen as a decentralised technology that can ensure the integrity of medical data. The advantage of blockchain technology is that it can realise distributed storage of medical data. The modification or deletion of the data of a few participants will not affect the medical data of other participants, and the medical data, with the help of the consensus mechanism of the blockchain, remain intact.

It is an interesting idea to address security and privacy problems for medical networks by making use of blockchain. For the key management and user authentication issues of medical networks, the task requires us to solve user anonymity, traceability and non-repudiation simultaneously. This paper provides an effective method to solve this kind of problem by using blockchain technology.

A. RELATED WORKS

To ensure the security of medical services, it is very important to prevent malicious network intrusion. There is no doubt that the core issue of security is to verify whether the remote user is legal and provide medical data integrity assurance. Recently, many user authentication schemes in e-health have been proposed [2]–[21]. Wong *et al.* [2] employed the features of hash function and put forth a key management and user authentication scheme for e-health systems. However, Tseng *et al.* [3] pointed out that their schemes were vulnerable to replay, forgery and password-guessing attacks. In addition, Lee [4] found that the computational

cost of Wong *et al.*'s scheme was too expensive to be suitable for lightweight devices. Das [5] presented an efficient two-factor authentication scheme for the IoT that improved efficiency in terms of computational cost. Unfortunately, Huang *et al.* [6] claimed that Das's scheme could not resist password-guessing attacks, user impersonation, etc. In addition, Das's scheme does not achieve user anonymity. Subsequently, Yoo *et al.* [7] declared that Huang *et al.*'s scheme was vulnerable to insider and parallel session attacks and could not achieve mutual authentication. Subsequently, Das [8] further claimed that Li *et al.*'s scheme [9] could not support strong authentication in the authentication process and could not achieve password updating locally. Meanwhile, An [10] claimed that Das's scheme [8] had security weaknesses, including vulnerability to user impersonation attacks, server-masquerading attacks, insider attacks, etc. An [10] also presented an enhanced version of the scheme. Unfortunately, Khan and Kumari [11] pointed out that this scheme could fail due to impersonation attacks and password-guessing attacks.

To achieve user anonymity, Chang *et al.* [12] presented a new key management and user authentication scheme for e-health systems. This scheme can update a secret value in the storage of a smart card every time authentication is performed. However, Das and Goswami [13] pointed out that their scheme had security failures, such as vulnerability to insider attacks and man-in-the-middle attacks, and did not support proper authentication. Arshad and Nikooghadam [14] presented a three-factor anonymous authentication scheme. They claimed that the scheme could provide better secure authentication and ensure user privacy. Afterwards, Lu *et al.* [15] proposed an improvement of Arshad *et al.*'s scheme by using an elliptic curve cryptosystem. Islam and Khan [16] presented an anonymous two-factor authentication scheme based on ECC in the random oracle model. They demonstrated that their scheme was secure under the computational Diffie-Hellman problem. Unfortunately, Zhang and Zu [17], Feng *et al.* [18] claimed that Islam and Khan [16] scheme had security flaws such as vulnerability to server-spoofing attacks and off-line password-guessing attacks. Zhang and Zu [17] proposed a dynamic key management scheme supporting the biometric authentication function at a medical service centre, in which the specific value of the biometric template is not known by the medical service centre. Furthermore, Zhang *et al.* claimed that their scheme could achieve user anonymity during authentication and untraceability.

The authentication of the above schemes mainly relies on flexible security models, and these schemes are required in multiple interactions between users and medical service centres, which will be a major obstacle for mobile users to achieve efficient access to the data centre. Moreover, all these schemes assume that there is a trusted authority centre, which makes the networks vulnerable to damage to the database stored and maintained by the authority centre. Blockchain enables cross-data-centre authentication [18] and provides an efficient method to achieve data integrity.

Huawei *et al.* [19] presented a blockchain-based key management scheme for an e-health system, which provides an efficient mechanism for protecting sensitive medical data in the health blockchain. Tang *et al.* [20] and Omar *et al.* [21] proposed blockchain-based authentication schemes for e-health systems, which are blockchain-based health systems in the consortium blockchain environment. Cao *et al.* [22] put forward a blockchain based cloud-assisted eHealth system, which aims to avoid outsourced electronic health records from malicious modification. Cheng *et al.* [23] proposed a blockchain based two-way medical data authentication scheme, which provides an efficient solution in the medical data sharing between hospitals and blockchain nodes. Yazdinejadl *et al.* [24] put forth a blockchain-based decentralized authentication scheme for hospital networks. Since re-authentication is not required in a distributed network of affiliated hospitals, this architecture not only ensures security and privacy protection, but also reduces transmission overhead. Compared to prior cross-data-centre authentication schemes, cross-data-centre authentication schemes in a public blockchain can improve the efficiency of authentication and can also protect against the attacks mentioned. However, the ledger is distributed (involving all transactions of information) and made public to all network members. Identity management and user authentication based on blockchain has become an interesting and emerging research topic for protecting the privacy of users.

B. MOTIVATION AND CONTRIBUTIONS

This paper makes the below contributions in achieving user authentication for e-health systems:

- We put forth a new method to resolve the security weaknesses of the existing schemes, which enables flexible cross-data-centre authentication.
- Our scheme can be applied to medical systems in which terminal devices require only lightweight computation.
- We analyze the correctness of the functionality of our scheme under the BAN logic, proving that our proposal meets the security requirements, simulating the scheme in the NS shows the efficiency of our scheme.

C. OUTLINE

The rest of the paper is structured as follows: Section II mainly reviews the required preliminaries. In Section III, the network model and security requirements are discussed in detail. Our construction is proposed and a security analysis is described in Section IV and Section V, respectively. Then, we present the performance analysis in Section VI, the evaluation and simulation results is described in Section VII. Finally, Section VIII summarises the paper.

II. PRELIMINARIES

A. HARD PROBLEMS

A non-regular elliptic curve E_p is defined by the equation $y^2 = x^3 + ax + b \pmod{p}$, where $a, b \in Z_p^*$ and p is a large prime. The sufficient condition is $4a^3 + 27b^2 \neq 0 \pmod{p}$.

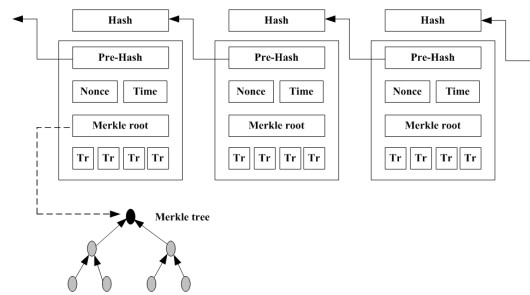


FIGURE 1. Blockchain structure.

In our scheme, there are two hard problems: the computational Diffie-Hellman problem (CDHP) and the discrete logarithm problem (DLP).

Definition 1 (Computational Diffie-Hellman Problem (CDHP): For any $a, b \in Z_q^*$, there is a generator P of the cycle group G of order q . As a result, for a given P, aP, bP , computing abP is a hard problem.

Definition 2 (Discrete Logarithm Problem (DLP): For any additive cycle group G of order q on the elliptic curve, there is $xP \in G$ such that computing x is a hard problem.

Remark 1: From the above definitions, we note that there is an equivalent result: given xP, yP and zP in G , calculating $z = xy$ is computationally infeasible.

B. PERMISSIONED BLOCKCHAIN SYSTEM

A blockchain consists of blocks that are interlinked to form a chain and protected by a cryptographic primitive, and a new block can be added to the blockchain. Blockchain contains many nodes, but these nodes are not required to trust each other; if enough nodes are honest, security in the blockchain can be guaranteed [25]. Specifically, each block includes three sections: a hash pointer (where the hash pointer points to the fore block), a time-stamp and transaction data. The validity of these transaction data can be verified by most nodes. As shown in Fig 1, *Hash*, *Pre – Hash*, *Nonce*, *Time* and *Tr* denote the current block hash value, previous block hash value, solutions for the proofs-of-work, time-stamp and transaction data, respectively.

Blockchain is an unchangeable ledger, which is constructed in a distributed way without central authorisation. Each member of the blockchain represents a node involved in the calculation. These nodes verify transactions in a process called “mining”, and these nodes are known as “miners”. These miners validate the transactions and produce blocks with an efficient set of transactions by reaching consensus using a consensus mechanism. Since Bitcoin was introduced to blockchain, different types of permissioned chains were introduced [26], such as public permissionless blockchain [27] and public permissioned blockchain [28], [29]. On the one hand, such blockchains are based on the idea that each participant is granted special permissions to execute specific functions. In a public blockchain, anyone can participate in mining without a designated

identity. Public blockchains usually involve local cryptocurrencies and utilise economic incentives and consensus mechanisms [30] like proof-of-work (POW) and delegated proof-of-stake (DPOS). Completely private or limited to a finite group of authorised nodes is considered as private permissioned blockchain.

On the other hand, permissioned blockchain implements the blockchain with a set of known, specific participants and provides a method to ensure interaction between a set of entities with common goals but not full trust in each other. Permissioned blockchain is limited to a set of authorised participants, which permits participants to create a network, and multiple organisations can join the network by having their own peers. Our scheme chooses a permissioned blockchain based on the design criteria of our model. First, widely accepted consensus algorithms such as proof-of-work (PoW) in the current blockchain-based e-health systems consumes too many calculations, and the transaction confirmation speed in these networks is slow. Due to the limitation of the networks, it is difficult to meet the complex security requirements of PoW. Second, a remarkable feature of permissioned blockchain compared to other classes of blockchains is that it has an authorisation function.

III. NETWORK MODEL, NETWORK ASSUMPTIONS AND SECURITY REQUIREMENTS

A. NETWORK MODEL

In our model, we assume a blockchain network in which each member holds a related distributed ledger. The network systems are formed with the following main participants: *Founder*, the user (U_i), registration center(*RC*), and medical server (MS_j). In essence, our model establishes a blockchain network containing trusted members, such as *Founder*, *RC* and MS_j . *Founder* is responsible for supervising *RC* and managing users. The responsibility of *RC* is to check the user's identity information and add this information to the blockchain as a transaction for mining user enrolment requests. After successful execution of the process, *RC* generates the credentials of user U_i , and U_i then proves himself to the medical server MS_j . The resulting network model is shown in Fig 2.

1) REGISTRATION CENTER (RC)

RC is a trusted server, which is in charge of enrolling U_i and tracing illegal participants. *RC* assigns all participants to key materials, and it can use smart contracts to record participants' key materials in the blockchain.

2) MEDICAL SERVER(MS_j)

The main responsibility of MS_j is to coordinate the access of end users. Each MS_j is responsible for supervising and managing a group of U_i . This enables better scalability and expands the limited functionality of U_i . MS_j reduces the burden of storage, memory, and computation involved in the

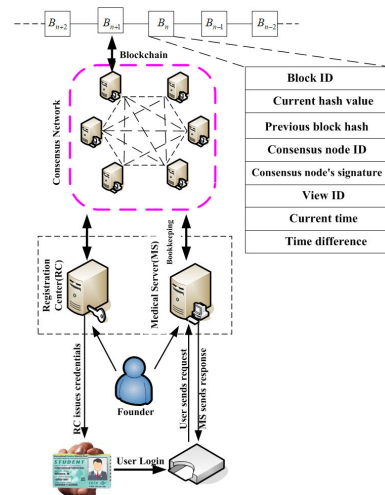


FIGURE 2. Blockchain network model.

authentication process for U_i . In addition, it serves as a trusted recorder for only key publishing and updating in our model.

3) END USERS

End users are terminals requesting access rights from smart contracts to access certain MS_j . Once each U_i gains access rights through a smart contract, U_i contracts MS_j , which completes the process of authentication and access.

In our scheme, suppose our scheme is in the permissioned blockchain environment. Based on the network, each legitimate member has a distributed ledger, and the system allows new members to join the network and accepts most existing members. Moreover, the transactions in our scheme are used to stimulate smart contracts for registration, while smart contracts help record public keys for efficient identity and maintain a key material table. The system uses the underlying smart contract to support conditional anonymous authentication for the participants.

B. NETWORK ASSUMPTIONS

For convenience, we consider the following network assumptions:

- We use blockchain technology as a distributed ledger, and smart contract records are considered reliable throughout the process.
- In e-health systems, the medical server and registration centre construct a permissioned blockchain network.
- Under normal conditions, the key of the medical server does not need to be updated in our scheme.

C. SECURITY REQUIREMENTS

Our distributed model in blockchain must meet the following design goals with regard to security and performance:

- Mutual authentication: Only enrolled U_i and MS_j are present in the e-health system to implement our scheme for verifying identity information before message exchange.

TABLE 1. Main notation.

Notation	Description
U_i	The i -th user (a patient or a doctor)
MS_j	The medical server
RC	The registration center
SC	A smart card reader
ID_i, PW_i	The identity and the password of U_i
ID_{MS_j}	The identity of medical server MS_j
ID_{RA}	The identity of registration center RC
α	The private key of RC
β_j	The private key of medical server MS_j
Bio_i	Biometric data
TS_1, TS_2, TS_3	The current time
ΔTS	The maximum time interval
Gen	Fuzzy extractor generation function
Rep	Fuzzy extractor reproduction function
$h(\cdot)$	A one-way hash function
\oplus	The exclusive-or operation
\parallel	Message concatenation
k_i, a_i, b_i, c_j, d_j	High-entropy random numbers

- User anonymity: To ensure the identity privacy of U_i , no potential attacker in the system can capture the identity information of U_i in the process of authentication.
- Non-repudiation property: Upon completing the related transaction, no adversary can deny the facts in the process of communication.
- Impersonation attack: In carrying out an impersonation attack, no adversary can impersonate one of the communicators during the authentication process.
- Conditional traceability: To monitor the malicious or misbehaving communicators, we assume that only a third party declares the real identity of the participants.
- Session key agreement: During the execution of the proposed scheme to further exchange confidential messages, the session key is shared only between participants, RA cannot even acquire any knowledge about the session key.
- Resilience against other attacks: Next, we consider some other types of attacks. Namely, our proposal should support the features resilient other main attacks including man-in-the-middle attack(MitM), stolen smart card attack and offline password-guessing attack.

IV. OUR CONSTRUCTION

In this part, we introduce an identity management and user authentication scheme maintained on a medical server. The proposal provides mutual authentication and privacy protection. Then, the details of the scheme are given. Some notation is described in Table 1. Normally, identity password information stored in a remote database is used to authenticate the medical server. Upon obtaining the login message of a user, the medical server inquires the identity information from the database, calculates the related password or the hash value with the target string, and compares it to see whether it matches previous values. However, identity

password information may be subject to a series of attacks, such as stolen smart card attacks and anonymity exposure. To overcome these weaknesses, we adopt the technology of Wazid *et al.* [31] and design a new identity management and user authentication scheme. The specific details are as follows:

A. INITIALISATION PHASE

For two large primes p, q and a non-regular elliptic curve E_p , there is an elliptic curve additive cyclic group G of order q and a generator P of G . Initially, *Founder* utilizes ECC to initialize e-health system, the system constructs a permissioned blockchain network with a trusted forum of members, including RC and MS_j , where the required participants (such as the RC and medical server (MS_j)) form a consortium. *Founder* writes smart contracts in order to provide access control function. Specifically, RC and MS_j establish a consortium blockchain and rely on practical Byzantine fault tolerance (PBFT) for the consensus mechanism. For simplicity, RC and MS_j can directly join a known blockchain system. They execute the operations below to initialise a series of system parameters:

- (1) Choose a cryptographic hash function h .
- (2) RC calculates $R = \alpha P$ by choosing a long-term secret key α and pushes it into the blockchain network.
- (3) MS_j calculates $A_j = \beta_j P$ by choosing a long-term secret key β_j and pushes it into the blockchain network.
- (4) Publish the system parameters (R, A_j, P, h) .

B. ENROLMENT PHASE

In this part, user U_i contacts RC with his/her personal biometric information. Under the process, RC checks the identity of U_i , issues him/her with a smart card and records the identity information of U_i on the blockchain. The details of this process are as below:

Step 1. U_i chooses ID_i and a random number $k_i \in \mathbb{Z}_q^*$ and calculates $RID_i = h(k_i \parallel ID_i)$. U_i then pushes the personal biometric data Bio_i into the reader and enables the fuzzy extractor to obtain the biometric information (σ_i, θ_i) ; we have $(\sigma_i, \theta_i) \leftarrow Gen(Bio_i)$, where σ_i and θ_i denote secret and public parameters, respectively. U_i then sends an enrolment request RID_i to RC .

Step 2. Upon receipt of the enrolment request, RC chooses $t_i \in \mathbb{Z}_q^*$ and calculates $s_i = \alpha h_i + t_i \pmod{q}$, where $h_i = h(h(RID_i \parallel T_i \parallel R) \parallel \alpha)$, $T_i = t_i P$. Next, RC sends the user enrolment-transaction $RT = (RID_i, R, s_i, T_i)$ to the blockchain system. Once RC completes mining, the information RT in the blockchain ledger is updated. Then, RC saves $SC = (RID_i, s_i, k_i, T_i)$ on the smart card and returns it to U_i securely.

Step 3. After receiving SC from RC , U_i chooses $\mu_i \in \mathbb{Z}_q^*$ and computes $L_i = k_i \oplus h(\sigma_i \parallel PW_i)$, $H_i = \mu_i \oplus h(RID_i \parallel PW_i \parallel \sigma_i)$, $s_i^* = s_i \oplus \mu_i \oplus h(RID_i \parallel \sigma_i)$, and $CH_i = h(RID_i \parallel PW_i \parallel \sigma_i \parallel k_i \parallel \mu_i)$. U_i replaces s_i with s_i^* and writes $(\theta_i, L_i, H_i, CH_i, s_i^*, T_i)$ on the smart card SC .

C. LOGIN PHASE

A registered user is eager to obtain the medical services provided by MS_j via a public channel, U_i produce login messages after obtaining information from MS_j by executing the below steps.

Step 1. U_i adds his/her smart card into the reader and submits his/her identity ID_i and password PW_i ; then, a search is performed to obtain the biometric Bio'_i .

Step 2. Using the information stored on the smart card, U_i computes as follows:

$$\sigma_i^* = Rep(Bio'_i, \theta_i) \tag{1}$$

$$k_i^* = L_i \oplus h(\sigma_i^* \parallel PW_i) \tag{2}$$

$$RID_i^* = h(ID_i \parallel k_i^*) \tag{3}$$

$$\mu_i^* = H_i \oplus h(RID_i^* \parallel PW_i \parallel \sigma_i^*) \tag{4}$$

$$CH_i^* = h(RID_i^* \parallel PW_i \parallel \sigma_i^* \parallel k_i^* \parallel \mu_i^*). \tag{5}$$

Upon completing the above computations, U_i checks that the validity of the equation $CH_i^* = CH_i$ holds. If it holds, the above verification passes. Otherwise, U_i terminates the session.

Step 3. U_i then chooses two random numbers a_i, b_i , creates the current time-stamp TS_1 , and performs the following operations using the stored information on the smart card:

$$\widehat{s}_i = s_i^* \oplus \mu_i^* \oplus h(RID_i^* \parallel \sigma_i^*) \tag{6}$$

$$x_i = h(\sigma_i^* \parallel A_j \parallel T_i) \tag{7}$$

$$\widehat{s}_i = h(\widehat{s}_i \parallel RID_i^* \parallel R \parallel A_j \parallel T_i) \tag{8}$$

$$B_i = a_i b_i P \tag{9}$$

$$X_i = x_i P \tag{10}$$

$$Y_i = \widehat{s}_i P \tag{11}$$

$$\eta_i = a_i \frac{1}{x_i + \widehat{s}_i} \text{ mod } q \tag{12}$$

$$S_i = b_i(X_i + Y_i). \tag{13}$$

Then, U_i hands the login request $(B_i, \eta_i, S_i, T_i, TS_1)$ to the medical server MS_j .

D. MUTUAL AUTHENTICATION AND KEY AGREEMENT PHASE

In this part, MS_j validates user U_i using the identity information recorded in the blockchain ledger. Next, the medical server MS_j establishes a session key with user U_i , as summarised in Fig 3. The related process is executed below.

Step 1. MS_j checks the freshness of TS_1 with $TS'_1 - TS_1 \leq \Delta TS_1$, where TS'_1 denotes the current time-stamp of U_i . If this condition holds, MS_j calculates

$$\eta_i S_i = a_i \frac{1}{x_i + \widehat{s}_i} b_i(X_i + Y_i) \tag{14}$$

$$= a_i b_i \frac{1}{x_i + \widehat{s}_i} (x_i + \widehat{s}_i) P \tag{15}$$

$$= a_i b_i P = B_i, \tag{16}$$

and then, MS_j checks whether $B_i = \eta_i S_i$. If so, the login request message is considered to be efficient. Otherwise, MS_j ends the session.

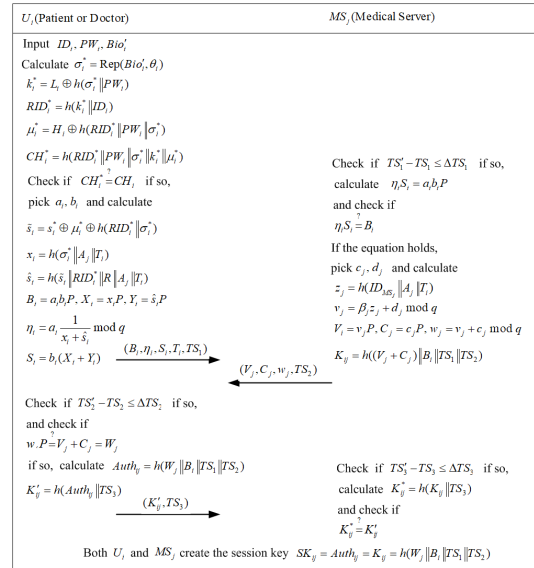


FIGURE 3. The login and authentication process.

Step 2. MS_j chooses two random numbers c_j, d_j and the current time-stamp TS_2 and calculates

$$z_j = h(ID_{MS_j} \parallel A_j \parallel T_i) \tag{17}$$

$$v_j = \beta_j z_j + d_j \text{ mod } q \tag{18}$$

$$V_j = v_j P, C_j = c_j P \tag{19}$$

$$w_j = v_j + c_j \text{ mod } q. \tag{20}$$

By using the current values, MS_j calculates the session key shared with U_i as $K_{ij} = h((V_j + C_j) \parallel B_i \parallel TS_1 \parallel TS_2)$. MS_j hands (V_j, C_j, w_j, TS_2) to U_i .

Step 3. Upon obtaining the messages (V_j, C_j, w_j, TS_2) from the medical server MS_j , user U_i checks the freshness of TS_2 with $TS'_2 - TS_2 \leq \Delta TS_2$, where TS'_2 denotes the current time-stamp of U_i . If it holds, U_i further checks if $w_j P = (\beta_j z_j + d_j) P + c_j P = V_j + C_j = W_j$. If so, U_i believes that this is a valid login response message. Otherwise, the connection ends. U_i creates the session key shared with MS_j as $Auth_{ij} = h(W_j \parallel B_i \parallel TS_1 \parallel TS_2)$. U_i then obtains the current time-stamp TS_3 , computes $K'_j = h(Auth_{ij} \parallel TS_3)$, and sends the message (K'_j, TS_3) to MS_j via a public channel.

Step 4. Upon receiving (K'_j, TS_3) from U_i , MS_j checks the freshness of TS_3 with $TS'_3 - TS_3 \leq \Delta TS_3$, where TS'_3 denotes the current time-stamp of MS_j . If it holds, MS_j calculates $K''_j = h(K'_j \parallel TS_3)$ and checks whether $K''_j = K'_j$. If so, this is $K''_j = K'_j$. Otherwise, MS_j terminates the process.

The above verification ensures successful mutual authentication between U_i and MS_j . Finally, U_i and MS_j generate a common secret session key $SK_{ij} = Auth_{ij} = K_{ij} = h(W_j \parallel B_i \parallel TS_1 \parallel TS_2)$.

E. PASSWORD UPDATE PHASE

As a legitimate user U_i , it is ready to update his/her password or biometrics for security reasons during the user registration phase, our scheme will perform the updating of the password

and biometrics. For each user U_i , his/her biometric information is unique and unchanged. The steps below complete the process.

Step 1. Upon adding U_i 's ID_i and new password PW_i^{new} into the smart card, then U_i provides new biometrics Bio_i^{new} if U_i wants to change Bio_i^{old} . But if U_i does not want to alter the biometrics, Bio_i^{old} will be considered Bio_i^{new} . Then, U_i performs the following update algorithms: $(\sigma_i^{new}, \theta_i^{new}) \leftarrow Gen(Bio_i^{new}), L_i^{new} = k_i^* \oplus h(\sigma_i^{new} \parallel PW_i^{new}), H_i^{new} = \mu_i^* \oplus h(RID_i^* \parallel PW_i^{new} \parallel \sigma_i^{new}), s_i^{new*} = s_i^* \oplus \mu_i^* \oplus h(RID_i^* \parallel \sigma_i^{new}),$ and $CH_i^{new} = h(RID_i^* \parallel PW_i^{new} \parallel \sigma_i^{new} \parallel k_i^* \parallel \mu_i^*).$

Step 2. MS_j replaces the prior values with the newly generated values in memory.

V. SECURITY EVALUATION

In this part, we consider a relevant security analysis that aims to analyze the below properties of our proposal, which can resist existing attacks and provides some additional features, such as conditional traceability and the non-repudiation property. Next, we provide some related methods to achieve security proof, such as BAN logic [33] and the Scyther tool [34], [35].

A. SECURITY ANALYSIS

1) MUTUAL AUTHENTICATION

Only an authenticated U_i can exchange information with MS_j . MS_j verifies the legitimacy of U_i based on the equation below, the robustness of which is shown next.

$$\eta_i s_i = a_i \frac{1}{x_i + \hat{s}_i} b_i (X_i + Y_i) \quad (21)$$

$$= a_i b_i \frac{1}{x_i + \hat{s}_i} (x_i + \hat{s}_i) P \quad (22)$$

$$= a_i b_i P = B_i. \quad (23)$$

An attacker cannot learn the information of a_i, b_i because of the hardness of the CDHP. That is, the value of B_i cannot be calculated by a malicious user. Therefore, MS_j achieves the authentication of U_i . Additionally, MS_j can be authenticated by U_i by verifying the above equation. Therefore, our scheme has the mutual authentication feature.

2) USER ANONYMITY

Our scheme uses a randomly produced unique identity $RID_i = h(ID_i \parallel k_i)$ for each enrolled user and stores $RT = \{RID_i, R, A_j, T_i\}$ as identity information on the blockchain, which is similar to storing a public key in a public blockchain. In each authentication phase, U_i 's pseudo-identity RID_i is adopted instead of the actual identity ID_i . Furthermore, in the network enrolment phase, RC stores RID_i in the blockchain, which does not leak ID_i . In short, the identity of U_i is hidden, and our scheme achieves anonymity.

3) NON-REPUDIATION PROPERTY

To obtain the non-repudiation property, personal user biometrics are built in our scheme. User biometrics have the

following characteristics: uniqueness, unforgeability and difficulty of replication. Moreover, our scheme also provides some additional features. Namely, if a user inadvertently loses the certificate, the system performs revocation and reissue/update of user credentials. This information is also recorded in the blockchain ledger. Thus, our scheme supports the non-repudiation property. In other words, once a transaction is completed and successfully logged, it cannot be rejected.

4) IMPERSONATION ATTACK

During the implementation of our scheme, there may be two types of attacks:

Case 1. RC impersonates user U_i : In this case, RC tries to create a valid request with the key K_{ij} , where K_{ij} denotes the shared key between U_i and MS_j . However, RC creating such a key is equivalent to computing $a_i b_i P$. Moreover, the confirmation message is considered to be $Auth_{ij} = h(W_j \parallel B_i \parallel TS_1 \parallel TS_2)$. However, using the above available tuple to compute the key $a_i b_i P$ is as hard as the CDHP in G .

Case 2. MS_j impersonates user U_i : As above, It is not feasible for adversaries to create valid requests and confirmations without user secrets, including MS_j . Suppose that the transmitted messages can be captured by an attacker \mathcal{A} . Now, \mathcal{A} attempts to extract a series of sensitive pieces of information to convince a medical server (MS_j) that it is a legitimate user. In this way, \mathcal{A} may create an effective message as a login request. Still, any knowledge of these parameters can be obtained by \mathcal{A} . To create a new login request, it is not feasible to simulate the message captured by \mathcal{A} 's task to impersonate a user. Thus, our proposal can avoid impersonation attacks by any \mathcal{A} , including MS_i and RC .

5) CONDITIONAL TRACEABILITY

Assume U_i is found to have behaved maliciously using identity information RID_i . RC is able to trace U_i and reveal the actual identity ID_i after specifying the malicious authentication message, as follows:

- (1) Calculate $\sigma_i^* = Rep(Bio_i^*, \theta_i), k_i^* = L_i \oplus h(\sigma_i^* \parallel PW_i), RID_i^* = h(ID_i \parallel k_i^*), \mu_i^* = H_i \oplus h(RID_i^* \parallel PW_i \parallel \sigma_i^*),$ and $CH_i^* = h(RID_i^* \parallel PW_i \parallel \sigma_i^* \parallel k_i^* \parallel \mu_i^*),$ such that $CH_i^* = CH_i.$
- (2) Obtain each transaction $RT = (RID_i, R, s_i, T_i)$ from the blockchain and ensure that each transaction outputs $CH_i.$
- (3) Based on $RT,$ obtain the information RID_i from local storage and confirm the identity of $U_i.$
- (4) No outside attacker can trace the information of $U_i.$

6) SESSION KEY AGREEMENT

Upon capturing the proper session key, \mathcal{A} may attempt to capture the information $(V_j, C_j, w_j),$ where $z_j = h(ID_{MS_j} \parallel A_j \parallel T_i), v_j = \beta_j z_j + d_j, V_j = v_j P, C_j = c_j P,$ and $w_j = v_j + c_j \bmod q.$ Even if the random number c_j and identity ID_{MS_j} are leaked to $\mathcal{A},$ the random nonce c_j and d_j cannot be exchanged over the public channel, and the attacker can learn an efficient session only if \mathcal{A} solves the DLP.

7) RESISTANCE TO OTHER ATTACKS

Our proposal is believed that can resist a series of existing attacks.

a: MitM ATTACK

To resist MitM attacks, it is assumed that the attacker \mathcal{A} has the ability to intercept the exchanged messages in the implementation of our proposal. \mathcal{A} then attempts to alter these messages to deceive U_i . Furthermore, to modify the messages, \mathcal{A} tries to intercept secret information $(\theta_i, L_i, H_i, CH_i, s_i^*, T_i)$. For similar reasons, \mathcal{A} also may not modify other messages. This manifests that our proposal can avoid the MitM attack.

b: REPLAY ATTACK

It is assumed that an attacker has the ability to capture the transmitted message. Even if the attacker responds to these messages later, we can verify the validation of the sent message by analyzing the relevant timestamp ΔTS in this message. Since ΔTS is very small, the proposal can against replay attack.

c: STOLEN SMART CARD ATTACK

After intercepting the information of the smart card, the attacker may extract secret information related to users. Conversely, even if RT is captured by the attacker, U_i can still control the smart card, and the unidirectionality of the hash function makes it almost impossible for the attacker to guess ID_i . Thus, our proposal can avoid stolen smart card attacks launched by the attacker.

Offline password-guessing attack: Upon obtaining the information (V_j, C_j, w_j) , the attacker aims to guess both ID_i and PW_i to satisfy the equation. Calculating the above parameters correctly simultaneously is impossible. Therefore, our proposal can avoid offline password-guessing attacks.

TABLE 2. BAN-logic notations.

Notation	Description
$P \equiv Y$	The formula Y can be believed by the entity P .
$P \triangleleft Y$	P sees Y .
$P \Rightarrow Y$	P has achieved jurisdiction over Y .
$P \sim Y$	P has once said Y .
$\#(Y)$	Y is fresh.
$\{Y\}_K$	Y is hidden under the secret K .
$P \xleftrightarrow{K} \Theta$	P and Θ establish a secret key K .

B. LOGIC PROOF BY BAN LOGIC

Burrows et al. [33] proposed a logic of authentication in 1989, which is popular in checking the correctness of authentication protocols. BAN logic is a belief-based model logic that can be used to prove whether the implementation of the protocol can achieve the expected goals and to discover shortages in the proposal design. The main notations are listed in Table 2.

Based on the idea, our proposal considers the below logical rules in our proof.

- **A1. Message-Meaning Rule(MMR):** $\frac{P \equiv P \xleftrightarrow{K} \Theta, P \triangleleft \{Y\}_K}{P \equiv \Theta \sim Y}$
- **A2. Nonce Verification Rule(NVR):** $\frac{P \equiv \#(Y), P \equiv \Theta \sim Y}{P \equiv \Theta \equiv Y}$
- **A3. Freshness Propagation Rule(FPR):** $\frac{P \equiv \#(Y)}{P \equiv \#(Y, X)}$
- **A4. Jurisdiction Rule(JR):** $\frac{P \equiv (\Theta \Rightarrow Y), P \equiv (\Theta \equiv Y)}{P \equiv Y}$

The method of using BAN logic for security proof is to infer from the security that the desired security target follows the four security assumptions given above.

- **Message 1:** $U_i \rightarrow MS_j: (B_i, \eta_i, S_i, T_i, TS_1)$.
- **Message 2:** $MS_j \rightarrow U_i: (V_j, C_j, w_j)$.
- **Message 3:** $U_i \rightarrow MS_j: h(h(W_j \parallel B_i \parallel TS_1 \parallel TS_2) \parallel TS_3)$.

Idealized form: The idealized form of our scheme is as below:

- **Message 1:** $U_i \rightarrow MS_j: \langle B_i, \eta_i, S_i, T_i, TS_1, U_i \xleftrightarrow{K_i} MS_j \rangle$.
- **Message 2:** $MS_j \rightarrow U_i: \langle V_j, C_j, w_j, MS_j \xleftrightarrow{K_{ij}} U_i \rangle$.
- **Message 3:** $U_i \rightarrow MS_j: \langle W_j, B_i, TS_3, U_i \xleftrightarrow{K_{ij}} MS_j \rangle$.

In terms of our scheme description, we provide the below security hypotheses in our scheme.

- **H 1:** $U_i \equiv \#(\eta_i)$.
- **H 2:** $MS_j \equiv \#(w_j)$.
- **H 3:** $U_i \equiv U_i \xleftrightarrow{K_{ij}} MS_j$.
- **H 4:** $MS_j \equiv \#(TS_1)$.
- **H 5:** $MS_j \equiv U_i \xleftrightarrow{K_{ij}} MS_j$.
- **H 6:** $U_i \equiv MS_j \implies MS_j \xleftrightarrow{K_{ij}} U_i$.
- **H 7:** $MS_j \equiv U_i \implies U_i \xleftrightarrow{K_{ij}} MS_j$.
- **H 8:** $MS_j \equiv \#(TS_3)$.

In addition, we provide the below security goals that aim to prove our scheme.

- **Goal 1.** $U_i \equiv U_i \xleftrightarrow{K_{ij}} MS_j$.
- **Goal 2.** $MS_j \equiv U_i \xleftrightarrow{K_i} MS_j$.
- **Goal 3.** $U_i \equiv MS_j \equiv MS_j \xleftrightarrow{K_{ij}} U_i$.
- **Goal 4.** $MS_j \equiv U_i \equiv U_i \xleftrightarrow{K_{ij}} MS_j$.

According to the Message 1 message, there is

$$MS_j \triangleleft \{B_i, \eta_i, S_i, T_i, TS_1, U_i \xleftrightarrow{K_i} MS_j\} \quad (24)$$

We employ MMR and the assumption H1, this is:

$$MS_j \equiv U_i \sim \{B_i, \eta_i, S_i, T_i, TS_1, U_i \xleftrightarrow{K_i} MS_j\} \quad (25)$$

We use the FPR, NVR and the assumption H7, this is

$$MS_j \equiv U_i \equiv \{B_i, \eta_i, S_i, T_i, TS_1, U_i \xleftrightarrow{K_i} MS_j\}. \quad (26)$$

According to (25), (26) and H4, we employ NVR, this is

$$MS_j \equiv U_i \equiv U_i \xleftrightarrow{K_i} MS_j \quad (27)$$

In addition, according to (27) and the assumption H7, we use JR, this is:

$$MS_j \equiv U_i \xleftrightarrow{K_i} MS_j \quad (28)$$

From the *Message 2* message, there is

$$MS_j \triangleleft \{V_j, C_j, w_j, MS_j \xleftrightarrow{K_{ij}} U_i\} \quad (29)$$

We use MMR and the assumption *H3*, this is:

$$U_i \equiv MS_j \mid \sim \{V_j, C_j, w_j, MS_j \xleftrightarrow{K_{ij}} U_i\} \quad (30)$$

According to *H2* and (30), we employ FPR, this is

$$U_i \equiv MS_j \equiv \{V_j, C_j, w_j, MS_j \xleftrightarrow{K_{ij}} U_i\}. \quad (31)$$

By (30) and (31), we use NVR, this is

$$U_i \equiv MS_j \equiv MS_j \xleftrightarrow{K_{ij}} U_i \quad (32)$$

According to the *Message 3* message, there is

$$MS_j \triangleleft \{B_i, W_j, TS_3, U_i \xleftrightarrow{K_{ij}} MS_j\} \quad (33)$$

and (32) via MMR, this is:

$$MS_j \equiv U_i \mid \sim \{B_i, W_j, TS_3, U_i \xleftrightarrow{K_{ij}} MS_j\} \quad (34)$$

Then, we employ FPR, this is

$$MS_j \equiv \sharp\{B_i, W_j, TS_3, U_i \xleftrightarrow{K_{ij}} MS_j\} \quad (35)$$

According to (35) and *H8*, we use JR, this is

$$MS_j \equiv U_i \equiv U_i \xleftrightarrow{K_{ij}} MS_j \quad (36)$$

Thus, the proof of the goals are achieved according to *H3*, (28), (32) and (36).

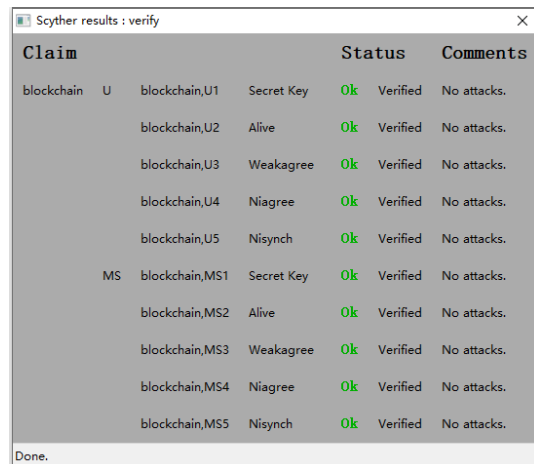
C. SCYTHYR TOOL VERIFICATION

In the part, the test is performed by the formal method Scyther tool [34], [35]. As an efficient test tool, the tool automatically validates some security protocols. It can achieve the proof of the protocols by using Scyther claims with the unbounded number of sessions, there are four claims including Alive, Nisynch, Secret and Commitment. The phase of achieving expected communication in certain events is called “Alive”. The attack model over Scyther tool is under the Dolev-Yao model [36]. In addition, Scyther produces a class of attacks graph by detecting possible attacks. Specifically, the verification process of our proposal is shown as below.

From Fig 4, we find that Scyther can check the security requirements of our scheme, and confirm the four claims. Thus, the results show that our proposal can avoid the known main attacks and guarantee the related security requirements.

VI. PERFORMANCE ANALYSIS

In this part, under the idea of performance evaluation, we provide a comparison with prior relevant schemes [15], [16], [19], [21], [32] in the literature in terms of functionality and computational/communication overhead. However, we only evaluate the performance of the authentication process.



Claim	Status	Comments
blockchain, U	Secret Key	Ok Verified No attacks.
blockchain,U2	Alive	Ok Verified No attacks.
blockchain,U3	Weakagree	Ok Verified No attacks.
blockchain,U4	Niagree	Ok Verified No attacks.
blockchain,U5	Nisynch	Ok Verified No attacks.
MS blockchain,MS1	Secret Key	Ok Verified No attacks.
blockchain,MS2	Alive	Ok Verified No attacks.
blockchain,MS3	Weakagree	Ok Verified No attacks.
blockchain,MS4	Niagree	Ok Verified No attacks.
blockchain,MS5	Nisynch	Ok Verified No attacks.

FIGURE 4. Scyther tool verification results.

A. FUNCTIONALITY COMPARISON

Table 3 shows the comparison of functionality features for the relevant key management and user authentication schemes [15], [16], [19], [21], [32]. We note that only our scheme meets the known security requirements in the fields of the core networks. Furthermore, our scheme considers a permissioned blockchain network with the features of blockchain. In the network, each legitimate member participates in the system and holds distributed ledgers. Unlike our scheme, the three schemes [15], [16], [32] cannot resist impersonation attacks. Therefore, our scheme is more in line with the features of practical applications. Moreover, Lu *et al.*'s scheme [15] is vulnerable to MitM attacks, replay attacks and stolen smart card attacks. Islam *et al.*'s scheme [16] does not resist the MitM attack. Zhao *et al.*'s scheme [19] cannot protect against offline password guessing attacks. Omar *et al.*'s scheme [21] does not provide the feature of private permissioned blockchain. Therefore, our scheme can achieve better performance.

B. COMPUTATIONAL OVERHEAD

For easy analysis, we employ the related cryptographic operations in the C/C++ OPENSLL library, which aims to simulate the computational overhead of a medical server and end user. We obtain the execution times from [37] and [38], as is described in Table 4. Next, we provide a comparison using these parameters. The results are listed in Table 5.

From Table 5, the computational overhead of He *et al.* [32] and Huawei [19] is lower than that of other schemes because the two schemes use hash functions. Comparatively speaking, the other four schemes are based on ECC. On the contrary, our proposal is lower than that of the other three schemes. However, the computational overhead of our scheme is not much different from that of scheme [16] and [21].

Although the methods of He *et al.* [32] and Huawei [19] seem to be more efficient than our proposal in terms of the number of participants, as expounded in Table 3, the results

TABLE 3. Comparison of functionality features.

Features	Lu et al.[15]	Islam et al.[16]	Zhao et al.[19]	Omar et al.[21]	He et al.[32]	Ours
Mutual authentication	Yes	Yes	Yes	Yes	Yes	Yes
User anonymity	Yes	Yes	Yes	Yes	Yes	Yes
Non-repudiation property	Yes	Yes	Yes	Yes	Yes	Yes
Impersonation attack	No	No	Yes	Yes	No	Yes
Untraceability	Yes	Yes	Yes	Yes	Yes	Yes
Session key agreement	Yes	Yes	Yes	Yes	Yes	Yes
Man-in-the middle attack	No	No	Yes	Yes	Yes	Yes
Replay attack	No	Yes	Yes	Yes	Yes	Yes
Stolen smart card attack	No	Yes	Yes	No	No	Yes
Offline password guessing attack	No	Yes	No	Yes	No	Yes
Private permissioned blockchain	No	No	No	No	No	Yes

TABLE 4. Execution times of different operations (ms).

Symbol	Description	Running time
T_{sm}	Scalar multiplication in G	1.97
T_h	General hash function	0.0004
T_s	Symmetric key cryptography operation	0.1303

TABLE 5. Comparison of computational overhead (ms).

Schemes	User	Medical Server	Overall computational overhead
Lu et al.[15]	$6T_h + 4T_{sm} \approx 7.8824$	$5T_h + 3T_{sm} \approx 5.912$	13.7944
Islam et al.[16]	$6T_h + 2T_{sm} \approx 3.9424$	$3T_h + T_{sm} \approx 1.9712$	5.9136
Zhao et al.[19]	$T_h + T_s \approx 0.1307$	$3T_h + 4T_s \approx 0.5524$	0.6531
Omar et al.[21]	$8T_h + 2T_{sm} \approx 3.9432$	$8T_h + 1T_{sm} \approx 1.9732$	5.9164
He et al.[32]	$4T_h + 3T_s \approx 0.3925$	$T_h + 3T_s \approx 0.3913$	0.7838
Ours	$2T_h + T_{sm} \approx 1.9708$	$3T_h + 2T_{sm} \approx 3.9412$	5.912

TABLE 6. Parameter lengths.

Parameters	Description	Size (bits)
G	Bit length of an element in G	512
ID	Bit length of an identity	256
T	Bit length of a time-stamp	32
r	Bit length of a random number	256
h	Bit length of a hash function	256
C	Bit length of the AES cipher	256

of the above methods are insecure. From the perspective of security, this makes our scheme a more appropriate method. Therefore, our proposal provides better security than others (shown in Table 3).

C. COMMUNICATION OVERHEAD

To better analyse our scenario, we define the bit size of the parameters in our experiments below, in Table 6. A comparison of the communication overhead between our proposal and previous methods is presented for e-health systems in Table 7.

In terms of communication overhead, we provide an analysis in Table 7. From this point of view, it is obvious that our proposal is more efficient than the others. Next, we analyse the bandwidth consumption of the related schemes, which is described in Table 7. Fig. 5 displays the analysis results for the communication overhead with the grown of the number of users and MS_j . From Fig. 5, the communication overhead of all mobility scenarios of our proposal is much better than

TABLE 7. Comparison of bandwidth consumption.

Scheme	Bandwidth consumption(bits)
Lu et al.[15]	2144
Islam et al.[16]	2304
Zhao et al.[19]	1792
Omar et al.[21]	2560
He et al.[32]	567
Ours	1600

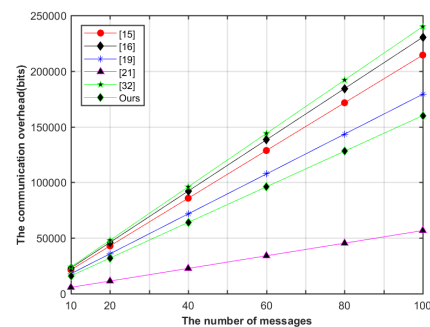


FIGURE 5. Communication overhead of the related schemes.

these schemes in [15], [16], [19], [21], but slightly larger than that of the scheme in [32].

In this context, the efficiency of the scheme in [15] is low, as it has a high communication overhead. Users in the schemes in [16], [19], [21] exchange messages with the

TABLE 8. Simulation parameters.

Parameters	Description
Platform	Ubuntu 16.04 LTS
Hardware platform	Intel Core i5-7500
Propagation model	Two ray channel
MAC protocol	IEEE 802.11n
Number of medical servers	2
Time interval between packets from each user	2 seconds
Speed	50 B/s
Number of patients/doctor	10/20/30/40
Simulation time	1500 seconds
Network coverage area	$10 \times 10 km^2$
Block Size	16 Byte
Previous block hash	100 Byte
Block Header	100 Byte

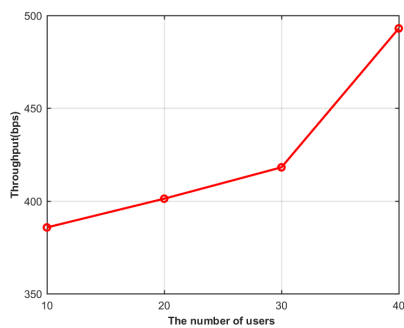


FIGURE 6. Comparison of throughput.

medical server remotely. Thus, the communication overhead incurred by the end users in these schemes is also very high.

VII. NS3 SIMULATION

In the section, our proposal is evaluated employing NS-3 V3.28 simulator [39]. We provide an efficient test method by using relevant feasible parameters. NS-3 is a practical network simulator that is widely used in many research fields, such as blockchain. The parameters of our evaluation proposal are shown in Table 8. In our scenario, the network simulation is performed about 1500 seconds, during which different medical transactions happened. For simplicity, we consider throughput, time overhead in the simulation metrics.

To compare the performance indicators of the scenario, we consider a single scenario in the simulation process as a basic case. Based on this, the basic model does not employ blockchain technology. Furthermore, these protocols only use traditional approaches to authenticate users in the medical systems, which require a third party and various medical servers that perform communication process between different entities.

A. THROUGHPUT

In our scheme, throughput represents the number of health transaction requests that are completed between different medical servers. In Fig. 6, since we use blockchain networks

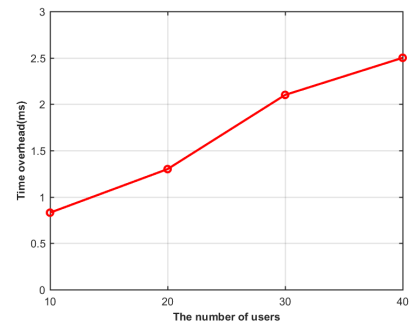


FIGURE 7. Comparison of time overhead.

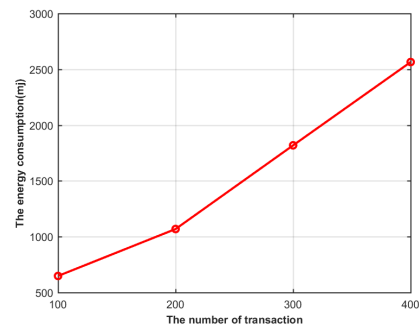


FIGURE 8. Average energy consumption.

and optimized patient authentication algorithms among the medical servers. From Fig. 6, it can be noted that the throughput is expanding with the increasing of the number of users.

B. TIME OVERHEAD

Here it represents the processing time in the authentication process. As indicated in Fig 7, the authentication process of our model for patients/doctors and other entities that is an effective manner of transmission. In addition, it is worth noticing that the time overhead increases with the growth of the number of users.

C. ENERGY CONSUMPTION

Here it represents the consumption when recording, creating or updating medical data during the transactions. It can be calculated as follows:

$$EC_t = U \times T + T \times (MS \times e_j) \quad (37)$$

where EC_t represents the whole energy consumption during transactions, U represents the number of user transactions, MS represents the number of medical service centres, e_j represents energy consumption during each transaction, T denotes the time.

In traditional application scenario, it takes a lot of energy to re-authentication between the user and the medical service center. In our model, we provide an efficient authentication method during transactions that do not require re-authentication. In comparison, our solution reduces energy consumption. However, the energy consumption is also

increasing when the number of transactions increases. The relevant results are illustrated in Fig 8.

VIII. CONCLUSION

The capability to achieve secure and efficient identity management and key authentication is crucial in e-health systems. In this paper, we put forward a PBBIMUA scheme for e-health systems using personal biometrics, which is a new key distribution mechanism. As far as we know, this is the first such scheme that achieves privacy protection by recording identity information using blockchain technology. The findings of the rigorous security analysis confirm that our proposal is secure and can avoid known attacks such as replay, impersonation, and MitM attacks. In addition, a highlight of our proposal is that it supports the function of user credential reissue/update with reduced communication overhead and computational overhead. The performance evaluation indicates that the proposal has better efficiency than most prior schemes. Thus, our scheme has strong scalability and can be widely used in IoT-based e-health environments.

REFERENCES

- [1] S. Krishnan, V. E. Balas, E. G. Julie, Y. H. Robinson, S. Balaji, and R. Kumar, "Blockchain-powered smart healthcare system," in *Handbook of Research on Blockchain Technology*. New York, NY, USA: Academic, 2020, pp. 245–270.
- [2] K. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in *Proc. IEEE Int. Conf. Sensor Netw., Ubiquitous, Trustworthy Comput. (SUTC)*, Taichung, Taiwan, Jun. 2006, pp. 244–251.
- [3] H.-R. Tseng, R.-H. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in *Proc. IEEE GLOBECOM-IEEE Global Telecommun. Conf.*, Washington, DC, USA, Nov. 2007, pp. 26–30.
- [4] T. H. Lee, "Simple dynamic user authentication protocols for wireless sensor networks," in *Proc. 2nd Int. Conf. Sensor Technol. Appl.*, Cap Esterel, France, Aug. 2008, pp. 657–660.
- [5] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009.
- [6] H. F. Huang, Y. F. Chang, and C. H. Liu, "Enhancement of two-factor user authentication in wireless sensor networks," in *Proc. 6th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP)*, Darmstadt, Germany, Oct. 2010, pp. 27–30.
- [7] S. G. Yoo, K. Y. Park, and J. Kim, "A security-performance-balanced user authentication scheme for wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 8, no. 3, Mar. 2012, Art. no. 382810.
- [8] A. K. Das, "Cryptanalysis and further improvement of a biometric-based remote user authentication scheme using smart cards," *Int. J. Netw. Secur. Appl.*, vol. 3, no. 2, pp. 13–28, Mar. 2011.
- [9] X. Li, J.-W. Niu, J. Ma, W.-D. Wang, and C.-L. Liu, "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 73–79, Jan. 2011.
- [10] Y. An, "Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards," *J. Biomed. Biotechnol.*, vol. 2012, pp. 1–6, Jul. 2012.
- [11] M. K. Khan and S. Kumari, "An improved biometrics-based remote user authentication scheme with user anonymity," *BioMed Res. Int.*, vol. 2013, pp. 1–9, Nov. 2013.
- [12] Y. F. Chang, S. H. Yu, and D. R. Shiao, "A uniqueness and anonymity-preserving remote user authentication scheme for connected health care," *J. Med. Syst.*, vol. 37, no. 2, pp. 9980–9988, 2013.
- [13] A. K. Das and A. Goswami, "A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care," *J. Med. Syst.*, vol. 37, no. 3, p. 9948, Jun. 2013.
- [14] H. Arshad and M. Nikooghadam, "Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 38, no. 12, pp. 1–12, Dec. 2014.
- [15] Y. Lu, L. Li, H. Peng, and Y. Yang, "An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem," *J. Med. Syst.*, vol. 39, no. 3, pp. 1–8, Mar. 2015.
- [16] S. H. Islam and M. K. Khan, "Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems," *J. Med. Syst.*, vol. 38, no. 10, pp. 135–142, Oct. 2014.
- [17] L. Zhang and S. Zhu, "Robust ECC-based authenticated key agreement scheme with privacy protection for telecare medicine information systems," *J. Med. Syst.*, vol. 39, no. 5, pp. 49–56, May 2015.
- [18] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019.
- [19] H. Zhao, P. Bai, Y. Peng, and R. Xu, "Efficient key management scheme for health blockchain," *CAAI Trans. Intell. Technol.*, vol. 3, no. 2, pp. 114–118, Jun. 2018.
- [20] F. Tang, S. Ma, Y. Xiang, and C. Lin, "An efficient authentication scheme for blockchain-based electronic health records," *IEEE Access*, vol. 7, pp. 41678–41689, 2019, doi: 10.1109/ACCESS.2019.2904300.
- [21] A. A. Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future Gener. Comput. Syst.*, vol. 95, pp. 511–521, Jun. 2019, doi: 10.1016/j.future.2018.12.044.
- [22] S. Cao, G. Zhang, P. Liu, X. Zhang, and F. Neri, "Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain," *Inf. Sci.*, vol. 485, pp. 427–440, Jun. 2019.
- [23] X. Cheng, F. Chen, D. Xie, H. Sun, and C. Huang, "Design of a secure medical data sharing scheme based on blockchain," *J. Med. Syst.*, vol. 44, no. 2, p. 52, Feb. 2020.
- [24] A. Yazdinejad, G. Srivastava, K.-K.-R. Choo, R. M. Parizi, A. Dehghantaha, and M. Aledhari, "Decentralized authentication of distributed patients in hospital networks using blockchain," *IEEE J. Biomed. Health Inform.*, vol. 24, no. 8, pp. 2146–2156, Aug. 2020, doi: 10.1109/JBHI.2020.2969648.
- [25] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [26] V. Buterin. *Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform*. Accessed: Nov. 19, 2017. [Online]. Available: https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf
- [27] (2019). *Sovrin-Protocol and Token-White-Paper.pdf*. Accessed: Jan. 17, 2019. [Online]. Available: <https://sovrin.org/wpcontent/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf>
- [28] JPMorgan Chase. (2016). *Quorum White Paper*. Accessed: Jan. 17, 2019. [Online]. Available: <https://github.com/jpmorganchase/quorum/blob/master/docs/quorum20whitepaper20v0.2.pdf>
- [29] (2016). *Hyperledger Whitepaper*. Accessed: Jan. 17, 2019. [Online]. Available: <http://blockchainlab.com/pdf/hyperledger-20whitepaper.pdf>
- [30] S. De Angelis, L. Aneillo, R. Baldoni, F. Monbardi, A. Margeheri, and V. Sassone, "PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain," in *Proc. Italian Conf. Cyber Secur.*, Milan, Italy, Feb. 2018.
- [31] M. Wazid, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "Secure three-factor user authentication scheme for Renewable-Energy-Based smart grid environment," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3144–3153, Dec. 2017.
- [32] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, and S.-S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," *Multimedia Syst.*, vol. 21, no. 1, pp. 49–60, Feb. 2015.
- [33] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.
- [34] C. Cremers, "The Scyther tool," Dept. Comput. Sci., Univ. Oxford, Oxford, U.K., 2008. [Online]. Available: <http://www.cs.ox.ac.uk/people/cas.cremers/scyther>
- [35] C. Cremers, "Scyther—semantics and verification of security protocols," Ph.D. dissertation, Inst. Program. Res. Algorithmics, Eindhoven Univ. Technology, Eindhoven, The Netherlands, 2006.
- [36] R. M. Amadio and W. Charatonik, "On name generation and set-based analysis in the Dolev-Yao model," in *Proc. Int. Conf. Concurrency Theory*. Berlin, Germany: Springer, 2002, pp. 499–514.

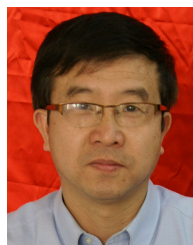
[37] L. Xu and F. Wu, "Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care," *J. Med. Syst.*, vol. 39, no. 2, pp. 10–25, Feb. 2015.

[38] L. Nanni and A. Lumini, "Random subspace for an improved Bio-Hashing for face authentication," *Pattern Recognit. Lett.*, vol. 29, no. 3, pp. 295–300, Feb. 2008.

[39] *Secure Hash Standard*, Standard FIPS PUB 180-1, National Institute of Standards and Technology(NIST), U.S. Department of Commerce, Apr. 1995. [Online]. Available: <http://csrc.nist.gov/publications/fips/fips1802/fips180-2.pdf>



XINYIN XIANG (Member, IEEE) received the Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2015. He has been an Associate Professor with the School of Information, Xi'an University of Finance and Economics, China, since 2011. He has published over 40 journal articles. His research interests include blockchain and lattice-based cryptography.



MINGYU WANG received the Ph.D. degree in statistics from Northwestern Polytechnic University, Xi'an, China, in 2000. He has been a Professor with the School of Information, Xi'an University of Finance and Economics, China, since 2007. He has published over 60 journal articles. His research interests include blockchain and statistics.



WEIGUO FAN (PATRICK) (Senior Member, IEEE) received the B.Sc. degree from Xi'an Jiaotong University, China, in 1995, the M.E. degree from the National University of Singapore in 1998, and the Ph.D. degree from the University of Michigan, in 2002. He is a Full Professor and the Henry B. Tippie Research Chair of business analytics with the Tippie College of Business, University of Iowa. His research has been cited more than 7750 times. He has published more than 200 refereed journal articles and conference papers. His research interests include the design and development of novel information technologies such as information retrieval, data mining, and social media analytics.

...