Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

A Blockchain-assisted Lightweight Anonymous Authentication Scheme for Medical Services in Internet of Medical Things

Shu Wu
Anhui Normal University
Aiqing Zhang (aqzhang2006@163.com)
Anhui Normal University
Jindou Chen
Anhui Normal University
Guangyu Peng
Anhui Normal University
Ya Gao
Anhui Normal University

Research Article

Keywords: Mutual authentication, privacy protection, ban logic, smart contract, IoMT

Posted Date: July 5th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1226695/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

A Blockchain-assisted Lightweight Anonymous Authentication Scheme for Medical Services in Internet of Medical Things

Shu Wu[1], Aiqing Zhang[1*], Jindou Chen[1], Guangyu Peng[1] and Ya Gao[1†]

[1*]College of Physics and Electronic Information, Anhui Normal Univresity, Jiuhua South Road, Wuhu, 241000, Anhui, China.

*Corresponding author(s). E-mail(s): aqzhang2006@163.com;
†These authors contributed equally to this work.

Abstract

Internet of Medical Things (IoMT) enable physicians to provide precise care over the Internet for registered patients anywhere, bringing convenience to people's everyday life. Considering the importance of patient's privacy in IoMT, data security between patients and medical servers should be protected. Therefore, the authentication of identity and the agreement of a shared secret key are particularly important. In this work, we propose a lightweight anonymous authentication scheme between patients and medical servers in IoMT. We combine blockchain technology with biometric technology in order to form a shared session secret key. It can protect the privacy of patients through mutual authentication between patients and servers. Afterwards, the formal analysis of BAN logic shows that our scheme is secure. Non-formal analysis shows that our scheme achieves designed security objectives. Finally, we implement the cryptography primitives to verify our scheme. Comprehensive comparative experiments show that our proposed scheme achieves a better performance in both computation and communication efficiency.

Keywords: Mutual authentication, privacy protection, ban logic, smart contract, IoMT

1 Introduction

With the development of information technology, Internet of Medical Things has been integrated into people's daily life, bringing great convenience to medical treatment. 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 internet of medical things, patients are facing privacy leakage and network attacks while enjoying the convenience of electronic medical services[1].

Accordingly, how to protect privacy has become a major issue in IoMT. Wang[2] demonstrates that authentication technology is usually used to achieve a high-level privacy protection scheme. In order to complete the authentication between the user and multiple servers in IoMT, a complex data sharing scheme is required. However, it is often believed that servers are centralized, honest, and curious[3]. Although the centralized "client-server" model can fulfill the patient's authentication, centralization brings various privacy and security challenges[4, 5]. How to achieve effective authentication between patients and medical servers while protecting privacy is a worthwhile studying question.

In the IoMT environment, there must be a lightweight authentication scheme to achieve patient authentication due to limited computing power of patient devices. Although many authentication schemes have been proposed by scholars[6–8], it is difficult to balance validity and computational complexity. They are deficient in security and reliability more or less.

In recent years, the research of blockchain has attracted more and more attentions. Blockchain-assisted technology provides a potential way for authentication scheme, especially in medical field, the internet of vehicles, and smart grid, etc. [9–11]. Unfortunately, there are little researches on lightweight authentication scheme for medical field based on blockchain currently.

Therefore, we propose a lightweight anonymous authentication scheme based on consortium blockchain in IoMT. Members of the consortium blockchain include server nodes and the registration center (RC). In summary, our scheme realizes lightweight mutual authentication between patients and medical servers based on the consortium blockchain. The main contributions of the article are as follows:

- we propose a lightweight anonymous authentication scheme between patients and medical servers based on consortium blockchain in IoMT. Our scheme achieves privacy protection, data confidentiality and integrity, resistance to replay attacks, resistance to masquerading attacks, and resistance to offline password guessing attacks.
- We design concrete implementation steps for the authentication protocol. It combines blockchain and fuzzy extraction technology. The secret key can be shared between the patient and the server when mutual authentication is completed in our protocol. What's more, we formalize the proof (using BAN logic language) in order to ensure the reliability and security of the protocol.

- We conduct a detailed comparison of our protocol with compared protocols. Our scheme can protect the privacy of patients well. Furthermore, our scheme mainly uses XOR and hash algorithms for mutual authentication, instead of using bilinear pairing with a large amount of calculation. Therefore, the authentication scheme is lightweight. It does not take up too much memory resource in IoMT environment. The time complexity and space complexity of our authentication scheme are low. It is particularly suitable for deployment in IoMT environment.

The remaining part of this paper is organized as follows: An overview about existing works is described in section 2. Preliminaries are presented in section 3. Section 4 describes the system architecture, the threat model and security requirements. Afterwards, section 5 describes the details of the agreement. Furthermore, we do security analysis, including formal analysis and nonformal analysis in section 6. We compare the computational overhead and communication overhead with comparative approaches in section 7. Finally, section 8 concludes the work.

2 Related Work

In this section, we first present research trends of authentication in IoMT. Then, we conduct a brief report about blockchain-assisted technology for medical services.

A. Authentication in IoMT

In recent years, scholars have proposed many authentication and key agreement schemes in IoMT. A user authentication scheme based on lightweight passwords was proposed by Lamport[12] for the first time. The scheme relies on the password only, thus it is not secure enough. Thereafter, several authentication schemes were proposed for various applications as follows.

Malasri[13] proposed a wireless sensor network authentication scheme based on an elliptic curve in IoMT. Unfortunately, the scheme is vulnerable to relay node attacks and denial of service provision. Chuang[14] proposed a multi-server environment-based biometric anonymous authentication scheme, but Mishr[15] pointed out that the scheme is vulnerable to server spoofing, smart card theft, and counterfeiting attacks. Based on the mobile edge computing network, He[16] designed an improved user authentication scheme. However, Odelu et al.[17] proved that He's scheme is prone to replay attack, tracking attacks, and user simulation. They[17] proposed a biometric based smart card authentication protocol, which could better overcome the above shortcomings. In [18], Jia et al. proposed an anonymous authentication scheme based on fog computing environment. It is also apt to a temporary session attack because the attacker can guess the identity of the user when the user session key is leaked. Irshad.[19] proposed a pairing-free lightweight authentication protocol for mobile cloud computing framework. The authentication was achieved without involvement of trusted entity. It also lacks the formal security analysis.

In addition, Kumari et al.[20] proposed a provable secure multi server authentication scheme based on cloud computing. However, Feng[21] found that the scheme proposed in [20] failed to guarantee user anonymity and perfect forward security. So they designed a multi server authentication scheme based on anonymous biometrics. Meanwhile, A three factor multi server authentication scheme based on elliptic curve cryptology system was proposed by Ali and Pal in [22]. But Wang[23] pointed out that it is vulnerable to user simulation and denial of service attacks. Thereafter, Wang et al. [23] proposed an improved authentication scheme. However, Wu[24] underlined that the scheme proposed by Wang et al. is vulnerable to user simulation and server simulation attacks.

The above authentication schemes mainly rely on flexible security models and ingenious interaction schemes. It is mainly assumed that there is a trusted authoritative center, which could make the network vulnerable to be damaged due to a single point of failure. One of the ideal ways to solve centralization problem is to use blockchain-assisted technology.

B. Blockchain for medical services

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 authenticity, reliability, and non-tampering of data.

Recently, Ekblaw[25] proposed an electronic medical record management system in IoMT, 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. Jiang[26] built a healthcare information exchange blockchain platform, which combines offline storage and online verification to ensure the privacy and authentication of healthcare data. In [27], Wang. et al. gave an authentication protocol based blockchain for user identity management, but Vivekanandan[28] pointed out that the computation cost of [27] is more higher. Siyal[29] 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 [29] could not guarantee the reliability of data. It would lead to the decline of data availability. What's more, Sastry et al. [30] proposed a user authentication protocol in mobile cloud environment based on blockchian. They used a three-factor authentication mechanism to authenticate users by bilinear pairing. However, the use of bilinear pairs brings high computational costs.

Yaz [31] proposed a novel decentralized authentication of patients in a distributed hospital network. However, the approach of [31] is decentralized. It was designed for IoT devices with limited computational, memory and energy capabilities. Nevertheless, it did not involve that how to implement a prototype of the proposed approach in a real-world setting. In[32], Fan et al. proposed a verifiable scheme to achieve one-to-many data sharing via blockchian. The

blockchain data is maintained by users, but it is difficult to determine the consortium blockchain members. Recently, Zhang et al. in [33] proposed a transaction processing scheme for IoT consortium blockchain adaptively with IoMT applications, which is proved to achieve anonymous, traceability, and nonframeability.

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 reliability of data. These works also did not provide detailed solutions for specific applications. In this work, we design an anonymous authentication scheme based on the consortium blockchain, in which the secret key is shared between the patient and the server. The protocol can protect patient privacy and achieve a variety of security requirements.

3 Preliminaries

3.1 Complexity assumption

We put forward technical preliminaries in this subsection. Our scheme is based on the following two difficult problems, which cannot be solved in finite polynomial time.

Definition 1. Elliptic Curve Discrete Logarithm Problem (ECDLP). Let G be an additive cycle consisting of points on the elliptic curve. P is a generator of G, and q is the order of group G. ECDLP problem can be described as: Given xP, output x in polynomial time.

ECDLP Assumption: It is assumed that it is difficult to calculate x under the circumstance of $xP \in G$ in polynomial time.

Definition 2. Computational Diffie-Hellman Problem (CDHP). Given $P, aP, bP \in G$, P is a generator of a cyclic group G with order q. a and b are unknown random numbers where $a, b \in Z_q^*$. An algorithm that solves the computational Diffie-Hellman problem is a probabilistic polynomial time turing machine. The input of turing machine is (P, aP, bP). The output of turing machine is abP.

CDHP Assumption: Computational Diffie-Hellman assumption means that there is no such a probabilistic polynomial time turing machine to solve the CDHP.

3.2 Fuzzy extraction technique

Considering that the biological characteristics of the same person may have small errors each time, we use fuzzy extraction technology to overcome the impact of such small differences. The same random string is restored when the difference in biological characteristics is less than the threshold. Specifically, 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 input is the patient's biometrics BIO_i. The output 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 re-input is less than the threshold.

3.3 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. In the absence of a trusted central node, the blockchain can achieve mutual trust and consensus among network nodes. 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 IoMT environment. The consortium blockchain generally consists of pre-selecting nodes in an industry consortium. These accounting nodes adopt a certain consensus to determine the generation and addition of blocks. 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.

4 System model

In this section, we describe composition of the system model and function of each entity. In addition, we also present the threat model and security goals in IoMT environment.

4.1 System architecture

The system consists of five entities: patients, smart terminals, registration center, servers, and blockchain network. In particular, the blockchain network includes blockchain and smart contracts. The system model is shown in Fig.1.

4.1.1 Patient

Firstly, 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. When the patient completes registration and identity verification, a shared key is formed and relevant medical services are provided for patients in turn.

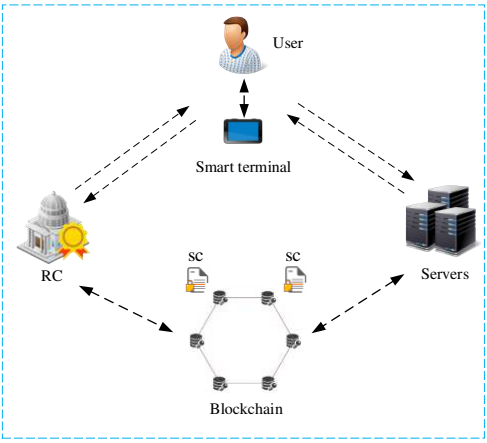

Fig. 1 System Model.

4.1.2 Smart terminal

The smart terminal can collect the patient's password, biometric information, and identity information in the mobile edge computing network. They are sent to *RC* subsequently. It's worth noting that the smart terminal can be authenticated by the server after being registered with the *RC*.

4.1.3 Registration center

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 and the user is not registered simultaneously. When the user completes the registration, the *RC* uploads relevant information (such as a hash value of the patient's identity, a hash value of the XOR of key and biological features) to the blockchain via a smart contract.

4.1.4 Servers

Once receiving the authentication request message from the smart terminal, the server decides whether the user authentication message is legal or not, by comparing the user authentication message with the registration information on the blockchain.

Furthermore, the user also needs to complete the authentication for the server. 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.

4.1.5 Blockchain

Blockchain can guarantee the imtamability and integrity of data. In details, patients upload their anonymous and real identities to the blockchain in IoMT. The server compares whether the user's real identity is tampered with by the attacker. As a general view, we use the consortium blockchain in our schemes. The consensus mechanism uses the PBFT algorithm. Members of the consortium blockchain include *RC* and every server in IoMT environment.

4.2 Threat model

In our scheme, we consider the registry to be credible, and the data stored in the server database to be secure. The attacker cannot steal the data in the server database. There is a pre-shared secret key between the registry and the server. Particularly, the secret key is only known to the registry and the server.

We assume that the communication between the registry and the server is secure in IoMT. It means that their pre-shared secret keys are not compromised. We assume that attackers can intercept the communication messages between the patient and the server in the mobile edge computing environment. We assume that attackers may launch the following attacks, such as replay attack, masquerading user attack, masquerading server attack, or offline password guessing attack.

4.3 Security requirements

Taking into account the above security threats in IoMT, security requirements are described as follows:

Date confidentiality and integrity. Date confidentiality and integrity should be guaranteed by encryption and signature. The key can guarantee the confidentiality of the patient's data. Attackers fail to recover the shared key from the intercepted message. Blockchain should ensure that the data uploaded to the ledger will not be tampered with. In a general way, it is critical to protect patients' medical information.

Resist replay attacks. An external adversary may capture the previous message and replays the out-of-date messages to victim. Replay attacks can render the system unservicable, causing delays in patient care. Here, our scheme uses a timestamp and random number mechanism. It can effectively resist the attacker's replay attack.

Resist masquerading attack. In order to maintain the security of the patient's identity, the unique identity of the patient should not be misused by strangers. In other words, the attacker cannot forge a legal patient's identity for authentication (i.e., the attacker cannot pretend to be a patient for authentication by spoofing the server).

Resistance to offline password guessing attacks. Patient's password is sensitive information. It is fairly important to keep it secure. Passwords should not be inferred from existing knowledge. It is not feasible for an attacker to try

Table 1 Symbols and description

Symbol	Description
$Gen()$:	Key generation algorithm
$Rep()$:	Key recovery algorithm
SP :	Random string
A_i :	Hash mapping of user's personal information calculated by RC
BIO_i :	Biometric information of the patient i
G :	The set of points on the additive
Z_q^* :	A reduced residue systems modulo q
m :	A nonce selected by RC
P :	Generator in elliptic curve group
V_u :	A intermediate parameters
PP :	Auxiliary string
μ :	A shared key between smart terminal and registration center
ID_i :	The identity of the patient i
B_i :	A Parameter calculated by registration center
PW_i :	The key entered by the patient i
AID_i :	The anonymous identity of patient i
m_i :	A secret number selected by patient i
k_{ij}, k_{ji} :	A shared key between patient i and server j
m_j :	A secret number selected by server j
PSK :	Pre-shared key between registration center and server

to log in by guessing the password offline, because an attacker can not access knowledge of the password.

Effective anonymous privacy protection. Attackers cannot deduce the patient's identity information from the anonymous information. Malicious attackers cannot infer the user's real identity from the user's anonymous information. The patient's private information should be guaranteed effectively.

5 Proposed protocol

In this section, we first present an overview about the process of our protocol briefly. Table 1 shows some of the parameters used in our protocol. Afterwards, we describe the proposed protocol in details, as shown in Fig.2.

5.1 Overview

The protocol is made up of three phases: system setup phase, registration phase, and authentication phase.

when a patient i with identity ID_i arrives at a hospital for a medical service, he/she firstly sent $Me1 = \{ID_i, PW_i, BIO_i\}$ to RC, then RC can obtain $Me1$. RC calculates SP and PP according to the user's biometrics BIO_i through the

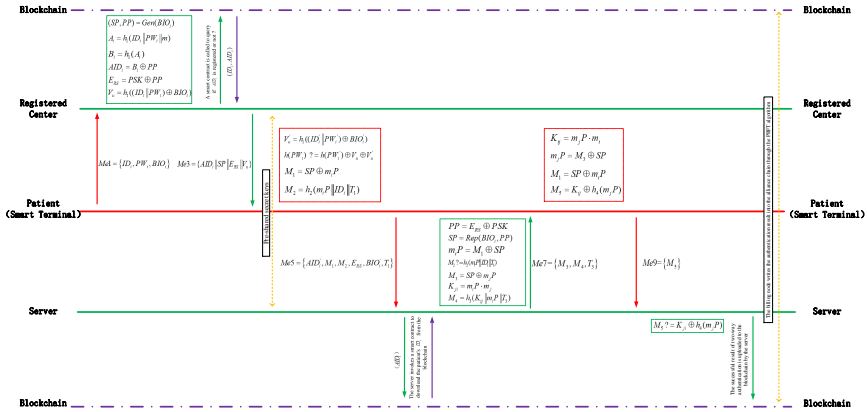

Fig. 2 The chart of protocol flow

fuzzy extraction function. Also, RC calculates $A_i, B_i, AID_i, E_{RS}, V_u$ respectively, where AID_i is an anonymity of the patient i. RC invokes the smart contract in blockchain to determine whether the patient i is registered. If AID_i has not been registered, RC will add AID_i to the registerable list using smart contracts.

Afterwards, the patient i generates $Me5=\{AID_i', M_1, M_2, E_{RS}, T_1\}$ and sends it as an authentication message to the server.

Once receiving the authentication message, the server invokes the smart contract to check the user's identity information ID_i. It checks whether the following equation is true or not:

$$M_2 \stackrel{?}{=} h_2(m_i P \| ID_i \| T_1)$$

Whereafter, the server has completed the one-way authentication of the patient. Similarly, the server replies the response information $\{M_3, M_4, T_3\}$ to the patient's smart terminal. The server is certified by the patient if the following equation is proved to be true.

$$M_4 \stackrel{?}{=} h_3(K_{ij} \| m_i P \| T_3)$$

Finally, the server and the patient form a shared session key k_{ij}. The server sends the authentication result to the accounting node and writes it to the consortium blockchain through the PBFT algorithm. The authentication message is disclosed on the consortium blockchain.

5.2 Protocol description

The proposed protocol contains three process: System setup phase, Registration phase, and Authentication phase.

Phase1: System setup phase

Step1: G_1 is an additive cyclic group of points on an elliptic curve. P is the generator of a cyclic group. 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

Step1: The patient i enters personal information such as ID_i, PW_i ,BIO_i on the smart terminal. Once the smart card receives the above information, it sents $Me1 = \{ID_i, PW_i, BIO_i\}$ to RC via a secure channel.

Step2: RC first carries out a preliminary identification of the user's ID_i to ensure that the patient can be effectively treated in the hospital. If the user's ID_i is valid, RC will authorize the patient's identity and continue to work on the next operation.

Step3: 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. m is a nonce selected by RC. AID_i is the anonymity of ID_i. E_{RS} and V_u are intermediate parameters.

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

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

$B_i = h_1(A_i)$

$AID_i = B_i \oplus PP$

$E_{RS} = PSK \oplus PP$

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

What is noteworthy is that PSK is the pre-shared key between RC and server, which is only shared between RC and server.

Step4: The 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 sents $Me3 = \{AID_i \| SP \| E_{RS} \| V_u \}$ 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 if AID_i has already existed on blockchain, it indicates that the patient has been registered before and it can directly enter the authentication phase.

Phase3: Authentication phase

Step1: The patient enters identity ID_i' , password PW_i' , and Biological characteristics BIO_i' on the smart terminal.

Step2: The smart terminal calculates the following equation:

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

Subsequently, it checks whether the following equation holds or not:

$h(PW_i) \stackrel{?}{=} h(PW_i') \oplus V_u \oplus V_u'$

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

Step3: 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 follows:

$M_1 = SP \oplus m_i P$

$M_2 = h_2(m_i P \| AID_i' \| T_1)$

Then it sends $Me5 = \{AID_i', M_1, M_2, E_{RS}, BIO_i', T_1\}$ as authentication information requested for the server.

Step4: 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. PP is recovered from E_{RS} using the pre-shared secret key PSK.

$PP = E_{RS} \oplus PSK$

$SP = Rep(BIO_i, PP)$

$m_i P = M_1 \oplus SP$

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

$M_2 \stackrel{?}{=} h_2(m_i P \| ID_i \| T_1)$

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

Step5: The server chooses a nonce $m_j \in Z_q^*$ secretly and calculates $m_j P$. Then the server calculates the following parameters:

$M_3 = SP \oplus m_j P$

$M_4 = h_3(K_{ji} \| m_i P \| T_3)$

The server can calculate the shared session key as follow:

$K_{ji} = m_j \cdot m_i P = m_i m_j P$

Server replies to the patient with a message $Me7 = \{M_3, M_4, T_3\}$.

Step6: 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 stops. Otherwise, it continues to perform as follows:

$m_j P = M_3 \oplus SP$

$K_{ij} = m_i \cdot m_j P = m_i m_j P$

Thus the smart terminal also verifies whether the following equation holds or not:

$M_4 \stackrel{?}{=} h_3(K_{ij} \| m_i P \| T_3)$

If it does not hold, it will stop. Otherwise, the smart terminal continues to calculate follow parameters:

$M_5 = K_{ij} \oplus h_4(m_j P)$

It sends a confirmation message $Me9 = \{M_5\}$ to the server.

Step7: The server verifies the following equation:

$M_5 \stackrel{?}{=} K_{ji} \oplus h_4(m_j P)$

If the equation holds, the certification is completed. 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.

6 Security analysis

In this section, we describe formal and informal security analysis for our scheme. Formal security analysis is done by BAN logic. It verifies the security features of our scheme to ensure the session key protocol between the patient and the server. Informal security analysis is accomplished by analyzing protocols against several related attacks.

6.1 Formal analysis

BAN logic is a formal analysis method proposed by Burrows [34]. It is used to define and analyze the communication process between two parties. The specific instructions are as follows:

1. The message-meaning rule: The entity A believes that the key k is shared by A and B. A receives X which is encrypted with k. Then A believes B once said X.

$$\frac{A \mid\equiv A \overset{K}{\leftrightarrow} B, A \triangleleft \{X\}_K}{A \mid\equiv\mid B \sim X}$$

2. The nonce verification rule: If A believes that X is fresh and B sends X to A, A believes that B believes X.

$$\frac{A \mid\equiv \#X, A \mid\equiv B \mid\sim X}{A \mid\equiv B \mid\equiv X}$$

3. The belief rule: If A has trusted in the set of messages (X, Y), A trusts in the message X.

$$\frac{A \mid\equiv (X, Y)}{A \mid\equiv X}$$

4. The fresh conjunction rule: If A believes the part of (X, Y) is fresh, A believes that the whole (X, Y) is fresh.

$$\frac{A \mid\equiv \#X}{A \mid\equiv \#(X, Y)}$$

5. The jurisdiction rule: If A believes that B has jurisdiction rule over the message X, and A trusts B on the trueness of X, A trusts B on the trueness of X.

$$\frac{A \mid\equiv B \Rightarrow X, A \mid\equiv B \mid\equiv X}{A \mid\equiv X}$$

Idealization

The protocol is idealized as follow:

$U \to S: < m_i P >_{u \overset{SP}{\leftrightarrow} s}, \ (m_j P, T_1)$

$S \to U: < \quad m_j P \quad >_{u \overset{SP}{\leftrightarrow} s}, \ (m_j \cdot m_i P, \ m_j P, \ T_1)$

Initial state assumption

In the protocol, there are the following assumptions in the initial state.

$A_1: \ U \mid\equiv \#m_i$

$A_2: \ S \mid\equiv \#m_j$

$A_3: \ U \mid\equiv U \overset{SP}{\leftrightarrow} S$

$A_4: \ \ S \mid\equiv U \overset{SP}{\leftrightarrow} S$

$A_5: \ \ U \mid\equiv S \Rightarrow (U \overset{k_{ij}}{\leftrightarrow} S)$

$A_6: \ \ S \mid\equiv U \Rightarrow (U \overset{k_{ji}}{\leftrightarrow} S$

Security goals

Our scheme is considered to meet the certification requirements if it achieves the following goals: $G_1: S \mid\equiv U \mid\equiv U \overset{k_{ij}}{\leftrightarrow} S$

$G_2: S \mid\equiv U \overset{k_{ij}}{\leftrightarrow} S$

$G_3: U \mid\equiv S \mid\equiv U \overset{k_{ij}}{\leftrightarrow} S$

$G_4: U \mid\equiv U \overset{k_{ij}}{\leftrightarrow} S$

Scheme analysis

Here, we analyze the protocol using rules and assumptions.

S_1: From A_3 and $U \triangleleft \ (U \overset{k_{ij}}{\leftrightarrow} S, \ m_i P, \ T_3)_{u \overset{SP}{\leftrightarrow} s}$, by applying the message-meaning rule, we get: $U \mid\equiv S \sim \ (U \overset{k_{ij}}{\leftrightarrow} S, \ m_i P, \ T_3)$.

S_2: Since A_1 and $U \mid\equiv S \sim \ (U \overset{k_{ij}}{\leftrightarrow} S, \ m_u P, \ T_3)$, From the fresh conjunction rule, we can reach: $U \mid\equiv \# \ (U \overset{k_{ij}}{\leftrightarrow} S, \ m_i P, \ T_3)$, by the nonce-verification rules, we reach: $U \mid\equiv S \mid\equiv \ (U \overset{k_{ij}}{\leftrightarrow} S, \ m_i P, \ T_3)$.

G_1: From S_2 and the belief rule, we obtain: $U \mid\equiv S \mid\equiv U \overset{k_{ij}}{\leftrightarrow} S$.

G_2: From A_5 and G_1 , by applying the jurisdiction rule, we get: $U \mid\equiv U \overset{k_{ij}}{\leftrightarrow} S$.

S_3: From A_4 and $S \triangleleft \ (U \overset{k_{ij}}{\leftrightarrow} S, \ m_j P, \ T_1)_{u \overset{SP}{\leftrightarrow} s}$, by applying the message-meaning rule, we get: $S \mid\equiv U \sim \ (U \overset{k_{ij}}{\leftrightarrow} S, \ m_j P, \ T_1)$.

S_4: Since A_2 and $S \mid\equiv U \sim \ (U \overset{k_{ij}}{\leftrightarrow} S, \ m_j P, \ T_1)$, from the fresh conjunction rule, we can reach: $S \mid\equiv \# \ (U \overset{k_{ij}}{\leftrightarrow} S, \ m_j P, \ T_1)$, by using the nonce-verification rules, we reach: $S \mid\equiv U \mid\equiv \ (U \overset{k_{ij}}{\leftrightarrow} S, \ m_j P, \ T_1)$.

G_3: From S_4 and the belief rule, we obtain $S \mid\equiv U \mid\equiv U \overset{k_{ij}}{\leftrightarrow} S$.

G_4: From A_6 and G_3, by the jurisdiction rule, we get: $S \mid\equiv U \mid \overset{k_{ij}}{\leftrightarrow} S$.

The above proof shows that the expected goal is realized. It demonstrates that our scheme achieves mutual authentication between patient i and server j in IoMT. Meanwhile, patient i and server j believe that the session key $K_{ij} = m_i m_j P$ is shared between them in the mobile edge computing network.

6.2 Nonformal analysis

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

6.2.1 The proposed protocol can achieve data confidentiality and integrity

The patient uses the shared session key K_{ij}=$m_i m_j P$ to encrypt the message when the authentication is completed. The patient will use the secret key $m_i m_j P$ to encrypt the registration message. So the ciphertext fail to be decrypted if there is no decryption key.

Under the assumptions of ECDLP, given $m_i P \in G$, it is difficult to calculate m_i. What's more, even if the attacker intercepts $m_i P$ and $m_j P$, it still cannot obtain $m_i m_j P$ because calculating K_{ij} from $m_i P$ and $m_j P$ is a CDHP difficult problem. Thus, only the expected user can decrypt the ciphertext, which enhances data confidentiality. Finally, the blockchain is a distributed multi-party secure ledger. Related information is stored on the blockchain. The data of the blockchain can't be tampered with, which ensures data integrity.

6.2.2 The proposed protocol can resist replay attacks

Our scheme uses timestamps and random numbers, which can resist replay attacks. Firstly, the timestamp T_1, T_2, T_3, T_4 is used to avoid replay attacks. It can ensure the freshness of the message.

Specifically, the patient's authentication message contains a timestamp such as $\{AID_i', M_1, M_2, E_{RS}, T_1\}$. Thereby the attacker's replay attack is avoided by comparing the timestamps. Secondly, replay attacks are avoided because of the use of random numbers. It can be avoided by judging whether the random numbers contained in the reply message are the same as the initial values.

6.2.3 The proposed protocol can resist masquerading attacks

The attacker cannot forge the patient's authentication message to pass authentication. On the one hand, the attacker does not have the user's ID_i and the server's random number m, so the attacker cannot forge AID_i. On the other hand, even if the user intercepts the user's anonymous identity, the attacker cannot forge $M_2 = h_2(m_i P \| AID_i' \| T_1)$ because the attacker cannot forge $m_i P$.

In addition, it is unrealistic for the attacker to recover $m_i P$ from M_1, because the attacker fail to obtain SP. SP is generated by the biological characteristics of the patient. So the attacker can't pretend to be the user.

6.2.4 The proposed protocol can resist offline password guessing attacks

If the attacker holds the patient's smart terminal and attempts to log in by guessing the password offline, it is also not feasible. Because the following equation can't be passed.

$h(PW_i) \stackrel{?}{=} h(PW_i') \oplus V_u \oplus V_u'$

Obviously, the attacker fails to obtain the user's identity information and biometric information. So the attacker fails to perform offline password guessing attacks.

6.2.5 The proposed protocol can achieve anonymity and privacy protection of information

Firstly, the user obtains the anonymity AID_i which is assigned by the registry. The generation of anonymity requires a random number m provided by the registry. The attacker cannot obtain the random number m, so the anonymity can not be faked by the attacker.

In addition, patients use anonymity AID_i for registration and authentication without revealing their real identity ID_i, which could protect personal privacy. Finally, even if a malicious attacker intercepts the patient's anonymous information such as AID_i, the attacker still could not obtain the patient's real ID_i from the anonymous AID_i due to the one-way nature of the hash function. It also protects the patient's privacy.

7 Implementation and performance evaluation

In this section, we compare security properties: the communication overhead and computational overhead with other comparative schemes.

7.1 Comparisons of security properties

To show the security of our scheme, we compared the security properties of our scheme with existing authentication schemes. From Table 2, it is very obvious that only our scheme has conducted multiple security properties. Existing schemes introduced in[35, 36, 38–40] are vulnerable to several security threats compared with our work.

In particularly, we use blockchain technology to protect the integrity and reliability of data in IoMT. What's more, the consortium blockchain also guarantees the security of data. Meanwhile, non-consortium members cannot access the ledger on the blockchain. So it easily comes to the conclusion that our scheme can achieve better security goals.

7.2 Comparisons of communication overhead

In this subsection, we compare the communication overhead of our scheme with that of several other schemes. We use the Type A curves defined within

the PBC library because they are widely used in primitives cryptography. In the PBC library, the Type A curve is chosen as $E(F_q) : y^2 = x^3 + x$. The group order of G_1 is $160bits$ and the order of the base field is $512bits$. So p is a $512bits$ prime number and q is also a $512bits$ prime number. The length of the element in $G1$ is $1024bits$. The output length of hash map is $160bits$.

We denote that $\mid G \mid$ is the size of an element in group G_1 and $\mid Q \mid$ is the size of an element in Zp. It's easy to figure out that $\mid G \mid = 1024bits$, and $\mid Q \mid = 160bits$. It should be pointed out that the length of a respose message or an identity were all set to $32bits$. The timestamp is set to 32 bits in our implementation. Specifically, the packet sizes in our experiment are as follows: $\mid AID_i \mid = 160bits$, $\mid SP \mid = 160bits$, $\mid E_{RS} \mid = 160bits$, $\mid V_u \mid = 160bits$, $\mid PW_i \mid = 32bits$ and $\mid ID_i \mid = 32bits$. As mentioned above, the blockchain is designed to guarantee the reliability and immutability of certificates, so the communication overhead of uploading and downloading to blockchain were ignored in order to unify the benchmark.

We mainly compare cryptography communication overhead with [38–40] in Table 3. In registration phase of our scheme, the content of communication overhead includes $Me1 = \{ID_i, PW_i, BIO_i\}$. $Me3 = \{AID_i \| SP \| E_{RS} \| V_u \}$. The total communication overhead is $5 \mid Q \mid +64 = 864$ $bits$. Meanwhile, the communication overhead of Kumar[38] is $\mid G \mid +32 = 1056$ $bits$. The communication overhead of Tsai[39] is $\mid G \mid +32 = 1056$ $bits$. The communication overhead of Lwamo.[40] is $3 \mid Q \mid +32 = 512$ $bits$. It can be found that the communication overhead of our scheme is lower than that of [38] and [39], except for [40].

In authentication phase, the communication overhead in our scheme contains $Me5$, $Me7$, and $Me9$. Communication overhead of $Me5 = \{AID_i', M_1, M_2, E_{RS}, BIO_i', T\}$ is $160bits + 1024bits + 160bits + 160bits + 160bits + 32bits = 1696bits$. Communication overhead of $Me7 = \{M_3, M_4, T_3\}$ is $1024bits + 160bits + 32bits = 1216bits$. Communication overhead of $Me9 = \{M_5\}$ is $160bits$. So the total communication overhead is $1696bits + 1216bits + 160bits = 2 \mid G \mid +6 \mid Q \mid +32 * 2 = 3072$ $bits$. As a contrast, the communication overhead of [38] is $2 \mid G \mid +2 \mid Q \mid +32 = 2400$ $bits$. The communication overheads of [39] and [40] are $3 \mid G \mid + \mid Q \mid +32 = 3264$ $bits$ and $10 \mid Q \mid +32 = 1632$ $bits$ respectively.

It should be pointed out that there are two reasons for higher communication overhead in our sheme contrasted to [38, 40]. One reason is that we hide the random secret number in the group elements (e.g. m_iP, m_jP) in the communication process in order to enhance the security of the protocol. The other reason is that we get a lower computational complexity and a more robust safety feature at the expense of some communication overhead.

7.3 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 used in this paper was evaluated by referring to the experimental

Table 2 Comparison of security properties

Properties	Chuang[35]	He[38]	Tsai[39]	Lwamo[40]	[The proposed]
Data confidentiality and integrity	√	√	√	√	√
Resist replay attacks	×	√	√	√	√
Resist masquerading attacks	√	×	×	√	√
Resist offline guessing attacks	√	√	×	×	√
Anonymity and privacy protection	×	√	√	√	√
The lightweight of the scheme	×	√	√	√	√
Blockchain technology utilized	×	×	×	×	√

Table 3 Communication overhead

Transactions	Registration phase	Authentication phase
The proposed	5 | Q | +64	2 | G | +6 | Q | +64
Kumar[38]	| G | +32	2 | G | +2 | Q | +32
Tsai[39]	| G | +32	3 | G | + | Q | +32
Lwamo[40]	3 | Q | +32	10 | Q | +32

Table 4 Computational overhead

Protocols	Registration phase	Authentication phase
The proposed	$3T_h + 3T_{xor}$	$7T_h + 2T_{xor} + 4T_{mul}$
Kumar[38]	$T_{mtp} + 3T_{mul} + 3T_{\exp} + 2T_{pa} + 4T_h$	$2T_{bp} + T_{pa} + 3T_{\exp} + 2T_{mul} + 5T_h + T_{mul}$
Tsai[39]	$T_{mtp} + 5T_{mul} + T_{\exp} + 4T_h$	$2T_{bp} + 2T_{mul} + 2T_{pa} + 2T_{\exp} + 4T_h$
Lwamo[40]	$5T_h + T_{xor} + T_{dec}$	$9T_h + T_{xor} + 3T_{enc} + 3T_{dec}$

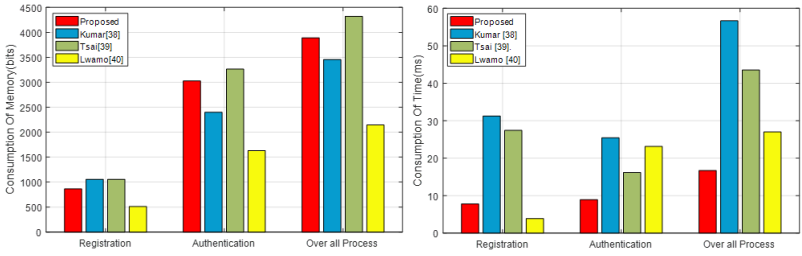

Fig. 3 Comparison of computational cost of experiment

benchmark given by Kilinc and Yanik[37]. In computational overhead analysis, 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 the computational overhead of XOR operation time is disregarded.

We compared the computational cost of our scheme with that of the comparative schemes. In Registration phase, the computational cost of our scheme is $3T_h + 3T_{xor} = 0.0069ms$. As a contrast, the computational cost of [38–40] is $31.23ms, 27.41ms$, and $3.86ms$ respectively. In authentication scenario, the computational cost of [38–40] is $25.44ms, 16.14ms$, and $23.13ms$, but in fact, the computational cost of our scheme is only $7T_h + 2T_{xor} + 4T_{mul} = 8.92ms$, which is the least amount of time compared with the other literatures in our experiment, as shown in Table 4.

Furthermore, Fig.3 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. This is because we used lightweight algorithms such as hash functions and XOR, instead of variable operation on groups and bilinear pairs. In details, our communication overhead is not too expensive. Therefore, our scheme achieves a better experimental performance in both computation and communication efficiency.

8 Conclusion

In this work, we have proposed a lightweight anonymous authentication scheme based on the consortium blockchain to achieve mutual authentication between patients and medical servers in IoMT. blockchain-assisted technology is used to ensure the confidentiality and integrity of patients private data. Meanwhile, fuzzy extraction technology is used to realize key aggregation. In addition, the proof of BAN logic demonstrates the security of the proposed scheme. Informal safety analysis shows that our scheme has achieved the designed security goals. Finally, comparative experiment shows that our scheme achieves a better performance in computation and communication overhead. It is an efficient mutual authentication protocol in IoMT.

Declarations

- Funding
  This study was funded by the National Natural Science Foundation of China (Grants No. 62072005), Natural Science Foundation of Anhui Province (No. 2108085Y22, 1808085MF164), and Anhui Provincial Engineering Laboratory on Information Fusion and Control of Intelligent Rabot (Grant No. IFCIR2020008).
- Conflict of interest
  The authors declare that they have no conflict of interest.
- Ethics approval
  This article does not contain any studies with human participants or animals performed by any of the authors.
- Consent to participate

Not applicable

- Consent for publication
  If the article is accepted for publication, the copyright of the English article will be transferred to Springer.
- Availability of data and materials
  Not applicable
- Code availability
  The software of experiments is based on the PBC library.
- Authors' contributions
  Shu Wu contributed to protocl design and manuscript preparation; Aiqing Zhang performed the protocol analysis and important guidance work; Jindou Chen contributed to protocol analysis and manuscript preparation; Guangyu Peng designed system model and security objectives; Xinrong Ye designed securiyt objectives and protocl analysis.

References

[1] Wei F., Kumar N., "Privacy-Preserving Implicit Authentication Protocol Using Cosine Similarity for Internet of Things", *IEEE Internet of Things Journal*, Volume 8, no. 7, pp. 5599-5606, 2021.

[2] Wang Z., "A privacy-preserving and accountable authentication protocol for IoT end-devices with weaker identity", *Future Generation Computer Systems*, pp.342-348, 2018.

[3] Zhang A., Chen J., "SeDS: Secure data sharing strategy for D2D communication in LTE-Advanced networks", *IEEE Transactions on Vehicular Technology*, vol. 65, no. 4, pp. 2659-2674, 2016.

[4] Guo S., "Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System", *IEEE Transactions on Industrial Informatics*, vol.16, no.3, pp.1972-1983, 2020.

[5] Renuka K., "Design of a Secure Three-Factor Authentication Scheme for Smart Healthcare", *Journal of Medical Systems*, 43(5): 133. 2019.

[6] Zhang A., Lin X., "Towards secure and privacy-preserving data sharing in e-Health systems via consortium blockchain", *Journal of Medical Systems*,vol. 42, no. 256, pp. 140(1-18), 2018.

[7] Feng Q., He D., Zeadally S., Khan M. K., and Kumar N., "A survey on privacy protection in blockchain system", *Journal Of Network And Computer Applications*, vol. 126, pp. 45-58, Jan. 2019.

[8] Omar A., A M.Z., Bhuiyan, Basu A., Kiyomoto S., and Rahman M. S., "Privacy-friendly platform for healthcare data in cloud based on blockchain

environment", *Future Generation Computer Systems*, vol. 95, pp. 511-521, Jun. 2019.

[9] Zhang K.,"Lightweight Searchable Encryption Protocol for Industrial Internet of Things", *IEEE Transactions on Industrial Informatics*,17(6), pp. 4248-4259, 2021.

[10] Zhang J., Cui J., Zhong H.,"PA-CRT: Chinese Remainder Theorem Based Conditional Privacy-Preserving Authentication Scheme in Vehicular Ad-Hoc Networks", *IEEE Transactions On Dependable And Secure Computing*,Vol.18, Issue.2, pp. 722-735, 2021.

[11] Srinivas.J, Das.AK, Li X.,"Designing Anonymous Signature-Based Authenticated Key Exchange Scheme for Internet of Things-Enabled Smart Grid Systems", *IEEE Transactions on Industrial Informatics*,Vol.17, Issue7 ,PP.4425-4436, 2021.

[12] Lamport L., "Password authentication with insecure communication", *Communications of the ACM*, 24(11), 770-772, 1981.

[13] Malasri K., Wang L., "Design and implementation of a securewireless mote-based medical sensor network", *Sensors*, vol.9, pp. 6273-6297, 2009.

[14] Chuang M., Chen M., "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics", *Expert Systems with Applications*, 41(4),pp.1411-1418, 2014.

[15] Mishra D., Das A., Mukhopadhyay S., "A secure user anonymity-preserving biometric-based multiserver authenticated key agreement scheme using smart cards", *Expert Systems with Applications*, 41(18):pp.8129-8143, 2014.

[16] He D., Kumar N., "A secure temporal credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks", *Inform. Sciences*, pp.263-277, 2015.

[17] Odelu V., Goswami A., "A secure biometrics-based multi-server authentication protocol using smart cards", *IEEE Transactions on Information Forensics and Security*, 10(9), pp.1953-1966, 2015.

[18] Jia X., He D., Kumar N., "Authenticated key agreement scheme for fog-driven IoT healthcare system", *Wireless Networks*, vol.25, pp.4737-4750, 2018.

[19] Irshad.A, Chaudhry.SA, Alomari.OA, "A novel pairing-free lightweight authentication protocol for mobile cloud computing framework", *IEEE Systems Journal*, 2020.

[20] Kumari S., Li X., Wu F., Das A.K., "Design of a provably secure biometrics-based multi-cloud-server authentication scheme", *Future Generation Computer Systems*, vol. 68, pp. 320-330, 2017.

[21] Feng Q., He D., Zeadally S., and Wang H., "DAnonymous biometrics-based authentication scheme with key distribution for mobile multi-server environment", *Future Generation Computer Systems*, vol. 84, pp. 239-251, 2018.

[22] Ali R. and Pal A.K., "An efficient three factorCbased authentication scheme in multiserver environment using ECC", *International Journal Of Communication Systems*, vol. 31, no. 4, 2018.

[23] Wang F., Xu G., Wang C., and Peng J., "A provably secure biometrics-based authentication scheme for multiserver environment", *Security and Communication Networks*, vol. 2019, pp. 1C15, Article ID 2838615, 2019.

[24] Wu T., Yang L., Lee Z., "Improved ECC-Based Three-Factor Multiserver Authentication Scheme", *Security and Communication Networks*, Article ID 6627956, 2021.

[25] Ekblaw A., "A case study for blockchain in healthcare: MedRec prototype for electronic health records and medical research data", *Proc. IEEE Open Big Data Conf*, 2016.

[26] Jiang S., Cao J., Wu H., Yang Y., Ma M. and He J., "BlocHIE: A blokchain-based platform for healthcare information exchange", *IEEE Int. Conf. Smart Comput (SMARTCOMP).*, pp. 49-56, 2018.

[27] Wang J., Wu L., "Blockchain based anonymous authentication with key management for smart grid edge computing infrastructure", *IEEE Transactions on Industrial Informatics*, 2019.

[28] Vivekanandan Manojkumar., Sastry V.N., Srinivasulu Reddy U., "Blockchain based Privacy Preserving User Authentication Protocol for Distributed Mobile Cloud Environment", *Peer-to-Peer Networking and Applications*, vol. 14, pp. 1572-1595, 2021.

[29] Siyal A., Junejo A., Zawish M., Ahmed K., Khalil A., and Soursou G., "Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives", *Cryptography*, vol. 3, no. 1, pp. 3-19, Jan. 2019.

[30] Vivekanandan M., Sastry VN.,"Biometric based user authentication protocol for mobile cloud environment". *2019 IEEE 5th International Conference on Identity, Security, and Behavior Analysis (ISBA)*, pp 1-6, 2019.

[31] Yazdinejad A., Srivastava G., Choo K., Parizi R., Dehghantanha A., Aledhari M., "Decentralized authentication of distributed patients in hospital networks using blockchain", *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 8, pp. 2146-2156, Aug. 2020.

[32] Fan K.,Pan Q.,Zhang K., "A Secure and Verifiable Data Sharing Scheme Based on Blockchain in Vehicular Social Networks", *IEEE Transactions on Vehicular Technology*,vol. 69, pp.5826-5835, 2020.

[33] Zhang A., Zhang P., Wang H., Lin X., "Application-Oriented Block Generation for Consortium Blockchain-Based IoT Systems With Dynamic Device Management", *IEEE Internet of Things Journal*,vol. 8, pp.7874-7888, 2021.

[34] Burrows M., Abadi M., Needham RM., "A logic of authentication", *Proc R Soc Lond A Math Phys Sci.*,vol. 426(1871), pp.233-271, 1989.

[35] Chuang M., Chen M., "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics", *Expert Systems with Applications*, vol.41, pp.1411-1418, 2014.

[36] Arshad H., Nikooghadam M., "Three-factor anonymous authentication and key agreement scheme for telecare medicine information syste", *Journal of Medical Systems*, 38(12):1-12, 2014.

[37] Kilinc H., Yanik.T., "A survey of sip authentication and key agreement schemes", *IEEE Communications Surveys and Tutorials*, vol.16, no.2, pp.1005-1023,2014.

[38] He D., Kumar N., "Efficient Privacy-Aware Authentication Schemen for Mobile Cloud Computing Services", *IEEE Systems Journal*,vol. 12, no. 2, 2018.

[39] Tsai.J., Lo N., "A privacy-aware authentication scheme for distributed mobile cloud computing services", *IEEE Systems Journal*, vol.9, no.3, pp.805-815, Sep. 2015.

[40] Lwamo N., Zhu L., "SUAA: A Secure User Authentication Scheme with Anonymity for the Single & Multi-server Environments", *Inform. Sciences*, vol. 477, pp. 369-385, 2019.