Wireless Personal Communications (2022) 124:763–781
https://doi.org/10.1007/s11277-021-09382-3

A Novel Three-Factor Authentication Scheme with High Security for Multi-Server Environments

Rui Chen[1] · **Yongcong Mou**[2] · **Min Zhang**[3]

Accepted: 7 November 2021 / Published online: 16 January 2022

Abstract
In a multi-sever scenario, a two-party remote user authentication scheme is faced with various kinds of security threats. The introduction of biometric technology can effectively improve the security on the user side and the resistance to password guessing attack. Therefore, many biometrics-based user authentication schemes have emerged in the last few years. However, in some recent authentication schemes, a server can easily impersonate a legal user by using the shared secret key and a randomly selected identity. In this study, we first analyze a study of these schemes and indicate the security weakness and vulnerability that might allow attacks. Then, we present an improved biometrics-based three-factor authentication scheme for multi-server environments that inherits most of the advantages of the original scheme and introduces digital signature to address the common security problem. Furthermore, the proposed scheme also has a simplified the authentication procedure and improves execution efficiency. Analysis results, including security analysis and performance comparison, indicate that the new scheme has good efficiency and is robust against various known attacks.

Keywords Three-factor authentication · Biometrics · Smart card · Multi-server

1 Introduction

With the rapid growth of the Internet and information technology, the human society has begun to move toward the information network era. People can obtain information or engage in online financial transactions, such as bank transfer, payment, and shopping, through the internet, using mobile devices any time. Given the openness of networks, transactions over the network are vulnerable to various kinds of attacks, which lead to leakage of sensitive user information or economic losses. Identity authentication technology can prevent network threats from illegal attackers by identifying users before they obtain

✉ Rui Chen
crs1934@hotmail.com

[1] College of Computer Science, Sichuan Normal University, Chengdu, China

[2] Sichuan Water Conservancy Vocational College, Chengdu, China

[3] College of Foreign Languages, Southwest Minzu University, Chengdu, China

system services. Meanwhile, the user can also identify the legitimacy of the servers to prevent server fraud attacks. Therefore, user authentication has become one of the important and effective means of ensuring the security of authentication systems, especially over an open network environment.

Since Lamport et al. [1] first put forward the authentication scheme based on username and password in 1981, many researchers have been working in this field and proposed numerous password-based authentication schemes [2, 3]. However, these schemes require the server to keep the identity information and passwords of users. Meanwhile, many schemes require users to communicate with the register server to update their passwords periodically given the lack of a password updating process, thereby adding to the burden of the register server. Ordinary users are most likely to use weak passwords, such as birthdays, ID numbers, phone numbers, or other strings, that are easy to remember and thus vulnerable to offline dictionary or exhaustive attacks. Hence, the security of this type of authentication schemes is weak.

To improve the safety of user authentication schemes, the smart card is introduced to the authentication process. In 1991, Chang CC et al. [4] first presented a user authentication scheme that uses a smart card. Subsequently, several scholars proposed various authentication protocols based on smart cards [5–14]. With the development of technology, authentication protocols have become vulnerable to attacks on smart cards, such as information extraction attacks [15] and smart card thefts. To compensate for these smart card shortcomings, personal biometrics-based solutions have emerged.

Combined with the user's personal biological signs, such as voice, fingerprint, face, and retina recognition, as the third element of authentication, this type of schemes is generally called three-factor user authentication schemes. Given the uniqueness and unforgeability of personal biometrics, even if the password of a user is compromised or the information stored in a smart card is extracted, the security of the entire system is still guaranteed. Therefore, researchers have proposed many biometrics-based authenticated key agreement schemes [16–32].

In 2010, Li et al. [17] proposed a biometrics-based user authentication scheme. Unfortunately, their scheme has two limitations in practical application and cannot achieve forward security. Later, Huang et al. [19] presented an improved three-factor authentication scheme for distributed systems. Afterwards, Khan et al. [29] designed an anonymity three-factor user authentication scheme and claimed that it can provide robust mutual authentication between communication parties even when the secret information is extracted from a smart card. However, Wen et al. [30] indicted that Khan et al.'s scheme cannot achieve anonymity and mutual authentication and is vulnerable to several attacks and presented an improved scheme.

In 2014, Li et al. [31] put forward a three-factor authentication scheme that employs the Elliptic Curve Cryptosystem (ECC) to enhance security. Nevertheless, Mishra et al. [26] demonstrated that the scheme in [31] cannot prevent off-line password guessing and replay attacks. Then, they presented an anonymous ID-based authentication scheme using light weight cryptographic technology. At the same year, Mishra et al. [33] designed an efficient biometrics-based authentication scheme for multi-server environments and claimed that it satisfies all security requirements. But, Lu et al. [34, 35] found that their scheme has several weaknesses and cannot resist replay, forgery, and server masquerading attacks. Hence, they proposed two different three-factor schemes to address these flaws. However, Chaudhry et al. [36] indicated that the schemes in [34, 35] cannot resist impersonation attack and preserve user anonymity. Chaudhry et al. [54] then presented an enhanced and lightweight authentication scheme and proved its

security with ProVerif. Later, Moon et al. [37] also found that the scheme in [35] cannot prevent outsider and impersonation attacks and implement efficient authentication during login and the authentication phase. Then they provided a robust solution using biometrics and smart cards to address the weakness. Later, Guo et al. [38] demonstrated that Moon et al.'s scheme is still insecure and vulnerable to various attacks from the server or user side. To overcome these shortcomings, Guo et al. put forward a novel biometrics-based authentication scheme for multi-server architecture. After that, Fan et al. [20] presented an ECC-based three-factor user authentication scheme and given a formal security proof. However, Jiang et al. [9] observed that Fan et al.'s scheme still have some flaws.

In 2017, Shingala et al. [28] recognized that the scheme in [30] cannot protect user privacy and is vulnerable to some known network attacks. Thus, an improved scheme was developed to address these drawbacks. In the same year, He et al. [32] summarized the advantages of biometric keys and proposed a three-party authentication scheme based on ECC. However, the authentication process of their scheme requires the assistance of a register center, which leads to high complexity and low-efficiency.

In 2019, Tomar et al. [39] designed an ECC-based authentication scheme which suitable for the scenario that the users and servers belong to the different registration center (multi-registration center). The mutual authentication of the user and the visited server require the participation of registration centers of both parties, which is highly inefficient and costly Later in the same year, another three-factor key agreement scheme using ECC was put forward by Qi et al. [40]. But their scheme have the same problem of the previous one. The participation of registration center results in low efficiency of computation. Later on, Sudhakar et al. [41] put forward a three-factor authentication scheme for multi-server environments by employing fuzzy embedder and hash function. However their scheme is still vulnerable to server fraud attack and denial of service (DoS) attack, and lack of new user registration process. A malicious server can easily fake the legal user identity to access other servers.

A lot of researches on the designing of authenticate protocol under multi-server architecture have been put forward since 2020. Chuang et al. [42] surveyed lots of three-factor authentication protocols and presented a secure user anonymity scheme with strong privacy preserving. However, their scheme does not suitable for wireless network environment due to using the time-consuming ECC algorithm and bilinear map. During the same period, Mo et al. [43] pointed out that the scheme in [44] is insecure to offline password guessing attacks and replay attack, they then presented an improved one for multi-server environments. After that, Wong et al. [45] proposed a lightweight time-bound authentication scheme with user anonymity for electronic healthcare (e-health) system in 5G wireless sensor networks. In Wong et al.'s scheme, the absence of registration center and universal registry service led to the user have to register to every server before getting the network service. Later Kandar et al. [46] considered how to provide personalized service to users and presented a remote authentication scheme in multi-server environments against conspiracy attack. But the authentication process of their scheme is complex and inefficient due to the participation of the registration center.

More recently, Le and HSU [47] introduced a key distribution scheme for group healthcare services by employing Rabin cryptosystem. Besides, Inam et al. [48] also presented a hash-based lightweight authentication scheme by improving the scheme in [49], and claimed that their scheme can resist key compromise impersonation attack. By using the cryptography characteristic of chebyshev chaotic map, Kumar and Om [50] designed an authentication protocol for multi-server environments with the support of server scalability.

Later, Wang et al. [51] proposed a blockchain-assisted remote authentication protocol for intelligent telehealth system (ITS) based on edge computing architecture, which can offer user strong anonymity and continuous authentication among multiple servers.

In this study, we find a common security problem in some studies [33–38], that is, the server in these schemes authenticates users only through user identity and shared secret keys. Thus, a hostile server can easily launch a user impersonation attack. Then, we focus on one of these schemes, that is, Guo et al.'s scheme [38], which was published recently. After a careful analysis of Guo et al.'s scheme, we discovered that it does not prevent impersonation attacks and is also vulnerable to replay attacks. To compensate for these drawbacks and enhance the security of the original scheme, we introduce digital signature, which can effectively solve this common problem, and propose a new improvement authentication scheme that can be used in a multi-server environments. Based on previous research [52], schemes that use symmetric encryption cannot achieve user anonymity. Thus, the proposed scheme adopts asymmetric encryption to enhance system security. Meanwhile, the new scheme also simplifies the authentication procedure and reduces energy consumption, computation cost, and communication cost. Security analysis indicates that the proposed scheme can not only resist several known attacks but is also efficient and low-cost. Furthermore, we introduce the Burrows-Abadi-Needham(BAN) [53] logic to prove the security of the proposed scheme.

The rest of this paper is arranged as follows. Section 2 introduces the network and adversary models. Section 3 discusses Guo et al.'s scheme and Sect. 4 analyzes its security weaknesses. In Sect. 5, we present a detailed description of the proposed authenticated scheme, and its security features are analyzed and formal security proof is given in Sect. 6. In Sect. 7, we compare the performance of the new scheme with those of three related works and draw some conclusions in Sect. 8.

2 Network Model and Adversary Model

2.1 Network Model

We assume that the network model consists of three parties: a register center (*RC*), a user with smart card (U_i), and a visited server (S_j), as shown in Fig. 1. *RC* is responsible for generating a secret key (*PSK*), which is shared by all registered servers, and providing a smart card to the registered user that contains user authentication information and hash functions. Each user should register and obtain a smart card before accessing any servers. Meanwhile, each server should register to the *RC* and obtain the shared secret key. Each server and user generates a public/private key pair for use in asymmetry encryption (e.g., RSA [56]) and in the digital signature algorithm (e.g., SHA-2 [55]). Finally, the *RC* publishes the public keys of users and servers and other related information (e.g., hash functions) as public parameters.

2.2 Adversary Model

We assume that the adversary model is as follows:

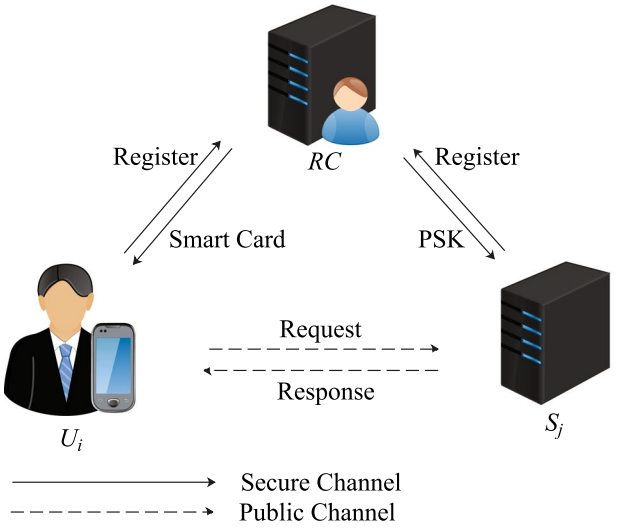

Fig. 1 Network model

- The adversary controls the public channel and can obtain all the messages transmitted in it.
- The adversary can extract the information stored in the smart card using power analysis [15].
- *RC* is a trusted third party.
- All servers in the system are untrusted entities.
- The hash function and asymmetric cryptosystem have sufficient security and cannot be compromised by the adversary.
- The adversary cannot obtain the password, biometrics, or private key of a user simultaneously.

3 Review of the Guo et al's Scheme

Some notations used in this paper are listed in Table 1. The scheme presented by Guo et al. involves three phases, namely, the registration phase, the login and authentication phase and the password change phase.

3.1 Registration

3.1.1 Server Registration

1. S_j first generates a public/private key pair $\{pk_j, sk_j\}$, and then sends his/her identity and public key $\{SID_j, pk_j\}$ to *RC*.

Table 1 Notations

Notations	Description
U_i, S_j	User and Server
RC	The registration center
ID_i, SID_j	Identity of U_i and S_j
PW_i	Password of U_i
BIO_i	Biometrics of U_i
PSK	Shared secret key between RC and S_j
$E()/D()$	Encryption and decryption operations
Sig	Digital signature operation
pk_x/sk_x	Public/Private key pair of an entity x
$h()$	One-way secure hash function
$H()$	Bio-hash function
$\|, \oplus$	Concatenation and exclusive-or operation

2. Upon receiving the information, RC then shares the secret key PSK with S_j.
3. RC publishes $\{SID_j, pk_j\}$ as public parameters.

3.1.2 User Registration

1. U_i randomly selects his/her identity (ID_i) and password (PW_i) and extracts biometrical features (BIO_i) through a special device. Then, U_i sends $\{h(ID_i), IDB_i, PW_i\}$ to RC where $IDB_i = h(ID_i \| H(BIO_i))$ and $PW_i = h(PW_i \| H(BIO_i))$.
2. After receiving the data from U_i, RC calculates $V_i = h(h(ID_i) \| PW_i)$ and $W_i = h(h(ID_i) \| PSK) \oplus IDB_i$, then saves $\{V_i, W_i, h(), H()\}$ into the smart card (SC) and sends it to U_i.

3.2 Login and Authentication

1. U_i inputs ID_i, PW_i, and BIO_i into the terminal that contains the SC. Then, SC computes $PW_i = h(PW_i \| H(BIO_i))$ and compares V_i with $h(h(ID_i) \| PW_i)$. If they are the same, then SC generates a random number (n_1) and calculates $K = h((W_i \oplus IDB_i) \oplus h(ID_i \| n_1)), M_1 = E_{pk_j}(ID_i \| n_1)$ and $Z_i = h(n_1 \| ID_i \| K \| T_1)$. Lastly, U_i generates the current timestamp T_1 and sends $\{M_1, Z_i, T_1\}$ to S_j.
2. When receiving $\{M_1, Z_i, T_1\}$, S_j first verifies T_1 and drops the message if it is not fresh. Otherwise, S_j decrypts M_1 to obtain $\{ID_i, n_1\}$) and computes $K = h(h(h(ID_i) \| PSK) \oplus h(ID_i \| n_1))$. Then, S_j verifies whether $Z_i? = h(n_1 \| ID_i \| K \| T_1)$. If they are equal, U_i is authorized by S_j. Then, S_j chooses a random number n_2 and calculates $M_2 = n_2 \oplus K, M_3 = h(ID_i \| n_1 \| n_2 \| K \| T_2)$ and $SK_{ij} = h(n_1 \| n_2 \| K \| ID_i)$. Finally, S_j obtains the current timestamp T_2 and sends $\{M_2, M_3, T_2\}$ to U_i.
3. Upon receipt of the reply information, U_i verifies the freshness of T_2 and aborts the message if it is not fresh. Next, U_i computes $n_2 = M_2 \oplus K$ and checks whether $M_3? = h(ID_i \| n_1 \| n_2 \| K \| T_2)$ holds. If it holds, S_j is authorized by U_i. Then, U_i com-

putes $SK_{ij} = h(n_1 \parallel n_2 \parallel K \parallel ID_i)$ and $M_4 = h(SK_{ij} \parallel ID_i \parallel n_2 \parallel T_3)$. Lastly, U_i chooses a timestamp T_3 and submits $\{M_4, T_3\}$ to S_j.
4. After verifying the validity of T_3, S_j then checks whether $M_4? = h(SK_{ij} \parallel ID_i \parallel n_2 \parallel T_3)$. If they are equal, then the authenticity of U_i and SK_{ij} is reconfirmed by S_j.

3.3 Password Changing Phase

1. U_i first enters the his/her identity ID_i and password PW_i and imprints his/her BIO_i at the sensor.
2. The SC calculates $PW_i = h(PW_i \parallel H(BIO_i))$ and checks $V_i? = h(ID_i \parallel PW_i)$. If the two values are different, the password updating procedure will be terminated.
3. U_i randomly selects a new password PW_i^* and enters it to the SC. The SC generates $PW_i^* = h(PW_i^* \parallel H(BIO_i))$, $V_i^* = h(h(ID_i) \parallel PW_i^*)$ and replaces V_i with V_i^*.

4 Cryptanalysis of Guo et al's Scheme

This section analyzes the safety of Guo et al.'s scheme detail and enumerates two attacks on their scheme. Despite Guo et al. claimed that their scheme is secure and resists many known attacks, we found that their scheme still suffers from user impersonation and message replay attacks. The following two subsections describe the attack procedures in detail.

4.1 User Impersonation Attack

4.1.1 Servers Can Pretend to any User to Access Another Server

In Guo et al.'s scheme and some other schemes, a hostile server (S_j) can masquerade as any users to access another server (e.g., S_m). The following steps describe this procedure in detail.

1. S_j first randomly chooses an identity (e.g., ID_A) and a number (n_1), and then computes $K = h(h(ID_A \parallel PSK) \oplus h(ID_A \parallel n_1))$. Next, S_j chooses a timestamp T_1 and computes $M_1 = E_{pk_m}(ID_A \parallel n_1)$ and $Z_i = h(n_1 \parallel ID_i \parallel K \parallel T_1)$, and then sends $\{M_1, Z_i, T_1\}$ to S_m.
2. Upon receipt of the login message, S_m checks if T_1 is valid. If it is valid, S_m then computes $(ID_A \parallel n_1) = D(M_1), K = h(h(h(ID_A) \parallel PSK) \oplus h(ID_A \parallel n_1))$ and verifies $Z_i? = h(n_1 \parallel ID_A \parallel K \parallel T_1)$. Obviously, Z_i is equal to $h(n_1 \parallel ID_A \parallel K \parallel T_1)$ because all servers have the PSK, which is generated and distributed by RC. Then, S_m generates n_2 and computes $M_2 = n_2 \oplus K, M_3 = h(ID_A \parallel n_1 \parallel n_2 \parallel K \parallel T_2)$ and $SK_{ij} = h(n_1 \parallel n_2 \parallel K \parallel ID_A)$ and sends M_2, M_3, T_2 to S_j as a response message.
3. S_j verifies the information after receipt of the response message and calculates $SK_{ij} = h(n_1 \parallel n_2 \parallel K \parallel ID_A)$ and $M_4 = h(SK_{ij} \parallel ID_A \parallel n_2 \parallel T_3)$, and then submits $\{M_4, T_3\}$ to S_m.
4. Finally, S_m checks whether $M_4? = h(SK_{ij} \parallel IDA \parallel n_2 \parallel T_3)$. If the two are equal, S_m considers S_j as a legitimate user and provides services to S_j.

4.1.2 Legitimate User can Impersonate any User to Access Another Server

We found that if a legitimate user (e.g. U_i) can fetch the data from smart card, he/she could impersonate other users by performing the following steps:

1. U_i obtains W_i from his/her smart card by some means.
2. U_i inputs ID_i and BIO_i and calculates $IDB_i = h(ID_i \parallel H(BIO_i)), W_i^* = W_i \oplus IDB_i = h(h(ID_i) \parallel PSK)$.
3. With the ID_i and W_i^*, U_i can easily get the PSK through offline key guessing attacks.
4. After obtaining the PSK, U_i can impersonate any users as in the previous subsection.

4.2 Replay Attack

When a user U_i submits a login request message to a hostile server S_j, S_j can launch a replay attack by forwarding this message to another server (e.g. S_m). The main steps are as follows.

U_i first sends the login data to S_j. When the login message $\{M_1, Z_i, T_1\}$ is received , S_j calculates $(ID_i \parallel n_1) = D(M_1)$ and $M_1^* = E_{pk_m}(ID_i \parallel n_1)$, and then forward $\{M_1^*, Z_i, T_1\}$ to S_m by pretending to be the user U_i. Due to the transported message does not contain the server information, the S_m take it for granted that the message is sent from U_i rather than other parties. Then, according to the response message from S_m, S_j can generate the same session key for U_i and S_m that equals to $h(n_1 \parallel n_2 \parallel K \parallel ID_i)$. Therefore in the lifetime of T_1, Guo et al.'s scheme can not prevent replay attacks.

It must be noted that it is difficult to choose a suitable time stamp lifetime, and this security issue must be seriously considered.

5 The Proposed Scheme

We will propose a new biometrics-based authenticated key agreement scheme for multi-server environments in this section. The new scheme involves in three parties: the RC, the U_i, and the S_j. In the new scheme there are also three phases: the registration, login and authentication and password change phases. Fig. 2 shows the details of the first two phases.

5.1 Registration

When U_i or S_j joins the authentication system, they must register on the RC first and obtain the related registration information. The main registration steps are as follows.

5.1.1 Server Registration

1. S_j generates a public/private key pair $\{pk_j, sk_j\}$ and submits his/her identity and public key $\{SID_j, pk_j\}$ to RC.

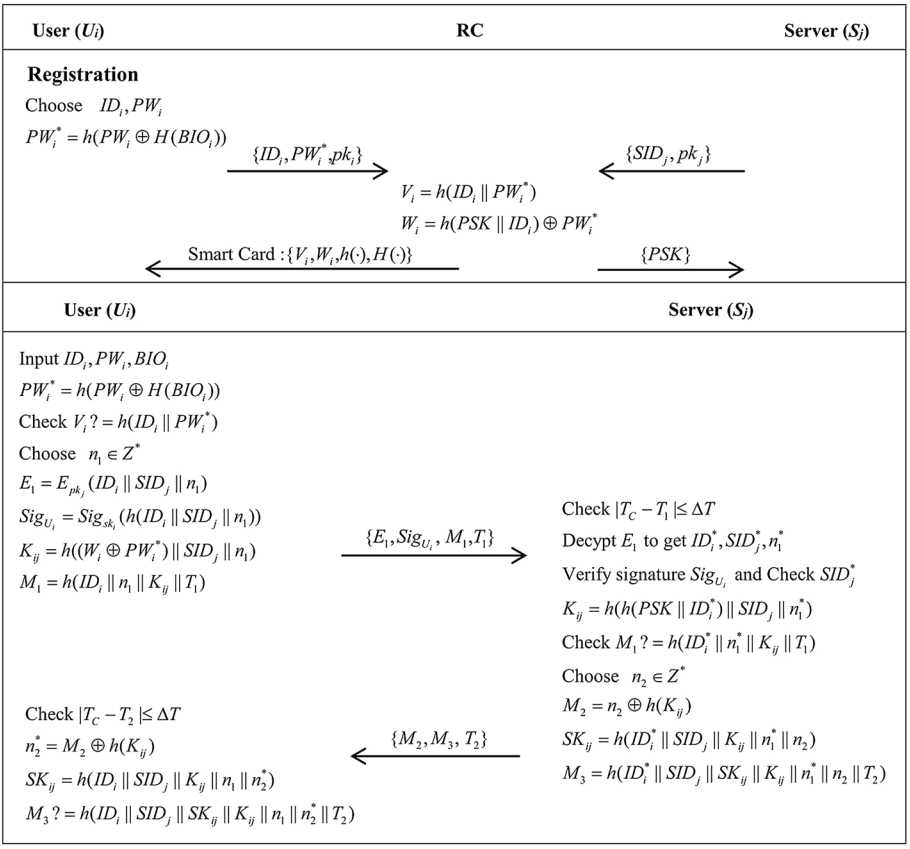

Fig. 2 Registration and authentication phases of the proposed scheme

2. When receiving the register information, *RC* returns the shared secret key *PSK* to S_j.
3. *RC* publishes the identity and public key of S_j.

5.1.2 User Registration

1. U_i chooses an ID_i and a PW_i randomly, and then generates his/her BIO_i and public/private key pair. Lastly, U_i sends $\{ID_i, PW_i^*, pk_i\}$ to *RC* as a registration message where $PW_i^* = h(PW_i \| H(BIO_i))$.
2. Upon receipt of the message, *RC* calculates $V_i = h(ID_i \| PW_i^*)$, $W_i = h(PSK \| ID_i) \oplus PW_i^*$ and stores $\{V_i, W_i, h(), H()\}$ into a *SC* and sends it to U_i.
3. *RC* publishes the public key of U_i.

5.2 Login and Authentication

1. U_i enters ID_i, PW_i, and BIO_i to the terminal device with a *SC*. Then, *SC* computes $PW_i^* = h(PW_i \| H(BIO_i))$ and checks $V_i ? = h(ID_i \| PW_i^*)$. If the two values are equal,

then SC randomly chooses a number $n_1 \in Z^*$ and calculates $E_1 = E_{pk_j}(ID_i \parallel SID_j \parallel n_1), Sig_{U_i} = Sig_{sk_i}(h(ID_i \parallel SID_j \parallel n_1)), K_{ij} = h((W_i \oplus PW_i^*) \parallel SID_j \parallel n_1))$ and $M_1 = h(ID_i \parallel n_1 \parallel K_{ij} \parallel T_1)$. Finally, U_i sends $\{E_1, Sig_{U_i}, M_1, T_1\}$ to S_j where T_1 is the current timestamp.

2. Upon receipt of $\{E_1, Sig_{U_i}, M_1, T_1\}$, S_j verifies the validation of T_1 and terminates the procedure if it is invalid. Otherwise, S_j decrypts E_1 to obtain ID_i^*, SID_j^* and n_1^* using his/her private key, and then verifies signatures Sig_{U_i} and SID_j^*. If the two values are valid, then S_j computes $K_{ij} = h(h(PSK \parallel ID_i^*) \parallel SID_j \parallel n_1^*))$ and verifies whether $M_1 ? = h(ID_i^* \parallel n_1^* \parallel K_{ij} \parallel T_1)$. If they are equal, U_i is authorized by S_j. Then, S_j randomly chooses a number $n_2 \in Z^*$ and calculates $M_2 = n_2 \oplus h(K_{ij})$ and the shared session key $SK_{ij} = h(ID_i^* \parallel SID_j \parallel K_{ij} \parallel n_1^* \parallel n_2)$. Lastly, S_j chooses a timestamp T_2 and computes $M_3 = h(ID_i^* \parallel SID_j \parallel SK_{ij} \parallel K_{ij} \parallel n_1^* \parallel n_2 \parallel T_2)$, and then submits $\{M_2, M_3, T_2\}$ back to U_i.
3. After receiving $\{M_2, M_3, T_2\}$, U_i first verifies the freshness of T_2 and aborts the message if T_2 is not fresh. Then, U_i computes $n_2^* = M_2 \oplus h(K_{ij})$ and $SK_{ij} = h(ID_i^* \parallel SID_j \parallel K_{ij} \parallel n_1^* \parallel n_2)$. Next, U_i checks whether $M_3 ? = h(ID_i \parallel SID_j \parallel SK_{ij} \parallel K_{ij} \parallel n_1 \parallel n_2^* \parallel T_2)$. If it holds, S_j is authorized by U_i. Then, the mutual authentication procedure is finished, and the shared session key SK_{ij} between U_i and S_j is established.

5.3 Password Changing Phase

1. U_i first puts the smart card into the terminal device, and then enters ID_i, PW_i, and BIO_i.
2. SC computes $PW_i^* = h(PW_i \parallel H(BIO_i))$ and compares V_i with $h(ID_i \parallel PW^*)$. If they are unequal, the phase is cancelled.
3. SC asks U_i for the new PW_i^*.
4. Upon receiving PW_i^*, SC calculates $PW_i^* = h(PW_i^* \parallel H(BIO_i^*)), V_i^* = h(h(ID_i) \parallel PW_i^*)$ and replaces V_i with V_i^*.

6 Security Analysis

In this section, we first give an informal security analysis of the proposed scheme, and then provide a formal proof using the BAN logic [53].

6.1 Informal Security Analysis

We discuss several common security functionalities of our scheme in the subsection below. The informal security analysis reveals that the our scheme is secure against many known attacks, thereby protecting the user's privacy.

Mutual Authentication

In the proposed protocol, the identity of U_i can be verified by S_j through E_1 and Sig_{U_i} because only a legal U_i can generate the correct signature $Sig_{U_i} = Sig_{sk_i}(h(ID_i \parallel SID_j \parallel n_1))$ by using his/her private key sk_i. Through checking whether M_1 is equal to $h(ID_i \parallel n_1 \parallel K_{ij} \parallel T_1)$, S_j can quickly verify the legitimacy of U_i because an adversary cannot simultaneously obtain ID_i and n_1 through $h(ID_i \parallel SID_j \parallel n_1)$. Meanwhile, U_i can extract n_2 from M_2 and generate the session key

$SK_{ij} = h(ID_i \parallel SID_j \parallel K_{ij} \parallel n_1 \parallel n_2^*)$. Then, the legitimacy of S_j can be verified by U_i through equation $M_3 = h(ID_i \parallel SID_j \parallel SK_{ij} \parallel K_{ij} \parallel n_1 \parallel n_2^* \parallel T_2)$ because only a legal S_j can generate a valid $K_{ij} = h(h(PSK \parallel ID_i^*) \parallel SID_j \parallel n_1^*))$ in which PSK is a secret value, and ID_i and n_1 are extracted from E_1 with S_j's private key sk_j. Then, S_j can compute the same shared session key $SK_{ij} = h(ID_i^* \parallel SID_j \parallel K_{ij} \parallel n_1^* \parallel n_2)$, and authentication message $M_3 = h(ID_i^* \parallel SID \parallel SK_{ij} \parallel K_{ij} \parallel n_1^* \parallel n_2 \parallel T_2)$ by using K_{ij} and SK_{ij}. Given that only a valid U_i can obtain n_2 and generate the correct session key SK_{ij}, mutual authentication between user and server can be achieved in our proposed scheme.

User Anonymity and Untraceability

In the proposed scheme, user anonymity and untraceability can be achieved because the true identification of U_i is included in E_1, Sig_{U_i}, M_1, and M_3. Obviously, the ID_i cannot be extracted from the hash value $M_1 = h(ID_i \parallel n_1 \parallel K_{ij} \parallel T_1), M_3 = h(ID_i^* \parallel SID_j \parallel SK_{ij} \parallel K_{ij} \parallel n_1^* \parallel n_2 \parallel T_2)$, and Sig_{U_i}. Meanwhile, the adversary cannot obtain ID_i by decrypting E_1 without the private key of S_j. Every login request message and response message contain the randomly selected number (i.e., n_1 and n_2). Given that the two random numbers in the communication messages $\{E_1, Sig_{U_i}, M_1, T_1\}$ and $\{M_2, M_3, T_2\}$ are different every time and unlinkable, even if the adversary intercepts all the transmitted information, a message directory cannot be associated with a user, and the actions trajectory and location information of the user will not be compromised. Therefore, user anonymity and untraceability can be achieved in the proposed scheme.

Resistance to Impersonate Attack

User impersonation attack If an attacker, such as a hostile person, an illegal user, or an illegal server, wants to impersonate a legal user (e.g., U_i) to communicate with S_j, he/she should generate a legal request message $\{E_1, Sig_{U_i}, M_1, T_1\}$. The public/private key pair of each user is randomly selected by the user independently. Thus, the sk_i is known to only user U_i. Obviously, without the sk_i, these attackers cannot generate a legal Sig_{U_i} and login request message. This can be achieved by verifying Sig_{U_i} on the server side.

Server impersonation attack Suppose an adversary (e.g. A) attempts to masquerade as a server (S_j) and intercepts the login request message $\{E_1, Sig_{U_i}, M_1, T_1\}$ of U_i, A cannot extract $\{ID_i, SID_j, n_1\}$ from E_1 without the private key of S_j. Hence, A also cannot generate the correct K_{ij} and SK_{ij} without ID_i and n_1. Finally, A cannot compute a legal M_2 and M_3. U_i can detect this kind of attack by verifying $M_3? = h(ID_i \parallel SID \parallel SK_{ij} \parallel K_{ij} \parallel n_1 \parallel n_2^* \parallel T_2)$.

Above all, no forged messages can pass validation during the authentication phase. Thus, the new scheme can efficiently prevent the above two types of impersonation attacks.

Resistance to Replay Attack

Given that T_1 is contained in the login request message $\{E_1, Sig_{U_i}, M_1, T_1\}$ and M_1, so T_1 tampering or replay attacks can be easily detected by the server. In addition, if a login request message is replayed by an adversary when the timestamp is still valid, the server who received the message can also easily detect this type of attack by verifying the signature Sig_{U_i} because it contains the identity of the original server, which is different from that of the replayed server. On the user side, the reply information includes the random number n_1 that is generated by the user. Thus, the user can immediately detect a replay attack by verifying these data.

Resistance to Off-line Guessing Attack

If an adversary obtains all the information transmitted between U_i and S_j, then the adversary cannot obtain the data in E_1 without the private key of S_j or obtain other useful information from hash values M_1, M_2, and M_3 because they are protected by the one-way hash

function. Therefore, the adversary cannot launch an off-line guessing attack due to the adoption of the cryptography method. Therefore, the proposed scheme is able to resist off-line guessing attack.

Resistance to Stolen Smart Card Attack

When the SC of U_i is stolen and the information (i.e., V_i, W_i) in the SC is extracted by an adversary, he/she cannot obtain $h(PSK \parallel ID_i)$ without the PW_i and the BIO_i of U_i. Furthermore, he/she cannot generate a legal Sig_{U_i} without the private key of U_i. Hence, our proposed scheme can prevent this kind of attack.

Perfect Forward Secrecy

The numbers (i.e., n_1 and n_2) in the communication messages are randomly chosen by the U_i and S_j during the login and authentication phase and are different every time, thereby effectively protecting the safety of the shared session key. Even if the current session key is compromised, the adversary still cannot link the session key with previous session keys or the secret key of the system. Hence, our scheme can provide a perfect forward secrecy.

6.2 Formal Security Analysis

In this section, we provide a formal security proof of the proposed scheme with the BAN logic [53], which can prove whether a protocol can reach the target and help with the further improvement of the protocol.

Some notations of BAN logic are given bellow:

$P|\equiv X$: P believes X;

$\#(X)$: X is fresh;

$P \Rightarrow X$: P controls X;

$P \lhd X$: P receives X;

$P|\sim X$: P sends X;

(X, Y): X or Y is one part of (X, Y);

$(X)_K$: X is hash with the key K;

$\{X\}_K$: X is cipher with the key K;

$\langle X \rangle_K$: X with the secret K;

$P \overset{K}{\longleftrightarrow} Q$: K is the shared key between P and Q;

$\overset{K}{\longrightarrow} P$: K is the public key of P.

To implement the BAN logic usually need to complete four steps: idealize the proposed scheme, make assumption, setting goal and analysis of the protocol.

(1) The idealized form of the transmitted messages:

$M_1 : U_i \rightarrow S_j : \{ID_i, SID_j, n_1\}_{SK_{ij}}, Sig_{sk_i}(h(ID_i, SID_j, n_1)), \{ID_i, SID_j, n_1, T_1\}_K, T_1$

$M_2 : S_j \rightarrow U_i : \{ID_i, SID_j, U_i \overset{K}{\longleftrightarrow} S_j, n_1, n_2, T_2\}_K$

(2) Initiative premises:

$p_1 : U_i \mid\equiv \#(n_2)$.

$p_2 : S_j \mid\equiv \#(n_1)$.

$p_3 : U_i \mid\equiv U_i \overset{K}{\longleftrightarrow} S_j$.

$p_4 : S_j \mid\equiv U_i \overset{K}{\longleftrightarrow} S_j$.

$p_5 : U_i \mid\equiv S_j \Rightarrow U_i \overset{K}{\longleftrightarrow} S_j$.

$p_6 : S_j \mid\equiv U_i \Rightarrow U_i \overset{SK_{ij}}{\longleftrightarrow} S_j$.

$p_7 : U_i \mid\equiv S_j \Rightarrow U_i \overset{SK_{ij}}{\longleftrightarrow} S_j$.

$p_8 : S_j \mid\equiv U_i \Rightarrow U_i \overset{K}{\longleftrightarrow} S_j$.

$p_9 : S_j \mid\equiv U_i \Rightarrow ID_i$.

(3) Establishment of security goals:
$G_1 : U_i \mid\equiv U_i \overset{SK_{ij}}{\longleftrightarrow} S_j$
$G_2 : U_i \mid\equiv S_j \mid\equiv U_i \overset{SK_{ij}}{\longleftrightarrow} S_j$
$G_3 : S_j \mid\equiv U_i \overset{SK_{ij}}{\longleftrightarrow} S_j$
$G_4 : S_j \mid\equiv U_i \mid\equiv U_i \overset{SK_{ij}}{\longleftrightarrow} S_j$
(4) Scheme analysis:
From M_1, we have
$S_0 : S_j \lhd_{pk_i} Sig_{sk_i}(h(ID_i, SID_j, n_1))$
Since $\longrightarrow U_i$, only U_i has correct ID_i, n_1 and generates signature $Sig_{sk_i}(h(ID_i, SID_j, n_1))$, we have
$S_1 : S_j \mid\equiv U_i \mid\sim Sig_{sk_i}(h(ID_i, SID_j, n_1))$
From S_1 and p_2 and the freshness conjuncatenation rule, we have
$S_2 : S_j \mid\equiv U_i \mid\equiv Sig_{sk_i}(h(ID_i, SID_j, n_1))$
From S_2 and p_9 and jurisdiction rule, we have
$S_3 : S_j \mid\equiv Sig_{sk_i}(h(ID_i, SID_j, n_1))$
From M_1, we have
$S_4 : S_j \lhd_{pk_j} \{ID_i, SID_j, n_1\}_{pk_j}$
Since $\longrightarrow S_j$, only S_j can get the value of ID_i, SID_j and n_1. Only when it is combined with sk_j and PSK can an attacker compute the correct K_{ij}.
$S_5 : S_j \lhd \{ID_i, n_1, T_1\}_{K_{ij}}, T_1$
From S_5 and p_6 and the message-meaning rule, we have
$S_6 : S_j \mid\equiv U_i \mid\sim \{ID_i, n_1, T_1\}$
From S_6 and p_2 and the freshness conjuncatenation rule, we have
$S_7 : S_j \mid\equiv U_i \mid\equiv \{ID_i, n_1, T_1\}$
From S_7 and S_3, we have
$S_8 : S_j \mid\equiv ID_i$
According to S_7, S_8 and p_2, p_4 and $SK_{ij} = h(ID_i, SID_j, K_{ij}, n_1, n_2)$, we apply freshness conjuncatenation rule and nonce verification rule to derive
$S_9 : S_j \mid\equiv U_i \equiv U_i \overset{SK_{ij}}{\longleftrightarrow} S_j\,(G_4)$
From S_9 and p_8 we have
$S_{10} : S_j \mid\equiv U_i \overset{SK_{ij}}{\longleftrightarrow} S_j\,(G_3)$
From M_2, we have
$S_{11} : U_i \lhd \{ID_i, SID_j, U_i \overset{SK_{ij}}{\longleftrightarrow} S_j, n_1, n_2, T_2\}_K$
According to S_{11} and p_3 and message-meaning rule, we have
$S_{12} : U_i \mid\equiv S_j \mid\sim \{ID_i, SID_j, U_i \overset{SK_{ij}}{\longleftrightarrow} S_j, n_1, n_2, T_2\}$
According to S_{12} and p_1 and freshness conjuncatenation rule, we have
$S_{13} : U_i \mid\equiv S_j \mid\equiv \{ID_i, SID_j, U_i \overset{SK_{ij}}{\longleftrightarrow} S_j, n_1, n_2, T_2\}$
Finally, according to S_{13} and belief rule, we have
$S_{14} : U_i \mid\equiv S_j \mid\equiv U_i \overset{SK_{ij}}{\longleftrightarrow} S_j\,(G_2)$
According to S_{14} and p_7 we have
$S_{15} : U_i \mid\equiv U_i \overset{SK_{ij}}{\longleftrightarrow} S_j\,(G_1)$

7 Functional and Performance Comparison

This section gives a analysis of the functional and performance between the proposed scheme and three recently works.

Table 2 Functionality comparison

	Lu [35]	Moon [37]	Guo [38]	Our scheme
Mutual authentication	Yes	Yes	Yes	Yes
User anonymity and untraceability	No	No	Yes	Yes
Impersonation attack resistance	No	No	No	Yes
Replay attack resistance	No	Yes	No	Yes
Off-line guessing attack resistance	Yes	No	Yes	Yes
Stolen-smartcard attack resistance	Yes	Yes	Yes	Yes
Perfect forward secrecy	Yes	Yes	Yes	Yes
Efficient password change phase	Yes	Yes	Yes	Yes

7.1 Functional Analysis

Table 2 presents a functional comparison between our scheme and other related works [35, 37, 38]. As can be seen from this table, our protocol satisfies all the functionality requirements, which are better security and robustness.

7.2 Performance Analysis

By computer simulation, we provide a simple performance comparison of our protocol and related works. To show the performance comparisons, some notations are introduced below:

- T_{AE}: The time for an asymmetric encryption operation.
- T_{AD}: The time for an asymmetric decryption operation.
- T_{Sign}: The time for a digital signature operation.
- T_{Ver}: The time for a signature verification operation.
- T_H: The time for a one-way hash operation.

Table 3 Time cost of related operations(ms)

Operations	Time
T_{AE}	1.49
T_{AD}	0.811
T_{Sign}	0.145
T_{Ver}	0.009
T_H	0.002

Table 4 The comparisons of computation cost(ms)

Scheme	Login	Authentication	Total
Lu [35]	$5T_H$	$13T_H$	0.036
Moon [37]	$5T_H$	$13T_H$	0.036
Guo [38]	$7T_H + T_{AE}$	$11T_H + T_{AD}$	2.337
Our scheme	$6T_H + T_{AE} + T_{Sign}$	$9T_H + T_{AD} + T_{Ver}$	2.485

Table 3 shows the execution time of the related operations using OpenSSL library (v1.1.1a) [57]. We use the 1024-bit RSA algorithm to implement asymmetric encryption/decryption and digital signature/verification operations, which are common in real communication scenarios. The operating system is Ubuntu 18.04 with Intel Core i5 2.4 GHz processor and 4 GB of RAM.

Table 4 presents the performance comparison result between our improved scheme and three other relevant studies. The table indicates that the new scheme has a higher computation cost than the scheme proposed by Lu et al. and Moon et al.. By only employing a one-way hash function, the performance time of Lu et al.'s scheme and Moon et al.'s scheme only requires 0.036 ms, but their security is poor and vulnerable to malicious attacks, such as replay and impersonation attacks. The time consumption of the new protocol is slightly higher than that of Guo et al.'s scheme because digital signature and verification operation are added during the authentication process. But it also is worthwhile, because it addresses the common security problem and improve the security of the authentication system.

8 Conclusion

In this paper, we first provide a brief introduction of the development of the authentication scheme under a multi-server environments and the unique advantages of biological feature recognitions. Then, we review recent biometrics-based authentication schemes and highlight the similar security drawback of some of those schemes that leads to impersonation attack. Subsequently, we analyze a latest scheme of them and show that this scheme not only suffers from user impersonation attack but apt to replay attacks, although the authors claimed their scheme can resist known attacks. A hostile server or an illegitimate user can impersonate a legal user to access another server and obtain network service illegally. We then proposed an improved scheme to address the common security problem and other security weaknesses. The new scheme has a simplified authentication procedure and improved efficiency. The result of security analysis and performance comparison illustrates that the new proposed scheme has good security and robustness, prevents various network menaces, and thus suited for multi-server environments.

Availability of data and material All data generated or analysed during this study are included in this published article (and its supplementary information files).

Declaration

Conflicts of interest The authors declared that they have no conflicts of interest to this work. We declare that we have no financial and personal relationships with other people or organizations that can inappropriately influence our work, there is no professional or other personal interest of any nature or kind in any product, service and/or company that could be construed as influencing the position presented in, or the review of, the manuscript entitled, "A novel three-factor authentication scheme with high security for multi-server environments"

References

1. Lamport, L. (1981). Password authentication with insecure communication. *Communications of the Acm, 24*(24), 770–772.
2. Tsai, J. L., & Lo, N. W. (2013). A new password-based multi-server authentication scheme robust to password guessing attacks. *Wireless Personal Communications, 71*(3), 1977–1988.
3. Nam, J., Choo, K. K., Han, S., Paik, J., & Won, D. (2015). Two-round password-only authenticated key exchange in the three-party setting. *Symmetry, 7*(1), 105–124.
4. Chang, C. C., & Wu, T. C. (1991). Remote password authentication with smart cards. *IEE Proceedings-E, 138*(3), 165–168.
5. Xiong, L., Niu, J., Kumari, S., Islam, S. H., Fan, W., Khan, M. K., & Das, A. K. (2016). A novel chaotic maps-based user authentication and key agreement protocol for multi-server environment with provable security. *Wireless Personal Communications, 89*(2), 569–597.
6. Jangirala, S., Mukhopadhyay, S., & Das, A. K. (2017). A multi-server environment with secure and efficient remote user authentication scheme based on dynamic id using smart cards. *Wireless Personal Communications, 95*(3), 1–33.
7. Mishra, D. (2016). Design and analysis of a provably secure multi-server authentication scheme. *Wireless Personal Communications, 86*(3), 1–25.
8. Mishra, D., & Dhal, S. (2017). Privacy preserving password-based multi-server authenticated key agreement protocol using smart card. *Wireless Personal Communications, 99*(3), 1–21.
9. Jiang, Q., Ma, J., Lu, X., & Tian, Y. (2015). An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks. *Peer-to-Peer Networking and Applications, 8*(6), 1070–1081.
10. Wang, D., He, D., Wang, P., & Chu, C. H. (2015). Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment. *Dependable & Secure Computing IEEE Transactions on, 12*(4), 428–442.
11. Maitra, T., Islam, S. H., Amin, R., Giri, D., Khan, M. K., & Kumar, N. (2016). An enhanced multi-server authentication protocol using password and smart-card: Cryptanalysis and design. *Security & Communication Networks, 9*(17), 4615–4638.
12. Maitra, T., Obaidat, M. S., Amin, R., Islam, S. H., Chaudhry, S. A., & Giri, D. (2016). A robust elgamal-based password-authentication protocol using smart card for client-server communication. *International Journal of Communication Systems, 30*(11), e3242.1-e3242.12.
13. Wang, C., Ding, W., Xu, G., & Guo, Y. (2017). A lightweight password-based authentication protocol using smart card. *International Journal of Communication Systems, 30*(11), e3336.
14. Azrour, M., Farhaoui, Y., & Ouanan, M. (2017). A new secure authentication and key exchange protocol for session initiation protocol using smart card. *International Journal of Network Security, 19*(6), 870–879.
15. Messerges, T. S., Dabbish, E. A., & Sloan, R. H. (2002). Examining smart-card security under the threat of power analysis attacks. *IEEE Transactions on Computers, 51*(5), 541–552.
16. He, D., & Wang, D. (2015). Robust biometrics-based authentication scheme for multiserver environment. *IEEE Systems Journal, 9*(3), 816–823.
17. Li, C. T., & Hwang, M. S. (2010). An efficient biometrics-based remote user authentication scheme using smart cards. *Journal of Network & Computer Applications, 33*(1), 1–5.
18. Das, A. K. (2011). Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards. *Iet Information Security, 5*(3), 145–151.
19. Huang, X., Yang, X., Chonka, A., Zhou, J., & Deng, R. H. (2011). A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. *IEEE Transactions on Parallel & Distributed Systems, 22*(8), 1390–1397.
20. Fan, W., Xu, L., Kumari, S., & Xiong, L. (2015). A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client-server networks. *Computers & Electrical Engineering, 45*(C), 274–285.
21. Qi, J., Khan, M. K., Xiang, L., Ma, J., & He, D. (2016). A privacy preserving three-factor authentication protocol for e-health clouds. *Journal of Supercomputing, 72*(10), 3826–3849.
22. Chuang, M. C., & Chen, M. C. (2014). An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. *International Journal of Network Security, 18*(5), 997–1000.
23. Mishra, D., Das, A. K., & Mukhopadhyay, S. (2016). A secure and efficient ecc-based user anonymity-preserving session initiation authentication protocol using smart card. *Peer-to-Peer Networking & Applications, 9*(1), 171–192.

24. Moon, J., Choi, Y., Kim, J., & Won, D. (2016). An improvement of robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps. *Journal of Medical Systems, 40*(3), 1–11.
25. S. Ibjaoun, A. A. E. Kalam, V. Poirriez, A. A. Ouahman, & M. D. Montfort, (2017). Analysis and enhancements of an efficient biometric-based remote user authentication scheme using smart cards, in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications*, 1–8.
26. Mishra, D., Kumari, S., Khan, M. K., & Mukhopadhyay, S. (2017). An anonymous biometric-based remote user-authenticated key agreement scheme for multimedia systems. *International Journal of Communication Systems, 30*(1), e2946.1-e2946.14.
27. Park, Y. H., Park, K. S., Lee, K. K., Song, H., & Park, Y. H. (2017). Security analysis and enhancements of an improved multi-factor biometric authentication scheme. *International Journal of Distributed Sensor Networks, 13*(8), 155014771772430.
28. Shingala, M., Patel, C., & Doshi, N. (2017). An improve three factor remote user authentication scheme using smart card. *Wireless Personal Communications, 99*(12), 1–25.
29. Khan, M. K., & Kumari, S. (2013). An improved biometrics-based remote user authentication scheme with user anonymity. *BioMed Research International, 2013*(5), 491289.
30. Wen, F., Susilo, W., & Yang, G. (2015). Analysis and improvement on a biometric-based remote user authentication scheme using smart cards. *Wireless Personal Communications, 80*(4), 1747–1760.
31. Xiong, L., Niu, J., Khan, M. K., Liao, J., & Zhao, X. (2014). Robust three-factor remote user authentication scheme with key agreement for multimedia systems. *Security & Communication Networks, 9*(13), 1916–1927.
32. He, D., Zeadally, S., Wu, L., & Wang, H. (2016). Analysis of handover authentication protocols for mobile wireless networks using identity-based public key cryptography. *Computer Networks, 128*(9), 154–163.
33. Mishra, D., Das, A. K., & Mukhopadhyay, S. (2014). A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards. *Expert Systems with Applications, 41*(18), 8129–8143.
34. Lu, Y., Li, L., Yang, X., & Yang, Y. (2015). A biometrics and smart cards-based authentication scheme for multi-server environment. *Security & Communication Networks, 8*(17), 3219–3228.
35. Lu, Y., Li, L., Yang, X., & Yang, Y. (2015). Robust biometrics based authentication and key agreement scheme for multi-server environment using smart cards. *Plos One, 10*(5), e0126323.
36. Chaudhry, S. A. (2016). A secure biometric based multi-server authentication scheme for social multimedia networks. *Multimedia Tools & Applications, 75*(20), 1–21.
37. Moon, J., Choi, Y., Jung, J., & Won, D. (2015). An improvement of robust biometrics-based authentication and key agreement scheme for multi-server environment using smart cards. *Plos One, 10*(12), e0145263.
38. Guo, H., Wang, P., Zhang, X., Huang, Y., & Ma, F. (2017). A robust anonymous biometric-based authenticated key agreement scheme for multi-server environment. *Plos One, 12*(11), e0187403.
39. Tomar, A., & Dhar, J. (2019). An ECC based secure authentication and key exchange scheme in multi-server environment. *Wireless Personal Communications, 107*, 351–372.
40. Qi, M., & Chen, J. (2019). Anonymous biometrics-based authentication with key agreement scheme for multi-server environment using ECC. *Multimedia Tools and Applications, 78*(19), 553–568.
41. Sudhakar, T., & Natarajan, V. (2019). A new three-factor authentication and key agreement protocol for multi-server environment. *Wireless Networks, 26*(3), 4909–4920.
42. Chuang, Y., & Lei, C. (2020). An independent three-factor mutual authentication and key agreement scheme with privacy preserving for multiserver environment and a survey. *International Journal of Communication Systems, 34*, e4660.
43. Mo, J., Chen, H., & Shen, W. (2020). Cryptanalysis of anonymous three factor-based authentication schemes for multi-server environment. *International Conference on Security with Intelligent Computing and Big-data Services,* 456–468.
44. Qi, F., He, D., Zeadally, S., & Wang, H. (2017). Anonymous biometrics-based authentication scheme with key distribution for mobile multi-server environment. *Future Generation Computer Systems, 84*, 239–251.
45. Wong, M. K., Hsu, C. L., Le, T. V., Hsieh, M. C., & Lin, T. W. (2020). Three-factor fast authentication scheme with time bound and user anonymity for multi-server e-health systems in 5g-based wireless sensor networks. *Sensors, 20*(9), 2511.
46. Kandar, S., Pal, S., & Dhara, B. C. (2021). A biometric based remote user authentication technique using smart card in multi-server environment. *Wireless Personal Communications, 120*(2), 1–24.
47. Le, T. V., & Hsu, C. L. (2021). An anonymous key distribution scheme for group healthcare services in 5g-enabled multi-server environment. *IEEE Access, 9*, 53408–53422.

48. Iuh, A., Jian, W. A., Yz, A., & Sm, B. (2021). An efficient hash-based authenticated key agreement scheme for multi-server architecture resilient to key compromise impersonation. *Digital Communications and Networks, 7*(1), 140–150.
49. Kumar, A., & Om, H. (2017). An improved and secure multi-server authentication scheme based on biometrics and smartcard. *Digital Communications and Networks, 4*, 27–38.
50. Kumar, A., & Om, H. (2021). An enhanced and provably secure authentication protocol using chebyshev chaotic maps for multi-server environment. *Multimedia Tools and Applications, 80*(9), 14163–14189.
51. Wwa, B., Hha, C., Lxa, C., Qi, L., Rm, D., & Yz, B. (2021). Blockchain-assisted handover authentication for intelligent telehealth in multi-server edge computing environment. *Journal of Systems Architecture, 115*, 102024.
52. Wang, D., & Wang, P. (2014). On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions. *Computer Networks, 73*(C), 41–57.
53. Burrows, M., Abadi, M., & Needham, R. (1990). A logic of authentication. *ACM Transactions on Computer Systems, 8*(1), 18–36.
54. M. Abadi B. Blanchet & H.C.L. (2009). Models and proofs of protocol security: A progress report, in a. bouajjani & o. maler (eds.). *Computer aided verification*, 35–49.
55. Sklavos N., Koufopavlou O. (2003). On the hardware implementations of the SHA-2 (256, 384, 512) hash functions. *Proceedings of the 2003 International Symposium on Circuits and Systems* 5.
56. Buchmann, J. (2004). *Introduction to cryptography* (2nd ed.). New York: Springer.
57. https://www.openssl.org/.

Rui Chen Rui Chen received the B.S. degree in computer science from Sichuan Normal University, Chengdu, P. R. China in 2004, and M.S. degree in computer software and theory from Sichuan Normal University in 2007, and the Ph.D. degree in computer science from Sichuan University in 2018, Chengdu, P. R. China. Now he is an associate professor of the College of Computer Science, Sichuan Normal University, Chengdu. His current interests include design and analysis of security protocols and handover authentication of wireless network etc.

Yongcong Mou Yongcong Mou received the B.S. degree in mathematics from Yibin University, Chengdu, P. R. China in 2008, and M.S. degree in operational research and cybernetics from Sichuan Normal University in 2011. Now she is an lecturer of the Sichuan Water Conservancy Vocational College, Chengdu. Her current interests include analysis and prove of security protocols etc.

Min Zhang Min Zhang received Ph.D. degree in Sichuan Province Key Lab of Signal and Information Processing at Southwest JiaoTong University, China in 2017. His research focuses on Network & Information security and authentication protocol etc.