A Robust IoT-Based Three-Factor Authentication Scheme for Cloud Computing Resistant to Session Key Exposure

Feifei Wang,1 Guosheng Xu,1,2 Guoai Xu,1,2 Yuejie Wang,3 and Junhao Peng4

1Beijing University of Posts and Telecommunications, Beijing 100876, China
2National Engineering Laboratory of Mobile Network Security, Beijing 100876, China
3Peking University, Beijing 100871, China
4Guangzhou University, Guangzhou 510006, China

Correspondence should be addressed to Guosheng Xu; guoshengxu@bupt.edu.cn

Received 1 November 2019; Revised 5 January 2020; Accepted 20 January 2020; Published 18 February 2020

Copyright © 2020 Feifei Wang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1. Introduction

With the rapid growth of Internet of Things (IoT) technologies, Internet-enabled devices have had a tremendous impact on people’s works and lives [1–3]. However, the Internet-enabled devices have limited storage, computing power, and communication ability. To solve this limitation, cloud computing emerged as a new service paradigm [4]. It provides a new method with high efficiency and convenience to realize information and resource sharing. The users are able to access the resources, services, or applications that are deployed in distributed cloud servers by utilizing a handheld device anywhere and anytime. And the control server is in charge of authorizing the users and distributed servers.

As the communication channel is open and unprotected, there are diverse and severe security threats for stealing sensitive data and resource in cloud computing environment [5, 6]. An authentication protocol is indispensable to prevent unauthorized access and protect the sensitive data and user privacy. From the first smart card-based authentication protocol [7] introduced by Yang and Shieh in 1999, there have been a large number of enhanced schemes proposed [2, 8–13]. Based on the authentication factors the user employs, the authentication schemes are divided into two-factor authentication schemes and three-factor authentication schemes. Based on the cryptosystem the authentication scheme adopts, the authentication schemes are divided into hash-based schemes, symmetric cryptosystem-based schemes, and public key cryptosystem-based schemes.
1.1. Related Works. In terms of authentication schemes for cloud computing, some proposals have been presented one after another to improve the security and efficiency [14–17]. In 2015, Tsai and Lo [18] put forward an anonymous authentication protocol using bilinear pairing, in which the user can directly login the distributed server without the help of control server. Afterwards, He et al. [19] revealed that their scheme is not resistant to server impersonation attack and put forward an enhanced scheme. In 2017, Kumari et al. [20] presented a biometric-based authentication protocol employing elliptic curve cryptosystem (ECC). However, their scheme cannot withstand known session-specific temporary information attack and fails to preserve three-factor secrecy. In 2018, Amin et al. [21] pointed out that two anonymous authentication schemes [22, 23] have weaknesses like forgery attack and session key disclosure attack and introduced a hash-based two-factor authentication scheme. Unfortunately, Wang et al. [24] revealed that their scheme still cannot resist session key disclosure attack. In 2019, Mo et al. [25] introduced an ECC-based single-server two-factor authentication protocol. But this protocol is not resistant to stolen-verifier attack. In the same year, Zhou et al. [26] put forward a two-factor authentication scheme employing hash function. But we observe that their scheme suffers from forgery attack and replay attack and does not preserve forward secrecy. For better understanding, we summarize these schemes in Table 1.

Among these schemes, the hash-based schemes [21–23, 26] are highly efficient, but they have diverse vulnerabilities, such as desynchronization attack, forgery attack, and failure to achieve forward secrecy and user anonymity. Wang et al. [27, 28] have demonstrated that public key technique is essential for achieving some security attributes such as user anonymity. However, the existing public key cryptosystem-based schemes [18, 20, 25] still have more or less security vulnerabilities due to design deficiencies. Besides, they have high computation overhead as time-consuming operations such as bilinear pairing and scalar multiplication are involved.

In addition, the security of the session key is a noteworthy issue. The existing schemes are not secure against various session key exposure attacks. A great many schemes such as the schemes in [20, 21, 25, 26] cannot withstand known session-specific temporary information attack. And many schemes such as the schemes in [21–23, 26] cannot provide forward secrecy. Besides, in some schemes like the scheme of Amin et al. [21], the attacker can even reveal the session key when he obtaining the smart card [29].

1.2. Motivation and Contributions. The existing schemes suffer from various security defects or involve high computation overhead. The security attributes or the efficiency needs to be improved. In particular, the great majority of schemes fail to guarantee the security of session key, as they are subjected to various session key exposure attacks. It motivates us to present an enhanced authentication scheme that can meet the security requirements at minimum cost and be secure against all the possible session key exposure attacks. We sum up the contributions of the paper as below:

(1) We reveal that Zhou et al.’s scheme [26] does not consider impersonation attack, known session-specific temporary information attack, and forward secrecy.

(2) We put forward an enhanced three-factor authentication scheme using chaotic maps. The session key comprises of a long-term secret value and the secret key generated by Chebyshev chaotic-based Diffie–Hellman key exchange. It can prevent all kinds of session key exposure attacks. The use of Chebyshev chaotic maps contributes to the establishment of secure session key and simultaneously reduces the computation cost.

(3) The Burrows–Abadi–Needham logic proof confirms the completeness of our scheme. The formal analysis under the random oracle model proves the semantic security of session key. And the informal analysis shows that our scheme can resist all kinds of potential attacks and provide desired properties like three-factor secrecy. The performance comparisons demonstrate that our scheme has high security, and its computation and communication overheads are acceptable.

1.3. Organization of the Paper. The rest of the paper is formed as below. We give some background materials in Section 2. We reveal the security defects of Zhou et al.’s scheme in Section 3. We present the enhanced three-factor authentication scheme in Section 4. We discuss the security of our scheme using several widely accepted security analysis methods in Section 5. We present the performance comparisons of our scheme and related schemes in Section 6. The conclusion is given in Section 7.

2. Preliminaries

2.1. Chebyshev Chaotic Maps. According to Zhang [30], the enhanced Chebyshev polynomial is defined as $T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \mod p$, where $n \geq 2$, $x \in [-\infty, +\infty]$, and $p$ is a big prime. The Chebyshev polynomials satisfy commutative law, i.e., $T_a(T_b(x)) = T_b(T_a(x)) \mod p$.

There is a hard mathematical problem on Chebyshev polynomials:

(i) Chebyshev chaotic Diffie–Hellman problem (CHDHP): for given $T_a(x)$, $T_b(x)$, and $x$, the computation of $T_{ab}(x) \equiv T_a(T_b(x)) \equiv T_b(T_a(x)) \mod p$ is infeasible.

2.2. Adversary Model. Based on [31], the abilities of adversary are summarized as below:

(i) The adversary can eavesdrop, replay, block, or alter the transmitted messages in open channel.
When testing forward secrecy, the adversary can obtain control server’s master key or cloud server’s secret key.

The adversary can disclose the password or the parameters of smart card.

When testing three-factor secrecy, the adversary is capable of obtaining any two kinds of authentication factors.

2.3. Notations. The notations of the paper are presented in Table 2.

3. Cryptanalysis of Zhou et al.’s Scheme

We briefly review Zhou et al.’s scheme [26] and point out its limitations in this section. In their scheme, the attacker can perform impersonation attack by replaying the intercepted message. Besides, their scheme is vulnerable to two kinds of session key exposure attacks.

3.1. Review of Zhou et al.’s Scheme

3.1.1. User Registration Phase. $U_i$ delivers an enrollment request to CS in this phase.

Step 1: $U_i$ picks his identity $ID_i$, pseudoidentity $PID_i$, and password $PW_i$. Then $U_i$ selects a random number $r_i$ and calculates $P_i = H_1(PW_i \| r_i)$. Afterwards, $U_i$ delivers the registration request $\{ID_i, PID_i\}$ to CS via the secure channel.

Step 2: after getting $\{ID_i, PID_i\}$, CS checks if $ID_i$ is valid. If it holds, CS computes $A_1 = H_1(PID_i \| ID_{CS} \| s)$ and $B_1 = H_1(ID_i \| s)$. CS saves $ID_i$ in its database and returns $\{A_1, B_1, ID_{CS}\}$ to $U_i$ via the secure channel.
3.1.2. Cloud Server Registration Phase. CS distributes the secret key to $S_j$ in this phase.

Step 1: $S_j$ chooses its identity $SID_j$ and pseudoidentity $PSID_j$ and delivers $\{SID_j, PSID_j\}$ to CS via the secure channel.

Step 2: after getting $\{SID_j, PSID_j\}$, CS computes $sm_1 = H_1(PSID_j || ID_{CS} || s)$ and $sm_2 = H_1(SID_j || s)$. CS delivers $\{sm_1, sm_2, ID_{CS}\}$ to $S_j$ via the secure channel.

Step 3: $S_j$ keeps $\{sm_1, sm_2, ID_{CS}\}$ as secret.

3.1.3. Login and Authentication Phase. $U_i$ and $S_j$ authenticate each other in the assistance of CS as shown in Figure 1.

Step 1: $U_i$ inputs $ID_i^*$ and $PW_i^*$. The smart card picks a new pseudoidentity $PID_{new}^{new}$ computes $r_i^* = E_i @ H_1(ID_i^* || PW_i^*)$, $A_i^* = C_i @ P_i^*$, $B_i^* = D_i @ H_1(ID_i^* || PW_i^*)$, $f_1 = A_i^* @ \alpha$, $f_2 = H_1(\alpha || PID_{new}^{new} || ID_{CS} || ID_i^* || PW_i^*)$, $f_3 = B_i^* @ PID_{new}^{new} @ H_1(\alpha || ID_i^*)$, and $f_4 = H_1(ID_i^* || PID_{new}^{new} || \alpha || f_3)$, where $\alpha$ is a nonce. The smart card delivers the login request $\{PID_i, f_1, f_2, f_3, f_4\}$ to $S_j$ via the public channel.

Step 2: upon receiving $\{PID_i, f_1, f_2, f_3, f_4\}$, $S_j$ picks a new pseudoidentity $PID_{new}^{new}$, computes $s_j = sm_1 @ \beta$, $f_5 = H_1(\beta || PID_{new}^{new} || \beta || ID_{CS} || \beta || SID_j)$, and $f_6 = H_1(\beta || PID_{new}^{new} || \beta || f_4)$, which is a random number. $S_j$ sends $\{PID_i, f_1, f_2, f_3, f_4, PID_j, f_5, f_6, f_7, f_8\}$ to CS via the public channel.

Step 3: after receiving $\{PID_i, f_1, f_2, f_3, f_4, PID_j, f_5, f_6, f_7, f_8\}$, CS computes $\alpha = f_1 @ H_1(PID_j || ID_{CS} || s)$, $ID_j = f_2 @ H_1(\alpha || PID_{new}^{new} || \alpha || ID_{CS} || ID_i^* || PW_i^*)$, $PID_{new} = f_3 @ H_1(\alpha || PID_{new}^{new} || \alpha || ID_j || \alpha || ID_{CS} || ID_i^* || PW_i^*)$, and $f_4 = H_1(\alpha || PID_{new}^{new} || \alpha || f_3)$, and verifies if $f_4 = f_4$. If the equation holds, CS computes $\beta = f_5 @ H_1(\beta || PID_{new}^{new} || \beta || ID_{CS} || s)$, $SID_j = f_6 @ H_1(\beta || PID_{new}^{new} || \beta || ID_{CS} || s || H_1(\beta || SID_j))$, and $f_8 = H_1(\beta || PID_{new}^{new} || \beta || f_7)$, and verifies if $f_8 = f_8$. If it holds, proceed next step, otherwise, the protocol aborts.

Step 4: $S_j$ computes $SK = H_1(\alpha @ \beta || \gamma)$, $f_9 = H_1(\alpha || PID_{new}^{new} || ID_{CS} || s || H_1(\beta || PID_{new}^{new}))$, $f_{10} = H_1(ID_j || ID_{CS} || s || H_1(\beta || PID_{new}^{new}))$, $f_{11} = H_1(SK || f_9 || f_{10} || H_1(ID_j || s))$, $f_{12} = H_1(PID_{new}^{new} || ID_{CS} || s || H_1(\beta || PID_{new}^{new}))$, $f_{13} = H_1(PID_{new}^{new} || ID_{CS} || s || H_1(\beta || PID_{new}^{new}))$, and $f_{14} = H_1(SK || f_{12} || f_8 || H_1(ID_j || s))$, where $\gamma$ is a nonce. $S_j$ sends $\{f_9, f_{10}, f_{11}, f_{12}, f_{13}, f_{14}\}$ to $S_j$.

Step 5: after receiving $\{f_9, f_{10}, f_{11}, f_{12}, f_{13}, f_{14}\}$, $S_j$ computes $\alpha = f_10 @ H_1(\alpha || f_9 || ID_j || ID_{CS} || s || H_1(\beta || PID_{new}^{new}))$, $SK = H_1(\alpha @ \gamma @ \beta)$, $f_{11} = H_1(SK || f_9 || f_{10} || sm_2)$, and verifies if $f_{11} = f_{11}$. If it holds, $S_j$ computes $sm_{new} = f_9 @ H_1(\beta || PID_{new}^{new})$, and removes $sm_1, PSID_j$. $S_j$ delivers $\{f_{12}, f_{13}, f_{14}\}$ to $U_i$.

Step 6: after receiving $\{f_{12}, f_{13}, f_{14}\}$, the smart card computes $\beta = f_9 @ H_1(\alpha || PID_{new}^{new} || \alpha || PID_j)$, $SK = H_1(\alpha @ \beta @ \gamma)$, $f_{14} = H_1(SK || f_9 || f_{10} || sm_2)$, and checks if $f_{14} = f_{14}$. If they are equal, the smart card calculates $C_i^{new} = f_9 @ H_1(\alpha || PID_{new}^{new} || \alpha || PID_j)$, and computes $C_i^{new}, PID_{new}^{new}$, and removes $C_i, PID_i$.

3.2. Cryptanalysis of Zhou et al.’s Scheme. In this section, we reveal that Zhou et al.’s scheme suffers from replay attack, user impersonation attack, server impersonation attack, and known session-specific temporary information attack and fails to provide forward secrecy.

3.2.1. Forward Secrecy. Forward secrecy ensures that when the long-term secret is compromised, the attacker still cannot reveal the established session key. In Zhou et al.’s scheme, with the master key $s$, the attacker can reveal $SK$ as follows:

Step 1: the attacker intercepts $\{PID_i, f_1, f_2, f_3, f_4\}$ and $\{f_{12}, f_{13}, f_{14}\}$ from the public channel.

Step 2: the attacker computes $\alpha = f_1 @ H_1(PID_j || ID_{CS} || s)$, $ID_j = f_2 @ H_1(\alpha || PID_{new}^{new} || ID_{CS} || s || H_1(\alpha || ID_j || s || H_1(\beta || PID_{new}^{new} || \beta || ID_{CS} || s || H_1(\beta || SID_j)))$, and $f_8 = H_1(\beta || PID_{new}^{new} || \beta || f_7)$.

When the long-term secret $s$ is compromised, all the established session keys will be disclosed.

3.2.2. User Impersonation Attack. User impersonation attack denotes that the attacker can masquerade as a valid user to login the cloud server. This attack is performed as follows:

Step 1: the attacker intercepts $\{PID_i, f_1, f_2, f_3, f_4\}$ from the public channel and sends this message to $S_j$.

Step 2: upon receiving $\{PID_i, f_1, f_2, f_3, f_4\}$, $S_j$ handles this message and sends $\{PID_j, f_1, f_2, f_3, f_4, PID_{new}^{new}, f_5, f_6, f_7, f_8\}$ to CS.

Step 3: CS handles the message $\{PID_i, f_1, f_2, f_3, f_4, PID_{new}^{new}, f_5, f_6, f_7, f_8\}$. As $f_4 = f_4$, $f_8 = f_8$, CS sends back $\{f_9, f_{10}, f_{11}, f_{12}, f_{13}, f_{14}\}$ to $S_j$.

Step 4: $S_j$ handles $\{f_9, f_{10}, f_{11}, f_{12}, f_{13}, f_{14}\}$ to the attacker.

$S_j$ and CS believe that $\{PID_i, f_1, f_2, f_3, f_4\}$ comes from the legitimate user $U_i$. Without compromising the smart card, the attacker can impersonate the user $U_i$ by replaying $\{PID_i, f_1, f_2, f_3, f_4\}$. Zhou et al.’s scheme is vulnerable to user impersonation attack.

3.2.3. Server Impersonation Attack. Server impersonation attack denotes that the attacker can masquerade as a valid cloud server to deceive the user. This attack is performed as follows:
Step 1: the attacker intercepts the message \{PID, f_1, f_2, f_3, f_4, PSID, f_5, f_6, f_7, f_8\} from the public channel.

Step 2: when intercepting a new login request \{PID_{new}, f_1', f_2', f_3', f_4'\} from the public channel, the attacker sends \{PID_{new}, f_1', f_2', f_3', f_4', PSID, f_5, f_6, f_7, f_8\} to CS.

Step 3: CS handles \{PID_{new}, f_1', f_2', f_3', f_4', PSID, f_5, f_6, f_7, f_8\}. As \(f_4' = f_8\), CS returns \(f_9, f_{10}, f_{11}, f_{12}, f_{13}, f_{14}\) to the attacker.

Step 4: the attacker delivers \(f_{12}, f_{13}, f_{14}\) to \(U_i\).

Step 5: after receiving \(f_{12}, f_{13}, f_{14}\), as \(f_{14} = f_{14}'\), \(U_i\) believes that the attacker is the legitimate cloud server \(S_j\).

In \{PID, f_1, f_2, f_3, f_4, PSID, f_5, f_6, f_7, f_8\} that \(S_j\) delivers to CS, \{PSID, f_5, f_6, f_7, f_8\} is completely independent with \{PID, f_1, f_2, f_3, f_4\}. CS verifies the validity of the two messages independently. It leads that the attacker can impersonate the cloud server by replaying \{PSID, f_5, f_6, f_7, f_8\}.

3.2.4. Known Session-Specific Temporary Information Attack.
This attack denotes that when the temporary secret such as random number is compromised, the attacker can reveal the established session key. With the random number \(\alpha\), the attacker reveals the session key as follows:

Step 1: the attacker intercepts \{PID, f_1, f_2, f_3, f_4, PSID, f_5, f_6, f_7, f_8\} from the public channel.

Step 2: when \(U_i\) generates a new login request using \{PID_{new}, f_1', f_2', f_3', f_4'\} and sends \{PID_{new}, f_1', f_2', f_3', f_4', PSID, f_5, f_6, f_7, f_8\} to \(S_j\). The attacker intercepts \{PID_{new}, f_1', f_2', f_3', f_4'\} from the public channel.

Step 3: the attacker computes \((\beta \oplus \gamma) = f_{13} \oplus H_1(PID_{new} \| \alpha(PID))\) and \(SK = H_1(\alpha \oplus \beta \oplus \gamma)\).
In Zhou et al.'s scheme, if the random number \( a \) is compromised, the attacker can reveal the session key. Zhou et al.'s scheme is vulnerable to known session-specific temporary information attack.

4. The Proposed Scheme

A robust three-factor authentication scheme for cloud computing is put forward in this section. The proposed scheme is described as below.

4.1. System Setup Phase. CS picks its master key \( s \), CS also selects a nonce \( y \) as its secret value. CS picks a hash function \( H_1() \) and a symmetric cryptosystem \( E_k() / D_k() \). In addition, CS publishes the Chebyshev polynomial's parameters \( x, p \).

4.2. User Registration Phase. \( U_i \) transmits the enrollment request to CS in this phase, as shown in Figure 2.

Step 1: \( U_i \) selects its identity \( ID_i \) and password \( PW_i \), as he wishes, imprints his biometric \( b_i \), and calculates \( A_i = H_1(\{PW_i, ID_i\}) \). Then, \( U_i \) delivers \( \{ID_i, A_i\} \) to CS through the secure channel.

Step 2: after receiving \( \{ID_i, A_i\} \), CS picks two random numbers \( t_i, r_i \), calculates \( C_i = H_1(s || ID_i) \), \( D_i = A_i \oplus C_i \), \( Z_i = H_1(A_i \oplus ID_i) \mod \mu \), and \( \text{PID}_i = E_i(ID || r_i) \), where the integer \( \mu \) satisfies \( 2^{9} \leq \mu \leq 2^{10} \). CS saves \( \{ID_i, t_i, \text{Counter} = 0\} \) into its database. Moreover, CS stores parameters \( \langle D_i, Z_i, \text{PID}_i, t_i, H_1(y \mod r_i), \mu \rangle \) in a smart card and delivers it to \( U_i \).

4.3. Cloud Server Registration Phase. CS issues the secret key to \( S_j \) in this phase.

Step 1: \( S_j \) delivers its identity \( SID_j \) to CS through the secure channel.

Step 2: after receiving \( \{SID_j\} \), CS calculates \( sm_j = H_1(SID_j \| s) \). CS sends back \( \{sm_j\} \) to \( S_j \) through the secure channel.

Step 3: \( S_j \) keeps \( sm_j \) as secret.

4.4. Login and Authentication Phase. \( U_i \) and \( S_j \) perform mutual authentication by the aide of CS in this phase, as shown in Figure 3.

Step 1: \( U_i \) inputs its identity \( ID_i^* \) and password \( PW_i^* \) and imprints the biometric \( b_i^* \). Then, the smart card calculates \( A_i^* = H_1(\text{PID}_i^* \| H_2(b_i^*)) \) and \( Z_i^* = H_1(A_i^* \oplus ID_i^*) \mod \mu \) and verifies whether \( Z_i^* \) is equal to \( Z_i \).

Step 2: after getting \( \{\text{PID}_i^*, R_i, L_i, O_i, T_i\} \). \( S_j \) verifies whether \( T_i \) is fresh. If it holds, \( S_j \) generates a random number \( \beta \) and calculates \( R_2 = T_2 \mod \beta \), \( G_1 = H_1(\text{PID}_i^* \| \text{PID}_i^* \| sm_j \| T_2) \), \( Q_2 = H_1(sm_j \| R_2) \), and \( N_2 = E_{G_1}(R_2) \). Where \( T_2 \) is the current timestamp. \( S_j \) sends \( \{\text{PID}_i^*, R_i, L_i, O_i, T_i, N_i, T_2\} \) to CS via the public channel.

Step 3: after receiving \( \{\text{PID}_i^*, R_i, L_i, O_i, T_i, N_i, T_2\} \), CS checks the freshness of \( T_2 \) and computes \( (ID_i || r_i) = D_i \). \( t_i = O_i \oplus H_1(T_i \| H_1(y \mod r_i)) \), \( C_i = H_1(s || ID_i) \), and \( L_i = H_1(ID || C_i \| R_i \| \text{SID}_j \| O_i \| T_i) \). and verifies \( t_i = t_i \), \( L_i = L_i \). The smart card is probably compromised. For the item \( \{ID_i, t_i, \text{Counter}\} \), CS performs \( \text{Counter} = \text{Counter} + 1 \). When it reaches the preset value, CS suspends \( U_i \). If \( t_i = t_i \), \( L_i = L_i \), CS believes the authenticity of \( S_j \) and performs the next step.

Step 4: CS computes \( sm_j = H_1(SID_j \| s) \), \( Q_1 = H_1(sm_j \| R_1) \), \( G_2 = H_1(\text{PID}_i^* \| R_i \| sm_j \| T_2) \), and verifies \( G_2 \). If it holds, CS believes the authenticity of \( S_j \). Otherwise, the protocol terminates.

Step 5: CS picks a nonce \( r_2 \), computes \( \text{PID}^{\text{new}} = E_i(ID || r_2) \), \( K_i = H_1(C_i \| R_i) \), \( F_i = E_{G_2}(O_i \| Q_i || R_i \| \text{PID}^{\text{new}}) \), and \( M_i = H_1(sm_j \| R_i \| F_i \| T_i) \), where \( T_i \) is the current timestamp. CS transmits \( \{F_i, M_i, T_i\} \) to \( S_j \) through the open channel.

Step 6: after getting \( \{F_i, M_i, T_i\} \), \( S_j \) checks the freshness of \( T_i \) and computes \( M_i = H_1(sm_j \| R_i \| F_i \| T_i) \), and verifies \( M_i = M_i \). If they are equal, \( S_j \) authenticates the user \( U_i \) successfully. \( S_j \) computes \( E_i = T_2 \oplus R_i \), \( SK = H_1(E_i \| Q_i) \), and \( M_2 = H_1(SK \| F_i \| Q_i \| T_i) \). \( S_j \) transmits \( \{F_i, M_i, T_i\} \) to \( U_i \) via the public channel.

Step 7: upon receiving \( \{F_i, M_i, T_i\} \), the smart card checks the freshness of \( T_i \). Then, the smart card computes \( K_i = H_1(C_i \| R_i) \), \( Q_i \| R_i \| \text{PID}^{\text{new}} = D_{K_i}(F_i) \), \( E_i = T_2 \oplus R_i \), \( SK = H_1(E_i \| Q_i) \), and \( M_i = H_1(SK \| F_i \| Q_i \| T_i) \). and checks \( M_i = M_i \). If it holds, \( U_i \) authenticates the cloud server \( S_j \) successfully. The smart card replaces \( PID \), with \( \text{PID}^{\text{new}} \) in the memory.

4.5. Password Update Phase. The original password is replaced by a new password in this phase.

Step 1: \( U_i \) enters \( ID_i^* \) and \( PW_i^* \) and imprints \( b_i^* \). The smart card calculates \( A_i = H_1(\text{PID}_i^* \| H_2(b_i^*)) \) and \( Z_i = H_1(A_i^* \| ID_i^*) \mod \mu \) and verifies whether \( Z_i^* \) is equal to \( Z_i \). If they are not equal, the protocol terminates.

Step 2: \( U_i \) keys a new password \( PW_i^{\text{new}} \). The smart card computes \( A_i^{\text{new}} = H_1(\text{PID}_i^{\text{new}} \| H_2(b_i^*)) \), \( Z_i^{\text{new}} = H_1(A_i^{\text{new}} \| ID_i^*) \mod \mu \) and verifies whether \( Z_i^{\text{new}} \) is equal to \( Z_i \). If they are not equal, the protocol terminates.
In this section, Burrows–Abadi–Needham (BAN) logic [32] proof demonstrates the completeness of our scheme. The formal analysis under the random oracle model shows that our scheme provides semantic security. Moreover, the informal analysis proves that our scheme is not susceptible to known attacks.

5. Security Analysis

In this section, Burrows–Abadi–Needham (BAN) logic [32] proof demonstrates the completeness of our scheme. The formal analysis under the random oracle model shows that our scheme provides semantic security. Moreover, the informal analysis proves that our scheme is not susceptible to known attacks.

5.1. BAN Logic Proof. We confirm the correctness of our scheme in this section. Table 3 lists the notations and rules of BAN logic.

Our scheme ought to fulfill the goals as below.

Goal 1: $S_1 \equiv U_1 \equiv (U_1^\text{sk} \rightarrow S_2)$

Goal 2: $S_1 \equiv (U_1^\text{sk} \rightarrow S_2)$

Goal 3: $U_1 \equiv S_1 \equiv (U_1^\text{sk} \rightarrow S_2)$

Goal 4: $U_1 \equiv (U_1^\text{sk} \rightarrow S_2)$

We idealize our scheme as below:
| Symbols | Description |
|---------|-------------|
| P, Q   | The principals |
| X      | A statement |
| P ⊢ X  | P sees X, P gets a message that consists of X |
| P ⊨ X  | P said X, P sent a message that consists of X |
| P ⊲ X  | P is convinced that X is true |
| P ⊞ X  | P has jurisdiction over X |
| P ≡ Q  | K is a secret shared by P and Q |
| ⌑(X)   | X is fresh |
| ⌑(X)   | X is combined with a secret K |
| ⊤(X)   | X is encrypted with a key K |

| Message meaning rule (Rule 1) | (P ⊨ P ≡ Q, P ⊢ ⌑(X)) or (P ⊨ P ≡ Q, P ⊢ ⌑(X)| ⌑(X) | ⊤(X) | P = X) |
| Nonce-verification rule (Rule 2) | (P ⊨ ⌑(X), P ⊨ ⌑(X) ∧ X) |
| Jurisdiction rule (Rule 3) | (P ⊨ ⌑(X), P ⊨ ⌑(X) ∧ X) |

The analysis of our scheme is based on the following initial assumptions:

A1: CS ⊨ U_i ⊢ S_j | ID_i, U_i | ⊲ R_i, T_i | ⊢ C_i |
A2: CS ⊨ ⌑(T_i) |
A3: CS ⊨ U_i | ⊲ R_i |
A4: S_j | ⊨ CS |
A5: S_j | ⊨ ⌑(T_j) |
A6: S_j | ⊨ CS | U_i | ⊲ R_i |
A7: S_j | ⊨ U_i ⊢ S_j |
A8: U_i | ⊨ CS |
A9: U_i | ⊨ ⌑(R_i) |
A10: U_i | ⊨ CS | U_i ⊢ S_j |
A11: U_i | ⊨ ⌑(T_j) |
A12: U_i | ⊨ S_j | U_i ⊢ SK | S_j |

The analysis of the proposed scheme is as follows. According to M2a, we get

(1) CS ⊨ (ID_i, U_i | ⊲ R_i, T_i | ⊢ C_i |
  From (1), A1, applying Rule 1, we get

(2) CS ⊨ U_i | ⊲ R_i |
  From (2), A2, applying Rule 2, we get

(3) CS ⊨ U_i | ⊲ R_i |
  From (3), A3, applying Rule 3, we get

(4) CS ⊨ U_i | ⊲ R_i |
  Applying to M3, we get

(5) S_j ⊨ (U_i | ⊲ R_i, F_i, T_3 | ⊲ R_i |

5.2. Formal Security Analysis. Based on the security model of two-factor authentication presented by Wang and Wang [33], we put forward a security model of three-factor authentication for cloud computing. Afterwards, we prove the semantic security of our scheme in this model.
5.2.1. Formal Security Model

(1) Participants. There are multiple instances of the control server CS, the cloud server $S_i$, and the user $U_i$ in the authentication scheme for cloud computing. We use $CS^a$, $S_i^a$, and $U_i^a$ to denote these instances.

(2) Queries. The attacker is capable of making the queries as follows:

- Execute $(CS^a/S_i^a/n/U_i^a)$: by making this query, the attacker can obtain the messages delivered via the open channel.
- Send $(CS^a/S_i^a/n/U_i^a/h,xm)$: by making this query, the attacker can impersonate the principal $(U_i^a,S_i^a,GW/N^a)$ to send a message $m$. If $m$ is valid, a response is sent back to the attacker.
- Reveal $(S_i^a/U_i^a)$: by making this query, the attacker can get the session key of $(S_i^a/U_i^a)$, if the principal involves a session key.
- Corrupt $(U_i^a, \tau)$: by making this query, the attacker is capable of getting one or two types of user authentication information.
  - When $\tau = 1$, the attacker acquires the password.
  - When $\tau = 2$, the attacker acquires the smart card.
  - When $\tau = 3$, the attacker acquires the biometric.
- Corrupt $(S_i^a/CS^a)$: by making this query, the attacker can obtain cloud server’s secret key or CS’s master key. This oracle corresponds to the forward secrecy.
- Test $(S_i^a/U_i^a)$: if the principal is fresh (see below) and involves a session key $\xi$, the oracle spins a coin $b$. When $b = 1$, it sends back $\xi$ to the attacker. When $b = 0$, it sends back a random string to the attacker. This oracle is used to simulate the semantic security of session key. The attacker is capable of asking this query only once.

(3) Freshness. We say $(S_i^a/U_i^a)$ is fresh, if the following conditions are met:

- (1) $(S_i^a/U_i^a)$ is accepted and involves a SK
- (2) The attacker never makes Corrupt $(S_i^a/CS^a)$ or Reveal $(S_i^a/U_i^a)$ query

(4) Semantic Security. After making the above queries, the attacker tries to reveal the value of $b$ in test query. The advantage of the attacker in breaking the semantic security is defined as follows:

$$Adv_{\alpha_{\text{se}}}^{\text{sk}}(\mathcal{A}) = 2\Pr(b' = b) - 1.$$  (1)

If for all the attackers, $Adv_{\alpha_{\text{se}}}^{\text{sk}}(\mathcal{A})$ is negligible, the authentication scheme provides semantic security.

5.2.2. Formal Security Analysis

Theorem 1. Let the password space $D_{PW}$ be subject to Zipf distribution [34]. A polynomial-time attacker $\mathcal{A}$ runs against our scheme. We presume $\mathcal{A}$ can ask less than $q_{c}$ Execute queries, $q_{e}$ Send queries, $q_{b}$ Biohash queries, $q_{h}$ Hash queries, and $q_{c}$ Encryption/Decryption queries. We have

$$Adv_{\alpha_{\text{sk}}}^{\text{sk}}(\mathcal{A}) \leq 2C' \cdot q_{e} + \frac{(q_{e} + q_{c})^{2}}{p} + \frac{6q_{e} + q_{h}^{2}}{2l} + \frac{2q_{e} + q_{h}^{2}}{2l} + 2q_{h}Adv_{\text{CHDHP}},$$  (2)

where $l_{1}, l_{2}, l_{3}$ are the length of hash output, bio-hash output, and symmetric encryption output, respectively. $Adv_{\text{CHDHP}}$ is the advantage of $\mathcal{A}$ in solving CHDHP. When using the Tianya password distribution [34], we have $|D_{PW}| = 13$ million, $C' = 0.062239$, and $s' = 0.155478$.

Proof. In order to obtain $Adv_{\alpha_{\text{sk}}}^{\text{sk}}(\mathcal{A})$, we define the games $\mathcal{G}_{i}$ ($0 \leq i \leq 6$), where $\mathcal{G}_{0}$ corresponds to the real attack. $\Pr[\mathcal{X}_{0}]$ is the advantage of $\mathcal{A}$ in revealing $b$ in game $\mathcal{G}_{i}$.

- $\Phi_{0}$: as it simulates the real attack, we get,

$$Adv_{\alpha_{\text{sk}}}^{\text{sk}}(\mathcal{A}) = 2(\Pr[\mathcal{X}_{0}] - 1).$$  (3)

- $\Phi_{1}$: in this game, a hash list $\Lambda_{hi}$ is used to simulate the hash oracle. A biohash list $\Lambda_{bi}$ is used to simulate the biohash oracle. And an encryption/decryption list $\Lambda_{e}$ is used to simulate the encryption/decryption oracle. For a hash query $H_{i}(a)$, if the hash value of $a$ already exists in $\Lambda_{hi}$, the oracle sends back the hash value. Otherwise, the oracle selects a nonce $b$ as the answer of $H_{i}(a)$ and stores $(a, b)$ in $\Lambda_{hi}$. The biohash oracle is performed in the similar way. For an encryption query $E_{k}(\phi)$, the oracle firstly uses $\phi$ and $k$ to search $\Lambda_{e}$. If there exists a tuple $(k, \phi, w)$, it answers $\omega$. Otherwise, it sends back a random string $\omega$ to the adversary and stores $(k, \phi, \omega)$ in $\Lambda_{e}$. For an decryption query $D_{k}(\omega)$, the oracle uses $\omega$ and $k$ to search $\Lambda_{e}$. If there exists a tuple $(k, \phi, \omega)$, it answers $\phi$. Otherwise, it sends back a random string $\omega$ to the adversary, and stores $(k, \phi, \omega)$ in $\Lambda_{e}$. $\Phi_{1}$ is indistinguishable from $\Phi_{0}$. We get

$$\Pr[\mathcal{X}_{0}] - \Pr[\mathcal{X}_{1}] = 0.$$  (4)

- $\Phi_{2}$: in this game, we terminate the execution when encountering some collisions.

- (1) The collision occurs on the outputs of hash function or biohash function with the probability of $(q_{e}^{2}/2^{l+1}) + (q_{h}^{2}/2^{l+1})$
- (2) The collision occurs on the outputs of symmetric encryption with the probability of $(q_{e}^{2}/2^{l+1})$
- (3) The collision occurs on the transcripts of messages, with the probability of $(q_{e} + q_{c})^{2}/2p$

We get

$$|\Pr[\mathcal{X}_{1}] - \Pr[\mathcal{X}_{2}]| \leq \frac{q_{e}^{2}}{2^{l+1}} + \frac{q_{h}^{2}}{2^{l+1}} + \frac{q_{e}^{2}}{2^{l+1}} + \frac{(q_{e} + q_{c})^{2}}{2p}.$$  (5)

$\Phi_{2}$: in this game, we terminate the execution when $\mathcal{A}$ guesses $\{l_{1}, G_{1}, M_{1}, M_{2}\}$. The probability is at most $(q_{e}/2^{l})$. We get
\[ |\Pr[X_3] - \Pr[X_2]| \leq \frac{q_s}{2^l}, \]  
(6)

\( \Phi_4 \): in this game, we terminate the execution when \( \mathcal{A} \) guesses user’s authentication value \( C_i \). The probability is less than \( (q_s/2^l) \). We obtain
\[ |\Pr[X_4] - \Pr[X_3]| \leq \frac{q_s}{2^l}, \]  
(7)

\( \Phi_5 \): in this game, we terminate the execution when \( \mathcal{A} \) has computed \( C_i \) with the help of Corrupt \( (U_i^a, z) \).

1. When Corrupt \( (U_i^a, z = 1, 2) \), \( \mathcal{A} \) is able to guess the biometric with the probability of \( (q_s/2^l) \)
2. When Corrupt \( (U_i^a, z = 2, 3) \), \( \mathcal{A} \) is able to guess the password with the probability of \( C^* q_s' \).
3. When Corrupt \( (U_i^a, z = 1, 3) \), \( \mathcal{A} \) is able to guess \( D_i \) with the probability of \( (q_s/2^l) \).

We obtain
\[ |\Pr[X_5] - \Pr[X_4]| \leq \frac{q_s}{2^l} + C^* q_s' + \frac{q_s}{2^l}, \]  
(8)

\( \Phi_6 \): we use the private hash oracle \( H_i' \) rather than the hash oracle \( H_i \) to compute the session key. \( \mathcal{A} \) knows nothing about \( H_i' \). Thus, we have
\[ \Pr[X_6] = \frac{1}{2}, \]  
(9)

\( \Phi_7 \): it is indistinguishable from \( \Phi_6 \), unless a hash query \( H_i (E_i||Q_i) \) is made by \( \mathcal{A} \). We use \( \Gamma_1 \) to denote this event. We have
\[ |\Pr[X_7] - \Pr[X_6]| \leq \Pr[\Gamma_1]. \]  
(10)

If the hash query \( H_i (E_i||Q_i) \) has been asked, by selecting randomly in \( \Lambda_{H_i} \), we can obtain \( E_i = T_{\alpha} (R_{\alpha}) = T_{\beta} (R_{\beta}) \) with the probability of \( (1/q_s) \). We get
\[ \Pr[\Gamma_1] \leq q_s \text{Adv}_{p}^{CHDHP}. \]  
(11)

From (3)–(11), we have
\[ \text{Adv}_{p}^{\text{new}} (\mathcal{A}) \leq 2C^* q_s' + \frac{(q_s + q_s')^2}{p} + \frac{6q_s + q_s^2}{2^l} \]  
(12)
\[ + \frac{2q_s + q_s^2}{2^l} + \frac{q_s}{2^l} + 2q_s \text{Adv}_{p}^{CHDHP}. \]

5.3. Informal Security Analysis. In this section, we prove that our scheme is resistant to diverse attacks. Particularly, our scheme is secure against all kinds of session key exposure attacks, as the session key is generated based on the long-term secret and Chebyshev chaotic-based Diffie–Hellman key exchange. Besides, we demonstrate that the proposed scheme preserves desired properties such as user anonymity and three-factor seccrety.

5.3.1. User Anonymity. In our scheme, only the control server who has the secret key \( y \) can retrieve ID, from PID. In addition, after authenticating \( U_i \), CS generates a new pseudoidentity PID\text{new} and delivers the encrypted PID\text{new} to \( U_i \). PID\text{new} is encrypted with the secret key \( K_i \) by CS. Only \( U_i \) is able to compute \( K_i \) and obtain PID\text{new}. The attacker knows nothing about PID\text{new}, and hence he cannot link PID\text{new} with PID\text{old}. It makes the user identity untraceable. Consequently, our scheme achieves user anonymity.

5.3.2. Resistance to Off-Line Guessing Attack. As the fuzzy verifier \( Z_i \) is employed in our scheme as suggested in [33], even if the attacker obtains the smart card as well as biometric at the same time, he is unable to reveal the password. With the smart card and biometric, the attacker chooses one pair of identity and password from dictionary space and checks if \( Z_i^* = Z_i \). However, there are a great many candidates conforming to \( Z_i^* = Z_i \). In order to distinguish the correct one from so many candidates, there is no alternative but to launch online guessing attack. However, we employ the “honeywords” technique [33] to prevent this attack. When the number of online guessing attacks reaches the preset value, for example, 10, \( U_i \) is suspended. Consequently, our scheme can resist off-line guessing attack.

5.3.3. Resistance to Session Key Disclosure Attack. The session key SK is computed using \( E_i \) and \( Q_i \). \( E_i \) is the secret key generated by the Chebyshev chaotic-based Diffie–Hellman key exchange. Only \( U_i \) and \( S_j \) who know the random number \( \alpha \) or \( \beta \) are able to compute \( E_i \), \( Q_i \) is computed based on the long-term secret \( sm_j \). Only \( S_j \) and CS who have \( sm_j \) are able to compute \( Q_i \). Besides, \( Q_i \) is transmitted to \( U_i \) by means of symmetric encryption with the secret key \( H_i (C_i||R_i) \). Only \( U_i \) and CS who have \( C_i \), are able to reveal \( Q_i \). Both \( E_i \) and \( Q_i \) are unavailable to the attacker. Therefore, our scheme can resist this attack.

5.3.4. Forward Secrecy. Suppose that the attacker has acquired the master key \( s \), he is able to compute \( Q_i \). However, \( E_i \) is the secret key generated by the Chebyshev chaotic-based Diffie–Hellman key exchange. To reveal \( E_i \), there is no alternative but to solve the CHDHP. Therefore, our scheme preserves forward secrecy.

5.3.5. Resistance to Session-Specific Temporary Information Attack. Assume that the attacker has acquired the random number \( \alpha \). To compute \( E_i = T_{\alpha} (R_{\alpha}) \), \( R_{\alpha} \) is required. \( R_{\alpha} \) is encrypted using the secret key \( Q_i \) or \( K_i \), where \( Q_i = H_i (sm_i||R_i) \) and \( K_i = H_i (C_i||R_i) \). To retrieve \( R_{\alpha} \), the attacker needs to reveal \( C_i \) or \( sm_i \). Assume that the attacker has acquired the random number \( \beta \), the attacker can calculate \( E_i = T_{\beta} (R_{\beta}) \). Afterwards, to derive \( Q_i \), the attacker has to get \( C_i \) or \( sm_i \). However, \( sm_i \) is only known to \( S_j \) and CS, \( C_i \) is only known to \( U_i \) and CS. Therefore, the attacker cannot reveal the session key when the nonce is disclosed.

5.3.6. Resistance to Forgery Attack. In our scheme, the hash values \( (L, G, M_1, M_2) \) of the transmitted parameters and
the secret value $A_i$, $sm_j$ are used to ensure message integrity and verify the sender’s identity. As $C_i$ and $sm_j$ are unavailable to the attacker, he cannot generate a message that is verified to be valid by the recipient.

5.3.7. Resistance to Desynchronization Attack. In each message, the hash value $(L_i, G_i, M_1, M_2)$ is used to ensure that the transmitted parameters are not tampered with. If the attacker alters a parameter of a message, the receiver will find that the received hash value is not equal to the one he computes, and the protocol terminates. Besides, if the attacker blocks a message, as it does not change the long-term parameters the participants have, it does not affect the user’s next login. For instance, if the attacker blocks the message $(F_i, M_3, T_4)$, the user fails to update his pseudoidentity. But with $PID_j$, the user still is able to access the cloud server.

5.3.8. Resistance to Replay Attack. In the proposed scheme, every message contains a timestamp. And the timestamps are involved in the hash values $(L_i, G_i, M_1, M_2)$. Upon receiving a message, the receiver first verifies whether the timestamp is fresh. If it holds, the receiver continues to process the message. Otherwise, the protocol aborts.

5.3.9. Resistance to Privileged Insider Attack. The user never submits his biometric or password to CS at registration. On the other hand, the user cannot masquerade as a cloud server or CS, as $sm_j$ is unavailable. The cloud server cannot masquerade as a user or CS, as $C_i$ is unavailable. Therefore, our scheme is immune to such an attack.

5.3.10. Resistance to Man-in-the-Middle Attack. In each message, the hash value $(L_i, G_i, M_1, M_2)$ of the transmitted parameters and the secret $A_i$, $sm_j$ are computed to ensure message integrity and verify the sender’s identity. As $A_i$ and $sm_j$ are unavailable, the attacker is unable to generate a valid message to replace the intercepted one. Consequently, the attacker is unable to launch man-in-the-middle attack.

5.3.11. Mutual Authentication. In our scheme, based on the authentication value $C_i$, CS verifies the authenticity of $U_i$ by checking $L_i = L_i$. Based on the secret key $sm_j$, CS verifies the authenticity of $S_j$ by checking $G_j = G_j$. If $L_i = L_i$ and $G_j = G_j$, CS believes that $U_i$ and $S_j$ are legitimate and sends a response message to $S_j$. After getting the response message from CS, $S_j$ verifies the authenticity of CS and $U_i$ by checking $M_i = M_i$. If it holds, $S_j$ believes that $U_i$ and CS are legitimate and sends back a response message to $U_i$. Afterwards, $U_i$ verifies the authenticity of CS and $S_j$ by checking $M_j = M_j$. If it holds, $U_i$ believes that CS and $S_j$ are legitimate. Therefore, our scheme provides mutual authentication among CS, $U_i$, and $S_j$.

5.3.12. Resistance to Eavesdropping Attack. The attacker can intercept messages from public channel. However, the secret parameters such as the user authentication value $C_i$, the user identity, the cloud server’s secret key $sm_j$, and the session key SK are protected with hash function and symmetric encryption. The attacker cannot acquire any useful information from the intercepted messages and uses them to launch active attacks.

5.3.13. Resistance to All Kinds of Session Key Exposure. The session key consists of two parts, $E_i$ and $Q_i$. $E_i$ is generated by Chebyshev chaotic-based Diffie–Hellman key exchange. $Q_i$ is computed using the cloud server’s secret key as well as a Chebyshev polynomial. The purpose of $E_i$ is to make sure that our scheme can be resistant to known key attack, as well as preserve forward secrecy. The purpose of $Q_i$ is to make sure that our scheme can withstand session-specific temporary information attack. The attacker can reveal neither $E_i$ nor $Q_i$. Hence, our scheme is resistant to all kinds of session key exposure attacks.

5.3.14. Three-Factor Secrecy. When the attacker reveals the biometric and smart card, he cannot retrieve the password as shown in 5.3.2. When the attacker reveals the smart card and password, he cannot retrieve the biometric from $Z_i$, as the hash function is irreversible. With the biometric and password, the attacker cannot retrieve the critical data of smart card. Hence, our scheme preserves three-factor secrecy.

Most of the existing three-factor authentication schemes fail to preserve three-factor secrecy, because when the biometric and smart card is disclosed, the attacker can guess user’s password based on the verification value that is used to verify the validity of the inputted password and biometric in smart card. However, our scheme employs the fuzzy verifier and “honeywords” technique to prevent revealing of the password.

6. Performance Comparisons

We give the comparisons of our scheme and the recently proposed schemes [20, 21, 25, 26, 35, 36] with regard to security attributes, communication, and computation costs in this section.

The security comparison is given in Table 4. Note that, as Mo et al.’s scheme is designed for single-server environment, it only involves a single cloud server. Ghani et al.’s scheme does not establish session key. We summarize the security requirements of authentication protocol, and based on it, we analyzes the security properties of related schemes in Table 4. It indicates that only the proposed scheme meets all the security requirements, while the related schemes have diverse weaknesses. The security of our scheme is superior to the hash function-based schemes [21, 26], the symmetric cryptosystem-based schemes [35, 36], as well as ECC-based schemes [20, 25].

In Table 5, we presents the computation cost, the communication overhead, and the smart card storage cost of the related schemes concerning the login and authentication phase. Furthermore, the computation cost comparison, communication overhead comparison, and smart card
Running time (ms)  

Zhou Amin Kumari Mo Ghani Martinez-
Pelaez
0 100 200 300 400 500

Table 4: Security features of related schemes.

| Security properties                      | Zhou et al. [26] | Amin et al. [21] | Kumari et al. [20] | Mo et al. [25] | Ghani et al. [35] | Martinez-Pelaez et al. [36] | Our scheme |
|------------------------------------------|------------------|------------------|--------------------|----------------|-------------------|-----------------------------|------------|
| User anonymity                           | ✓                | ✓                | ✓                  | ✓              | ×                 | ✓                           | ✓          |
| Efficient typo detection                 | ×                | ✓                | ✓                  | ×              | ×                 | ✓                           | ✓          |
| Resist desynchronization attack          | ✓                | ✓                | ✓                  | ×              | ×                 | ×                           | ×          |
| Resist off-line guessing attack          | ×                | ×                | ✓                  | ×              | ×                 | ×                           | ×          |
| Resist session key disclosure attack     | ✓                | ×                | ×                  | ×              | ×                 | ×                           | ×          |
| Resist forgery attack                    | ×                | ✓                | ✓                  | ×              | ×                 | ×                           | ×          |
| Resist replay attack                     | ×                | ✓                | ✓                  | ×              | ×                 | ×                           | ×          |
| Resist known session-specific            |                 | ×                | ×                  | ×              | ×                 | ×                           | ×          |
| temporary information attack             |                 | ×                | ×                  | ×              | ×                 | ×                           | ×          |
| Forward secrecy                          | ×                | ×                | ✓                  | ×              | ×                 | ×                           | ×          |
| Three-factor secrecy                     | ×                | ×                | ×                  | ×              | ×                 | ×                           | ×          |
| Stolen-verifier attack                   | ✓                | ✓                | ✓                  | ×              | ×                 | ×                           | ×          |
| Resist all kinds of session key exposure | ×                | ×                | ×                  | ×              | ×                 | ×                           | ×          |

Table 5: Computation and communication costs and smart card storage cost of related schemes.

| Computation overhead | User | Server | CS | Running time (ms) | Communication cost (bits) | Storage cost (bits) |
|----------------------|------|--------|----|-------------------|---------------------------|-------------------|
| Zhou et al. [26]     | 10T_H | 7T_H   | 19T_H| 18                | 3584                      | 640               |
| Amin et al. [21]     | 9T_H  | 4T_H   | 10T_H| 11.5              | 2560                      | 512               |
| Kumari et al. [20]   | 2T_H + 5T_H + 3T_P | 5T_H + 3T_P | 6T_H + 2T_P | 554.64             | 2624                      | 576               |
| Mo et al. [25]       | 7T_H + 1T_A + 3T_P | 6T_H + 1T_A + 3T_P | - | 385.998            | 960                      | 712               |
| Ghani et al. [35]    | 2T_H  | 2T_H   | 4T_H + 2T_s | 21.4             | 1792                      | 384               |
| Martinez-Pelaez et al. [36] | 7T_H + 3T_s | 6T_H + 3T_s | 26T_H + 2T_s | 89.1             | 3456                      | 640               |
| Our scheme            | 1T_H + 2T_C + 7T_H + 1T_s | 5T_H + 2T_C + 1T_s | 9T_H + 3T_s | 159.1            | 2304                      | 532               |

Figure 4: The computation cost of related schemes.

storage cost comparison are shown in Figure 4, Figure 5, and Figure 6, respectively. As shown in Figure 4, the computation overhead of our scheme is not as good as the hash-based schemes and the symmetric cryptosystem-based schemes, as public key operations are used to guarantee the security. But it is obviously better than the ECC-based schemes. As shown in Figure 5, the communication cost of our scheme is higher than Mo et al.’s scheme and Ghani et al.’s scheme, but it is lower than the other schemes. As shown in Figure 6, the storage cost of our scheme is inferior to Amin et al.’s scheme and Ghani et al.’s scheme, but it is superior to the other schemes.

$T_H$, $T_{BH}$, $T_S$, and $T_C$ denote a hash function, a biohash function, a symmetric encryption/decryption, and a Chebyshev polynomial, respectively. $T_P$ and $T_A$ denote a point multiplication and a point addition on elliptic curve group. The computing time of lightweight operation “XOR” is negligible. In accordance with [3, 37], when performed on a smart phone with a Hisilicon kirin 960 CPU, 6 GB RAM, and the storage of 64 GB, the computations of $T_H$, $T_S$, $T_P$, $T_A$, $T_C$, and $T_{BH}$ take 0.5 ms, 8.7 ms, 63.075 ms, 0.262 ms, 21.02 ms, and 21.02 ms, respectively. Besides, we assume that the bit length of timestamp, random number, the user identity, the identity of cloud server, the hash value, Chebyshev polynomial, and the output of symmetric encryption are 128 bits. The point on elliptic curve group is 160 bits.

The hash-based schemes and the symmetric cryptosystem-based schemes have obvious advantage in efficiency as they just involve lightweight cryptographic operations. However, they suffer from various security vulnerabilities. In Zhou et al.’s scheme, the attacker is capable of impersonating the user and the cloud server by replaying the intercepted message. In Amin et al.’s scheme, the attacker can retrieve user’s password, disclose the session key, and impersonate the user when smart card is compromised. Martinez-Pelaez et al.’s scheme and Ghani et al.’s scheme are vulnerable to diverse and serious security weaknesses. They are unable to provide the essential security protection.
The ECC-based schemes have low efficiency. They have better security than the hash-based schemes and the symmetric cryptosystem-based schemes, but still have security flaws. In Mo et al.’s scheme, the attacker can impersonate the user when the verifier table is leaked. Kumari et al.’s scheme achieves many security features, but it does not provide three-factor secrecy.

In terms of the security of session key, only our scheme is resistant to all kinds of session key exposure attacks, as Chebyshev chaotic-based Diffie–Hellman key exchange and the long-term secret are used to establish the session key. None of the related schemes can withstand known session-specific temporary information attack. If one communication end uses unsecure random number generator, it will lead to the disclosure of the session key. The ECC-based schemes provide forward secrecy, as the elliptic curve-based Diffie–Hellman key exchange is employed. Furthermore, in Amin et al.’s scheme and Martinez-Pelaez et al.’s scheme, the attacker can retrieve the session key when the smart card is compromised.

To sum up, the security of our scheme is optimal. In addition, its computation and communication overheads are obviously lower than the ECC-based schemes. Hence, our scheme is more practical.

7. Conclusion

In this paper, we pointed out that Zhou et al.’s scheme is unable to provide the essential security protection for cloud computing, as it does not consider replay attack, known session-specific temporary information attack, and forward secrecy. Furthermore, we present a novel IoT-based three-factor authentication scheme for cloud computing using chaotic maps. The use of Chebyshev chaotic maps guarantees the security of session key and simultaneously reduces the computation cost. In addition, the BAN logic analysis demonstrates that our scheme achieves mutual authentication as well as session key negotiation. The formal analysis confirms the semantic security of session key. The informal analysis proves that our scheme can withstand known attacks and achieve desired attributes such as user anonymity and resistance to all kinds of session key exposure attacks. Finally, the performance comparisons show that our scheme has significant advantage compared with the related schemes. As our scheme has high security, it is especially applicable to the security-critical cloud applications such as cloud-based healthcare systems. Afterwards, on the basis of our current work, we plan to make further study on the authentication protocol for smart healthcare systems.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This research was funded by the National Key Research and Development Program of China under Grant no. 2018YFB0803600, the National Natural Science Foundation of China under Grant no. 61831003, and the National Natural Science Foundation of China under Grant no. 61873069.

References

[1] W. Ding, X. Jing, Z. Yan, and L. T. Yang, “A survey on data fusion in Internet of Things: towards secure and privacy-preserving fusion,” Information Fusion, vol. 51, pp. 129–144, 2019.
[2] Q. Jiang, Y. Qian, J. Ma, X. Ma, Q. Cheng, and F. Wei, “User-centric three-factor authentication protocol for cloud-assisted wearable devices,” International Journal Communication Systems, vol. 32, no. 6, p. e3900, 2019.
[3] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and M. Jo, “Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing internet of things,” IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2884–2895, 2018.
[4] J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, and R. Buyya, “Ensuring security and privacy preservation for cloud data services,” ACM Computing Surveys, vol. 49, no. 1, pp. 1–39, 2016.

[5] W. Meng, W. H. Lee, S. R. Murali, and S. P. T. Krishnan, "Charging me and I know your secrets!: towards juice filming attacks on smartphones," in Proceedings of the 2015 ACM Workshop on Cyber-Physical System Security, ACM, Singapore, April 2015.

[6] P. Gope and A. K. Das, "Robust anonymous mutual authentication scheme for," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1764–1772, 2017.

[7] W. H. Yang and S. P. Shieh, “Password authentication schemes with smart cards,” Computers & Security, vol. 18, no. 8, pp. 727–733, 1999.

[8] F. Wu, L. Xu, and X. Li, “A new chaotic map-based authentication and key agreement scheme with user anonymity for multi-server environment,” in Proceedings of the International Conference on Frontiers Computing 2017, vol. 464, pp. 335–344, Osaka, Japan, July 2017.

[9] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and S. A. Chaudhry, “Efficient end-to-end authentication protocol for wearable health monitoring systems,” Computers & Electrical Engineering, vol. 63, pp. 182–195, 2017.

[10] A. Ostad-Sharif, H. Arshad, M. Nikooghadam, and D. Abbasiinezhad-Mood, "Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme," Future Generation Computer Systems, vol. 100, pp. 882–892, 2019.

[11] X. Huang, X. Chen, J. Li, Y. Xiang, and L. Xu, “Further observations on smart-card-based password-authenticated key agreement in distributed systems,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 7, pp. 1767–1775, 2014.

[12] M. Wazid, A. K. Das, S. Kumari, X. Li, and F. Wu, “Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for TMIS,” Security and Communication Networks, vol. 9, no. 13, pp. 1983–2001, 2016.

[13] F. Wang, G. Xu, C. Wang, and J. Peng, “A provably secure biometrics-based authentication scheme for multi-server environment,” Security and Communication Networks, vol. 2019, Article ID 2388615, 15 pages, 2019.

[14] V. Odelu, A. K. Das, S. Kumari, X. Huang, and M. Wazid, “Provably secure authenticated key agreement scheme for distributed mobile cloud computing services,” Future Generation Computer Systems, vol. 68, pp. 74–88, 2017.

[15] P. Chandrakar and H. Om, “A secure and robust anonymous three-factor remote user authentication scheme for multi-server environment using ECC,” Computer Communications, vol. 110, pp. 26–34, 2017.

[16] C. Wang, K. Ding, B. Li et al., "An enhanced user authentication protocol based on elliptic curve cryptosystem in cloud computing environment," Wireless Communications and Mobile Computing, vol. 2018, Article ID 1048697, 13 pages, 2018.

[17] M. R. Ogila and L. Ogila, “Expert knowledge-based authentication protocols for cloud computing applications,” in Proceedings of the 10th International Conference on Intelligent Networking and Collaborative Systems, vol. 23, pp. 82–27, Oita, Japan, September 2019.

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

[19] D. He, N. Kumar, M. K. Khan, L. Wang, and J. Shen, "Efficient privacy-aware authentication scheme for mobile cloud computing services," IEEE Systems Journal, vol. 12, no. 2, pp. 1621–1631, 2018.

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

[21] R. Amin, N. Kumar, G. P. Biswas, R. Jqbal, and V. Chang, "A lightweight authentication protocol for IoT-enabled devices in distributed cloud computing environment," Future Generation Computer Systems, vol. 78, pp. 1005–1019, 2018.

[22] K. Xue, P. Hong, and C. Ma, "A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture," Journal of Computer and System Sciences, vol. 80, no. 1, pp. 195–206, 2014.

[23] M. C. Chuang and M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smartcards and biometrics," Expert Systems with Applications, vol. 41, no. 4, pp. 1411–1418, 2014.

[24] P. Wang, B. Li, H. Shi, Y. Shen, and D. Wang, “Revisiting anonymous two-factor authentication schemes for IoT-enabled devices in cloud computing environments,” Security and Communication Networks, vol. 2019, Article ID 2516963, 13 pages, 2019.

[25] J. Mo, Z. Hu, H. Chen, and W. Shen, “An efficient and provably secure anonymous user authentication and key agreement for mobile cloud computing,” Wireless Communications and Mobile Computing, vol. 2019, Article ID 4520685, 12 pages, 2019.

[26] L. Zhou, X. Li, K. Yeh, C. Su, and W. Chiu, “Lightweight IoT-based authentication scheme in cloud computing circumstance,” Future Generation Computer Systems, vol. 91, pp. 244–251, 2019.

[27] D. Wang, D. He, P. Wang, and C. Chu, “Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment,” IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 4, pp. 428–442, 2015.

[28] D. Wang and P. Wang, “On the anonymity of two-factor authentication schemes for wireless sensor networks: attacks, principle and solutions,” Computer Networks, vol. 73, pp. 41–57, 2014.

[29] S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, “Secure biometric-based authentication scheme using Chebyshev chaotic map for multi-server environment,” IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 5, pp. 824–839, 2018.

[30] L. Zhang, “Cryptanalysis of the public key encryption basing on multiple chaotic systems,” Chaos Solitons & Fractals, vol. 37, no. 3, pp. 669–674, 2008.

[31] D. Dolev and A. Yao, “On the security of public key protocols,” IEEE Transactions on Information Theory, vol. 29, no. 2, pp. 198–208, 1983.

[32] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," ACM Transactions on Computer Systems, vol. 8, no. 1, pp. 18–36, 1990.

[33] D. Wang and P. Wang, "Two birds with one stone: two-factor authentication with security beyond conventional bound," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4, pp. 708–722, 2018.

[34] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf’s law in passwords," IEEE Transactions on Information Forensics and Security, vol. 12, no. 11, pp. 2776–2791, 2017.

[35] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Rahman, and M. N. Saqib, “Security and key..."
management in IoT-based wireless sensor networks: an authentication protocol using symmetric key,” *International Journal of Communication Systems*, vol. 32, no. 16, p. e4139, 2019.

[36] R. Martínez-Peláez, H. Toral-Cruz, J. Parra-Michel et al., “An enhanced lightweight IoT-based authentication scheme in cloud computing circumstances,” *Sensors*, vol. 19, no. 9, p. 2098, 2019.

[37] D. Abbasinezhad-Mood and M. Nikooghadam, “Efficient anonymous password-authenticated key exchange protocol to read isolated smart meters by utilization of extended Chebyshev chaotic maps,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4815–4828, 2018.