IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 23, 2018, accepted July 5, 2018, date of publication July 10, 2018, date of current version July 30, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2854798

Provably Secure Multi-Server Authentication Protocol Using Fuzzy Commitment

SUBHAS BARMAN[1], ASHOK KUMAR DAS[2], (Senior Member, IEEE), DEBASIS SAMANTA[3], SAMIRAN CHATTOPADHYAY[4], JOEL J. P. C. RODRIGUES[5,6,7,8], (Senior Member, IEEE), AND YOUNGHO PARK[9], (Member, IEEE)

[1]Jalpaiguri Government Engineering College, Jalpaiguri 735102, India
[2]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology at Hyderabad, Hyderabad 500 032, India
[3]Department of Computer Science and Engineering, IIT Kharagpur, Kharagpur 721302, India
[4]Department of Information Technology, Jadavpur University, Kolkata 700 098, India
[5]National Institute of Telecommunications (Inatel), Santa Rita do Sapucaí 37540-000, Brazil
[6]Instituto de Telecomunicações, 1049-001 Lisbon, Portugal
[7]ITMO University, 197101 Saint Petersburg, Russia
[8]University of Fortaleza, Fortaleza 60811-905, Brazil
[9]School of Electronics Engineering, Kyungpook National University, Daegu 41566, South Korea

Corresponding author: Youngho Park (parkyh@knu.ac.kr)

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Science, ICT and Future Planning under Grant 2017R1A2B1002147, in part by the BK21 Plus Project through the Ministry of Education, Korea, under Grant 21A20131600011, in part by the National Funding from the FCT-Fundação para a Ciência e a Tecnologia through the UID/EEA/50008/2013 Project, in part by the Government of the Russian Federation, under Grant 08-08, in part by Finep, with resources from Funttel, through the Centro de Referência em Radiocomunicações - CRR Project of the Instituto Nacional de Telecomunicações (Inatel), Brazil, under Grant 01.14.0231.00, in part by the Brazilian National Council for Research and Development (CNPq) under Grant 309335/2017-5, and in part by the Information Security Education & Awareness Phase II Project, Department of Electronics and Information Technology (DeitY), India.

ABSTRACT Remote user authentication is a cryptographic mechanism through which a remote server verifies the legitimacy of an authorized user over an insecure communication channel. Most of the existing authentication schemes consider single-server environments and require multiple registrations of the same user for multiple servers. Moreover, most of these schemes do not consider biometric template revocation and error correction for noisy biometric signals. In addition, the existing schemes have several weaknesses, including stolen smart card attack, lack of user anonymity, user impersonation attack, and non-diversification of biometric data. To overcome these disadvantages, we propose a new three-factor authenticated key agreement scheme using a fuzzy commitment approach. The three factors used in the proposed scheme are the user's password, smart card, and personal biometrics. The security of the proposed scheme is verified using a formal security analysis under the broadly accepted Real-Or-Random model for the session key security. The widely accepted Burrows-Abadi-Needham logic is also applied for mutual authentication between a legally registered user and a server, and formal security verification using the broadly accepted Automated Validation of Internet Security Protocols and Applications is performed for the proposed scheme through simulation to show that it is secure. In addition, the informal security analysis of the proposed scheme shows that the scheme can resist other known attacks. Finally, a comparative study of the proposed scheme with the existing related schemes is conducted to measure the tradeoff among the security and functionality features and the communication and computation costs.

INDEX TERMS Multi-server authentication, fuzzy commitment, security, BAN logic, AVISPA.

I. INTRODUCTION

The advancement of Information and Communication Technology (ICT) has made many services available to the people through the Internet. People can access different servers for their services to satisfy their requirements wherever and whenever they want. Different mobile devices (e.g., PDAs, mobile phones and notebooks) are available to users within their budget, and users can use these devices anytime from anywhere to obtain the desired services from a remote server through a public channel (e.g., the Internet). In this context, remote authentication is required to establish a secure communication between a user (client) and a remote server.

2169-3536 © 2018 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

For example, only authorized patients can access a medical server for medical services.

Password-based authentication is the earliest authentication system and is widely used in different systems to make services available only to authorized users. The first password-based authentication scheme was introduced by Lamport [1] in 1981. In this scheme, a server maintains a password table; hence, this scheme is not able to prevent a stolen-verifier attack. Later, many researchers reported improved password-based authentication schemes to address the above problem [2]–[4]. However, passwords are often chosen from user's social information or are composed of low-entropy information. These passwords can be computed via either social engineering or dictionary attacks. To overcome this problem, researchers have studied token-based authentication combined with knowledge-based authentication to provide two-factor authentication [3]–[7]. Unfortunately, the smart card (i.e., token) may be damaged or stolen by an attacker. The stored information is easily extracted from the stolen smart card using power analysis attacks [8], [9].

He *et al.* [6] observed that Wu *et al.*'s smart-card-based remote authentication scheme [5] is vulnerable to impersonation and privileged-insider attacks if the smart card is stolen. Subsequently, He *et al.* proposed an improved authentication scheme to overcome the weaknesses found in Wu *et al.*'s scheme [5]. Unfortunately, Zhu [7] found that He *et al.*'s scheme [6] is also not secure with respect to offline password guessing attacks, and they proposed an RSA-based authentication scheme [7]. Similarly, the literature contains many two-factor-based authentication schemes [10]–[13].

A user's biometrics (e.g., fingerprint, iris, palm print, face and voice) [14] have been integrated with a password and smart card to enhance the level of security of a remote authentication scheme [15]–[21]. Lee *et al.* [15] proposed a fingerprint-based authentication scheme following ElGamal's public key cryptosystem. In their scheme, the user's password, smart card and fingerprint minutiae are used for strengthening the security level of the authentication scheme. However, their scheme is vulnerable to masquerade and server spoofing attacks [19], [20]. To withstand these security flaws, Lin and Lai [20] proposed an improved authentication scheme by combining a password and fingerprint minutiae template to form a super password. Unfortunately, Mitchell and Tang [22] analyzed Lin and Lai's scheme [20] and observed that it is not secure because the smart card stores insufficient information for checking the correctness of old passwords.

Most of the existing authentication and session key agreement protocols reported in the literature consider a single-server environment. In reality, users may want to access multiple servers for different services. In a single-server environment, if a user wants to access multiple servers, he/she needs to register with all the servers, and multiple logins are required. This limitation of single-server authenticated key agreement schemes can be addressed with the implementation of multi-server authentication schemes. Therefore, it is essential to provide an authentication scheme for multi-server environments. Several three-factor authentication schemes [23]–[27] have been proposed for multi-server environments. Li *et al.* [28] noted that the scheme in [24] is vulnerable to stolen smart card attacks. Mishra *et al.* [27] also observed that the schemes in [23] and [26] fail to resist insider attacks, and the scheme in [25] cannot resist stolen smart card, server spoofing & impersonation attacks.

Amin and Biswas proposed an authenticated key agreement scheme for a multi-medical-server environment. However, Das *et al.* [29] observed that Amin and Biswas's scheme [30] is vulnerable to multiple attacks, and it does not support a biometric update phase. Subsequently, Das *et al.* [29] incorporated this phase into their scheme.

Lu *et al.* [31] and Wang *et al.* [32] also designed improved authentication schemes over Mishra *et al.*'s scheme [27]. He and Wang [33] presented a robust biometrics-based multi-server authentication protocol. However, Odelu *et al.* [34] noted that He-Wang's protocol [33] cannot prevent known session temporary information, replay and impersonation attacks. In addition, the protocol does not preserve strong user anonymity. To erase these security loopholes, Odelu *et al.* [34] proposed a new multi-server authentication protocol.

Reddy *et al.* [35] cryptanalyzed Lu *et al.*'s scheme [31] and noted its security weaknesses, such as impersonation and man-in-the-middle attacks. In addition, Lu *et al.*'s scheme [31] lacks user anonymity and perfect forward secrecy properties. Then, they designed an improved robust elliptic-curve-cryptography-based authentication scheme for multi-server environments.

Reddy *et al.* [36] analyzed the scheme of Wang *et al.* [32] and noted several weaknesses, such as vulnerability to impersonation and insider attacks. Additionally, Wang *et al.*'s scheme [32] lacks anonymity. To overcome the security loopholes found in Wang *et al.*'s scheme, Reddy *et al.* [36] proposed an enhanced multi-server authentication scheme.

Chatterjee *et al.* [37] designed a new biometric-based authentication protocol using the Chebyshev chaotic map. Their protocol offers small key size, fast computation and high efficiency for multi-server environments compared to existing schemes. Furthermore, Kumari *et al.* [38] proposed a biometrics-based authentication scheme for multi-server environments. Their scheme applies the fuzzy extractor method to provide proper matching of biometric patterns.

Most of the existing biometric-based authentication schemes for mutual authentication and session key agreement in multi-server environments do not consider the following requirements: 1) the privacy of the biometric identity of a user, 2) diversification of the biometric template for revocability and 3) periodic biometric template update. In this paper, we aim to design a new multi-server authentication protocol that makes use of the fuzzy commitment approach for biometric verification.

A. THREAT MODEL

We assume that any two participants in a network communicate over an insecure channel using the broadly accepted Dolev-Yao threat (DY) model [39]. Under the DY model, an adversary $\mathcal{A}$ can not only eavesdrop on the messages transmitted between the communicating participants but also can modify and delete the contents of the transmitted messages or even insert an entirely fake message during the communication. In addition, via a power analysis attack [8], [9], $\mathcal{A}$ can extract all the sensitive secret credentials stored in the lost or stolen smart card of a legal registered user. Another adversary model known as the Canetti and Krawczyk adversary model (CK-adversary model) [40] is the current *de facto* standard in modeling authentication and key agreement protocols. The CK-adversary model allows $\mathcal{A}$ to not only intercept, modify and delete messages (as in the DY model) but also to compromise the secret credentials, including the session keys and the session states. Therefore, the security of an authentication and key agreement protocol should ensure that the leakage of some forms of secret credentials, such as session ephemeral secrets or session keys, will lead to the minimum possible effect on the security of the other secret credentials of the entities involved in the communication [34].

B. RESEARCH CONTRIBUTIONS

The main contributions are listed below:

- A new multi-server authentication mechanism scheme using the fuzzy commitment approach is proposed. In the proposed scheme, each server S_j and user U_i need to register with the trusted registration center RC. After mutual authentication, both U_i and S_j establish a session key SK_{ij} for their secure communication. The session key is constructed using both the short-term and long-term secret credentials, so the proposed scheme achieves the ephemeral secret leakage (ESL) attack under the CK-adversary model (as discussed in the threat model in Section I-A). In addition, the proposed scheme supports an efficient password/biometric update phase and a smart card revocation phase.
- The proposed scheme's formal security analysis is tested with the widely used ROR model. Furthermore, the mutual authentication between U_i and S_j is proved using the broadly accepted BAN logic proof. In addition, informal security analysis and formal security verification using the widely used AVISPA simulated tool are conducted to show that the proposed scheme can resist several known attacks.
- A detailed comparative study on the security & functionality features and the communication and computation overheads demonstrates that the proposed scheme provides superior security and efficiency compared to other related authentication schemes.

C. ORGANIZATION

The remainder of this paper is organized as follows. Section II presents the necessary mathematical preliminaries needed to discuss and analyze the proposed scheme in this paper. In Section III, various phases related to the proposed scheme are discussed. Section IV gives a rigorous security evaluation of the proposed scheme using both formal and informal security analysis. In addition, formal security verification using the AVISPA tool is performed in Section V. In Section VI, a detailed comparative study of the proposed scheme and other related schemes is conducted. The paper is finally concluded in Section VII.

II. PRELIMINARIES

In this section, we briefly discuss about the cryptographic one way hash function, revocable template generation, error correction coding and fuzzy commitment scheme that are needed to describe and analyze the proposed scheme.

A. CRYPTOGRAPHIC ONE-WAY HASH FUNCTION

A hash function h: $A \rightarrow B$ is defined as a deterministic mapping from a set $A = \{0, 1\}^*$ of *documents* (strings) of variable length to another set $B = \{0, 1\}^l$ of strings of fixed length, say l bits (called the hash outputs or message digests). The one-way cryptographic hash function is a specialized hash function that has the following properties:

- For any input $x \in A$, it is easy to compute $h(x)$. The term *easy* refers to polynomial or less time complexity. Additionally, the function $h(\cdot)$ is deterministic in nature, i.e., the same message always results in the same hash value.
- Any change in an input $x \in A$ would result in a hash value that is completely uncorrelated with the hash value $h(x)$, and it appears to be random.
- *Preimage resistance*: As the name "one-way" implies, it is computationally infeasible to find the original message x given the message digest $h(x)$ of $x \in A$. This property is also referred to as the *one-way property*.
- *Second preimage resistance*: For any given $x \in A$, it is computationally infeasible to find another $x' \in A$ such that $h(x) = h(x')$. This property is also called the *weak-collision resistant property*.
- *Strong collision resistance*: A collision in a one-way hash function is defined as $h(x) = h(x')$ for any $x, x' \in A$ and $x \neq x'$. The collision resistance property states that it is also computationally infeasible to find any two inputs $x, x' \in A$ such that $x \neq x'$ with $h(x) = h(x')$.

The above one-way hash function $h(\cdot)$ with collision resistance is formally defined as follows [41].

Definition 1: If $Adv_{\mathcal{A}}^{HASH}(t)$ denotes the advantage of an adversary $\mathcal{A}$ in finding a hash collision in polynomial time t, then

$$Adv_{\mathcal{A}}^{HASH}(t) = Pr[ins_1, ins_2 \in_R \mathcal{A} : ins_1 \neq ins_2, \\ h(ins_1) = h(ins_2)],$$

where $Pr[X]$ is the probability of a random event X, and the pair $(ins_1, ins_2) \in_R \mathcal{A}$ indicates that the input strings ins_1 and ins_2 are randomly picked by $\mathcal{A}$. An (ψ, t)-adversary $\mathcal{A}$ attacking the collision resistance of $h(\cdot)$ means that the runtime of $\mathcal{A}$ is at most t and that $Adv_{\mathcal{A}}^{HASH}(t) \leq \psi$.

B. REVOCABLE TEMPLATE GENERATION

A revocable template, also known as a cancelable template [42], is used in biometric-based systems to ensure the privacy and revocability of biometric data. Biometric data (for example, the minutiae set of fingerprint *BIO*) is transformed into a revocable form, say revocable or cancelable template C_T, using a transformation function, say $f(\cdot)$, with the help of a transformation parameter T_p, that is, $C_T = f(BIO, T_p)$. The following properties should be satisfied by a revocable template generation process:

(i) *Collision-free template generation:* If $C_{T_i} = f(BIO_i, T_p)$ and $C_{T_j} = f(BIO_j, T_p)$, then $C_{T_i} \neq C_{T_j}$ for $BIO_i \neq BIO_j$. Moreover, if $C_{T_k} = f(BIO, T_{p_k})$ and $C_{T_l} = f(BIO, T_{p_l})$, then $C_{T_k} \neq C_{T_l}$ for $T_{p_k} \neq T_{p_l}$.

(ii) *Intra-user variability tolerance:* A cancelable template $C_{T_i} = f(BIO_i, T_p)$ and another template $C'_{T_i} = f(BIO'_i, T_p)$ can be generated from two different instances of the same fingerprint. Let us assume that $MS(\cdot)$ is a function to detect the matching score of two sets of biometric data. The matching score of two cancelable templates (enrolled and query) should be similar, as in the case of feature sets BIO_i and BIO'_i. In other words, if $MS(BIO_i, BIO'_i) > th$, then $MS(C_{T_i}, C'_{T_i}) > th$, where th is a threshold matching score.

(iii) *Biometric template revocation:* If any template is compromised, the same transformation function can be used to generate a new template with the help of a new transformation parameter, and the system can issue the new template. In other words, the biometric data must be reusable.

(iv) *Privacy of user:* The privacy of a user should be protected through the cancelable template; that is, the cancelable template should not leak any information about the real biometric data of a user.

C. ERROR CORRECTION TECHNIQUE

In a biometric system, intra-user variation is treated as error in the biometric template. Error correction coding is used to handle errors in the biometric template due to noise in the biometric image [43]. Assume that the template is generated from an instance BIO_{enrol} (i.e., $C_{T_{enrol}} = f(BIO_{enrol}, T_p)$) at the time of enrollment and that the query template is generated from another instance BIO_{query} (i.e., $C_{T_{query}} = f(BIO_{query}, T_p)$) of the same biometric data at the time of authentication. The difference between the two templates can be computed using the Hamming distance, that is, $e = HammDist(C_{T_{enrol}}, C_{T_{query}})$, which is known as the error. The error e can be corrected if and only if the error correction capacity of the error correction technique is not less than e bits. The error correction technique [44], [45] includes two main steps: 1) encoding and 2) decoding. In the encoding part, an input string is encoded, which produces a codeword. It is assumed that during the transmission of the codeword, some noise may result in error in the transmitted signal, and the recipient therefore receives the erroneous codeword. According to the error correction capacity, erroneous codewords may be decoded correctly into the original string.

D. FUZZY COMMITMENT SCHEME

In the literature, biometric data are used in many remote authentication and key exchange protocols using one-way hashing, biohashing and fuzzy extractor techniques. According to the analysis of Nagar *et al.* [46], biohashing template transformation is vulnerable to intrusion and linkage attacks. An intruder may obtain a close approximation of the original biometric template using a biohashed value of the biometric data. A one-way hash function may enhance the error due to the fuzziness of biometric data. The one-way hash function may generate a completely different template for even a single-bit variation in the biometric data [47], [48]. Therefore, a fuzzy extractor is introduced to extract an error-tolerant random string similar to the enrolled string from the same biometric data but with noise.

The fuzzy commitment technique introduced by Juels and Wattenberg [49] is used in biometric-based remote authentication. This scheme has two main steps: 1) locking a secret and 2) releasing the secret. In the literature, many works have reported on the biometric-based fuzzy commitment scheme [43]. A randomly generated cryptographic key K_r is encoded into its equivalent codeword, that is, $\theta_{ps} = \varepsilon_{enc}(K_r)$, where ε_{enc} is an error correction encoding technique. A binary string C_{T_i} is then derived from the biometric data and is called the cancelable biometric template. This template is used to lock (i.e., commit) the encoded key θ_{ps} following bit-wise XOR operation of C_{T_i} and θ_{ps}, which produces helper data $H = C_{T_i} \oplus \theta_{ps}$. In the system, only H and the hash of key $(h(K_r))$ are stored, and H may be declared as public. This phase is called enrollment. By contrast, in the authentication phase, a genuine user provides his/her biometric data and transformation parameters to produce a query biometric template C'_{T_i}. The query template is then XORed with the helper data H to unlock θ_{ps}, that is, $\theta'_{ps} = H \oplus C'_{T_i} = C_{T_i} \oplus \theta_{ps} \oplus C'_{T_i}$. If the Hamming distance between the enrolled template and the query template is e, then $\theta'_{ps} = \theta_{ps} \oplus e$. The error in the query template is propagated to the encoded key, and this error can be corrected by the error correction technique during the decoding process (i.e., $K'_r = \varepsilon_{dec}(\theta'_{ps})$) if the error correction capacity is greater than the error. In other words, in this scheme, the key K_r is decoded exactly with a sufficiently closed biometric template C'_{T_i}. $h(K_r)$ is used to compare the regenerated key K_r' from H with the original key K_r.

III. THE PROPOSED SCHEME

This section presents six procedures to describe our remote multi-server authentication and key agreement scheme using biometrics: 1) server registration, 2) user registration, 3) login, 4) mutual authentication and key agreement, 5) password and biometric template update, and 6) smart card revocation.

- In the registration phase, each server, say S_j, is registered with the registration center RC; then, the users register themselves through the registration center RC.
- In the login phase, any registered user authenticates smart card SC_i by providing his/her identity ID_i, password PW_i and biometric information BIO_i to initiate the protocol.
- In the authentication and key exchange phase, mutual authentication between an authorized registered user U_i and a registered server S_j is performed, and a session key SK_{ij} between U_i and S_j is established between them.
- The proposed scheme also includes a password and biometric template update phase. If a user U_i needs to update their biometric data and password, he/she can login and update the information.
- If the smart card is lost or damaged, a new smart card can be issued by the provided smart card revocation phase in our scheme.

The notations used in this scheme are given in Table 1.

TABLE 1. Notations.

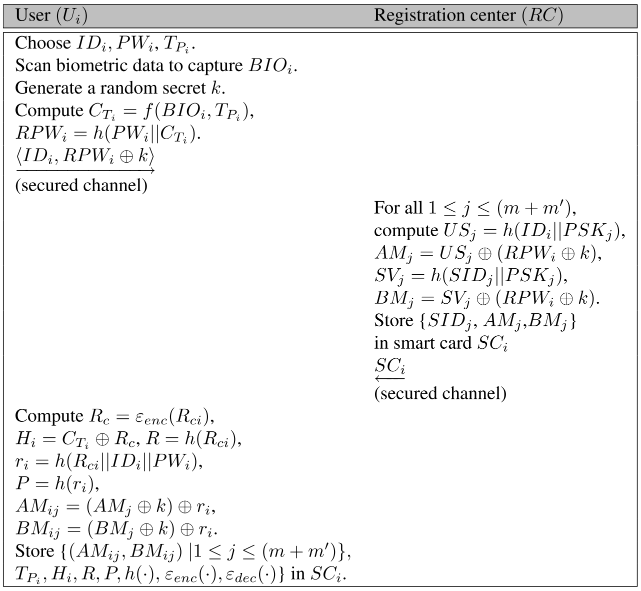
Symbol	Description
U_i	i^{th} user
ID_i	Identity of user U_i
PW_i	Password of user U_i
BIO_i	Biometric data of user U_i
SID_j	Identity of application server S_j
C_{T_i}	Cancelable template of user U_i
T_{P_i}	Transformation parameter for cancelable template generation
$f(\cdot)$	Transformation function
RC	Trusted registration center
X_c	Secret key of RC
R_{ci}	Random number selected by user
H_i	Helper data of fuzzy commitment
$SK_{i,j}$	The common session key between user U_i and server S_j
PSK_j	A secure preshared key among server S_j and RC
$h(\cdot)$	A one-way collision-resistant cryptographic hash function
N_1	Random nonce generated by U_i
N_2	Random nonce generated by S_j
TS_i	Current time stamp generated by U_i
TS_j	Current time stamp generated by S_j
ΔT	Acceptable threshold for transmission delay
$\oplus$	Bitwise exclusive-OR (XOR) operator
$\|\|$	String concatenation operator
$\varepsilon_{enc}(.)$	Encoding operator of the error correction technique
$\varepsilon_{dec}(.)$	Decoding operator of the error correction technique

A. SERVER REGISTRATION PROCEDURE

In the proposed scheme, all the servers S_j, $1 \leq j \leq m$, where m is the total number of available servers in the network initially, are required to register with the trusted registration center RC. For this purpose, each server S_j must dispatch a registration request along with its unique identity SID_j to the RC if it is willing to become an authorized server for providing services to the registered users. Accordingly, the RC sends a secret key $PSK_j = h(SID_j||X_c)$ to each S_j $(1 \leq j \leq m)$ via the Internet Key Exchange Protocol version 2 (IKEv2) [50]. Note that PSK_j is unique for each server S_j and that it is used during the mutual authentication process of a user U_i and a server S_j discussed in Section III-D. Simultaneously, the RC assumes that another m' servers may register themselves with the RC in the near future. Therefore, the RC chooses their identities SID_l and generates the shared keys $PSK_l = h(SID_l||X_c)$ for $m + 1 \leq l \leq m + m'$. The server identities (for $m + m'$ servers) and their corresponding secret keys pairs $\{(SID_j, PSK_j)|1 \leq j \leq m + m'\}$ are stored in the database of the RC. In this way, the registered users do not need to reregister with the RC to gain access to newly registered servers.

B. USER REGISTRATION PROCEDURE

Initially, each user U_i is required to register with the RC through a secure channel. In this phase, U_i needs to choose a user identity ID_i, password PW_i, an application specific transformation parameter T_{P_i} and a random number R_{ci}. U_i also provides his/her biometric data to a biometric sensor, which captures biometric data BIO_i. U_i applies T_{P_i} to generate the cancelable biometric template C_{T_i} from BIO_i using a cancelable transformation function $f(\cdot)$. The user registration procedure is summarized in Figure 1. The detailed steps are described as follows.



User (U_i)	Registration center (RC)
Choose ID_i, PW_i, T_{P_i}. Scan biometric data to capture BIO_i. Generate a random secret k. Compute $C_{T_i} = f(BIO_i, T_{P_i})$, $RPW_i = h(PW_i\|\|C_{T_i})$. $\xrightarrow{\langle ID_i, RPW_i \oplus k\rangle}$ (secured channel)	
	For all $1 \leq j \leq (m + m')$, compute $US_j = h(ID_i\|\|PSK_j)$, $AM_j = US_j \oplus (RPW_i \oplus k)$, $SV_j = h(SID_j\|\|PSK_j)$, $BM_j = SV_j \oplus (RPW_i \oplus k)$. Store $\{SID_j$, AM_j,$BM_j\}$ in smart card SC_i $\xleftarrow{SC_i}$ (secured channel)
Compute $R_c = \varepsilon_{enc}(R_{ci})$, $H_i = C_{T_i} \oplus R_c$, $R = h(R_{ci})$, $r_i = h(R_{ci}\|\|ID_i\|\|PW_i)$, $P = h(r_i)$, $AM_{ij} = (AM_j \oplus k) \oplus r_i$, $BM_{ij} = (BM_j \oplus k) \oplus r_i$. Store $\{(AM_{ij}, BM_{ij})\ \|1 \leq j \leq (m + m')\}$, $T_{P_i}, H_i, R, P, h(\cdot), \varepsilon_{enc}(\cdot), \varepsilon_{dec}(\cdot)\}$ in SC_i.	

FIGURE 1. User registration process.

1) U_i generates the cancelable biometric template $C_{T_i} = f(BIO_i, T_{P_i})$ from his/her biometric data and computes $RPW_i = h(PW_i||C_{T_i})$ and $r_i = h(R_{ci}||ID_i||PW_i)$. U_i then generates a random 160-bit secret k and sends the registration request message $\langle ID_i, RPW_i \oplus k\rangle$ to the RC via a secure channel. The purpose of embedding the random secret k in this step is to protect the privileged-insider attack where a privileged-insider user of the RC can try to derive the secret credentials BIO_i and PW_i using the registration information $\{ID_i, RPW_i \oplus k\}$ (see Section IV-C.4).
2) The RC checks the validity of ID_i and computes $US_j = h(ID_i||PSK_j)$, $AM_j = US_j \oplus (RPW_i \oplus k)$, $SV_j = h(SID_j||PSK_j)$ and $BM_j = SV_j \oplus (RPW_i \oplus k)$ for $1 \leq j \leq (m + m')$. Then, the RC issues a smart card SC_i containing the information $\{(SID_j, AM_j, BM_j)|1 \leq j \leq (m + m')\}$ and sends it to U_i via a secure channel. The RC also stores ID_i in the database of S_j for $1 \leq j \leq (m + m')$.
3) U_i encodes R_{ci} with error correction technique ε and generates a codeword R_c, that is, $R_c = \varepsilon_{enc}(R_{ci})$, computes the helper data $H_i = C_{T_i} \oplus R_c$, $R = h(R_{ci})$ and $P = h(r_i)$. U_i also computes $AM_{ij} = (AM_j \oplus k) \oplus r_i$ and $BM_{ij} = (BM_j \oplus k) \oplus r_i$ for $1 \leq j \leq (m + m')$. U_i then stores $\{(AM_{ij}, BM_{ij})|1 \leq j \leq (m + m')\}$, $T_{P_i}, H_i, R, P, h(\cdot), \varepsilon_{enc}(\cdot), \varepsilon_{dec}(\cdot)\}$ in the received smart card SC_i. U_i discards $R_{ci}, BIO_i, C_{T_i}, r_i, AM_j$ and BM_j for security purposes.

C. LOGIN PROCEDURE

In this phase, a registered user U_i inserts the smart card SC_i into the card reader of a specific terminal, and provides his/her identity ID_i and password PW_i. U_i also scans his/her biometrics at the biometric sensor for authentication. The detailed steps are given below.

1) U_i scans his/her biometrics, e.g., fingerprint, and extracts feature BIO_i' from the captured fingerprint image.
2) U_i inserts the smart card into the card reader and enters the credentials ID_i, PW_i and BIO_i' for authentication.
3) The smart card SC_i generates the cancelable fingerprint $C'_{T_i} = f(BIO_i', T_{P_i})$, extracts $R_c' = H_i \oplus C'_{T_i}$ and decodes R_c' using error correction, that is, $R'_{ci} = \varepsilon_{dec}(R_c')$. SC_i then compares the computed $h(R'_{ci})$ with the stored R. If they are not equal, the session is terminated.
4) SC_i computes $r_i' = h(R_{ci}||ID_i||PW_i)$ and checks whether $h(r_i') = h(r_i)$. If it does not, SC_i terminates the session immediately.
5) SC_i computes $US_j = AM_{ij} \oplus h(PW_i||C_{T_i}) \oplus r_i' = h(ID_i||PSK_j)$ and $SV_j = BM_{ij} \oplus h(PW_i||C_{T_i}) \oplus r_i' = h(SID_j||PSK_j)$. SC_i then selects a random nonce N_1, generates current time stamp TS_i, and computes $M_1 = h(ID_i||US_j)$, $M_2 = ID_i \oplus h(SV_j||TS_i)$, $M_3 = M_1 \oplus N_1$, $M_4 = h(ID_i||M_1||M_2||TS_i||N_1)$.
6) Finally, SC_i publicly sends the login request message $\langle M_2, M_3, M_4, TS_i\rangle$ to the application server S_j.

D. MUTUAL AUTHENTICATION AND KEY AGREEMENT PROCEDURE

After the successful login of a registered user U_i, the authentication of an application server S_j is verified. After successful mutual authentication, the session key is established between U_i and S_j. The login & mutual authentication and key agreement procedures are briefly described in Figure 2. The detailed steps are given below.

1) S_j receives the login request $\langle M_2, M_3, M_4, TS_i\rangle$ at time TS_i' and computes the time delay, $|TS_i' - TS_i|$, in the message transmission. If $|TS_i' - TS_i| < \Delta T$ holds, S_j computes $M_5 = M_2 \oplus h(h(SID_j||PSK_j)||TS_i)$, $M_6 = h(M_5||h(M_5||PSK_j))$, $M_7 = M_3 \oplus M_6 = N_1$ and

User (U_i)/Smart Card (SC_i)	Server (S_j)
Scan biometrics, e.g., fingerprint. Extract feature BIO_i' from biometrics. Input ID_i, PW_i and BIO_i'. Calculate $C'_{T_i} = f(BIO_i', T_{P_i})$, $R_c' = H_i \oplus C'_{T_i}$, $R'_{ci} = \varepsilon_{dec}(R_c')$. Check whether $h(R'_{ci}) = R$? If not, terminate the session. Calculate $r_i' = h(R_{ci}\ \|\|ID_i\ \|\|PW_i)$. Check whether $h(r_i') = h(r_i)$? If so, compute $US_j = AM_{ij} \oplus h(PW_i\|\|$ $C_{T_i}) \oplus r_i' = h(ID_i\ \|\|PSK_j)$, $SV_j = BM_{ij} \oplus h(PW_i\ \|\|C_{T_i}) \oplus r_i'$ $= h(SID_j\ \|\|PSK_j)$. Generate random nonce N_1 and current time stamp TS_i. Calculate $M_1 = h(ID_i\ \|\|US_j)$, $M_2 = ID_i \oplus h(SV_j\ \|\|TS_i)$, $M_3 = M_1 \oplus N_1$, $M_4 = h(ID_i\ \|\|M_1\ \|\|M_2\ \|\|TS_i\ \|\|N_1)$. $\xrightarrow{\langle M_2, M_3, M_4, TS_i\rangle}$ (public channel)	
	Check validity of $\|TS_i' - TS_i\| < \Delta T$. If not, terminate the session. Calculate $M_5 = M_2 \oplus h(h(SID_j\|\|PSK_j)\|\|TS_i)$. If M_5 $(= ID_i)$ exists in its database, compute the following: $M_6 = h(M_5\|\|h(M_5\|\|PSK_j))$, $M_7 = M_3 \oplus M_6 = N_1$, $M_8 = h(M_5\|\|M_6\|\|M_2\|\|TS_i\|\|M_7)$. If $M_8 \neq M_4$, terminate the session. Generate N_2 and TS_j. Compute $M_9 = h(h(M_5\|\|PSK_j)\|\|N_1) \oplus N_2$, $SK_{ij} = h(M_5\|\|h(SID_j\|\|PSK_j)$ $\|\|N_1\|\|N_2\|\|TS_i\|\|TS_j)$, $M_{10} = h(h(M_5\|\|PSK_j)$ $\|\|SK_{ij}\|\|TS_j\|\|N_2)$. $\xleftarrow{\langle M_9, M_{10}, TS_j\rangle}$ (via public channel)
If $\|TS^*_{ij} - TS_j\| < \Delta T$, compute $N_2' = M_9 \oplus h(US_j\|\|N_1)$, $SK'_{ij} = h(ID_i\|\|SV_j\|\|N_1$ $\|\|N_2'\|\|TS_i\|\|TS_j)$, $M_{11} = h(US_j\|\|SK'_{ij}\|\|TS_j\|\|N_2')$. If $M_{11} \neq M_{10}$, terminate the session.	
Store $SK'_{ij}(= SK_{ij})$ for secure communication with S_j.	Store $SK_{ij}(= SK'_{ij})$ for secure communication with U_i.

FIGURE 2. Mutual authentication and key agreement process.

$M_8 = h(M_5||M_6||M_2||TS_i||M_7)$. If $M_8 \neq M_4$, S_j rejects the login request and terminates the session.

2) S_j then randomly selects a nonce N_2, generates current time stamp TS_j, and computes $M_9 = h(h(M_5||PSK_j)||N_1) \oplus N_2$, the session key $SK_{ij} = h(M_5||h(SID_j||PSK_j)||N_1||N_2||TS_i||TS_j)$ shared with U_i and $M_{10} = h(h(M_5||PSK_j)||SK_{ij}||TS_j||N_2)$. Then, S_j publicly sends the authentication request message $\langle M_9, M_{10}, TS_j\rangle$ to U_i.

3) The SC_i of U_i receives the authentication request message $\langle M_9, M_{10}, TS_j\rangle$ at time TS_j^*. SC_i computes the transmission delay, $|TS_j^* - TS_j|$, and if $|TS_j^* - TS_j| < \Delta T$ does not hold, the session is terminated. SC_i also computes $N_2' = M_9 \oplus h(US_j||N_1)$, the session key $SK_{ij}' = h(ID_i||SV_j||N_1||N_2'||TS_i||TS_j)$ shared with S_j and $M_{11} = h(US_j||SK_{ij}'||TS_j||N_2')$. SC_i then verifies the condition $M_{11} = M_{10}$. If the condition does not hold, the authentication is terminated by SC_i. Otherwise, the session key SK_{ij} is established for secure message communication between U_i and S_j.

E. PASSWORD AND BIOMETRIC TEMPLATE UPDATE PROCEDURE

In this section, we describe the password change and biometric template update procedures for a legal registered user U_i. To update the current password and biometric template, U_i needs to login successfully to the system. In these procedures, there is no involvement of the registration center RC, and the entire process is executed locally without involving the RC. The process is summarized in Figure 3. The detailed steps are described below.

1) U_i inputs the credentials ID_i, PW_i, and BIO_i after inserting his/her SC_i into a card reader to login to the system. The extracted feature BIO_i' from the captured BIO_i is computed. SC_i then computes $C_{T_i}' = f(BIO_i', T_{P_i})$ and $R_{ci}' = \varepsilon_{dec}(H_i \oplus C_{T_i}')$. If $h(R_{ci}') = R$, SC_i further computes $r_i' = h(R_{ci}'||ID_i||PW_i)$. If $h(r_i') = P$, SC_i then asks user U_i to change their password and biometric template.

2) For a password change, SC_i asks U_i for a new password. U_i inputs the new password PW_i^{new}. Then, SC_i computes $r_i^{new} = h(R_{ci}'||ID_i||PW_i^{new})$, $AM_{ij}^{new} = AM_{ij} \oplus r_i' \oplus r_i^{new} = h(ID_i||PSK_j) \oplus h(PW_i^{new}||C_{T_i}) \oplus h(R_{ci}'||ID_i||PW_i^{new})$, $BM_{ij}^{new} = BM_{ij} \oplus r_i' \oplus r_i^{new} = h(SID_j||PSK_j) \oplus h(PW_i^{new}||C_{T_i}) \oplus h(R_{ci}'||ID_i||PW_i^{new})$ for $1 \leq j \leq (m + m')\}$ and $P^{new} = h(r_i^{new})$. SC_i updates its parameters $\{AM_{ij}, BM_{ij}, P\}$ with the newly computed values $\{AM_{ij}^{new}, BM_{ij}^{new}, P^{new}\}$ in its memory.

3) For a biometric template update, SC_i asks U_i for a new transformation parameter. It is worth noting that the user U_i's biometric does not change over time and hence, U_i may not opt to update his/her biometric template. In this case, SC_i keeps the old biometric transformation parameter, that is, the new transformation parameter is set as $T_{P_i}^{new} = T_{P_i}$. Otherwise, U_i chooses $T_{P_i}^{new}$ as the new transformation parameter. Subsequently, the new cancelable template is generated as $C_{T_i}^{new} = f(BIO_i', T_{P_i}^{new})$. SC_i also computes $RPW_i^{new} = h(PW_i||C_{T_i}^{new})$, $AM_{ij}^{new} = AM_{ij} \oplus RPW_i \oplus RPW_i^{new} = h(ID_i||PSK_j) \oplus h(PW_i||C_{T_i}^{new}) \oplus r_i'$, $BM_{ij}^{new} = BM_{ij} \oplus RPW_i \oplus RPW_i^{new} = h(SID_j||PSK_j) \oplus h(PW_i||C_{T_i}^{new}) \oplus r_i'$, and the new helper data $H_i^{new} = C_{T_i}^{new} \oplus \varepsilon_{enc}(R_{ci}')$. Accordingly, the information $\{AM_{ij}, BM_{ij}, H_i\}$ is replaced by $\{AM_{ij}^{new}, BM_{ij}^{new}, H_i^{new}\}$ in the memory of SC_i.

User (U_i)	Smart card (SC_i)
Insert SC_i. Input ID_i, PW_i. Imprint BIO_i. $\xrightarrow{\langle ID_i, PW_i, BIO_i\rangle}$	
	Compute $C_{T_i}' = f(BIO_i, T_{P_i})$, $R_{ci}' = \varepsilon_{dec}(H_i \oplus C_{T_i}')$. If $h(R_{ci}') = R$, compute $r_i' = h(R_{ci}'\|\|ID_i\|\|PW_i)$. If $h(r_i') = P$, login is successful. Ask U_i to provide a new password and biometric data.
Password change	
Select new password PW_i^{new} $\xrightarrow{\langle PW_i^{new}\rangle}$	
	Compute $r_i^{new} = h(R_{ci}'\|\|ID_i\|\|PW_i^{new})$, $AM_{ij}^{new} = AM_{ij} \oplus r_i' \oplus r_i^{new}$, $BM_{ij}^{new} = BM_{ij} \oplus r_i' \oplus r_i^{new}$, $P^{new} = h(r_i^{new})$. Update $AM_{ij} \leftarrow AM_{ij}^{new}$, $BM_{ij} \leftarrow BM_{ij}^{new}$ for $1 \leq j \leq (m + m')$, $P \leftarrow P^{new}$.
Biometric template update	
	Choose new transformation parameter $T_{P_i}^{new}$. Compute $C_{T_i}^{new} = f(BIO_i', T_{P_i}^{new})$, $RPW_i^{new} = h(PW_i\|\|C_{T_i}^{new})$, $AM_{ij}^{new} = AM_{ij} \oplus RPW_i \oplus RPW_i^{new}$, $BM_{ij}^{new} = BM_{ij} \oplus RPW_i \oplus RPW_i^{new}$, $H_i^{new} = C_{T_i}^{new} \oplus \varepsilon_{enc}(R_{ci}')$. Update $AM_{ij} \leftarrow AM_{ij}^{new}$, $BM_{ij} \leftarrow BM_{ij}^{new}$, $H_i \leftarrow H_i^{new}$.

FIGURE 3. Password and biometric template update process.

F. SMART CARD REVOCATION PROCEDURE

If the smart card of a legal user U_i is lost, damaged or stolen, U_i can issue a new smart card SC_i from the RC. U_i needs to enter ID_i and PW_i and to imprint BIO_i. The following steps are essential to complete this procedure.

1) U_i computes $C_{T_i}' = f(BIO_i, T_{P_i})$ and $RPW_i = h(PW_i||C_{T_i}')$, generates a random 160-bit secret k', computes $RPW_i' = RPW_i \oplus k'$, and transmits the request message $\langle ID_i, RPW_i'\rangle$ to the RC via a secure channel for a new smart card SC_i^{new}.

2) The RC computes $AM_j = h(ID_i||PSK_j) \oplus RPW_i'$, $BM_j = h(SID_j||PSK_j) \oplus RPW_i'$ for $j = 1, 2, \ldots, (m + m')$ and issues a new smart card SC_i^{new} containing the credentials $\{(SID_j, AM_j, BM_j)|1 \leq j \leq m + m'\}$. SC_i^{new} is then sent to U_i via a secure channel.

3) U_i chooses a new random number R_{ci}^{new} and computes $r_i = h(R_{ci}^{new}||ID_i||PW_i)$, $H_i^{new} = C'_{T_i} \oplus \varepsilon_{enc}(R_{ci}^{new})$, $AM_{ij} = (AM_j \oplus k') \oplus r_i, BM_{ij} = (BM_j \oplus k') \oplus r_i, R = h(R_{ci}^{new})$, $P = h(r_i)$ and stores these values in SC_i^{new}'s memory. U_i also stores $\{T_{P_i}, \varepsilon_{enc}(\cdot), \varepsilon_{dec}(\cdot), h(\cdot)\}$ in SC_i^{new}'s memory.

The smart card revocation procedure is summarized in Figure 4.

User (U_i)	Registration center (RC)
Input ID_i, PW_i, T_{P_i}. Compute $C'_{T_i} = f(BIO_i, T_{P_i})$, $RPW_i = h(PW_i \,\|\|C'_{T_i})$, Generate a random secret k'. Compute $RPW'_i = RPW_i \oplus k'$. $\xrightarrow{\langle ID_i, RPW'_i \rangle}$ (secured channel)	
	For all $1 \leq j \leq (m + m')$, compute $AM_j = h(ID_i \,\|\|PSK_j) \oplus RPW'_i$, $BM_j = h(SID_j \,\|\|PSK_j) \oplus RPW'_i$. Store $\{(SID_j, AM_j, BM_j) \mid 1 \leq j \leq m + m'\}$ in new smart card SC_i^{new}. $\xleftarrow{SC_i^{new}}$ (secured channel)
Choose new random number R_{ci}^{new}. Compute $r_i = h(R_{ci}^{new} \,\|\|ID_i \,\|\|PW_i)$, $H_i^{new} = C'_{T_i} \oplus \varepsilon_{enc}(R_{ci}^{new})$, $AM_{ij} = (AM_j \oplus k') \oplus r_i$, $BM_{ij} = (BM_j \oplus k') \oplus r_i$, $R = h(R_{ci}^{new})$, $P = h(r_i)$. Store these values in smart card's memory. Also, store $\{T_{P_i}, \varepsilon_{enc}(\cdot), \varepsilon_{dec}(\cdot)$, $h(\cdot)\}$ in smart card's memory.	

FIGURE 4. Smart card revocation process.

IV. SECURITY ANALYSIS

In this section, we evaluate the proposed scheme from the security analysis perspective using all possible analyses, namely, formal security under the broadly accepted Real-Or-Random (ROR) model [40], [51], mutual authentication proof using the widely used Burrows-Abadi-Needham (BAN) logic [52] and informal (non-mathematical) security analysis.

A. FORMAL SECURITY USING THE ROR MODEL

The purpose of the formal security analysis of the proposed scheme using the ROR model [40], [51] is to prove that it provides session key (SK) security against a passive/active adversary, say $\mathcal{A}$. Recently, the ROR-model-based formal security analysis has gained popularity and has been applied in various authentication key exchange protocols [37], [53]–[59]. To proceed with the formal security, we first briefly discuss the ROR model and then provide the main proof in Theorem 1.

1) ROR MODEL

There are two participants in the proposed scheme, namely, a user U_i and a server S_j, during the mutual authentication and key agreement procedure. The principal components related to the ROR model for the proposed scheme are discussed below.

a: PARTICIPANTS

$\mathcal{I}_{U_i}^u$ and $\mathcal{I}_{S_j}^s$ are denoted as the instances u and s of U_i and S_j, respectively. These are also called the *oracles*.

b: ACCEPTED STATE

Let an instance $\mathcal{I}^t$ be in an accept state after receiving the final message. Then, we call $\mathcal{I}^t$ the accepted state. If we arrange all the communication messages, including the messages sent and received by $\mathcal{I}^t$, in order, these messages form the session identification (sid) for $\mathcal{I}^t$ for the current session.

c: PARTNERING

The instances $\mathcal{I}^u$ and $\mathcal{I}^s$ are called partners if the following three conditions are concurrently satisfied: 1) they are in an accepted state, 2) they mutually authenticate among each other and share the same sid, and 3) they are mutual partners of each other.

d: FRESHNESS

If the session key SK_{ij} established between U_i and S_j is not leaked via the reveal oracle *Reveal* defined below, we call $\mathcal{I}_{U_i}^u$ or $\mathcal{I}_{S_j}^s$ fresh.

e: ADVERSARY

Under the ROR model, an adversary is modeled using the broadly accepted Dolev-Yao (DY) threat model, as defined in our threat model in Section I-A. According to the DY model, $\mathcal{A}$ can intercept, modify, delete, or even inject some or all messages exchanged between the communicating participants U_i and S_j with the help of the following queries:

Execute$(\mathcal{I}^u, \mathcal{I}^s)$: This query implements an eavesdropping attack that allows $\mathcal{A}$ to read the messages exchanged between U_i and S_j.

Send$(\mathcal{I}^t, M)$: This query implements an active attack wherein $\mathcal{A}$ can send a message M to a participant instance $\mathcal{I}^t$, and in reply, it receives a response from $\mathcal{I}^t$.

Reveal$(\mathcal{I}^t)$: Using this query, $\mathcal{A}$ can know the session key SK_{ij} established between $\mathcal{I}^t$ and its partner in the current session.

CorruptSmartCard$(\mathcal{I}_{U_i}^u)$: This query is modeled as an active attack, wherein $\mathcal{A}$ can extract all the sensitive secret information stored in its memory via power analysis attacks [8], [9].

Test$(\mathcal{I}^t)$: In this query, an unbiased coin c is flipped before the game is started, and its output is used as a decider. Let $\mathcal{A}$ execute this query. If the session key SK_{ij} shared between U_i and S_j is fresh, $\mathcal{I}^t$ returns SK_{ij} when $c = 1$ or a random number when $c = 0$. Otherwise, a null value ($\perp$) is returned.

In this formal security analysis, we restrict $\mathcal{A}$ to permit a limited number of *CorruptSmartCard*$(\mathcal{I}_{U_i}^u)$ queries. However, $\mathcal{A}$ is permitted to execute an unlimited number of *Test*$(\mathcal{I}^t)$ queries.

f: SEMANTIC SECURITY

Under the semantic security, it is required that $\mathcal{A}$ cannot distinguish the real session key SK_{ij} from a random number. The output of $Test(\mathcal{I}^t)$ is checked for consistency verification against a random bit c. Let $\mathcal{A}$'s guessed bit be c' and let $Succ$ be the winning probability in the game. Then, a polynomial time t adversary $\mathcal{A}$'s advantage in breaking the session key (SK) security of the proposed scheme, say $\mathcal{P}$, is defined as $Adv_{\mathcal{P}}^{\mathcal{A}}(t) = |2.Pr[Succ] - 1| = |2.Pr[c' = c] - 1|$, where $Pr[X]$ denotes the probability of an event X.

g: RANDOM ORACLE

In our scheme, we use the one-way cryptographic hash function $h(\cdot)$ that is accessible by all the participants, including the adversary $\mathcal{A}$. We model $h(\cdot)$ as a random oracle, say $\mathcal{H}$.

2) SECURITY PROOF

The SK security of the proposed scheme under the ROR model is provided in Theorem 1.

Theorem 1: Let $Adv_{\mathcal{P}}^{\mathcal{A}}(t)$ be polynomial-time t-adversary $\mathcal{A}$'s advantage function in breaking the SK security of the proposed scheme $\mathcal{P}$. Then,

$$Adv_{\mathcal{P}}^{\mathcal{A}}(t) \leq \frac{q_h^2}{|Hash|} + \frac{q_s}{2^{l-1}.|D|},$$

where q_h, q_s, l, $|Hash|$ and $|D|$ are the number of $\mathcal{H}$ queries, the number of $Send$ queries, the number of bits in the biometric key, the range space of the hash function $h(\cdot)$ and the size of a uniformly distributed password dictionary D, respectively.

Proof: The formal security proof followed in this theorem is similar to that presented in [37], [53], and [57]–[59].

We require the following four games, $Gm_j (j = 0, 1, 2, 3)$, in this proof. We denote $Succ_{Gm_j}^{\mathcal{A}}$ as an event in which the adversary $\mathcal{A}$ can win the game Gm_j. Additionally, $\mathcal{A}$'s advantage in winning Gm_j is denoted and defined by $Adv_{Gm_j}^{\mathcal{A}} = Pr[Succ_{Gm_j}^{\mathcal{A}}]$.

- *Game Gm_0:* In the initial game Gm_0, bit c is first selected by a polynomial-time t adversary $\mathcal{A}$. Since the Gm_0 and the actual protocol in the ROR are basically identical, it follows that
$$Adv_{\mathcal{P}}^{\mathcal{A}}(t) = |2.Adv_{Gm_0}^{\mathcal{A}} - 1|. \quad (1)$$
- *Game Gm_1:* The eavesdropping attack is implemented in the game, wherein $\mathcal{A}$ calls the $Execute$ query. Then, $\mathcal{A}$ calls the $Test$ query after the game is completed. Note that the output of the $Test$ query acts as a decider to distinguish a real session key SK_{ij} between U_i and S_j from a random number in a session. The session key formation is as follows. S_j computes the session key $SK_{ij} = h(M_5||h(SID_j||PSK_j)||N_1||N_2||TS_i||TS_j)$ shared with U_i, and the same session key computed by U_i is shared with S_j as $SK'_{ij} = h(ID_i||SV_j||N_1||N'_2||TS_i||TS_j)(= SK_{ij})$. Suppose $\mathcal{A}$ intercepts messages $Msg_1 = \langle M_2, M_3, M_4, TS_i\rangle$ and $Msg_2 = \langle M_9, M_{10}, TS_j\rangle$. The session key computation by $\mathcal{A}$ needs the long-term secrets ID_i, SID_j and PSK_j and also the short-term secrets N_1 and N_2. Without these secret credentials, the chance of winning game Gm_1 by intercepting messages Msg_1 and Msg_2 is not increased. Since both games Gm_0 and Gm_1 are essentially indistinguishable, we have the following:
$$Adv_{Gm_1}^{\mathcal{A}} = Adv_{Gm_0}^{\mathcal{A}}. \quad (2)$$
- *Game Gm_2:* The $Send$ and $\mathcal{H}$ queries are simulated in this game. This game is modeled as an active attack, wherein by intercepting the messages $Msg_1 = \langle M_2, M_3, M_4, TS_i\rangle$ and $Msg_2 = \langle M_9, M_{10}, TS_j\rangle$, $\mathcal{A}$ tries to compute the session key SK_{ij} between U_i and S_j. Both messages Msg_1 and Msg_2 involve the random nonces N_1 and N_2 and also the current time stamps TS_i and TS_j. Hence, there is no collision in hash outputs when $\mathcal{A}$ makes $\mathcal{H}$ queries on these intercepted messages (see Definition 1). Thus, the computation of the long-term secrets ID_i, SID_j and PSK_j and the short-term secrets N_1 and N_2 is computationally infeasible due to the collision-resistant property of the one-way cryptographic hash function $h(\cdot)$. Since game Gm_2 is identical to game Gm_1 when the simulation of $Send$ and $\mathcal{H}$ queries is not involved, the results from the birthday paradox give the following result:
$$|Adv_{Gm_2}^{\mathcal{A}} - Adv_{Gm_1}^{\mathcal{A}}| \leq \frac{q_h^2}{2|Hash|}. \quad (3)$$
- *Game Gm_3:* In this game, the $CorruptSmartCard$ query is simulated. Therefore, $\mathcal{A}$ has the secret credentials $\{(AM_{ij}, BM_{ij})|1 \leq j \leq (m + m')\}$, T_{P_i}, H_i, R, P, $h(\cdot)$, $\varepsilon_{enc}(\cdot)$, $\varepsilon_{dec}(\cdot)\}$ from U_i's smart card SC_i's memory, where $H_i = C_{T_i} \oplus R_c$, $R = h(R_{ci})$, $P = h(r_i)$, $AM_{ij} = US_j \oplus RPW_i \oplus r_i$ and $BM_{ij} = SV_j \oplus RPW_i \oplus r_i$ for $1 \leq j \leq (m+m')$. Without the secret credentials r_i and R_c, it is computationally infeasible to derive the biometric secret key C_{T_i} and the password PW_i of user U_i. Assuming C_{T_i} is l bits, the guessing probability of $C_{T_i} \in \{0, 1\}^l$ by $\mathcal{A}$ is approximately $\frac{1}{2^l}$ [34]. In addition, it is assumed that the system will permit the adversary $\mathcal{A}$ to enter a limited number of wrong passwords. Note that games Gm_2 and Gm_3 are identical when password and biometrics guessing attacks are not involved. Hence, we have the following result:
$$|Adv_{Gm_3}^{\mathcal{A}} - Adv_{Gm_2}^{\mathcal{A}}| \leq \frac{q_s}{2^l.|D|}. \quad (4)$$

Since all the games are executed, $\mathcal{A}$ can only guess the correct bit c. It then follows that

$$Adv_{Gm_3}^{\mathcal{A}} = \frac{1}{2}. \quad (5)$$

Eqs. (1), (2) and (5) give the following result:

$$\begin{aligned} \frac{1}{2}Adv_{\mathcal{P}}^{\mathcal{A}}(t) &= |Adv_{Gm_0}^{\mathcal{A}} - \frac{1}{2}| \\ &= |Adv_{Gm_1}^{\mathcal{A}} - \frac{1}{2}| \\ &= |Adv_{Gm_1}^{\mathcal{A}} - Adv_{Gm_3}^{\mathcal{A}}|. \quad (6) \end{aligned}$$

The following result is obtained via the triangular inequality:

$$\begin{aligned}|Adv_{Gm_1}^{A} - Adv_{Gm_3}^{A}| &\leq |Adv_{Gm_1}^{A} - Adv_{Gm_2}^{A}| \\ &\quad + |Adv_{Gm_2}^{A} - Adv_{Gm_3}^{A}| \\ &\leq \frac{q_h^2}{2|Hash|} + \frac{q_s}{2^l.|D|}. \end{aligned} \tag{7}$$

Eqs. (6) and (7) lead to the following result:

$$\frac{1}{2}Adv_{\mathcal{P}}^{A}(t) \leq \frac{q_h^2}{2|Hash|} + \frac{q_s}{2^l.|D|}. \tag{8}$$

Finally, multiplying both sides of Eq. (8) by a factor of 2 and simplifying the terms, we obtain the required result:

$$Adv_{\mathcal{P}}^{A}(t) \leq \frac{q_h^2}{|Hash|} + \frac{q_s}{2^{l-1}.|D|}.$$

B. MUTUAL AUTHENTICATION USING BAN LOGIC

We apply the widely accepted Burrows-Abadi-Needham (BAN) logic [52] to prove the mutual authentication between a legal registered user U_i and a registered server S_j for the proposed scheme in Theorem 2. The BAN logic has been widely used to provide mutual authentication of the authentication and session key agreement protocols [29], [34], [36], [60].

TABLE 2. Notations and their meanings in the BAN logic.

Notation	Meaning
$A\mid\equiv X$	A believes or is entitled to believe a statement X
$A \overset{K}{\leftrightarrow} B$	K is a shared key between A and B
$\sharp X$	X is considered as fresh
$A \lhd X$	A sees statement X
$A \mid\sim X$	A once said statement X
$A \Rightarrow X$	A has jurisdiction over statement X
$\{X, Y\}_K$	X and Y are encrypted with key K
$(X, Y)_K$	X and Y are hashed with key K
$\langle X \rangle_K$	X is combined with key K

The notation used in the BAN logic is given in Table 2. The main rules of BAN logic are given below:

Rule-1: $\frac{A|\equiv A \overset{K}{\leftrightarrow} B, A\lhd\{X\}}{A|\equiv B|\sim X}$ and $\frac{A|\equiv A \overset{K}{\leftrightarrow} B, A\lhd\langle X\rangle}{A|\equiv B|\sim X}$

Rule-2: $\frac{A|\equiv\sharp(X), A|\equiv B|\sim X}{A|\equiv B|\equiv X}$

Rule-3: $\frac{A|\equiv B\Rightarrow X, A|\equiv B|\equiv X}{A|\equiv X}$

Rule-4: $\frac{A|\equiv\sharp(X)}{A|\equiv\sharp(X,Y)}$

Rule-5: $\frac{A|\equiv(X), A|\equiv(Y)}{A|\equiv(X,Y)}$

Rule-6: $\frac{A|\equiv\sharp(X), A|\equiv B|\equiv X}{A|\equiv A \overset{K}{\leftrightarrow} B}$

Rule-1, Rule-2, Rule-3, Rule-4, Rule-5 and Rule-6 are known as the message meaning, nonce verification, jurisdiction, freshness-conjuncatenation, belief and session key rules, respectively.

Theorem 2: The proposed scheme achieves secure mutual authentication between a user U_i and a server S_j.

Proof: To prove this theorem, we first list the assumptions related to the proposed scheme.

- **A1**: $U_i| \equiv \sharp(N_1, TS_i)$
- **A2**: $S_j| \equiv \sharp(N_2, TS_j)$
- **A3**: $U_i| \equiv S_j \Rightarrow N_2$
- **A4**: $S_j| \equiv U_i \Rightarrow N_1$
- **A5**: $U_i| \equiv U_i \overset{SV_j}{\leftrightarrow} S_j$
- **A6**: $S_j| \equiv U_i \overset{SV_j}{\leftrightarrow} S_j$
- **A7**: $U_i| \equiv U_i \overset{US_j}{\leftrightarrow} S_j$
- **A8**: $S_j| \equiv U_i \overset{US_j}{\leftrightarrow} S_j$

Goals: We set the following goals:

- G_1: $S_j| \equiv U_i \overset{SK_{ij}}{\leftrightarrow} S_j$
- G_2: $U_i| \equiv U_i \overset{SK_{ij}}{\leftrightarrow} S_j$

Idealized forms of messages: In the proposed scheme, messages $Msg_1 = \langle M_2, M_3, M_4, TS_i\rangle$ and $Msg_2 = \langle M_9, M_{10}, TS_j\rangle$ can be written in their respective idealized forms as follows:

- $Msg_1 : S_j \lhd \langle M_2, M_3, M_4, TS_i\rangle$, that is, $Msg_1 : S_j \lhd \langle ID_i \oplus h(SV_j, TS_i), h(ID_i, US_j) \oplus N_1, N_1, TS_i\rangle_{SV_j}$.
- $Msg_2 : S_j \rightarrow U_i$: $\langle M_9, M_{10}, TS_j\rangle$, that is, $Msg_2 : U_i \lhd \langle h(US_j, N_1) \oplus N_2, SK_{ij}, TS_j, N_2\rangle_{US_j}$.

The main security proof consists of the following steps:

- Consider the message Msg_1, the assumptions **(A1, A6)** and the message meaning rule (**Rule-1**). We obtain
  SS1: $S_j| \equiv U_i \mid\sim N_1$.
- By applying assumption **A1** and the nonce verification rule (**Rule-2**) on **SS1**, we obtain the following:
  SS2: $S_j| \equiv U_i| \equiv N_1$.
  Now, N_1 is a necessary parameter of the session key SK_{ij} in the proposed scheme.
- We then apply the jurisdiction rule (**Rule-3**) and assumption **A4** on **SS2** to obtain:
  SS3: $S_j| \equiv N_1$.
- The server S_j believes that N_2 is fresh (according to assumption **A2**), and it is another necessary parameter of the session key SK_{ij}. Therefore, by applying the session key rule (**Rule-6**), we obtain the following result:
  SS4: $S_j| \equiv U_i \overset{SK_{ij}}{\leftrightarrow} S_j$. **(Goal** G_1**)**
- From message Msg_2, we obtain
  SS5: $U_i \lhd < N_2 >_{US_j}$.
- Considering assumption **A7**, statement **SS5** and **Rule-1**, we obtain
  SS6: $U_i| \equiv S_j \mid\sim N_2$.
- Applying **Rule-2** and assumption **A2** on statement **SS6**, we obtain
  SS7: $U_i| \equiv S_j| \equiv N_2$,
  where N_2 is a necessary parameter for session key SK_{ij}.
- Using assumption **A3**, statement **SS7** and **Rule-3**, we obtain
  SS8: $U_i| \equiv N_2$.
- U_i believes that N_1 is fresh (from **A1**), and the combination of N_1 and N_2 produces an outcome that is also fresh. Therefore, by applying **Rule-6** and assumption **A1** on statement **SS8**, we obtain
  SS9: $U_i| \equiv U_i \overset{SK_{ij}}{\leftrightarrow} S_j$. **(Goal** G_2**)**

It is then clear that both defined goals G_1 and G_2 are fulfilled in the proposed scheme. Hence, the secure mutual authentication between U_i and S_j is maintained in the proposed scheme.

C. INFORMAL SECURITY ANALYSIS AND OTHER DISCUSSIONS

In this section, we first provide the correctness of the proposed scheme in Theorem 3. Then, we discuss the security of our scheme informally (non-mathematical) for other known attacks. In addition, we discuss some important functionality features that are supported in the proposed scheme.

Theorem 3: In the proposed scheme, both user U_i and server S_j establish the same session key during the login and mutual authentication & key agreement phases.

Proof: After receiving the login request message $Msg_1 = \langle M_2, M_3, M_4, TS_i \rangle$ from user U_i, server S_j computes the session key shared with U_i as $SK_{ij} = h(M_5||h(SID_j||PSK_j)||N_1||N_2||TS_i||TS_j)$. During the mutual authentication and key agreement phase, after receiving the authentication request message $\langle M_9, M_{10}, TS_j \rangle$ from S_j, U_i computes the session key shared with the server S_j as $SK'_{ij} = h(ID_i||SV_j||N_1||N'_2||TS_i||TS_j)$. It then suffices to show that $SK_{ij} = SK'_{ij}$. We have $M_5 = M_2 \oplus h(h(SID_j||PSK_j)||TS_i) = ID_i$, $SV_j = BM_{ij} \oplus h(PW_i||C_{T_i}) \oplus r'_i = h(SID_j||PSK_j)$ and $N'_2 = M_9 \oplus h(US_j||N_1) = N_2$. Therefore, $SK_{ij} = h(M_5||h(SID_j||PSK_j)||N_1||N_2||TS_i||TS_j) = h(ID_i||SV_j||N_1||N'_2||TS_i||TS_j) = SK'_{ij}$. Hence, the theorem is proved.

In the following, we show that the proposed scheme is secure against other attacks and that it provides some functionality features.

1) REPLAY ATTACK

Suppose an adversary $\mathcal{A}$ intercepts messages $Msg_1 = \langle M_2, M_3, M_4, TS_i \rangle$ and $Msg_2 = \langle M_9, M_{10}, TS_j \rangle$ during the login and mutual authentication & agreement procedures and then tries to re-send these messages later to gain access to secret credentials. Note that after receiving Msg_1, S_j first checks the condition $|TS'_i - TS_i| < \Delta T$ to validate the freshness of the message. Since TS_i is the current time stamp and is also included in M_2 and M_4, the condition will fail due to the short maximum transmission delay threshold ΔT used in the verification. A similar situation occurs when U_i checks the validity of Msg_2 by the condition $|TS^*_j - TS_j| < \Delta T$ and it will fail again. Therefore, $\mathcal{A}$ will not be successful in launching the replay attack in the proposed scheme.

2) MAN-IN-THE-MIDDLE ATTACK

In a man-in-the-middle attack, an adversary $\mathcal{A}$ may attempt to modify intercepted messages $Msg_1 = \langle M_2, M_3, M_4, TS_i \rangle$ and $Msg_2 = \langle M_9, M_{10}, TS_j \rangle$ during communication. Suppose $\mathcal{A}$ tries to modify message Msg_1 into another valid message, say $Msg'_1 = \langle M'_2, M'_3, M'_4, TS^a_i \rangle$, by generating the current time stamp TS^a_i and random nonce N^a_1. To calculate $M'_1 = h(ID_i||US_j)$, $M'_2 = ID_i \oplus h(SV_j||TS^a_i)$, $M'_3 = M'_1 \oplus N^a_1$, $M'_4 = h(ID_i||M'_1||M'_2||TS^a_i||N^a_1)$, $\mathcal{A}$ requires the secret credentials ID_i, PSK_j and SID_j. Without these secret credentials, it is a computationally infeasible task for $\mathcal{A}$ to modify message Msg_1 into a valid message Msg'_1. Similarly, it is also computationally infeasible for $\mathcal{A}$ to modify message Msg_2 into a valid message. Therefore, the proposed scheme is resilient against this type of attack.

3) STOLEN SMART CARD ATTACK

According to the threat model discussed in Section I-A, an adversary $\mathcal{A}$ can extract all the secret credentials $\{(AM_{ij}, BM_{ij})|1 \le j \le (m+m')\}, T_{P_i}, H_i, R, P, h(\cdot), \varepsilon_{enc}(\cdot), \varepsilon_{dec}(\cdot)\}$ stored in a lost or stolen smart card SC_i of an authorized user U_i via power analysis attacks [8], [9], where $H_i = C_{T_i} \oplus R_c$, $R = h(R_{ci})$, $P = h(r_i)$, $AM_{ij} = US_j \oplus RPW_i \oplus r_i$ and $BM_{ij} = SV_j \oplus RPW_i \oplus r_i$ for $1 \le j \le (m+m')$. However, without the secret credentials r_i and R_c, it is a computationally infeasible task for $\mathcal{A}$ to derive biometric secret key C_{T_i} and password PW_i of U_i. Therefore, the proposed scheme resists stolen smart card attacks. In addition, offline password guessing attacks are also prevented in the proposed scheme.

4) PRIVILEGED-INSIDER ATTACK

An insider user of the trusted RC may act as a privileged-insider attacker, say $\mathcal{A}$. Then, $\mathcal{A}$ can record the registration information $\{ID_i, RPW_i \oplus k\}$ that is submitted to the RC by a registered user U_i, where $C_{T_i} = f(BIO_i, T_{P_i})$ and $RPW_i = h(PW_i||C_{T_i})$. Assume that after the user registration process, $\mathcal{A}$ has the lost or stolen smart card SC_i of U_i and extracts all the credentials stored in SC_i, as stated in Section IV-C.3. However, according to Section IV-C.3, it is computationally infeasible for $\mathcal{A}$ to derive biometric secret key C_{T_i} and password PW_i. Hence, the privileged-insider attack is also prevented by the proposed scheme.

5) IMPERSONATION ATTACKS

In this section, we discuss the following two impersonation attacks related to the proposed scheme.

- *User impersonation attack:* To convince server S_j with the message sent on behalf of a legal user U_i, an adversary $\mathcal{A}$ can generate a random nonce N^*_1 and also current time stamp TS^*_i. Then, $\mathcal{A}$ can attempt to calculate the terms $M_1 = h(ID_i||US_j)$, $M_2 = ID_i \oplus h(SV_j||TS^*_i)$, $M_3 = M_1 \oplus N^*_1$ and $M_4 = h(ID_i||M_1||M_2||TS^*_i||N^*_1)$ to form the login request message $\langle M_2, M_3, M_4, TS^*_i \rangle$, where $US_j = h(ID_i||PSK_j)$ and $SV_j = h(SID_j||PSK_j)$. However, this attempt by $\mathcal{A}$ will not succeed as the secret credentials ID_i, SID_j and PSK_j are unknown to him/her. This indicates that the proposed scheme is resilient against user impersonation attacks.
- *Server impersonation attack:* In this attack, $\mathcal{A}$ tries to convince user U_i with the message sent on behalf of the server S_j. To achieve this goal, $\mathcal{A}$ can generate a random nonce N^*_2 and current time stamp TS^*_j and then attempt to calculate the terms M_9 and M_{10} in the formed

authentication request message $\langle M_9, M_{10}, TS_j^* \rangle$, where $M_9 = h(h(ID_i||PSK_j)||N_1) \oplus N_2^*$, $SK_{ij} = h(ID_i|| h(SID_j||PSK_j)||N_1||N_2^*||TS_i||TS_j^*)$, $M_{10} = h(h(ID_i|| PSK_j)||SK_{ij}||TS_j^*||N_2^*)$ and the random number N_1 and time stamp TS_i are generated by U_i. However, without having the short-term secret N_1 and the long-term secrets ID_i, SID_j and PSK_j, it is computationally infeasible for $\mathcal{A}$ to form a valid message $\langle M_9, M_{10}, TS_j^* \rangle$. Therefore, it is clear that the server impersonation attack is also protected in the proposed scheme.

6) PASSWORD CHANGE ATTACK

In the password and biometric template update phase discussed in Section III-E, the smart card SC_i of an authorized registered user U_i first authenticates U_i based on his/her entered identity ID_i, current password PW_i and biometrics BIO_i by calculating $C'_{T_i} = f(BIO'_i, T_{P_i})$, $R'_{ci} = \varepsilon_{dec}(H_i \oplus C'_{T_i})$ and $r'_i = h(R'_{ci}||ID_i||PW_i)$, and then verifying the conditions $h(R'_{ci}) = R$ and $h(r'_i) = P$. If these conditions are valid, then only SC_i allows U_i to update the current password with a new password. Therefore, without knowing the secret credentials ID_i, PW_i and BIO_i, it is computationally infeasible task for an adversary to update the password of U_i. As a result, the password change attack is protected in the proposed scheme.

7) EPHEMERAL SECRET LEAKAGE (ESL) ATTACK

In the proposed scheme, the session key between a legal registered user U_i and the server S_j is computed as $SK_{ij} = h(M_5||h(SID_j||PSK_j)||N_1||N_2||TS_i||TS_j) = h(ID_i||SV_j||N_1|| N'_2||TS_i||TS_j) = SK'_{ij}$. In the following, we consider two cases.

- *Case 1:* Suppose an adversary $\mathcal{A}$ knows the short-term secrets N_1 and N_2. However, without the long-term secrets ID_i, SID_j and PSK_j, it is computationally infeasible to construct SK_{ij}.
- *Case 2:* Assume $\mathcal{A}$ knows the long-term secrets ID_i, SID_j and PSK_j. Then, without the short-term secrets N_1 and N_2, it is computationally infeasible to construct SK_{ij}.

The above two cases clearly show that $\mathcal{A}$ will be successful in computing SK_{ij} when both the short-term and long-term secrets are available. Thus, the proposed scheme is secure under the CK-adversary model (discussed in the threat model in Section I-A). In addition, we also assume that a particular session key is compromised by $\mathcal{A}$. However, due to both long-term secrets and newly generated random nonces, the session keys created in the previous and future sessions are different. This means that the forward and backward secrecy goals as well as session key security are achieved. Moreover, a session hijacking attack does not help $\mathcal{A}$ to compromise the security of other previous and future sessions. As a consequence, our scheme is secure against ESL attack.

8) ANONYMITY AND UNTRACEABILITY

In our scheme, user identity ID_i is incorporated within the r_i, that is, $r_i = h(R_{ci}||ID_i||PW_i)$, and $P = h(r_i)$ is stored in SC_i. The SC_i of U_i transmits M_2 (i.e., $M_2 = ID_i \oplus h(SV_j||TS_i)$ over the public channel in the message $Msg_1 = \langle M_2, M_3, M_4, TS_i \rangle$. The value of M_2 changes in each session depending on the TS_i, and it is computationally infeasible to extract the actual ID_i from the intercepted M_2 due to the collision-resistant property of the hash function $h(\cdot)$ (see Definition 1). It is also worth noting that the terms M_2, M_3 and M_4 in message $Msg_1 = \langle M_2, M_3, M_4, TS_i \rangle$ and the terms M_9 and M_{10} in message $Msg_2 = \langle M_9, M_{10}, TS_j \rangle$ are dynamic and unique in each session due to the inclusion of the timestamps TS_i and TS_j and the random nonces N_1 and N_2. As a result, an adversary cannot trace the same user over multiple sessions. Therefore, the untraceability property is preserved in the proposed scheme.

9) BIOMETRIC TEMPLATE PROTECTION

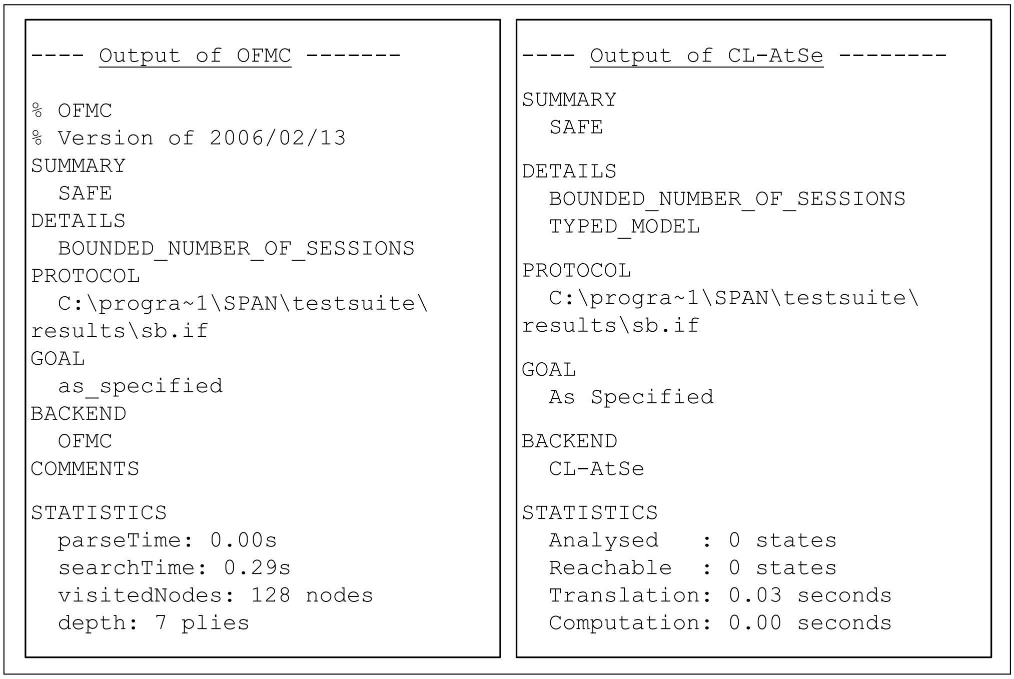
In the proposed scheme, the biometric data are transformed into a cancelable template to prevent the privacy of the biometric data of a legal registered user. Moreover, the template is not stored anywhere without protection. Biometric template extraction from a lost or stolen smart card of a user is computationally infeasible without knowledge of the user-specific random number R_{ci}. Thus, the user biometric template is protected in the proposed scheme.

10) EFFICIENT PASSWORD/BIOMETRIC TEMPLATE UPDATE

During the password/biometric template update procedure of the proposed scheme, to change the current password and biometric template, a legal registered user U_i inputs his/her identity, current password and biometrics into his/her smart card SC_i. If all the entered secret credentials are valid, then U_i is permitted to update the password and biometric template. Then, SC_i updates the password and biometric template in its memory locally without contacting the RC. Thus, the password/biometric template update procedure is efficiently executed.

V. FORMAL SECURITY VERIFICATION USING AVISPA TOOL: A SIMULATION STUDY

The Automated Validation of Internet Security Protocols and Applications (AVISPA) tool [61] is widely used for formal security verification and is applied in many existing key management and authentication protocols [29], [30], [53]–[57], [59], [62]. The security of our scheme is also verified with the AVISPA tool. AVISPA provides four back ends, namely, 1) On-the-fly Model-checker (OFMC), 2) Constraint-Logic-based Attack Searcher (CL-AtSe), 3) SAT-based Model-Checker (SATMC) and 4) Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP). In AVISPA, HLPSL (High Level Protocols Specification Language), a role-based language, is used to specify the target protocol. The roles of all the participants (user, server and registration center) are represented as basic roles, whereas the composition of basic roles is represented as a composition role. The intruder (denoted by i in HLPSL) is modeled using the Dolev-Yao (DY) threat model. In the DY model, a channel is represented by channel(dy). This means that an adversary can intercept, modify, delete or insert



```
---- Output of OFMC -------

% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  C:\progra~1\SPAN\testsuite\
results\sb.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS

STATISTICS
  parseTime: 0.00s
  searchTime: 0.29s
  visitedNodes: 128 nodes
  depth: 7 plies
```

```
---- Output of CL-AtSe --------

SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  C:\progra~1\SPAN\testsuite\
results\sb.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS
  Analysed    : 0 states
  Reachable   : 0 states
  Translation: 0.03 seconds
  Computation: 0.00 seconds
```

FIGURE 5. Analysis of results under the OFMC and CL-AtSe backends.

fake message content during communication over a public channel. An HLPSL program implemented for a security protocol is compiled and converted into an Intermediate Format (IF) with the help of the HLPSL2IF translator. Then, the IF is provided to one of the four back ends, and the corresponding summary of security analysis is produced in an Output Format (OF). The analysis of a protocol indicates safe, unsafe or inconclusive. If the protocol is unsafe, the attack trace is included in the OF. Moreover, the overall statistics of the parse time, search time, translation time and computation time are displayed in the OF. The proposed scheme uses bitwise XOR operations in the protocol implementation. At present, the SATMC and TA4SP back ends do not support implementation of XOR operations; therefore, the output results under these back ends are inconclusive. Hence, we have omitted the simulation results under SATMC and TA4SP, and the results under only the OFMC and CL-AtSe back ends are presented and discussed below.

We have implemented the basic roles for the user U_i, the server S_j and the *RC* for the proposed scheme in HLPSL. Moreover, the mandatory composite roles, such as session and goal & environment, are also implemented. The details of AVISPA, HLPSL and protocol implementation in HLPSL can be found in [61].

The executability check ensures that a security protocol can reach to a state where a possible attack can occur during the run of that protocol. The HLPSL implementation of the proposed scheme is properly translated to HLPSL specification, and it meets the design goals by ensuring the executability. The proposed scheme is executed for the execution test and for a bounded number of sessions of model checking. For replay attack checking, both the OFMC and CL-AtSe back ends check where the authorized agents can execute the specified protocol by performing a search of a passive intruder. In addition, both the OFMC and CL-AtSe back ends also check for the occurrence of a man-in-the-middle attack by intruder i for the DY model checking. The simulation results of the proposed scheme using the OFMC and CL-AtSe back ends are shown in Figure 5. Under the OFMC back end, the search time is 0.29 seconds, the number of visited nodes is 128 and the depth is 7 plies. The CL-AtSe back end takes 0.03 seconds for translation. The results reported in this figure clearly indicate that our scheme protects against replay & man-in-the-middle attacks.

VI. PERFORMANCE COMPARISON

In this section, we conduct a detailed comparative study of the proposed scheme and other related multi-server authentication schemes, namely, the schemes of Chuang and Chen [23], Amin and Biswas [30], Sood *et al.* [24], Mishra *et al.* [27], He and Wang [33], Lu *et al.* [31], and Ali and Pal [63].

A. SECURITY AND FUNCTIONALITY FEATURES COMPARISON

In Table 3, we compare our scheme with other multi-server remote authentication schemes with respect to resilience against various attacks and preservation of various functionality features. It is worth noting that none of the existing schemes are completely free from security attacks. However, our proposed protocol is able to resist various known attacks and also supports more functionality features compared to other schemes.

TABLE 3. Security and functionality features comparison.

Property/Feature	Our	Chuang-Chen [23]	Amin-Biswas [30]	Sood *et al.* [24]	Mishra *et al.* [27]	He-Wang [33]	Lu *et al.* [31]	Ali-Pal [63]
A_1	$\surd$	$\times$	$\surd$	$\surd$	$\times$	$\times$	$\times$	$\times$
A_2	$\surd$	$\surd$	$\surd$	$\times$	$\surd$	$\surd$	$\surd$	$\surd$
A_3	$\surd$	$\surd$	$\times$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$
A_4	$\surd$	$\surd$	$\surd$	$\times$	$\surd$	$\surd$	$\surd$	$\surd$
A_5	$\surd$	$\surd$	$\surd$	$\times$	$\surd$	$\surd$	$\surd$	$\surd$
A_6	$\surd$	$\surd$	$\surd$	$\times$	$\surd$	$\surd$	$\surd$	$\surd$
A_7	$\surd$	$\surd$	$\surd$	$\surd$	$\times$	$\surd$	$\surd$	$\surd$
A_8	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$
A_9	$\surd$	$\surd$	$\times$	$\times$	$\surd$	$\surd$	$\surd$	$\surd$
A_{10}	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\times$	$\times$	$\surd$
A_{11}	$\surd$	$\times$	$\surd$	$\surd$	$\surd$	$\times$	$\surd$	$\surd$
A_{12}	$\surd$	$\surd$	$\times$	$\times$	$\surd$	$\surd$	$\times$	$\times$

A_1: user anonymity and untraceability; A_2: three-factor security; A_3: early error detection; A_4: mutual authentication; A_5: session key exchange; A_6: secure password update; A_7: stolen smart card attack resistance; A_8: offline password guessing attack resistance; A_9: replay attack resistance; A_{10}: forgery attack resistance; A_{11}: no registration center assistance; A_{12}: privileged-insider attack resistance.

$\surd$: a scheme preserves the security property/functionality feature; $\times$: a scheme does not preserve the security property/functionality feature.

TABLE 4. Communication costs comparison.

Scheme	Cost in login phase (in bits)	Cost in authentication phase (in bits)	Total cost (in bits)	Communication mode between entities
Chuang-Chen [23]	512	512	1024	$U_i \rightarrow S_j, S_j \rightarrow U_i$
Amin-Biswas [30]	768	1152	1920	$U_i \rightarrow MS, MS \rightarrow PS, PS \rightarrow U_i$
Sood *et al.* [24]	896	1216	2112	$U_i \rightarrow S_j, S_j \rightarrow CS, CS \rightarrow S_j, S_j \rightarrow U_i, U_i \rightarrow S_j$
Mishra *et al.* [27]	640	640	1280	$U_i \rightarrow S_j, S_j \rightarrow U_i, U_i \rightarrow S_j$
He-Wang [33]	640	2880	3520	$U_i \rightarrow S_j, S_j \rightarrow RC, RC \rightarrow S_j, S_j \rightarrow U_i, U_i \rightarrow S_j$
Lu *et al.* [31]	672	554	1226	$U_i \rightarrow S_j, S_j \rightarrow U_i, U_i \rightarrow S_j$
Ali-Pal [63]	1344	320	1664	$U_i \rightarrow S_j, S_j \rightarrow U_i$
Our	512	352	864	$U_i \rightarrow S_j, S_j \rightarrow U_i$

Note: U_i: i^{th} user; S_j: j^{th} server; MS: medical server; PS: physician server; CS: control server; RC: registration center.

TABLE 5. Computation costs comparison.

Scheme	Login phase	Authentication phase	Total cost	Rough estimation (in milliseconds)
Chuang-Chen [23]	$4C_h$	$13C_h$	$17C_h$	0.0391
Amin-Biswas [30]	$C_{bh} + 4C_h$	$14C_h$	$C_{bh} + 18C_h$	2.2674
Sood *et al.* [24]	$7C_h$	$24C_h$	$31C_h$	0.0713
Mishra *et al.* [27]	$6C_h$	$12C_h$	$18C_h$	0.0414
He-Wang [33]	$3C_h + 2C_{ecm}$	$18C_h + 6C_{ecm}$	$21C_h + 8C_{ecm}$	17.856
Lu *et al.* [31]	$C_{bh} + 4C_h$	$11C_h$	$C_{bh} + 15C_h$	2.2605
Ali-Pal [63]	$6C_h + C_{asym} + C_{bh}$	$7C_h + C_{asym}$	$13C_h + C_{bh} + 2C_{asym}$	2.2651
Our	$C_{fcs} + 6C_h$	$11C_h$	$C_{fcs} + 17C_h$	2.2651

B. COMMUNICATION COSTS COMPARISON

We compare our scheme with related existing schemes in terms of communication costs in Table 4. The communication cost is computed with respect to the requirement of the number of bits for the transmission of various messages among entities during the login and authentication phases. In this table, the third column (communication mode) represents message communication between various entities in the network. We assume that the bit lengths of user identity, server identity, hash output (message digest) (if we apply SHA-1 as the one-way hash function [64]), time stamp and an elliptic curve point $P = (P_x, P_y)$ are 160, 160, 160, 32 and $(160 + 160) = 320$ bits, respectively, where P_x and P_y denote the x and y coordinates of point P, respectively. Moreover, it is also assumed that the security level of a 1024-bit RSA public key cryptosystem [65] is equivalent to that for 160-bit ECC (elliptic curve cryptography) [66].

In our scheme, the communication cost required for the login request message $\langle M_2, M_3, M_4, TS_i\rangle$ transmitted from a user U_i to a server S_j is $(160+160+160+32) = 512$ bits and that for the authentication request message $\langle M_9, M_{10}, TS_j\rangle$ transmitted to user U_i from server S_j is $(160+160+32) = 352$ bits. Thus, the total communication cost for our scheme is $(512 + 352) = 864$ bits. On the other hand, the communication costs for the schemes of Chuang and Chen [23], Amin and Biswas [30], Sood *et al.* [24], Mishra *et al.* [27], He and Wang [33], Lu *et al.* [31], and Ali and Pal [63] are 1024, 1920, 2112, 1280, 3520, 1226 and 1664 bits, respectively. It is worth noting that the communication overhead of our scheme is lower than that for all the other existing schemes.

C. COMPUTATION COSTS COMPARISON

Finally, we compare our scheme with the existing multi-server schemes with respect to the computation cost of login and authentication phases. The comparison results are shown in Table 5. The following notation is used to represent the computation cost:

- C_h: cost for executing a one-way cryptographic hash function
- C_{bh}: execution cost for bio-hashing function
- C_{fe}: cost for executing a fuzzy extractor function
- C_{fcs}: cost for executing a fuzzy commitment scheme
- C_{ecm}: cost for executing an elliptic curve point multiplication
- C_{asym}: cost for executing an asymmetric (public key) encryption/decryption

Based on the experimental results reported in [34] and [36], we have $C_h \approx 0.0023$ ms, $C_{ecm} \approx 2.226$ ms and $C_{asym} \approx 0.0046$ ms. Moreover, $C_{fe} \approx C_{ecm}$ [33]. In addition, we assume that $C_{bh} \approx C_{ecm}$ and $C_{fcs} \approx C_{ecm}$. Based on these results, we calculate the rough computation time (in milliseconds) and present the results in Table 5. It is worth noting that our scheme has low computation cost compared to He-Wang's scheme [33], and its cost is also comparable with the schemes of Amin-Biswas [30], Lu *et al.* [31] and Ali-Pal [63]. Although our scheme has high computation cost compared to that for the schemes of Chuang-Chen [23], Sood *et al.* [24] and Mishra *et al.* [27], our scheme offers superior security and more functionality features (see Table 3).

VII. CONCLUDING REMARKS

In this article, we proposed a new remote authentication and session key agreement protocol for multi-server environments using a fingerprint-based fuzzy commitment scheme. The proposed scheme supports correction of errors from noisy biometric data using an error correction technique under a fuzzy commitment scheme. The proposed scheme offers various security services, such as privacy preservation of user's identity and biometric data, mutual authentication and session key establishment between user and server, and facility of any time password updating and biometric data revocation without interaction with the *RC* and server, and a smart card revocation phase. The proposed scheme also provides an early error detection mechanism at the time of login, which resists denial of service attacks. The use of a hash function and fuzzy commitment scheme satisfies the computational complexity and overhead requirements during login, and the mutual authentication and session key agreement procedures of the proposed scheme are under control. The security of the proposed scheme is proved through a rigorous formal security assessment using the ROR model, informal (non-mathematical) security analysis, and formal security verification using the AVISPA simulation tool.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers and the Associate Editor for their valuable feedback on the paper, which helped us to improve its quality and presentation.

REFERENCES

[1] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, pp. 770–772, Nov. 1981.

[2] C.-I. Fan, Y.-C. Chan, and Z.-K. Zhang, "Robust remote authentication scheme with smart cards," *Comput. Secur.*, vol. 24, no. 8, pp. 619–628, 2005.

[3] W.-S. Juang, S.-T. Chen, and H.-T. Liaw, "Robust and efficient password-authenticated key agreement using smart cards," *IEEE Trans. Ind. Electron.*, vol. 55, no. 6, pp. 2551–2556, Jun. 2008.

[4] D.-Z. Sun, J.-P. Huai, J.-Z. Sun, J.-X. Li, J.-W. Zhang, and Z.-Y. Feng, "Improvements of Juang's password-authenticated key agreement scheme using smart cards," *Comput. Standards Interfaces*, vol. 56, no. 6, pp. 2284–2291, 2009.

[5] Z.-Y. Wu, Y.-C. Lee, F. Lai, H.-C. Lee, and Y. Chung, "A secure authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 3, pp. 1529–1535, 2012.

[6] D. He, C. Jianhua, and Z. Rui, "A more secure authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 3, pp. 1989–1995, 2012.

[7] Z. Zhu, "An efficient authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 6, pp. 3833–3838, 2012.

[8] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology—CRYPTO*. Santa Barbara, CA, USA: Springer, 1999, pp. 388–397.

[9] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.

[10] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," *IEEE Trans. Consum. Electron.*, vol. 50, no. 2, pp. 629–631, May 2004.

[11] M.-S. Hwang and L.-H. Li, "A new remote user authentication scheme using smart cards," *IEEE Trans. Consum. Electron.*, vol. 46, no. 1, pp. 28–30, Feb. 2000.

[12] M. Sandirigama, A. Shimizu, and M. T. Noda, "Simple and secure password authentication protocol (SAS)," *IEICE Trans. Commun.*, vol. E86, no. B6, pp. 1363–1365, 2000.

[13] H. Arshad and M. Nikooghadam, "An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC," *Multimedia Tools Appl.*, vol. 75, no. 1, pp. 181–197, 2016.

[14] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. New York, NY, USA: Springer-Verlag, 2003.

[15] J. K. Lee, S. R. Ryu, and K. Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," *Electron. Lett.*, vol. 38, no. 12, pp. 554–555, Jun. 2002.

[16] J. Xu, W. T. Zhu, and D. G. Feng, "Improvement of a fingerprint-based remote user authentication scheme," in *Proc. Int. Conf. Inf. Secur. Assurance (ISA)*, Apr. 2008, pp. 87–92.

[17] C. I. Fan and Y. H. Lin, "Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 933–945, Dec. 2009.

[18] M. K. Khan and J. Zhang, "An efficient and practical fingerprint-based remote user authentication scheme with smart cards," in *Proc. Inf. Secur. Pract. Experience*, K. Chen, R. Deng, X. Lai, and J. Zhou, Eds. Berlin, Germany: Springer, 2006, pp. 260–268.

[19] C. C. Chang and I. C. Lin, "Remarks on fingerprint-based remote user authentication scheme using smart cards," *ACM SIGOPS Oper. Syst. Rev.*, vol. 38, no. 4, pp. 91–96, 2004.

[20] Y. L. C. H. Lin, "A flexible biometrics remote user authentication scheme," *Comput. Standards Interfaces*, vol. 27, no. 1, pp. 19–23, 2004.

[21] C.-T. Li and M.-S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *J. Netw. Comput. Appl.*, vol. 33, no. 1, pp. 1–5, Jan. 2010.

[22] C. J. Mitchell and Q. Tang, "Security of the Lin-Lai smart card based user authentication scheme," Dept. Math., Royal Holloway, Univ. London, Egham, U.K., Tech. Rep. RHUL-MA-2001-0, 2005. [Online]. Available: http://www.rhul.ac.uk/mathematics/techreports

[23] M.-C. Chuang and M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics," *Expert Syst. Appl.*, vol. 41, no. 4, pp. 1411–1418, Mar. 2014.

[24] S. K. Sood, A. K. Sarje, and K. Singh, "A secure dynamic identity based authentication protocol for multi-server architecture," *J. Netw. Comput. Appl.*, vol. 34, no. 2, pp. 609–618, 2011.

[25] B. Wang and M. Ma, "A smart card based efficient and secured multi-server authentication scheme," *Wireless Pers. Commun.*, vol. 68, no. 2, pp. 361–378, 2013.

[26] D. Yang and B. Yang, "A biometric password-based multi-server authentication scheme with smart card," in *Proc. Int. Conf. Comput. Design Appl.*, vol. 5, 2010, pp. 554–559.

[27] D. Mishra, A. K. Das, and S. Mukhopadhyay, "A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards," *Expert Syst. Appl.*, vol. 41, no. 18, pp. 8129–8143, 2014.

[28] X. Li, Y. Xiong, J. Ma, and W. Wang, "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards," *J. Netw. Comput. Appl.*, vol. 35, no. 2, pp. 763–769, 2012.

[29] A. K. Das, V. Odelu, and A. Goswami, "A secure and robust user authenticated key agreement scheme for hierarchical multi-medical server environment in TMIS," *J. Med. Syst.*, vol. 39, no. 9, pp. 1–24, 2015.

[30] R. Amin and G. P. Biswas, "A novel user authentication and key agreement protocol for accessing multi-medical server usable in TMIS," *J. Med. Syst.*, vol. 39, no. 3, pp. 1–17, 2015.

[31] Y. Lu, L. Li, X. Yang, and Y. Yang, "Robust biometrics based authentication and key agreement scheme for multi-server environments using smart cards," *PLoS ONE*, vol. 10, no. 5, p. e0126323, 2015.

[32] C. Wang, X. Zhang, and Z. Zheng, "Cryptanalysis and improvement of a biometric-based multi-server authentication and key agreement scheme," *PLoS ONE*, vol. 11, no. 2, p. e0149173, 2016.

[33] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Syst. J.*, vol. 9, no. 3, pp. 816–823, Sep. 2015.

[34] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1953–1966, Sep. 2015.

[35] A. G. Reddy, A. K. Das, V. Odelu, and K. Y. Yoo, "An enhanced biometric based authentication with key-agreement protocol for multi-server architecture based on elliptic curve cryptography," *PLoS ONE*, vol. 11, no. 5, p. e0154308, 2016.

[36] A. G. Reddy, E. J. Yoon, A. K. Das, V. Odelu, and K. Y. Yoo, "Design of mutually authenticated key agreement protocol resistant to impersonation attacks for multi-server environment," *IEEE Access*, vol. 5, pp. 3622–3639, 2017.

[37] 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 Trans. Dependable Secure Comput.*, to be published, doi: 10.1109/TDSC.2016.2616876.

[38] S. Kumari *et al.*, "A provably secure biometrics-based authenticated key agreement scheme for multi-server environments," *Multimedia Tools Appl.*, vol. 77, no. 2, pp. 2359–2389, 2018.

[39] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[40] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Adv. Cryptol. (EUROCRYPT)*. Tyrol, Austria: Springer, 2001, pp. 453–474.

[41] P. Sarkar, "A simple and generic construction of authenticated encryption with associated data," *ACM Trans. Inf. Syst. Secur.*, vol. 13, no. 4, p. 33, 2010.

[42] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[43] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Trans. Comput.*, vol. 55, no. 9, pp. 1081–1088, Sep. 2006.

[44] S. S. Agaian, *Hadamard Matrices and Their Applications* (Lecture Notes in Mathematics), vol. 1168. Berlin Germany: Springer-Verlag, 1985.

[45] J. H. F. Mattson, Jr., "The theory of error-correcting codes (F. J. MacWilliams and N. J. A. Sloane)," *SIAM Rev.*, vol. 22, no. 4, pp. 513–519, 1980.

[46] A. Nagar, K. Nandakumar, and A. K. Jain, "Biometric template transformation: A security analysis," *Proc. SPIE*, vol. 7541, p. 75410O, Jan. 2010.

[47] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards," *IET Inf. Secur.*, vol. 5, no. 3, pp. 145–151, Sep. 2011.

[48] X. Li, J. W. Niu, J. Ma, W. D. Wang, and C. L. Liu, "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 73–79, 2011.

[49] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. 6th ACM Conf. Comput. Commun. Secur. (CCS)*, Singapore, 1999, pp. 28–36.

[50] C. Kaufman, *Internet Key Exchange (IKEv2) Protocol*, document RFC 4306, 2005. [Online]. Available: https://tools.ietf.org/html/rfc4306

[51] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Adv. Cryptol. (EUROCRYPT)*, Amsterdam, The Netherlands, 2002, pp. 337–351.

[52] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.

[53] A. Dua, N. Kumar, A. K. Das, and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Trans. Vehicular Technol.*, vol. 67, no. 5, pp. 4359–4373, May 2018, doi: 10.1109/TVT.2017.2780183.

[54] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K.-K. R. Choo, and Y. Park, "Design of secure and lightweight authentication protocol for wearable devices environment," *IEEE J. Biomed. Health Inform.*, vol. 22, no. 4, pp. 1310–1322, Jul. 2017, doi: 10.1109/JBHI.2017.2753464.

[55] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Trans. Dependable Secure Comput.*, to be published, doi: 10.1109/TDSC.2017.2764083.

[56] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, Feb. 2018.

[57] J. Srinivas, A. K. Das, N. Kumar, and J. Rodrigues, "Cloud centric authentication for wearable healthcare monitoring system," *IEEE Trans. Dependable Secure Comput.*, to be published, doi: 10.1109/TDSC.2018.2828306.

[58] C.-C. Chang and H.-D. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 357–366, Jan. 2016.

[59] D. Chattaraj, M. Sarma, and A. K. Das, "A new two-server authentication and key agreement protocol for accessing secure cloud services," *Comput. Netw.*, vol. 131, pp. 144–164, Feb. 2018.

[60] O. Mir and M. Nikooghadam, "A secure biometrics based authentication with key agreement scheme in telemedicine networks for E-health services," *Wireless Pers. Commun.*, vol. 83, no. 4, pp. 2439–2461, 2015.

[61] *AVISPA: Automated Validation of Internet Security Protocols and Applications*. Accessed: Jan. 2018. [Online]. Available: http://www.avispa-project.org/

[62] A. K. Das, "A secure user anonymity-preserving three-factor remote user authentication scheme for the telecare medicine information systems," *J. Med. Syst.*, vol. 39, no. 3, pp. 1–20, 2015.

[63] R. Ali and A. K. Pal, "Three-factor-based confidentiality-preserving remote user authentication scheme in multi-server environment," *Arabian J. Sci. Eng.*, vol. 42, no. 8, pp. 3655–3672, 2017.

[64] *National Institute of Standards and Technology (NIST)*, Standard FIPS PUB 180-1, U.S. Department Commerce, Apr. 1995. Accessed: Apr. 2018. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

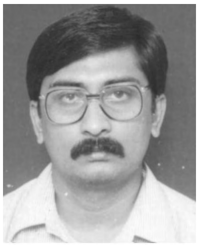
[65] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[66] E. Barker, "Recommendation for key management," NIST, Gaithersburg, MD, USA, Tech. Rep. NIST Special Publication 800-57 Part 1, 2016. Accessed: Apr. 2018. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-57pt1r4.pdf

SUBHAS BARMAN received the B.Tech. degree in computer science and engineering from Kalyani University and the M.Tech. degree in information technology from IIT Kharagpur, India. He is currently pursuing the Ph.D. degree in information technology from Jadavpur University, Kolkata, India. He is also an Assistant Professor with the Department of Computer Science and Engineering, Jalpaiguri Government Engineering College, Jalpaiguri, India. His current research interests include biometrics-based network security. He has authored eight papers in international journals and conferences in the above areas.

ASHOK KUMAR DAS (M'17–SM'18) received the M.Sc. degree in mathematics, the M.Tech. degree in computer science and data processing, and the Ph.D. degree in computer science and engineering from IIT Kharagpur, India. He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology Hyderabad, India. His current research interests include cryptography, wireless sensor network security, hierarchical access control, security in vehicular ad hoc networks, smart grid, Internet of Things, cyber-physical systems and cloud computing, and remote user authentication. He has authored over 160 papers in international journals and conferences in the above areas, including over 140 reputed journal papers. Some of his research findings are published in top cited journals, such as the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, the IEEE TRANSACTIONS ON SMART GRID, the IEEE INTERNET OF THINGS JOURNAL, the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, the IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS (formerly IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE), the IEEE *Consumer Electronics Magazine*, the IEEE ACCESS, the IEEE *Communications Magazine*, *Future Generation Computer Systems*, *Computers & Electrical Engineering*, *Computer Methods and Programs in Biomedicine*, *Computer Standards & Interfaces*, *Computer Networks*, *Expert Systems with Applications*, and the *Journal of Network and Computer Applications*. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He has served as a Program Committee Member in many international conferences. He is on the Editorial Board of the KSII *Transactions on Internet and Information Systems*, *International Journal of Internet Technology and Secured Transactions* (Inderscience), and *Recent Advances in Communications and Networking Technology*. He is a Guest Editor for *Computers & Electrical Engineering* (Elsevier) for the special issue on Big data and IoT in e-healthcare.

DEBASIS SAMANTA received the B.Tech. degree from Calcutta University, India, the M.Tech. degree from Jadavpur University, Kolkata, India, and the Ph.D. degree from IIT Kharagpur, India, all in computer science and engineering. He is currently an Associate Professor with the Department of Computer Science and Engineering, IIT Kharagpur. His current research includes human computer interaction, brain computing interaction, biometric-based system security, and data analytics.



SAMIRAN CHATTOPADHYAY received the bachelor's and master's degree in computer science and engineering from IIT Kharagpur, India, and the Ph.D. degree from Jadavpur University, Kolkata, India. He is currently a Professor with the Department of Information Technology, Jadavpur University. He has over 25 years of teaching experience at Jadavpur University, four years of industry experience, and 12 years of technical consultancy in reputed industry houses. He has authored over 110 papers in international journals and conferences.

JOEL J. P. C. RODRIGUES (S'01–M'06–SM'06) received the five-year B.Sc. degree (licentiate) in informatics engineering from the University of Coimbra, Portugal, the M.Sc. degree and the Ph.D. degree in informatics engineering from the University of Beira Interior (UBI), Portugal, and the Habilitation degree in computer science and engineering from the University of Haute Alsace, France. He is currently a Professor and a Senior Researcher with the National Institute of Telecommunications (Inatel), Brazil, and a Senior Researcher with the Instituto de Telecomunicações, Portugal. He has been a Professor with UBI, and a Visiting Professor with the University of Fortaleza, Brazil. He has authored or co-authored over 550 papers in refereed international journals and conferences, three books, and two patents. He is a Licensed Professional Engineer (as a Senior Member), a member of the Internet Society, and a Senior Member ACM. He received the Academic Title of Aggregated Professor in informatics engineering from UBI. He is the Past-Chair of the IEEE ComSoc Technical Committees on eHealth and on communications software. He is the editor-in-chief of three International Journals. He is also the Leader of the Internet of Things Research Group (CNPq), the Director for the Conference Development-IEEE ComSoc Board of Governors, the IEEE Distinguished Lecturer, the President of the Scientific Council at ParkUrbis–Covilha Science and Technology Park.

YOUNGHO PARK (M'17) received the B.S., M.S., and Ph.D. degrees in electronic engineering, Kyungpook National University, Daegu, South Korea, in 1989,1991, and 1995, respectively. From 1996 to 2008, he was a Professor with the School of Electronics and Electrical Engineering, Sangju National University, South Korea. From 2003 to 2004, he was a Visiting Scholar with the School of Electrical Engineering and Computer Science, Oregon State University, USA. He is currently a Professor with the School of Electronics Engineering, Kyungpook National University. His research interests include computer networks, multimedia, and information security.