Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

A Secure Authentication Protocol for Multi-server-based e-Healthcare using a Fuzzy Commitment Scheme

SUBHAS BARMAN[1], HUBERT P. H. SHUM[2], (Member, IEEE), SAMIRAN CHATTOPADHYAY[3], and DEBASIS SAMANTA[4]

[1]Jalpaiguri Government Engineering College, Jalpaiguri, West Bengal, India (e-mail: subhas.barman@gmail.com)
[2]Faculty of Engineering and Environment, Northumbria University, UK (e-mail: hubert.shum@northumbria.ac.uk)
[3]Department of Information Technology, Jadavpur University, Salt Lake City, Kolkata 700 098, India (e-mail: samirancju@gmail.com)
[4]Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur 721 302, India (e-mail: dsamanta@iitkgp.ac.in)

Corresponding author: Hubert P. H. Shum (e-mail: hubert.shum@northumbria.ac.uk)

This work was supported in part by the Engineering and Physical Sciences Research Council (REF: EP/M002632/1) and the Royal Society (REF: IE160609).

ABSTRACT Smart card-based remote authentication schemes are widely used in multi-medical-server-based telecare medicine information systems (TMIS). Biometric is one of the most trustworthy authenticators, and is presently being advocated to use in the remote authentication of TMIS. However, most of the existing TMISs consider a single-server-environment-based authentication system. Therefore, patients need to register and log into every server separately for different services. Furthermore, these schemes do not employ error correction technique to remove the errors from biometric data. Also, biometrics are inherent and demand diversification to generate a revocable template from inherent biometric data. In this paper, we propose a mutual authentication and key agreement scheme for a multi-medical server environment to overcome the limitations of the existing schemes. In the proposed scheme, a cancelable transformation of the raw biometric data is used to provide the privacy and the diversification of biometric data. The errors of the biometric data are corrected with error-correction techniques under the fuzzy commitment mechanism. Formal security analysis using the widely accepted Real-Or-Random (ROR) model, the Burrows-Abadi-Needham (BAN) logic and the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool concludes that the proposed scheme is safe against known attacks. We also compare the computation and communication costs of our scheme to evaluate the performance with the others.

INDEX TERMS Telecare Medicine Information System (TMIS), Fuzzy Commitment Scheme, BAN Logic, Real-Or-Random (ROR), AVISPA tool.

I. INTRODUCTION

NOWADAYS, people are accessing more and more services through the Internet. For example, they use different electronic gadgets like mobile phones and notebooks to get access to a remote server from anywhere through a public channel. Many countries already introduced e-Health and telemedicine services for easy and wide access to health care services with high availability. Example e-Heath and telemedicine systems include ManageMyHealth (New Zealand), National Health Portal (Government Of India), eCW Heath Care Portal (eClinicalWorks, Georgia), and Boynton Health (University of Minnesota). In recent years, Internet services and low-cost mobile devices make the e-Health care and telemedicine services available directly to the patient [15]. With e-Health care, patients are able to access different healthcare assistance without visiting the healthcare center physically but through the Internet. Conventional clinical medical service system can be replaced by distance nursing, e-health care and home monitoring facility [15], [17], [18]. In TMIS, patients can remotely check-up their vital signs and physician can read the up-to-date medical information of a patient using a public network channel. However, the security of the patient's sensitive information to prevent unauthorized access by an attacker is crucial. At the same time, the protection of patient's privacy during the remote access of telecare services is another important

concern [15], [64].

With respect to the aforementioned context, a remote authentication scheme can be employed to ensure a secure access to TMIS by patients as well as physicians over insecure channels. Lamport introduced password-based authentication in 1981 [13], in which the server stored all the passwords into a password table. Therefore, the scheme is susceptible to stolen-verifier attacks. Dictionary attacks may guess a password with low entropy. Moreover, since the social information of a user is typically used to select a password, social engineering may reveal the password easily with the knowledge of the user's social information. To overcome these problems, smart cards have been combined with the traditional password authentication to form a two-factor-based authentication scheme. Unfortunately, the stolen smart card may reveal stored information under power analysis [10] and differential attacks [11].

Recently, Wu *et al.* [23] used passwords and smart cards to design a two-factor-based remote authentication scheme for TMIS. He *et al.* [24] performed a cryptanalysis on Wu et al.'s scheme [23] and they concluded that the scheme [23] failed to resist the impersonation attacks, the insider attacks and the stolen smart card attacks. He *et al.* [24] proposed another authentication scheme for TMIS, which can overcome all weaknesses of [23]. Unfortunately, such a scheme is vulnerable to off-line password guessing attacks. As a remedy, Zhu [25] proposed an authentication scheme using RSA-cryptosystem. The research from [26]–[29] also failed to ensure the robustness of the remote authentication scheme using passwords and smart cards. As a new direction, researchers are exploring the use of biometric data (e.g. fingerprint, iris [6], [16], [20]) with traditional authentication schemes [3]. In general, three-factor-based authentication schemes are introduced to improve the security of the patient's information [30]–[34].

Furthermore, the existing schemes from [21]–[25], [35] overlook the user's privacy as the user's identity is transmitted openly to the server via an insecure channel. However, a user's privacy should be protected in TMIS to hide the identity of the patients from unauthorized users. Therefore, user anonymity is expected to preserve the privacy of patients. Put et al. [36] reported an elliptic-curve-cryptosystem-based strong authentication scheme to ensure user anonymity. However, this scheme [36] requires high communication, storage and computation costs. Chen et al. [37] proposed a dynamic id-based authentication scheme that reduced costs. Jiang *et al.* [38] did a thorough cryptanalysis of Chen *et al.*'s scheme [37] and observed that the scheme failed to provide user anonymity. They suggested an authentication scheme that achieved user anonymity. Kumari *et al.* [39] found that Jiang *et al.*'s scheme is not able to resist password guessing attacks, user impersonation attacks, Denial-of-Service (DoS) attacks and session key disclosure attacks. Accordingly, they addressed all the limitations with an improved authentication scheme. Lately, researchers reported many authentication and key agreement schemes for TMIS [40], [41], [43], [64].

In the literature, the authentication schemes are either for a single server environment or a multi-server and cloud-based environment [2], [4], [9], [82], [83]. Researchers proposed multi-medical-server-based TMIS because a patient may need access to multiple medical servers with a single registration for different services. In other words, patients may communicate with different medical servers to get services from multiple servers such as Anesthesiologist, Cardiologist, Gastroenterologist, Hematologist, Neurologist, etc. Therefore, multi-server-based TMIS essentially need a remote authentication scheme and a key sharing protocol for a secure message communication. There are several three-factor-based authentication schemes [1], [45]–[48] for a multi-server environment using knowledge (e.g. the password), token (e.g. the smart card) and biometric (e.g. the fingerprint, iris, face, etc.). Chuang and Chen [1] proposed an authentication scheme for a multi-server environment. Mishra et al. [48] and Lin *et al.* [60] observed that the scheme [1] was vulnerable to insider attacks, Denial-of-Service (DoS) attacks, server spoofing attacks and user impersonation attacks. Moreover, user anonymity property was not provided in the Chuang-Chen's scheme. As an improvement, Mishra *et al.* designed another authentication scheme for expert systems [48]. However, Wang *et al.* [68] and Lu *et al.* [61] revisited Mishra *et al.*'s scheme and found that user anonymity and perfect forward secrecy of the session key were not provided in the scheme [48]. Moreover, Mishra *et al.*'s scheme failed to resist replay attacks, forgery attacks, Denial-of-Service (DoS) attacks, user and server masquerading attacks. In 2016, Reddy *et al.* [62] analyzed Lu *et al.*'s scheme and observed several drawbacks like user impersonation attacks, Man-in-the-middle attacks and clock synchronization problems. Also, the perfect forward secrecy and user anonymity are not ensured in the scheme [61]. In 2016, Wang *et al.* [68] proposed an authentication scheme with low computation cost. In addition, this scheme alleviated different security issues of Mishra *et al.* scheme and they included a user revocation phase in [68]. Unfortunately, Wang *et al.'s* scheme failed to resist different known attacks. Irshad *et al.* [66] and Reddy *et al.* [65] identified many drawbacks like insider attacks, the lack of user anonymity and mutual authentication in the scheme of [68]. Reddy *et al.* [65] proposed a multi-server authentication scheme to resist impersonation attacks. Irshad *et al.* [66] proposed an improved and light-weight authentication scheme to address the impersonation attacks, user traceability attacks, privileged insider attacks of Wang *et al.*'s scheme [68]. However, Irshad *et al.* [66] do not include the biometric template update phase in their scheme. In addition, user revocation and re-registration provisions were not considered. Later on, Yang and Zheng [69] proposed an authentication scheme for expert systems and remote distributed networks, addressing the drawbacks of Wang *et al.* scheme. However, this scheme does not consider the biometric template revocation option. Recently, Barman *et al.* proposed an authentication scheme using fuzzy commitment for a multi-server environment [78]. Still, the smart card

revocation process did not consider any checking of user authentication before issuing a new smart card to a user. Also, if an attacker (i.e. insider attacker) knows the user id of a genuine user, he/she can request for a new smart card from the registration center. An attacker can generate a template from his/her biometrics data and he/she can compute the request message using his/her biometric template, password and random number. The registration center cannot differentiate the genuine request message from attacker's one. This limitation is addressed in our proposed scheme.

Amin and Biswas [49] proposed a multi-medical-server-based TMIS and claimed that their scheme is able to resist different know attacks. However, Das *et al.* [50] thoroughly analyzed the Amin-Biswas's scheme and found that the scheme [49] failed to protect privileged insider attacks, strong replay attacks and man-in-the-middle attacks. Truong *et al.* [63] proposed an elliptic-curve-cryptosystem-based authentication for a multi-server environment with the provable identity. However, Zhao *et al.* [70] identified the offline password guessing attacks, user and server impersonation attacks in the Troung *et al.*'s scheme [63]. Moreover, existing remote authentication protocols for a multi-server environment do not consider (1) the privacy of the biometric identity of a patient, (2) the diversification of the biometric template for revocability, (3) the provision of the biometric template update if required, and (4) error correction from a biometric template.

In this paper, the fuzzy commitment scheme is used to design a remote authentication and key agreement protocol for a TMIS with multi-medical servers. We consider the privacy of the identity and the diversification of the biometric data. The erroneous template can be corrected and the enrolled template can be updated successfully in the proposed scheme. Our proposed scheme also employs only exclusive-OR operations and one-way hash functions to optimize its computation cost. Moreover, the mutual authentication between a user and a server is proved using BAN logic [53]. The Real-Or-Random (ROR) model is used to test the security of the proposed scheme. Furthermore, informal security analysis is also applied to our proposed scheme to ensure the security against some known attacks. The AVISPA tool is used to simulate and test the formal security of the proposed scheme. Finally, we discuss the performance of our scheme with respect to computation and communication costs, and security functions. The performance of our scheme is compared with the existing ones, showing that our scheme requires less computation cost.

A. THE THREAT MODEL

We assume that the Dolev-Yao threat (DY) model [12] and CK-adversary model [73] are applicable in our scheme as the *de facto* standard threat model and adversary model, respectively. As per the DY model, an adversary $\mathcal{A}$ can intercept all messages communicated between the genuine participants, modify the content of the messages or intentionally tamper the messages and delete either the total or a part of the messages communicated between the genuine participants. $\mathcal{A}$ can even inject his/her own message to compromise the integrity of the communicated messages. Moreover, the power analysis attacks [10], [11] may reveal the information from a smart card. In addition, an adversary $\mathcal{A}$ can compute some temporary or long-term secrets of the communicating participants as per the Canetti and Krawczyk's adversary model (CK-adversary model) [73]. Therefore, $\mathcal{A}$ should not able to compromise the security of a remote authentication and key establishment scheme even when the ephemeral secrets (temporary or long-term secrets) and the old session keys are compromised during the communication.

B. RESEARCH CONTRIBUTIONS

The contributions of this paper are as follows:

- Designing an authentication protocol for multi-medical-server-based e-Healthcare using fuzzy commitment scheme. Recently, Barman *et al.* proposed a remote authentication scheme using fuzzy commitment [78]. However, Barman *et al.*'s scheme is vulnerable to insider attacks. An insider $\mathcal{A}$ trusted by the MSRC knows the user id ID_i, generates biometric template $C_{T_\mathcal{A}}$ using his/her own biometric data, $BIOM_\mathcal{A}$, selects a random number $k_\mathcal{A}$ and generates $RPW_\mathcal{A} = h(PW_\mathcal{A}||C_{T_\mathcal{A}})$. The attacker $\mathcal{A}$ then sends the smart card revocation message, $< ID_i, RPW_\mathcal{A} \oplus k_\mathcal{A} >$ to the registration center. The registration center will issue a new smart card to the attacker as the registration center does not have any scope to check the authenticity of the revocation message. In our proposed protocol, this problem of the scheme [78] is addressed. Our proposed scheme provides a secure smart card revocation phase.
  The session key security is ensured under the CK-adversary model (I-A). Moreover, our scheme considers error correction to remove the noise from a user's biometric data. The privacy and identity of the biometric data are strongly preserved. The diversification of the biometric template is provided in such a way that it is easy to revoke a biometric template, if required.
- The proposed scheme is tested with the widely accepted Real-Or-Random (ROR) model, BAN logic and AVISPA tool.
- The proposed scheme is compared with the existing schemes and the proposed scheme is found as the most efficient scheme with respect to the cost and security functions.

C. ORGANIZATION

In Section 2, we discuss the definition and mathematical preliminaries of the fuzzy commitment scheme, error correction techniques and revocable template generation, which are essential for describing our proposed scheme. The proposed protocol is presented in Section 3. In Section 4, we provide the ROR model, BAN logic and AVISPA simulation for the formal security analysis of the proposed scheme. In Section 5, we discuss the informal security analysis for different

known attacks and compare our proposed protocol with other existing schemes. The performance of the proposed scheme is discussed and compared with other schemes in Section 6. Finally, we conclude the work in Section 7.

II. DEFINITIONS AND MATHEMATICAL PRELIMINARIES

We propose a biometric-based fuzzy commitment scheme and a one-way hash function. In the fuzzy commitment scheme, we use a cancelable biometric template and an error correction technique. In this section, we briefly describe the basic concepts of cancelable biometric template generation, one-way hash functions, error correction coding technique and a fuzzy commitment scheme.

A. THE CANCELABLE BIOMETRIC TEMPLATE GENERATION FUNCTION

The cancelable biometric template provides privacy to the original biometric data [19]. The cancelable biometric template is generated using a transformation function (say $f(.)$), which is irreversible in nature. The transformation function uses a transformation key (say T_{p_i}) to convert the biometric data (say $BIOM_i$) into a cancelable biometric template (say C_{T_i}), that is, $C_{T_i} = f(BIOM_i, T_{p_i})$. Note that multiple numbers of irreversible templates may be generated from a single biometric using multiple transformation parameters. Moreover, a cancelable transformation process should satisfy the following properties.

(i) A collision-free cancelable template: (a) Say, C_{T_i}, C'_{T_i} are two templates generated from a biometric data $BIOM_i$ using two different transformation parameters, T_{p_i} and T'_{p_i}, respectively. According to this property, $C_{T_i} \neq C'_{T_i}$ when $T_{p_i} \neq T'_{p_i}$. (b) Again, if $C_{T_k} = f(BIOM_k, T_{p_k})$ and $C_{T_l} = f(BIOM_l, T_{p_l})$, due to the inter-person variability of biometric data (i.e. $BIOM_k \neq BIOM_l$), $C_{T_k} \neq C_{T_l}$ even when $T_{p_k} = T_{p_l}$.

(ii) Intra-user variability: Suppose we use two instances of a biometric to generate two cancelable templates, $C_{T_i} = f(BIOM_i, T_p)$ and $C'_{T_i} = f(BIOM'_i, T_p)$. If the similarity between two sets of biometric data is greater than a threshold value, say, δ, the similarity between two cancelable templates should also be greater than δ. Assume that the function of matching score computation is $MS()$. Then, if the similarity score between the biometric instances is greater than δ, that is, $MS(BIOM_i, BIOM'_i) > \delta$, the similarity between the templates is also greater than the threshold value δ, that is, $MS(C_{T_i}, C'_{T_i}) > \delta$.

(iii) The reusability of biometric data: The biometric template should be easy to revoke if required. An existing template can be cancelled and a new cancelable biometric template can be generated from the same biometric data using the same transformation function but with a new transformation key. Therefore, the biometric data is reusable even when a cancelable template is compromised.

B. THE ERROR CORRECTION CODING TECHNIQUE

The errors between two instances of a biometric signal result in the false rejection of genuine users. These errors can be corrected using error correction coding (ECC) techniques [7], [8]. Say, there are two instances $BIOM_{enrol}$ and $BIOM_{query}$ of a biometric signal. $BIOM_{enrol}$ is captured and used at the time of the enrollment. A cancelable template $C_{T_{enrol}}$ is generated for the enrollment from $BIOM_{enrol}$, that is, $C_{T_{enrol}} = f(BIOM_{enrol}, T_{P_i})$. Similarly, another cancelable template $C_{T_{query}}$ is generated from $BIOM_{query}$, that is, $C_{T_{query}} = f(BIOM_{query}, T_{P_i})$). Here, the bitwise dissimilarity of two templates, that is, $e = C_{T_{enrol}} \oplus C_{T_{query}}$ is called an error. An error correction coding technique (say, Ψ) can correct the error e only when the size of e is less than the capacity of the ECC techniques. There are mainly two steps in any ECC technique, encoding (Ψ_{enc}) and decoding (Ψ_{dec}). An error correction codeword is generated and used to encode a secret string [6], [7]. The encoded string may be transmitted over network channel and few bits may be integrated with the original signal and generate an erroneous message for the recipient. The recipient receives the erroneous message and removes the errors using decoding of the ECC technique. Therefore, the error may be corrected completely if the number of erroneous bits is not more than the error correction capacity of the ECC technique.

C. THE FUZZY COMMITMENT SCHEME

This scheme is used to conceal a secret under the security of a witness. The secret can be unlocked using a witness, which is sufficiently close to the witness used during the enrollment. It was initially proposed by Juels and Wattenberg [5] in 1999. This scheme is successfully followed to construct a cryptographic system using the biometric data [6]. In this scheme, say K_r is a randomly generated key and the K_r is encoded with a codeword, that is, $K_{CW} = \Psi_{enc}(K_r)$. The K_{CW} is called a pseudo code, which looks like an original biometric code. A biometric code is a binary string (C_{T_i}), extracted from a biometric imprint. This biometric code is also called a cancelable biometric template. A pseudo code K_{CW} is locked by a cancelable biometric template C_{T_i} using bit-wise exclusive-OR operation, that is, $LTK_i = C_{T_i} \oplus K_{CW}$. Here, LTK_i is called helper data as it helps to release the secret key. The genuine biometric template is applied to extract the secret key from the helper data. In the fuzzy commitment scheme, the biometric template and the random secret, both are deleted carefully. However, the system stores the helper date HTK_i and $(h(K_r))$ for future use. According to the said scheme, a genuine biometric template with minimum dissimilarity can decode the secret exactly. The $h(K_r)$ is used for the verification of the similarity of the regenerated key K'_r from LTK_i using C'_{T_i}.

In the key regeneration process, a newly generated biometric template (say C'_{T_i}) is XORed with the helper data LTK_i,

that is,

$$\begin{aligned} K'_{CW} &= LTK_i \oplus C'_{T_i} \\ &= C_{T_i} \oplus K_{CW} \oplus C'_{T_i} \\ &= K_{CW} \oplus e \end{aligned} \tag{1}$$

Due to the intra-person variability, there must be some errors in C'_{T_i}, that is, $e = C'_{T_i} \oplus C_{T_i}$. This error is propagated to K'_{CW} and can be corrected with the help of the decode phase of the error correction technique (i.e. $K_r = \Psi_{dec}(K'_{CW})$). As the error of the intra-person variability is lower than the capacity of the error correction of Ψ, therefore, a genuine patient can unlock a key correctly using her fresh biometric instance. The high inter-person variability creates the error in the impostor template (with respect to a genuine template) and that is higher than the error correction capacity of Ψ.

D. ONE-WAY CRYPTOGRAPHIC HASH FUNCTION

A one-way hash function is a mapping function $h : A \leftarrow B$ which takes an arbitrary length message $A = \{0,1\}^*$ as input and outputs a fixed-length (say l-bits) compressed message $B = \{0,1\}^l$ with the following properties:

- Say, an input $m \in A$ and the output is $y = h(m)$, $y \in B$. For any $h(.)$, it is easy to compute y of m but it is difficult to recompute the m from the y.
- Any changes (say in a single bit of m) in input results in a completely uncorrelated hash value which is different from hash value $h(m)$ before changes.
- *Preimage resistance:* For an one-way hash function $h(.)$, the computation of the original message from a given message digest (hash value) is computationally infeasible, that is, $m \neq h^{-1}(y)$.
- *Second preimage resistance:* It is difficult to find two messages, $m, m' \in A$ such that $m \neq m'$, but both inputs produce the same outputs, that is, $h(m) = h(m')$.
- *Strong collision resistance:* For two different inputs m, $m' \in A$, the hash values are $y = h(m)$ and $y' = h(m')$. If $m \neq m'$ but $y = y'$, it is called the collision of a cryptographic one-way hash function. However, the collision resistance property of a hash function states that for any two different inputs ($m, m' \in A$ and $m \neq m'$), a hash function $h(.)$ never outputs the same message digests.

E. SMART CARD

A smart card is a device that includes an embedded integrated circuit (i.e. secure micro controller or equivalent intelligence) with internal memory. A smart card connects to a smart card reader with a direct physical contact or with a remote contactless radio frequency interface. Smart cards provide secure storage of personal data, biometric data security and mechanisms like encryption, authentication, communication. They interact intelligently with a smart card reader. Generally, the smart card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443). We have considered the physical contact smart card with the embedded circuit to store the confidential information of the registered patients and the smart card can process the data for authentication of the registered patients. The smart card can generate and send the login message to the server to establish a secure connection between a registered patient and medical server.

TABLE 1: Notations

Symbol	Description
U_i, UID_i, PW_i	The patient's name, unique identity, password
$BIOM_i$, T_{P_i}, C_{T_i}, $f()$	The biometric data, the transformation parameter, the cancelable template of U_i, and the transformation function used to transform $BIOM_i$ to C_{T_i}
PWD_i	The pseudo-random password of the patient U_i
$MSRC$, K_{RC}	The medical service registration center, and its secret key
MS_i, SID_i, X_j	The medical server, its unique identity and secret key
K, K_{CW}	A secret key randomly chosen by U_i, and its codeword
$\Psi_{enc}()$, $\Psi_{dec}()$	The encoding and decoding functions of error correction technique
LTK_i	The helper data or locked key of the patient U_i
$\oplus, \|\|$	The bitwise XOR operation, the concatenation operation
SK_{ij}	The session key between U_i and MS_j
$h(.)$	The one way hash function
TS	Time stamp
SC_i	The smart card of the patient U_i

III. THE PROPOSED PROTOCOL

This section includes three procedures: registration of the server and the patient, the session key establishment protocol, and the update phase. In our discussion, we have used several symbols and notations which are given in Table 1.

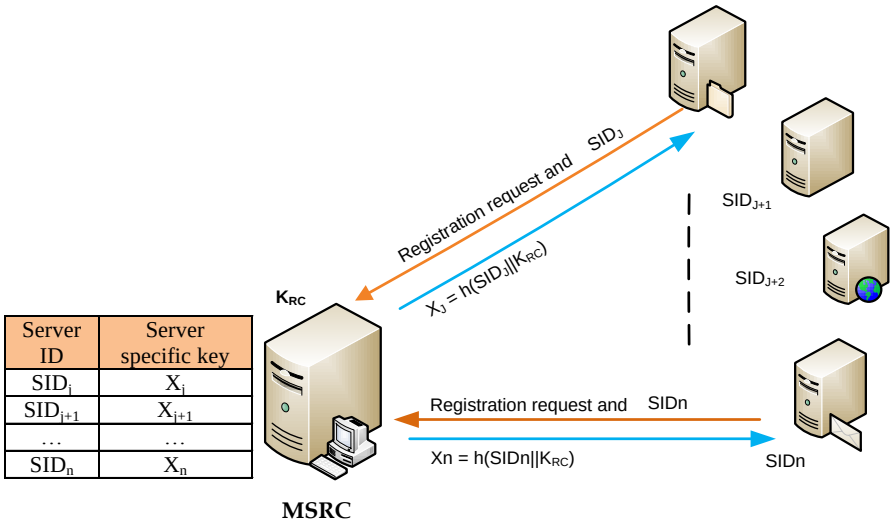
In our proposed scheme, initially, the medical servers and the patients are enrolled with medical service registration center. User authentication is verified by the smart card and only the authentic patients can log into the system. The medical server also checks the authenticity of the patient with respect to the received login message. The medical server transmits a reply-message to the patient after verification of authentication. Then, the patient checks the authenticity of the medical server based on the received message. Finally, the same session key is computed by the patient and the medical server. In the update phase, a patient can update his/her password, biometric template and smart card.

We apply the fuzzy commitment scheme in order to strengthen our scheme. The error correction technique is adopted along with the fuzzy commitment scheme to handle the noisy biometric signal. Furthermore, we use the time-stamp and the random nonce to make our scheme resilient to the replay and man-in-the-middle attacks.

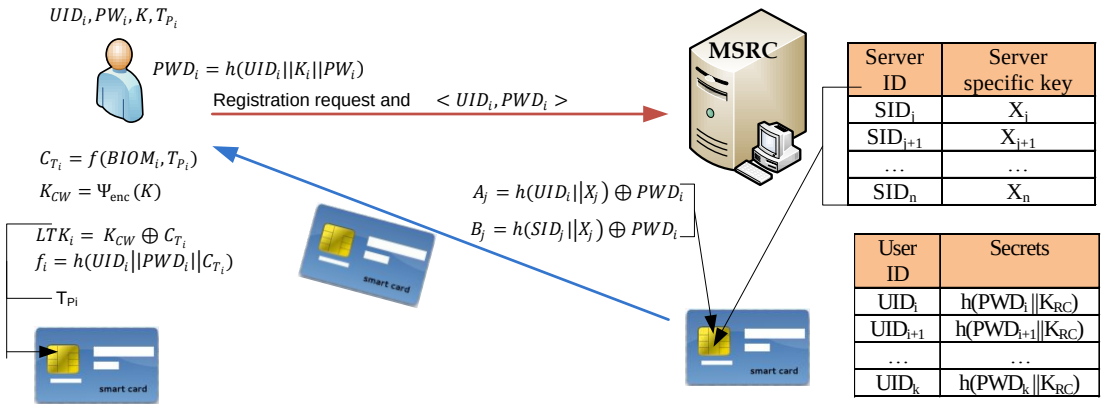
The details of the different phases are discussed in the following subsections.

A. THE REGISTRATION PROCEDURE

In this proposed scheme, all the medical servers and patients are enrolled to the telecare medical system through the med-



(a} Server registration process



(b} User registration process

FIGURE 1: The medical server and patients registration procedure

ical service registration center (MSRC). Both registration procedures are presented in the Figure 1.

1) The Server Registration Procedure

In our scheme, all medical servers (MS_j, $j = 1$ to $(m + m')$) are required to be registered with the medical service registration center ($MSRC$). We assume that initially m medical servers are ready to be registered. We also assume that another m' medical servers may be registered in the future. A medical server chooses its unique id, that is, SID_j and sends it to the $MSRC$ for the registration. The registration center $MSRC$ computes a server specific key $X_j = h(SID_j||K_{RC})$, where K_{RC} to be the secret key of $MSRC$. Then, $MSRC$ sends X_j to MS_j. This X_j is used during the authentication process of a patient. The $MSRC$ repeats the same process for m number of the medical server registrations. At the same time, the $MSRC$ assumes that m' number of medical servers may register themselves with the $MSRC$ in the future. Therefore, the $MSRC$ chooses a unique medical server id SID_k for $m + 1 \leq k \leq m + m'$ and computes the shared key X_k for $m + 1 \leq k \leq m + m'$. The medical server ids and the corresponding keys are stored in the database of the $MSRC$. In the future, if any medical server requests for registration, the $MSRC$ provides them with an unused unique id and a corresponding key from the database.

2) The Patient Registration Process

Initially, every patient should register to the medical service registration center ($MSRC$) via a secure channel. Each patient (say U_i) chooses a user id (UID_i), a password (PW_i) and a transformation key (T_{P_i}). The patient U_i imprints

his/her biometric data ($BIOM_i$) through a biometric scanner. We have used the fingerprint biometric in our approach. This biometric has been chosen because it is universal, unique and invariant over time. More significantly, it is processable in real-time with almost near 100% accuracy. In this work, minutiae-based approach has been followed. The minutiae points are extracted from a fingerprint image using the publicly available NIST Biometric Software (NBIS). The MINDTCT module of NBIS is used as a minutiae detector to extract minutiae points (i.e. ridge ending and ridge bifurcation) from fingerprint image. A set of minutiae points (say, $BIOM_i$) captured from the fingerprint image of a user is used to generate the cancelable template (i.e. C_{T_i}) with a transformation parameter (T_{P_i}) using a transformation function $f(.)$. This canelable template is used in the implementation of the proposed authentication protocol. The detailed steps of the patient registration procedure are described as follows.

1) The patient generates a cancelable templates, that is, $C_{T_i} = f(BIOM_i, T_{P_i})$.
2) U_i selects a key K randomly and encodes K into a codeword, K_{CW} uses the error correction encoding technique Ψ_{enc}, that is, $K_{CW} = \Psi_{enc}(K)$.
3) U_i locks K_{CW} with the cancelable biometric template C_{T_i} (i.e. $LTK_i = K_{CW} \oplus C_{T_i}$).
4) U_i computes $PWD_i = h(UID_i||K||PW_i)$ and sends (UID_i, PWD_i) along with a registration request to the $MSRC$.
5) After receiving the registration request from a patient, the $MSRC$ computes $A_j = h(UID_i||X_j) \oplus PWD_i$ and $P_j = h(SID_j||X_j) \oplus PWD_i$ for $1 \leq j \leq m+m'$.
6) The $MSRC$ stores all authentication parameters $\{< SID_j, A_j, P_j > |1 \leq j \leq m + m'), h(.)\}$ in a smart card, SC_i. Then, the SC_i is delivered to patient U_i through a secure channel. The $MSRC$ stores $UID_i, h(PWD_i||X_j)$ in the database for future use.
7) U_i computes $f_i = h(UID_i||PWD_i||C_{T_i})$ and stores $\{T_{P_i}, LTK_i, h(K), f_i, f(.), \Psi_{enc}(), \Psi_{dec}()\}$ into SC_i.

Finally, the smart card SC_i contains $\{< SID_j, A_j, P_j > |1 \leq j \leq m+m'), h(.), T_{P_i}, LTK_i, h(K), f_i, f(.), \Psi_{enc}(.), \Psi_{dec}(.)\}$. Therefore, the biometric data of the users/patients need not to be directly stored anywhere in the system. In the proposed approach, the cancelable fingerprint template of a user C_{T_i} is used to lock a randomly generated key K and the locked key/template (i.e. helper data, LTK_i) is to be stored in the internal memory of the respective user's smart card.

B. THE SESSION KEY ESTABLISHMENT PROTOCOL

This procedure includes the login phase, the mutual authentication phase and the agreement protocol.

1) The Login Phase

Any registered patient U_i can access any registered medical server MS_j after a successful authentication. Initially, a registered patient inserts SC_i to a smart card reader (SCR), captures biometric imprint, enters UID_i and PW_i to access a desired medical server. In the login phase, SC_i verifies the authenticity of the patient U_i. The smart card generates a valid login message only when the patient passes the authentication checking through the password, the biometric and the smart card. Detailed steps are described below and illustrated in Table 2.

TABLE 2: The login process

Patient U_i/SC_i	Medical Server MS_j
U_i inputs UID_i, PW_i, inserts SC_i	
Provides query $BIOM_i^*$	
Computes $C_{T_i}^* = f(BIOM_i^*, T_{P_i})$	
$K^* = \Psi_{dec}(LTK_i \oplus C_{T_i}^*) = \Psi_{dec}(K_{CW}^*)$	
If $h(K^*) \neq h(K)$, SC_i terminates session	
Else computes	
$PWD_i^* = h(UID||K^*||PW_i)$	
$f_i^* = h(UID_i||PWD_i^*||C_{T_i}^*)$	
If $f_i^* \neq f_i$, terminates	
Else continues	
SC_i generates R_c and TS_1	
$M_1 = A_j \oplus PWD_i^*$	
$M_2 = P_j \oplus PWD_i^*$	
$M_3 = UID_i \oplus M_2$	
$M_4 = M_1 \oplus R_c$	
$M_5 = h(M_1||R_c||TS_1)$	
$< M_3, M_4, M_5, TS_1 >$	$\xrightarrow{\quad\quad}$

1) U_i inserts the SC_i to a SCR and inputs UID_i, PW_i and scans his/her biometric to capture a query $BIOM_i^*$.
2) SC_i computes a cancelable template $C_{T_i}^*$ from query $BIOM_i^*$ using transformation function $f()$ and transformation parameter T_{P_i}, that is, $C_{T_i}^* = f(BIOM_i^*, T_{P_i})$.
3) SC_i unlocks K_{CW}^* with $C_{T_i}^*$ and decodes it to regenerate the key K^* as follows: $K^* = \Psi_{dec}(LTK_i \oplus C_{T_i}^*) = \Psi_{dec}(K_{CW}^*)$
4) SC_i checks $h(K^*)? = h(K)$ and if it is wrong, it rejects the session immediately. Otherwise it continues.
5) SC_i computes: $PWD_i^* = h(UID_i||K^*||PW_i)$, $f_i^* = h(UID_i||PWD_i^*||C_{T_i}^*)$. Then, SC_i checks $f_i^*? = f_i$. If it does not hold, the login process is terminated. Otherwise, U_i passed all the login check points. SC_i generates a random number R_c and a time stamp TS_1.
6) SC_i computes the following messages

$$\begin{aligned} M_1 &= A_j \oplus PWD_i^* = h(UID_i||X_j) \\ M_2 &= P_j \oplus PWD_i^* = h(SID_j||X_j) \\ M_3 &= UID_i \oplus M_2 \\ M_4 &= M_1 \oplus R_c \\ M_5 &= h(M_1||R_c||TS_1) \end{aligned}$$

7) The smart card SC_i sends the login message $< M_3, M_4, M_5, TS_1 >$ to the medical server MS_j.

2) The Mutual Authentication and Key Agreement Phase

A legal patient and a registered server are mutually authenticated to each other before the agreement of a session key. The medical server checks the login messages of the patient and authenticates the patient. Similarly, the patient checks the authenticity of the server to achieve mutual authentication. Then, a session key is established between them for future secure message communication. This process is illustrated in Table 3. The detailed steps are described below.

1) The medical server MS_j receives the login message from the patient/the smart card SC_i at time TS_c and checks the validity of the time stamp (TS_1) with respect to a predefined threshold delay ΔT. If $(TS_c - TS_1) \leq \Delta T$ holds then continues, otherwise MS_j terminates the session.
2) The MS_j computes the parameters as follows:

$$\begin{aligned} M_6 &= h(SID_j||X_j) \\ M_7 &= M_3 \oplus M_6 = UID_i \\ M_8 &= h(M_7||X_j) = h(UID_i||X_j) \\ M_9 &= M_4 \oplus M_8 = R_c \\ M_{10} &= h(M_8||M_9||TS_1) \\ &= h(h(ID_i||X_j)||R_c||TS_1) \end{aligned}$$

3) MS_j compares M_{10} with received M_5. If $M_5 = M_{10}$ holds, it generates a random number R_s and the current time stamp TS_2.
4) Then, MS_j computes the following parameters:

$$\begin{aligned} M_{11} &= h(M_8||R_c) \oplus R_s \\ &= h(h(UID_i||X_j)||R_c) \oplus R_s \\ SK_{ij} &= h(M_6||M_8||M_9||R_s||TS_2) \\ &= h(h(SID_j||X_j)||h(UID_i||X_j) \\ &\quad ||R_c||R_s||TS_2) \\ M_{12} &= h(SK_{ij}||M_8||M_9||TS_2) \\ &= h(SK_{ij}||h(UID_i||X_j)||R_c||TS_2) \end{aligned}$$

5) MS_j sends $< SID_j, M_{11}, M_{12}, TS_2 >$ to the patient U_i/the smart card SC_i.
6) SC_i receives the message at time TS_{c1}, checks the time delay (i.e. $(TS_{c1} - TS_2)$ and if it is less than ΔT, it computes the following:

$$\begin{aligned} M_{13} &= M_{11} \oplus h(M_1||R_c) \\ SK_{ij} &= h(M_1||M_2||R_c||M_{13}||TS_2) \\ M_{14} &= h(SK_{ij}||M_1||R_c||TS_2) \end{aligned}$$

7) SC_i compares M_{12} with M_{14} and if $M_{12} = M_{14}$, the session key SK_{ij} is generated correctly at the patient's site.
8) SC_i generates a time stamp TS_3 and computes $M_{15} = h(SK_{ij}||M_1||M_{13}||TS_3)$ and sends $< M_{15}, TS_3 >$ to the medical server MS_j for further checking of the right session key.
9) After receiving the message $< M_{15}, TS_3 >$ at time TS_{c3}, the server computes $M_{16} = h(SK_{ij}||M_8||R_s||TS_3)$ if $(TS_{c3} - TS_3 < \Delta T)$.
10) MS_j compares M_{16} with M_{15}. If $M_{16} = M_{15}$, the session key is shared between U_i and MS_j successfully. Now, the medical server MS_j may send a message to the patient U_i through the session key SK_{ij}.

C. THE UPDATE PHASE

1) The Password Change Phase

A patient U_i may require to update his/her password. Password change phase requires a successful login of the patient. In our proposed scheme, the registration center $MSRC$ is not to be involved in the password change phase. A patient can update his/her password locally. The detailed steps of the password changing process, are as follows.

1) U_i inputs (UID_i, PW_i) and scans the biometric to extract $BIOM_i$ and inserts the SC_i to SCR for successful login.
2) If U_i fails to log in, the password update process is terminated by the SC_i. Otherwise, the SC_i asks U_i for new password.
3) The U_i enters a new password PW_i^{new}.
4) SC_i computes $PWD_i^{new} = h(UID_i||K||PW_i^{new})$ and subsequently, computes A_j^{new} and P_j^{new} and f_i^{new} using PWD_i^{new} as follows:

$$\begin{aligned} A_j^{new} &= A_j \oplus PWD_i \oplus PWD_i^{new} \\ P_j^{new} &= P_j \oplus PWD_i \oplus PWD_i^{new} \\ f_i^{new} &= h(UID_i||PWD_i^{new}||C_{T_i}) \end{aligned}$$

5) The SC_i removes the $A_j, P_j \& f_i$ and stores $A_j^{new}, P_j^{new} \& f_i^{new}$.

2) The Biometric Template Revocation Phase

In any biometric based security system, the biometric template is required to be updated for better security of the system. The biometric template update procedure is described in the following.

1) The patient U_i captures a new instance of a biometric image through scanner and extracts the unique features from the newly captured biometric image. Say, the feature set is represented by $BIOM_i^*$.
2) The U_i provides UID_i, PW_i along with $BIOM_i^*$ to the terminals and inserts the SC_i to the SCR for successful login.
3) The SC_i computes C'_{T_i} from $BIOM_i^*$ using $f(.)$ and T_{P_i}.
4) After successful login, the patient U_i provides a new transformation parameter $T_{P_i}^{new}$ to the SC_i.
5) The SC_i computes the following: $C_{T_i}^{new} = f(BIOM_i^*, T_{P_i}^{new})$, $LTK_i^{new} = LTK_i \oplus C'_{T_i} \oplus C_{T_i}^{new}$, $f_i^{new} = h(UID_i||PWD_i||C_{T_i}^{new})$.
6) The SC_i replaces LTK_i and f_i with LTK_i^{new} and f_i^{new}, respectively.

TABLE 3: The mutual authentication and key agreement protocol

Patient U_i/SC_i	Medical Server MS_j
	MS_j receives $< M_3, M_4, M_5, TS_1 >$ 1. Check the validity of TS_1, MS_j computes $M_6 = h(SID_j \|\| X_j)$ $M_7 = M_3 \oplus M_6$, $M_8 = h(M_7 \|\| X_j)$ $M_9 = M_4 \oplus M_8$, $M_{10} = h(M_8 \|\| M_9 \|\| TS_1)$ 2.Check if $M_{10} = M_5$ If so, U_i is authenticated MS_j generates R_s and TS_2 3. MS_j computes, $M_{11} = h(M_8 \|\| R_c) \oplus R_s$ $SK_{ij} = h(M_6 \|\| M_8 \|\| M_9 \|\| R_s \|\| TS_2)$ $M_{12} = h(SK_{ij} \|\| M_8 \|\| M_9 \|\| TS_2)$ 5. MS_j sends $< M_{11}, M_{12}, TS_2 >$ to U_i $< M_{11}, M_{12}, TS_2 >$ $\longleftarrow$ (via public channel)
6. Check the validity of TS_2 If $\|TS_{c1} - TS_2\| \leq \Delta T$, computes $M_{13} = M_{11} \oplus h(M_1 \|\| R_c) \oplus R_c$ $SK_{ij} = h(M_1 \|\| M_2 \|\| R_c \|\| M_{13} \|\| TS_2)$ $M_{14} = h(SK_{ij} \|\| M_1 \|\| R_c \|\| TS_2)$ 7. If $M_{12} \neq M_{14}$, SC_i terminates Else U_i authenticates the MS_j $M_{15} = h(SK_{ij} \|\| M_1 \|\| M_{13} \|\| TS_3)$ U_i sends $< M_{15}, TS_3 >$ to MS_j $< M_{15}, TS_3 >$ $\longrightarrow$ (via public channel)	
	8. If $(TS_{c2} - TS_3 < \Delta T)$, MS_j computes $M_{16} = h(SK_{ij} \|\| M_8 \|\| R_s \|\| TS_3)$ If $M_{16} = M_{15}$, SK_{ij} is established

3) The Smart Card Revocation Phase

A patient may need to revoke his/her smart card. The proposed scheme allows the genuine patient to revoke his/her smart card after the verification of the patient's authentication. In this case, the patient sends a request for a new smart card to the MSRC, which checks the message of the patient before issuing a new smart card.

- A patient enters the user id UID_i, password PW_i, imprints his/her biometric $BIOM_i'$ and scans the smart card SC_i through the smart card reader. The SC_i generates C'_{T_i} from the $BIOM_i'$ and computes (K^*, PWD_i', f_i^*).
- If $h(K^*) = h(K)$ and $f_i^* = f_i$, the patient sends UID_i, PWD_i' to the $MSRC$ for a new smart card.
- The $MSRC$ checks the database for the corresponding UID_i. If $h(PWD_i' \|\| X_j) = h(PWD_i \|\| X_j)$, the $MSRC$ stores SID_j, $A_j = h(UID_i \|\| X_j) \oplus PWD_i$, $P_j = h(SID_j \|\| X_j) \oplus PWD_i$ for $j = 1$ to $m + m'$ into the memory of a new smart card SC_i^{new}. Then, the SC_i^{new} is delivered to the patient U_i through a secure channel.
- U_i computes $f_i = h(UID_i \|\| PWD_i' \|\| C_{T_i})$ and stores $\{T_{P_i}, LTK_i, h(K), f_i, f(.), \Psi_{enc}(), \Psi_{dec}()\}$ into SC_i.

IV. FORMAL SECURITY ANALYSIS

In this section, the formal security of the proposed scheme is tested using the ROR model, BAN logic and AVISPA tool simulation.

A. VERIFICATION OF SESSION KEY SECURITY

The ROR model [73], [74] is widely used in the existing authentication-based key agreement protocols [72], [75]–[77] to verify the security of a session-key (SK). The proposed scheme is also applied the ROR model to proof the security of session key.

1) The ROR Model

In our scheme, the participants are the patient U_i and the medical server MS_j. The principal components of the ROR model related to our scheme are given below.

Participants. $\mathcal{I}^u_{U_i}$ and $\mathcal{I}^s_{MS_j}$ are the *oracles* to represent the instances u and s of U_i and MS_j, respectively.

Accepted state. Assuming that the final message is received by an instance $\mathcal{I}^t$ and it enters in an accept state. Then, we call $\mathcal{I}^t$ is an accepted state. Now, all the communication messages (the send and received messages) by the accepted state $\mathcal{I}^t$ are arranged in order and it forms the session identification (sid) for $\mathcal{I}^t$ of the current session.

Partnering. Two instances $\mathcal{I}^u$ and $\mathcal{I}^s$ are known as the partners to each other if they satisfy following three conditions concurrently : 1) both are in accepted state, 2) both share the same sid and they can mutually authenticate each other, and 3) $\mathcal{I}^u$ and $\mathcal{I}^s$ must be mutual partners of each other.

Freshness. The participant $\mathcal{I}^u_{U_i}$ or $\mathcal{I}^s_{MS_j}$ is fresh only when the reveal oracle $Reveal$ is not able to leak the session key SK_{ij} established between the patient U_i and the server MS_j.

Adversary. According to Dolev-Yao (DY) threat model, an adversary $\mathcal{A}$ is capable to intercept, modify and delete few or all messages communicated between the participants. Moreover, CK-adversary model states that an adversary can inject an error to the communicated messages. In ROR model, the adversary may execute the following queries:

$Execute(\mathcal{I}^u, \mathcal{I}^s)$: In ROR model, the adversary $\mathcal{A}$ uses this query to read the intercepted messages during the communication between U_i and MS_j.

$Send(\mathcal{I}^t, M)$: $\mathcal{A}$ can send and receive a message to and from $\mathcal{I}^t$ by executing this active attack.

$Reveal(\mathcal{I}^t)$: . The attacker $\mathcal{A}$ uses $Reveal$ query to leak the session key SK_{ij} established between $\mathcal{I}^t$ and its partner in the current session.

$CorruptSmartCard(\mathcal{I}^u_{U_i})$: Assume that the smart card SC_i is with an attacker $\mathcal{A}$. An attacker can apply the power analysis attack [10], [11] $\mathcal{A}$ on SC_i and can reveal all the secret information from SC_i.

$Test(\mathcal{I}^t)$: An unbiased coin is flipped in this query and its output is used as a decider for the game. Say, $\mathcal{A}$ executes $Test(\mathcal{I}^t)$ query. For a fresh session key SK_{ij} established between U_i and MS_j, $\mathcal{I}^t$ returns the session key if $c = 1$ or it returns a random number if $c = 0$. Otherwise, a null value ($\perp$) is returned.

$\mathcal{A}$ can execute $CorruptSmartCard(\mathcal{I}^u_{U_i})$ queries for a limited number of times. However, there is no restriction for $\mathcal{A}$ on the execution of $Test(\mathcal{I}^t)$ queries.

Random oracle. We model the hash function $h(\cdot)$ as a random oracle, say $\mathcal{H}$. We assume that the $h(\cdot)$ is publicly available.

Definition 1 (Semantic security): According to the semantic security, the session key SK_{ij} is not distinguishable from a random number. $\mathcal{A}$ executes $Test(\mathcal{I}^t)$ query and check the consistency of the guessed bit c' against the bit c of the session key. Assume that the probability of winning the game by $\mathcal{A}$ is $Succ$. The advantage of $\mathcal{A}$ to break the security of SK_{ij} of our proposed scheme, say denoted by $\mathcal{P}$ in a polynomial time t is defined by $Adv^{\mathcal{A}}_{\mathcal{P}}(t) = |2.Pr[Succ] - 1|$ $= |2.Pr[c' = c] - 1|$, where $Pr[X_i]$ is the probability of an event X_i.

Definition 2: The proposed protocol is denoted as $\mathcal{P}$ and it is semantically secure if $Adv^{\mathcal{A}}_{\mathcal{P}}$ is only negligibly larger than $max\{C'.q_s^{s'}, q_s(\frac{1}{2^{l_b}}, \varepsilon_{bm})\}$ where $C', s', q_s, l_b, \varepsilon_{bm}$ denote their usual meanings as tabulated in Table 4.

2) Security Proof

The session key security proof is provided in Theorem 1. We have considered the Zipf's law for the attack of password guessing [79]. In this case, when we consider only trawling guessing attacks, advantage of an adversary will be over 0.5 for $q_s = 10^7 or 10^8$ [79], [80]. The advantage of an adversary for targeted guessing attack using user's personal information will be over 0.5 for $q_s \leq 10^6$ [85].

TABLE 4: Symbols used in the real-or-random (ROR) model

Symbol	Meaning
q_H	Total number of hash oracle (H) queries
q_s	Total number of *Send* oracle queries
q_e	Total number of *Execute* oracle queries
l_r, l_b	Length of random number and cancelable biometric template
l_H	Length of hash output string
ε_{bm}	Probability of collision between biometric templates
$\mathcal{D}$	Password space as per Zipf's law [79]
$C'.s'$	Zipf parameter [79]
L_H	List of hash H oracle queries
L_A	List of random oracle outputs
L_T	List of message transcripts between U_i and MS_j

Theorem 1: Let the advantage of a polynomial-time t- adversary $\mathcal{A}$ to break the semantic security of the proposed scheme $\mathcal{P}$ be denoted as $Adv^{\mathcal{A}}_{\mathcal{P}}(t)$. Then,

$$Adv^{\mathcal{A}}_{\mathcal{P}}(t) \leq \frac{q_H^2 + 16q_H}{2^{l_H}} + \frac{(q_s + q_e)^2 + 6q_s}{2^{l_r}} + 2max\{C'.q_s^{s'}, q_s(\frac{1}{2^{l_b}}, \varepsilon_{bm})\}$$

where the meaning of all symbols are given in Table 4.

Proof: The proof is similar to that as presented in [72], [77], [78], [81]. In this proof, we need four games, namely, Gm_0, Gm_1, Gm_2, Gm_3, and Gm_4. We denote the success of an adversary $\mathcal{A}$ as $Succ^{\mathcal{A}}_{Gm_j}$ when $\mathcal{A}$ win the game Gm_j, where $j = 0, 1, 2, 3, 4$. At the same time, advantage of $\mathcal{A}$ for winning Gm_j is denoted and defined by $Adv^{\mathcal{A}}_{Gm_j} = Pr[Succ^{\mathcal{A}}_{Gm_j}]$.

- *Game* Gm_0*:* This game is the actual attack by $\mathcal{A}$ to our scheme $\mathcal{P}$. The game begins when $\mathcal{A}$ chooses bit c. Since the game Gm_0 and the actual protocol $\mathcal{P}$ are basically identical to each other, therefore by definition we have,

$$Adv^{\mathcal{A}}_{\mathcal{P}}(t) = |2.Adv^{\mathcal{A}}_{Gm_0} - 1|. \quad (2)$$

- *Game* Gm_1*:* In this game, $\mathcal{A}$ executes the eavesdropping attack by calling the $Execute$ query. After that, $\mathcal{A}$ executes the $Test$ query once the game is completed. The output of this query is the decider to distinguish the SK_{ij} from any random number. According to the formation of the session key, $\mathcal{A}$ needs the long-term secrets (UID_i, SID_j and X_j) and the short-term secrets (R_c, R_s), to compute the session key accurately. Otherwise, the chance of winning the game Gm_1 is not increased even all the messages Msg_1, Msg_2 and Msg_3 are intercepted. Here, Gm_0 and Gm_1 are essentially indistinguishable. Therefore, we have the following:

$$Adv^{\mathcal{A}}_{Gm_1} = Adv^{\mathcal{A}}_{Gm_0}. \quad (3)$$

- *Game* Gm_2*:* This is an active attack. The $Send$ and $\mathcal{H}$ queries are implemented in this game. The attacker $\mathcal{A}$ intercepts all the messages $Msg_1 = \langle M_3, M_4, M_5, TS_1\rangle$ and $Msg_2 = \langle M_{11}, M_{12}, TS_2\rangle$, $\mathcal{A}$, and $Msg_3 = M_{15}, TS_3$. $\mathcal{A}$ uses the intercepted messages for deriving the session key SK_{ij}. It is found

that Msg_1 and Msg_2 involve the random nonces R_c and R_s. The current time stamps TS_1,TS_2 and TS_3 are also involved in the messages Msg_1, Msg_2 and Msg_3, respectively. Hence, random nonces and current time stamps prevent collision in the messages of different session.
Therefore, the game Gm_2 is identical with the game Gm_1 without the involvement of the $Send$ and $\mathcal{H}$ queries. Then, we have the following result:

$$|Adv^{\mathcal{A}}_{Gm_2} - Adv^{\mathcal{A}}_{Gm_1}| \leq \frac{(q_s+q_e)^2}{2^{l_r+1}} + \frac{q_H^2}{2^{l_H+1}}. \quad (4)$$

- *Game Gm_3:* In this game, $\mathcal{A}$ executes $Send(MS_j, Msg_1)$, $Send(U_i, Msg_2)$ and $Send(MS_j, Msg_3)$ queries to win the game. This results in the collision probality at most $\frac{(3q_H+4q_H+q_H)}{2^{l_H}} = \frac{8q_H}{2^{l_H}}$. Accordingly, due to transcript of three messages, collision probability is up to $\frac{3q_s}{2^{l}_r}$. As a whole, we get,

$$|Adv^{\mathcal{A}}_{Gm_3} - Adv^{\mathcal{A}}_{Gm_2}| \leq \frac{3q_s}{2^{l_r}} + \frac{8q_H}{2^{l_H}}. \quad (5)$$

- *Game Gm_4:* The adversary $\mathcal{A}$ plays this game to simulate the $CorruptSmartCard$ query and extracts the secret credentials $\{< SID_j, A_j, P_j > |1 \leq j \leq m+m'), h(.), T_{P_i}, LTK_i, h(K), f_i, f(.), \Psi_{enc}(.), \Psi_{dec}(.)\}$ stored into SC_i, where $LTK_i = K_{CW} \oplus C_{T_i}$, $f_i = h(UID_i||PWD_i||C_{T_i})$, $A_j = h(UID_i||X_j) \oplus PWD_i$, $P_j = h(SID_j||X_j) \oplus PWD_i$ for $1 \leq j \leq (m+m')$. The adversary is not able to extract the biometric template C_{T_i} and the password PW_i of the user id UID_i. The maximum probability to guess the biometric template is upto $max\{q_s(\frac{1}{2^{l_b}}, \varepsilon_{bm})\}$ [81]. The guessing of password has a probability upto $C'.q_s^{s'}$ [79]. Therefore, the game Gm_4 and Gm_3 are identical without the guessing attacks on biometric and password. Overall, we have,

$$|Adv^{\mathcal{A}}_{Gm_4} - Adv^{\mathcal{A}}_{Gm_3}| \leq max\{C'.q_s^{s'}, q_s(\frac{1}{2^{l_b}}, \varepsilon_{bm})\}. \quad (6)$$

To guess the correct bit c, $\mathcal{A}$ executes all the games with the following advantage

$$Adv^{\mathcal{A}}_{Gm_4} = \frac{1}{2}. \quad (7)$$

Using Eqs. (2), (3) and (6), we get

$$\begin{aligned} Adv^{\mathcal{A}}_{\mathcal{P}}(t) &= 2|Adv^{\mathcal{A}}_{Gm_0} - 1| \\ &= 2|Adv^{\mathcal{A}}_{Gm_1} - 1| \\ &= 2|Adv^{\mathcal{A}}_{Gm_1} - Adv^{\mathcal{A}}_{Gm_4}|. \end{aligned} \quad (8)$$

Applying the triangular inequality, we get

$$\begin{aligned} |Adv^{\mathcal{A}}_{Gm_1} - Adv^{\mathcal{A}}_{Gm_4}| &\leq |Adv^{\mathcal{A}}_{Gm_1} - Adv^{\mathcal{A}}_{Gm_2}| \\ &\quad + |Adv^{\mathcal{A}}_{Gm_2} - Adv^{\mathcal{A}}_{Gm_4}| \\ &\leq |Adv^{\mathcal{A}}_{Gm_1} - Adv^{\mathcal{A}}_{Gm_2}| \\ &\quad + |Adv^{\mathcal{A}}_{Gm_2} - Adv^{\mathcal{A}}_{Gm_3}| \\ &\quad + |Adv^{\mathcal{A}}_{Gm_3} - Adv^{\mathcal{A}}_{Gm_4}| \\ &. \end{aligned} \quad (9)$$

Finally, from Eq. (2) to (9), we get the required result:

$$\begin{aligned} Adv^{\mathcal{A}}_{\mathcal{P}}(t) &\leq \frac{q_H^2 + 16q_H}{2^{l_H}} + \frac{(q_s+q_e)^2 + 6q_s}{2^{l_r}} \\ &\quad + 2max\{C'.q_s^{s'}, q_s(\frac{1}{2^{l_b}}, \varepsilon_{bm})\} \end{aligned}$$

B. THE VERIFICATION OF MUTUAL AUTHENTICATION WITH BAN LOGIC

Recently, the BAN logic is used to check the mutual authentication in the existing key agreement protocols [50], [54], [65]. We have assessed the mutual authentication between U_i and MS_j with BAN logic proof.

Notations

We use different notations in our analysis of the BAN logic. The notations are given in Table 5.

TABLE 5: Notations used in BAN logic

Notations	Meanings
$P\| \equiv X$	P believes a statement X
$\sharp X$	The statement X is fresh
$P \lhd X$	P sees the statement X
$P\|\sim X$	P once said the statement X
$P \Rightarrow X$	P has jurisdiction over statement X
$P \overset{K}{\leftrightarrow} Q$	K is a secret shared key between P and Q
$\{X, Y\}_K$	X and Y are encrypted with the key K
$(X, Y)_K$	X and Y are hashed with the key K
$< X >_K$	X is XORed with the key K

Rules

There are mainly five rules in BAN logic. The rules are given below:
Message meaning rules: $\frac{P\|\equiv P \overset{K}{\leftrightarrow} Q, P\lhd\{X\}}{P\|\equiv Q\|\sim X}$ and $\frac{P\|\equiv P \overset{K}{\leftrightarrow} Q, P\lhd <X>}{P\|\equiv Q\|\sim X}$ - *Rule-1*.
Nonce verification rule: $\frac{P\|\equiv \sharp(X), P\|\equiv Q\|\sim X}{P\|\equiv Q\|\equiv X}$ - *Rule-2*.
Jurisdiction rule: $\frac{P\|\equiv Q \Rightarrow X, P\|\equiv Q\|\equiv X}{P\|\equiv X}$ - *Rule-3*.
Freshness-conjuncatenation rule: $\frac{P\|\equiv \sharp(X)}{P\|\equiv \sharp(X,Y)}$ - *Rule-4*.
Belief rule: $\frac{P\|\equiv (X), P\|\equiv (Y)}{P\|\equiv (X,Y)}$ - *Rule-5*.

Assumptions

We assume that the following holds at the beginning of every run of our scheme.

- **A1**: $U_i\| \equiv \sharp(R_c), U_i\| \equiv \sharp(TS_1)$
- **A2**: $MS_j\| \equiv \sharp(R_s), MS_j\| \equiv \sharp(TS_2)$
- **A3**: $U_i\| \equiv U_i \overset{M_1}{\leftrightarrow} MS_j$

- **A4**: $MS_j| \equiv MS_j \overset{M_1}{\leftrightarrow} U_i$
- **A5**: $U_i| \equiv MS_j \Rightarrow U_i \overset{SK_{ij}}{\longleftrightarrow} MS_j$
- **A6**: $MS_j| \equiv U_i \Rightarrow U_i \overset{SK_{ij}}{\longleftrightarrow} MS_j$

Goals

- **g1:** $MS_j| \equiv U_i| \equiv U_i \overset{SK_{ij}}{\longleftrightarrow} MS_j$
- **g2:** $MS_j| \equiv U_i \overset{SK_{ij}}{\longleftrightarrow} MS_j$
- **g3:** $U_i| \equiv MS_j| \equiv U_i \overset{SK_{ij}}{\longleftrightarrow} MS_j$
- **g4:** $U_i| \equiv U_i \overset{SK_{ij}}{\longleftrightarrow} MS_j$

The Idealized Form of Messages

The messages are transmitted through a public channel by either patient U_i or medical server MS_j for authentication and key establishment. The messages are given below.

- **Message(1):** $U_i \rightarrow MS_j$: $< M_3, M_4, M_5, TS_1 >$
- **Message(2):** $MS_j \rightarrow U_i$: $< M_{11}, M_{12}, TS_2 >$
- **Message(3):** $U_i \rightarrow MS_j$: $< M_{15}, TS_3 >$

By combining message 1 and 3, we can write messages as given below:

- **Message(1):** $U_i \rightarrow MS_j$: $< M_3, M_4, M_5, TS_1 >, < M_{15}, TS_3 >$
- **Message(2):** $MS_j \rightarrow U_i$: $< M_{11}, M_{12}, TS_2 >$

The idealized forms of the messages are given below:

- **Message(1):** $MS_j \lhd< M_3, M_4, M_5, TS_1 >, < M_{15}, TS_3 >$, that is,
  m1: $MS_j \lhd< UID_i >_{(SID_j)_{X_j}}, < R_c >_{M_1}, TS_3, (SK_{ij}, R_s, TS_3)_{M_1}$
- **Message(2):** $MS_j \rightarrow U_i$: $< M_{11}, M_{12}, TS_2 >$, that is,
  m2: $U_i \lhd< R_s >_{(R_c)_{M_1}}, TS_2, (U_i \overset{SK_{ij}}{\longleftrightarrow} MS_j, R_c, TS_2)_{M_1}$

Scheme Analysis

1) According to the assumption **A3**, the message **m2** and using the message meaning rule (i.e. *Rule-1*), we obtain: $U_i|| \equiv MS_j| \sim (U_i \overset{SK_{ij}}{\longleftrightarrow} MS_j, R_c, TS_2)$ (Say, **S1**).
2) Using **A1** and **S1**, applying the fresh conjuncatenation (i.e. *Rule-4*) and nonce-verification rules (i.e. *Rule-2*), we obtain: $U_i| \equiv MS_j| \equiv (U_i \overset{SK_{ij}}{\longleftrightarrow} MS_j, R_c, TS_2)$. (Say **S2**).
3) By the belief rule (i.e. *Rule-5*), we obtain the goal **(g3)**: $U_i| \equiv MS_j| \equiv U_i \overset{SK_{ij}}{\longleftrightarrow} MS_j$, from **S2**.
4) Using the assumption **A5** and the goal **g3**, according to the jurisdiction rule (i.e. *Rule-3*), we obtain the goal **g4**: $U_i| \equiv U_i \overset{SK_{ij}}{\longleftrightarrow} MS_j$
5) Considering assumption **A4**, the message-meaning rule (i.e. *Rule-1*) is applied on the message **m1**. We obtain formula **S3** as: $MS_j| \equiv U_i| \sim (U_i \overset{SK_{ij}}{\longleftrightarrow} MS_j, R_s, TS_3)_{M_1}$
6) We obtain a statement **(S4)** using **A2**, **S3**, *Rule-4* and *Rule-2*, that is, **S4**: $MS_j| \equiv U_i| \equiv (U_i \overset{SK_{ij}}{\longleftrightarrow} MS_j, R_s, TS_3)$
7) Applying the belief rule on **S4**, we can conclude as follows: $MS_j| \equiv U_i| \equiv (U_i \overset{SK_{ij}}{\longleftrightarrow} MS_j)$. Therefore, our goal **g1** is proved for our scheme.
8) Considering the truthfulness of the goal **g1** and our assumption **A6**, according to the jurisdiction rule (i.e. *Rule-3*), we obtain $MS_{ij}| \equiv U_i \overset{SK_{ij}}{\longleftrightarrow} MS_j$, which is equivalent to our goal **g2**.

C. FORMAL SECURITY VERIFICATION USING AVISPA

Recently, security of the existing schemes [50], [52], [49], [76], [67], [77], [78] is tested using widely accepted AVISPA tool [58]. Mainly, the OFMC and CL-AtSe back-ends are used to check the security of the existing schemes. AVISPA tool executes the simulated protocol specified by HLPSL language [59]. In the protocol specification, three basic roles for three participants (i.e. the user role U_i, the medical service registration center role $MSRC$ and the medical server role MS_j) are defined. Accordingly, session role, environment role and goals are specified in HLPSL.

In our protocol specification in HLPSL language, we have considered four secrecy goals and five authentication properties for verification of our scheme. These goals and authentication properties are described below.

- **secrecy_of sub1** : KRC is kept secret to the MS_j.
- **secrecy_of sub2**: PWi and K are kept secret to the U_i.
- **secrecy_of sub3**: UIDi is kept secret between U_i and MS_j.
- **secrecy_of sub4**: Xj is kept secret to the MS_j.
- **authentication_on user_msj_ts1**: The server MS_j receives $TS1$ from the patient U_i and MS_j authenticates U_i based on $TS1$.
- **authentication_on user_msj_rc**: The server MS_j authenticates the patient U_i based on Rc received from the message of the patient U_i.
- **authentication_on msj_user_ts2** : The patient U_i receives $TS2$ from the message of the server MS_j and U_i authenticates the server MS_j based on $TS2$.
- **authentication_on msj_user_rs** : The patient U_i also authenticates the server MS_j based on the received Rs from the server MS_j.
- **authentication_on user_msj_ts3**: The server MS_j authenticates the patient U_i based on $TS3$ received from the message of the patient U_i.

The results of AVISPA simulation are given in the Figure 2. The results contain the verification of security of the proposed scheme under OFMC and CL-AtSe back-ends models. The simulation results show that the depth of search is 7 plies and total number of visited nodes is 100 in OFMC model. Moreover, OFMC backend needs 0.28 seconds and CL-AtSe backend takes 0.05 seconds to complete the search for attacks. The results of the simulation reported in Fig.2 clearly indicate that the proposed scheme is safe against replay and man-in-the-middle attacks.

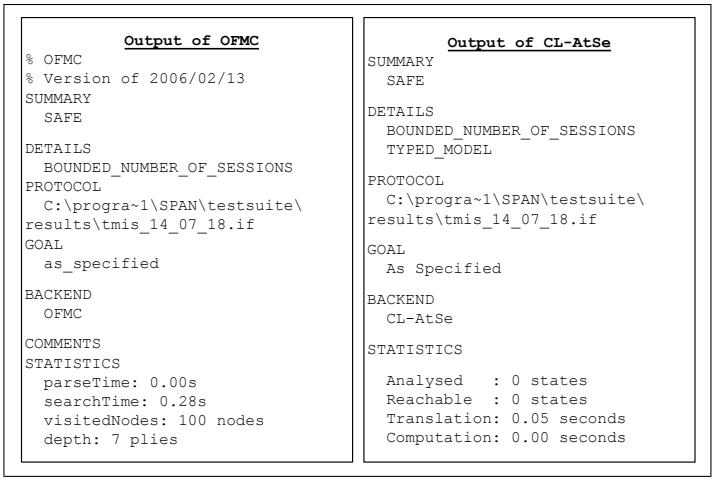


FIGURE 2: The Simulation results of security analysis using the proposed scheme with the AVISPA tool

V. INFORMAL SECURITY ANALYSIS

The informal security analysis is used in the existing key agreement schemes [50], [49], [1], [54], [56], [66], [64], [65], [67], [78]. In this section, we have discussed the security strength of our proposed scheme against different known attacks. The security features of other existing schemes are compared with the proposed scheme.

A. USER ANONYMITY

The user id of a patient is protected under the security of either the biometric data of the patient ($f_i = h(UID_i||PWD_i||C_{T_i})$), or the secret key of the medical server ($A_j, P_j, M_3 = UID_i \oplus M_2 = UID_i \oplus h(SID_j||X_j)$). To know the UID_i from the data stored in the smart card, an adversary should know the password PW_i and the secret key K of a patient U_i. The secret key K is locked with the cancelable biometric template C_{T_i} of U_i. On the other side, only a registered server MS_j knows the secret key of the server. Therefore, only the genuine server may compute the user identity. Say, the server S_j knows the secret key X_j. The message M_2 can be generated by MS_j as $M_2 = h(SID_j||X_j)$. Therefore, after receiving the message from patient U_i, the medical server MS_j computes patient id UID_i from M_3 as $UID_i = M_3 \oplus M_2$. However, in [1], [32], user anonymity is not satisfied.

B. PRIVILEGED-INSIDER ATTACKS

A patient sends $PWD_i = h(UID_i||K||PW_i)$ to the $MSRC$ in the registration phase. An insider user of the trusted $MSRC$ may behave like an attacker $\mathcal{A}$ and the registration message of U_i can be recorded by $\mathcal{A}$ during registration of the patient U_i. Furthermore, we assume that $\mathcal{A}$ can access all secret information of SC_i. In the proposed scheme, deriving the PW_i from PWD_i without exact knowledge of the key K is a hard problem. Therefore, a privileged insider cannot pretend the patient U_i to log into the medical server because the attacker does not know PW_i. Whereas, the schemes [2], [47], [49] do not resist insider attacks.

C. OFF-LINE PASSWORD GUESSING ATTACKS

An attacker $\mathcal{A}$ may target the SC_i to obtain the password from $f_i = h(UID_i||PWD_i||C_{T_i})$. However, $\mathcal{A}$ needs to know UID_i, the K, and the C_{T_i} to know PW_i from f_i. Again, it is hard to know the biometric template C_{T_i}, the secret key K and the user id UID_i of a patient U_i to guess the password PW_i by the $\mathcal{A}$. However, in case of Arshad and Nikooghadam's scheme [33], it is possible to guess the password off-line.

D. IMPERSONATION ATTACKS

There are two types of impersonation attacks, namely, the user and the server impersonation attacks.

- *User impersonation attacks:* An attacker $\mathcal{A}$ may try to convince a medical server on behalf of a registered patient U_i. Here, $\mathcal{A}$ needs to generate a random nonce $R_c^{\mathcal{A}}$ and a current time stamp $TS_1^{\mathcal{A}}$ to compute a login message. Then, $\mathcal{A}$ may try to compute $M_1 = h(UID_i||X_j)$, $M_2 = h(SID_j||X_j)$, $M_3 = UID_i \oplus M_2$, $M_4' = M_1 \oplus R_c^{\mathcal{A}}$, $M_5' = h(M_1||R_c^{\mathcal{A}}||TS_1^{\mathcal{A}})$ in order to generate a valid login message $< M_3, M_4', M_5', TS_1^{\mathcal{A}} >$. However, $\mathcal{A}$ needs to know the long-term secrets UID_i, SID_j and X_j to impersonate a user with a valid login message. Therefore, the user impersonation attack is prevented in our proposed scheme.
- *Server impersonation attacks:* An attacker $\mathcal{A}$ may try to send a message to U_i on behalf of MS_j. To compute the response message, $\mathcal{A}$ generates a random nonce $R_s^{\mathcal{A}}$, a current time stamp $TS_2^{\mathcal{A}}$ and attempts to compute $M_{11} = h(h(UID_i||X_j)||R_c') \oplus R_s^{\mathcal{A}}$, $M_{12} = h(SK_{ij}||h(UID_i||X_j)||R_c'||TS_2^{\mathcal{A}})$ in order to compute a valid response message. In the proposed scheme, an attacker $\mathcal{A}$ is not capable to compute the message without the short-term secret credential (R_c) and long-term credentials (UID_i, SID_j and X_j). It means that our proposed scheme is protected from the server impersonation attacks.

Some existing schemes [1], [33], [61], [68] are vulnerable to the impersonation attacks.

E. MUTUAL AUTHENTICATION

The server validates the time stamp TS_1 and checks whether M_5 is equal to M_{10}. Any legitimate server can be authenticated by extracting the R_c from the login request message. On the other hand, only a legal patient can extract the nonce of the server R_s, that is, the patient is authenticated here. Similarly, only the genuine server can generate the message M_{10} and can extract the nonce R_c of a legal patient. In this way, the mutual authentication between the patient and the medical server is achieved in the proposed scheme. However, some existing schemes [1], [60], [68] are failed to achieve this security function.

F. REPLAY ATTACKS

The proposed scheme uses the current time stamp and randomly generated nonce in every session to prevent the replay attacks. Say, an adversary, $\mathcal{A}$ intercepts messages ($< M_3, M_4, M_5, TS_1 >, < M_{11}, M_{12}, TS_2 >, < M_{15}, TS_3 >$) of the login, authentication and key agreement procedures. If $\mathcal{A}$ replays an old message by resending to the server or the patient, the server or the patient will detect the attack immediately when the freshness of the time stamps will be verified. Chuang-Chen's scheme [1] and Mishra *et al.*'s scheme [48] are failed to resist replay attacks.

G. MAN-IN-THE-MIDDLE ATTACK PROTECTION

In this attack, an adversary $\mathcal{A}$ pretends himself as a medical server to a patient U_i and as a patient to a medical server MS_j. $\mathcal{A}$ intercepts a login message $< M_3, M_4, M_5, TS_1 >$ from U_i and attempt to generate another login message, say $< M_3', M_4', M_5', TS_1^m >$ for the server MS_j. The adversary $\mathcal{A}$ computes the R_c^m randomly and generates a time stamp TS_1^m to compute a login message. To compute $M_3' = UID_i \oplus h(SID_j||X_j)$, $M_4' = h(UID_||X_j) \oplus R_c^m$, $M_5' = h(h(UID_|||X_j)||R_c^m||TS_1^m)$, $\mathcal{A}$ needs to know the long-term secrets UID_i, SID_i and X_j. Moreover, $\mathcal{A}$ can not compute the genuine nonce R_c of U_i without the knowledge about the long-term secret credential X_j. Hence, the proposed scheme is able to resist the man-in-the-middle attacks. However, Lu *et al.*'s scheme [61] is prone to Man-in-the-Middle attacks.

H. NO ENCRYPTION/DECRYPTION

In our scheme, we do not use any symmetric or asymmetric encryption but only the cryptographic hash function $h(.)$. The cryptographic one way hash function is irreversible and it demands less execution time with respect to encryption/decryption algorithms. Therefore, our proposed scheme is efficient. However, Amin and Biswas in 2015 [49], Irshad *et al.* [66] in 2017 and Chaudhry *et al.* [64] in 2017 used encryption in their schemes.

I. FAST ERROR DETECTION

In the proposed scheme, the SC_i of a legal patient U_i verifies the credentials of a patient. The patient U_i computes $C_{T_i}^* = f(BIOM_i^*, T_{P_i})$, $K^* = \Psi_{dec}(LTK_i \oplus C_{T_i}^*)$. If $h(K^*) \neq h(K)$, SC_i terminates the session in the very beginning of the session initiation. Therefore, our scheme is able to detect unauthorized patients immediately to avoid extra computation and communication costs. A medical server MS_j checks whether $M_{10} = M_5$. If it fails the check, the session is terminated by the server. This way, our scheme achieves the early error detection property.

J. STOLEN SMART CARD ATTACKS

We assume that a smart card SC_i is stolen by an adversary $\mathcal{A}$ and he/she can extract all stored information $\{< SID_j, A_j, P_j > |1 \leq j \leq m + m'), h(.), T_{P_i}, LTK_i, h(K), f_i, f(.), \Psi_{enc}(.), \Psi_{dec}(.)\}$ from the SC_i using power analysis attacks [10], [11]. Here, $LTK_i = K_{CW} \oplus C_{T_i}$, $PWD_i = h(UID_i||K||PW_i)$, $A_j = h(UID_i||X_j) \oplus PWD_i$, $P_j = h(SID_j||X_j) \oplus PWD_i$, for $1 \leq j \leq m + m'$, $f_i = h(UID_i||PWD_i||C_{T_i})$. Now, the attacker may try to compute the long-term secret from the extracted information of the smart card. However, it is a hard problem to reveal any information from the hash values. Therefore, the smart card stolen attacks is avoided in our scheme.

K. PHISHING ATTACKS

Phishing is a type of attack in which an authentic user tries to masquerade any other genuine user to steal his/her important data. In the proposed approach, if any registered user attempts to compromise the protocol through a phishing attack, he/she will not be able to hide his/her identity. Hence, the impersonation attack is not possible. Furthermore, if an attacker tries to compute the login message (such as M3, M4, M5, TSi), he/she needs the complete knowledge of UIDi, K, PWi, Aj, Pj. In fact, for an attacker without the necessary knowledge, it is impossible to compute a valid login message of a registered patient. Any invalid message will be detected at the server side and the login request will be rejected. Therefore, the server will not send any information to the attacker without proper authentication.

L. MAN-AT-THE-END ATTACKS

Man-at-the-end (MATE) attacks can take place in several forms if the adversary has physical and authorized access to the attack target. Suppose the adversary has access to the smart card, the data in the smart card is still protected in the sense that it needs the genuine biometric data and other credentials like the password to retrieve the information of the smart card owner. We further assume that with the sufficient expertise and skills, the adversary may compromise all the information stored in the card. Side channel attacks and power analysis attacks can help the adversary to reveal the information stored in a smart card. Nevertheless, the adversary will not be able to extract user?s biometric, key and password

from $(SID_j, A_j, P_j, TP_i, LTK_i, h(K))$. Only the genuine cancelable template of the smart card owner can unlock the secret key K from LTK_i. Hence, the proposed approach is secured against MATE. Moreover, if an attacker accesses the database of a medical server where $h(PWD_i||K_{RC})$ and patient's ID UID_i is stored, then from this information, the adversary will not be able to retrieve anything to compromise the actual information.

M. EASY BIOMETRIC TEMPLATE REVOCATION

In this scheme, the biometric data of the patient is easy to revoke if required. The transformation parameter needs to be changed to generate a new cancelable biometric template. The patient can randomly choose a new transformation parameter. Moreover, the privacy of the biometric identity of the patient is preserved in our scheme using the cancelable transformation of the biometric data. However, Wang *et al.* [68], Irshad *et al.* [66] and Siddiqui *et al.* [83] did not include the biometric template revocation phase.

N. EPHEMERAL SECRET LEAKAGE (ESL) ATTACKS

In this attack, an adversary $\mathcal{A}$ may try to compute a session key (SK_{ij}) with partial knowledge about the secret credentials. The SK_{ij} is computed as $SK_{ij} = h(M_6||M_8||M_9||R_s||TS_2) = h(M_1||M_2||R_c||M_{13}||TS_2)$ $(= SK'_{ij})$. In this scheme, the long-term secrets are UID_i, SID_i and X_j. Similarly, there are two short-term secrets R_c and R_s. Say, an adversary $\mathcal{A}$ knows R_c and R_s. In this case, $\mathcal{A}$ needs to know the secrets UID_i, SID_i and X_j to compute the session key SK_{ij}. Again, we assume that the adversary $\mathcal{A}$ knows the secrets UID_i, SID_i and X_j. In this case, the adversary $\mathcal{A}$ needs to know the secrets R_c and R_s, to construct the session key SK_{ij}.

Therefore, an adversary $\mathcal{A}$ can compute the SK_{ij} successfully, when all the secret credentials of U_i are known to him. Hence, the proposed scheme resists the ESL attacks even under the assumption of the CK-adversary model. Moreover, the complete knowledge of a particular session key SK_{ij}^{known} does not help the attacker to compromise any other session key. There is no similarity between two different session keys, because short-term secret credentials are changed in every session. This means that the forward and backward secrecy of the session key is achieved in our proposed scheme. Furthermore, an attacker $\mathcal{A}$ by compromising a session does not affect other sessions. The ESL attack is opposed in our scheme.

Finally, we consider different known attacks and compare the proposed scheme with the related existing schemes. The comparison is presented in Table 6. According to the informal security analysis, it has been observed that our proposed protocol resists all the known attacks.

VI. PERFORMANCE COMPARISONS

In this section, we consider the recent existing schemes related to our method. The performance of the proposed scheme is compared with the existing ones [1], [48], [49], [60], [61], [68], [64], [65], [67], [66], [78] with respect to their time complexities, computation costs and communication cost.

In our scheme, the password is protected by hash function under the security of the user-specified secret key K. This secret key is locked by the patient's biometric data. It is required to extract the K from a smart card using unlock operation with the help of the genuine biometric data. We consider that the time taken for unlocking K from the smart card is T_{fcs} and time taken by the hash function is represented by T_h. We measure the total time taken by a scheme is the addition of time taken for the login and time taken for the authentication. The comparison is shown in Table 7. In this table, some other notations are used to represent execution times of different functions such as, T_{fe} : the execution time for a fuzzy extractor function; T_{spm}: the execution time for symmetric/asymmetric encryption/decryption, T_M: the execution time of the elliptic curve point multiplication, T_H: the execution time of bio-hash function. We assume, $T_h \approx T_H$, $T_{spm} \approx T_{fe} \approx T_{fcs}$. We also assume that $T_h \approx 0.0023$ms, $T_{spm} \approx 2.226$ms and $T_M \approx 0.0046$ ms for execution time evaluation [65], [78]. We also assume that the length of the hash value is 160 bits, the length of a time stamp is 32 bits, the length of a random number is 160 bits, and the size of an elliptic curve point is 320 bits. We also assume that the security of a 1024-bit public key crypto-system is equivalent to 160-bit ECC. The computation time and the communication cost of each scheme are presented in the fifth and sixth columns of Table 7.

In comparison, the communication cost of our scheme is lower than the other schemes except [1], [64], [78]. However, Chuang-Chen's scheme [1] does not satisfy user anonymity and is vulnerable to server spoofing and Denial-of-Service (DoS) attacks. According to the analysis of Qi-Chen's scheme [71] in 2018, Chaudhry *et al.*'s scheme [64] is not fit for a multi-server environment and fails to resist the Denial-of-Service attacks (DoS). Chaudhry *et al.*'s scheme does not provide the perfect forward secrecy. Barman *et al.*' scheme does not provide a secure smart card revocation process and it takes more time for the login and authentication procedures. Therefore, our scheme is more efficient than the existing ones with respect to the computation cost and security functions.

VII. CONCLUSION

This work provides sufficient security measure to the sensitive information of the patients using a biometric-based authentication scheme on a multi-server environment. In our scheme, the fuzzy commitment scheme and the error correction technique are used to handle the noise of the biometric. The security of our scheme is verified with the BAN logic, the Real-Or-Random Oracle and the AVISPA tool. The highly sensitive biometric data is stored neither in the registration center nor in the medical server. The patient even does not need to share biometric data with the medical server. The fast error detection property of the proposed scheme helps to

TABLE 6: Comparison with respect to security features

	[1]	[48]	[49]	[60]	[61]	[68]	[64]	[65]	[67]	[66]	[78]	Our
SP1	×	√	√	×	×	×	√	√	√	√	√	√
SP2	√	√	√	√	√	√	√	√	√	√	√	√
SP3	×	×	√	√	√	√	√	√	√	√	√	√
SP4	√	√	√	×	√	×	√	√	×	√	×	√
SP5	√	√	√	√	√	√	√	√	√	√	√	√
SP6	×	√	√	√	√	√	√	√	√	√	√	√
SP7	×	√	√	√	×	×	√	√	√	√	√	√
SP8	×	×	√	×	√	√	×	√	√	-	√	√
SP9	×	×	√	√	×	√	×	√	√	√	√	√
SP10	×	√	√	×	√	×	√	√	√	√	√	√
SP11	×	×	×	×	×	√	×	√	×	×	×	√

SP1: User anonymity; SP2: Three-factor security; SP3: Resistance to replay attacks; SP4: Resistance to insider attacks; SP5: Resistance to off-line password guessing attacks; SP6: Resistance to stolen smart card attacks; SP7: Resistance to user impersonation attacks; SP8: Resistance to Denial-of-Service attacks; SP9: Perfect forward secrecy; SP10: Mutual authentication; SP11: Secure smart card revocation; √: a scheme preserves the security property (SP); ×: a scheme does not preserve the security property.

TABLE 7: Performance (computation and communication costs) comparisons with existing work

Schemes	Login phase	Authentication phase	Total	Computation time (in milliseconds)	Communication cost (inb bits)
Chuang and Chen, 2014 [1]	$4T_h$	$12T_h$	$16T_h$	0.0368	1024
Mishra *et al.* 2014 [48]	$7T_h$	$11T_h$	$18T_h$	0.039	1280
Amin and Biswas, 2015 [49]	$5T_h$	$14T_h$	$19T_h$	0.0437	1980
Lin *et al.* 2015 [60]	$5T_h + T_{spm}$	$10T_h + 4T_M + 5T_{spm}$	$15T_h + 4T_M + 6T_{spm}$	8.945	2528
Lu *et al.* 2015 [61]	$5T_h$	$13T_h$	$18T_h$	0.036	1216
Wang *et al.* 2016 [68]	$4T_h$	$11T_h$	$15T_h$	0.032	1472
Chaudhry *et al.* 2017 [64]	$5T_h$	$7T_h + 2T_{spm}$	$12T_h + 2T_{spm}$	4.4796	1024
Reddy *et al.* 2017 [65]	$6T_h + 1T_M$	$9T_h + 3T_M$	$15T_h + 4T_M$	8.9385	1280
Ali and Pal, 2017 [67]	$7T_h + 1T_{spm}$	$9T_h + T_{spm}$	$16T_h + 2T_{spm}$	4.4888	1664
Irshad *et al.* 2017 [66]	$8T_h$	$13T_h + 2T_{spm}$	$21T_h + 2T_{spm}$	0.0575	1120
Barman *et al.* 2018 [78]	$1T_{fcs} + 7T_h$	$11T_h$	$1T_{fcs} + 18T_h$	2.2674	864
Our	$1T_{fcs} + 3T_h$	$11T_h$	$1T_{fcs} + 14T_h$	2.2582	1116

detect the login failure in an early stage. The performance analysis shows that our scheme is more efficient than the existing schemes with respect to cost and security.

REFERENCES

[1] Chuang, Ming-Chin, and Meng Chang Chen. "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics." *Expert Systems with Applications* 41.4 (2014): 1411-1418

[2] Yoon, Eun-Jun and Yoo, Kee-Young,"Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem", *The Journal of Supercomputing*. 63(1): 235-255, 2013.

[3] Khan M.K., Kumari S., Gupta M.K., More efficient key-hash based fingerprint remote authentication scheme using mobile device. *Computing* 2014: 96(9):793-816.

[4] J.L. Tsai, "Efficient multi-server authentication scheme based on one-way hash function without verification table," *Computers & Security,* 27 (3-4) (2008), pp. 115-121.

[5] Juels, A. and Wattenberg, M. "A fuzzy commitment scheme," in Proc. ACM Conf. Computer and Communications Security (CCS), 1999, pp. 28-36.

[6] Hao, F., Anderson, R., and Daugman, J.,"Combining Crypto with Biometrics Effectively," IEEE Transactions on Computers, vol. 55, no. 9, pp. 1081-1088, 2006.

[7] S.S. Agaian, Hadamard Matrix and Their Applications. Springer Verlag, 1985.

[8] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes. North Holland, 1991.

[9] C. T. Li, C. C. Lee, H. H. Chen, M. J. Syu and C. C. Wang, "Cryptanalysis of an anonymous multi-server authenticated key agreement scheme using smart cards and biometrics," 2015 International Conference on Information Networking (ICOIN), Cambodia, 2015, pp. 498-502. doi: 10.1109/ICOIN.2015.7057955

[10] Kocher P., Jaffe J., Jun B. Differential power analysis. In: Advances in Cryptology- CRYPTO99. Springer; 1999. p. 388-397.

[11] Messerges, T.S., Dabbish, E. A., and Sloan, R. H. (2002) Examining smart-card security under the threat of power analysis attacks, *IEEE Transactions on Computers*, Vol. 51, No. 5, pp. 541-552.

[12] D. Dolev and A. Yao, "On the security of public key protocols," IEEE Trans. Inform. Theory, vol. 29, no. 2, pp. 198-208, 1983.

[13] Lamport L., Password Authentication with Insecure Communication, *Commun. ACM*, 1981, vol.24, No. 11, pp. 770-772, doi = 10.1145/358790.358797

[14] Yeh H-L.,Chen T-H.,Hu K-J., Shih W-K., Robust elliptic curve cryptography-based three factor user authentication providing privacy of biometric data. *IET Inform Secur* 2013, 7(3),247-252.

[15] Li, S. H.,Wang, C. Y., Lu,W. H., Lin, Y. Y., and Yen, D. C., Design and implementation of a telecare information platform. *J. Med. Syst.* 36(3):1629-1650, 2012. doi:10.1007/s10916-010-9625-6.

[16] Panchal, G., Samanta, D. & Barman, S. "Biometric-based cryptography for digital content protection without any key storage", Multimed Tools Appl (2017). https://doi.org/10.1007/s11042-017-4528-x

[17] Gritzalis, S., Lambrinoudakis, C., Lekkas, D., and Deftereos, S., Technical guidelines for enhancing privacy and data protection in modern electronic medical environments. *IEEE Trans. Inf. Technol. Biomed.* 9(3):413-423, 2005.

[18] Lambrinoudakis, C., and Gritzalis, S., Managing medical and insurance information through a smart-card-based information system. *J. Med. Syst.* 24(4):213-234, 2000.

[19] Ratha, N. K., Chikkerur, S., Connell, J. H., and Bolle, R. M., "Generating Cancelable Fingerprint Templates," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 561-572, April 2007.

[20] Subhas Barman, Samiran Chattopadhyay, Debasis Samanta, Gaurang Panchal, "A novel secure key-exchange protocol using biometrics of the sender and receiver," Computers & Electrical Engineering, Volume 64, 2017,Pages 65-82.

[21] Liu, J.-Y., Zhou, A.-M., & Gao, M.-X. A new mutual authentication scheme based on nonce and smart cards. *Computer Communications,* 31(10), 2205-2209, 2008.

[22] Xu, X., Zhu, P., Wen, Q., Jin, Z., Zhang, H., & He, L. A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems. *J. Med. Syst.,* 38(1), 1-7, 2014.

[23] Wu, Z.-Y., Lee, Y.-C., Lai, F., Lee, H.-C., & Chung, Y. (2012). A secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(3), 1529–71535, 2012

[24] He, D., Jianhua, C., & Rui, Z. (2012). A more secure authentication scheme for telecare medicine information systems. *Journal of Medical Systems*, 36(3), 1989-1995.

[25] Zhu, Z. (2012). An efficient authentication scheme for telecare medicine information systems. *Journal of Medical Systems,* 36(6), 3833-3838, 2012.

[26] Das, M. L., Saxena, A., & Gulati, V. P. (2004). A dynamic id-based remote user authentication scheme. *IEEE Transactions on Consumer Electronics,* 50(2), 629-631.

[27] Hwang, M. S., & Li, L. H. (2000). A new remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics,* 46(1), 28-30. doi:10.1109/30.826377.

[28] Sandirigama, M., Shimizu, A., & Noda, M. T. (2000). Simple and secure password authentication protocol(sas). *IEICE Transactions on Communications,* E83(B6), 1363-1365.

[29] Arshad, H., & Nikooghadam, M. (2014). An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC. *Multimedia Tools and Applications.* doi:10.1007/s11042-014-2282-x.

[30] Guo, D., Wen, Q., Li, W., Zhang, H., & Jin, Z. (2015). An improved biometrics-based authentication scheme for telecare medical information systems. *Journal of Medical Systems,* 39(3), 1-10, 2015.

[31] Li, C. T., & Hwang, M. S. (2010). An efficient biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications,* 33, 1-5.

[32] Awasthi, A. K., & Srivastava, K. (2013). A biometric authentication scheme for telecare medicine information systems with nonce. *Journal of Medical Systems.* doi:10.1007/s10916-013-9964-1.

[33] Arshad, H., & Nikooghadam, M. (2014). Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems. *J. Med. Syst.* 38(12):1-12, 2014.

[34] Srivastava, K., Awasthi, A. K., Kaul, S. D., & Mittal, R. C. (2015). A hash based mutual RFID tag authentication protocol in telecare medicine information system. *J. Med. Syst.* doi:10.1007/s10916-014-0153-7.

[35] Wei, J., Hu, X., and Liu, W., An improved authentication scheme for telecare medicine information systems. J. Med. Syst. 36(6):3597-3604, 2012.

[36] Pu, Q., Wang, J., and Zhao, R., Strong authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(4):2609-2619, 2012. doi:10.1007/s10916-011-9735-9.

[37] Chen, H. M., Lo, J. W., and Yeh, C. K., An efficient and secure dynamic id-based authentication scheme for telecare medical information systems. *J. Med. Syst.* 36(6):3907-3915, 2012. doi:10.1007/s10916-012-9862-y.

[38] Jiang, Q., Ma, J., Ma, Z., and Li, G., A privacy enhanced authentication scheme for telecare medical information systems. *J. Med. Syst.* 37:9897, 2013. doi:10.1007/s10916-012-9897-0.

[39] Kumari, Saru and Khan, Muhammad Khurram and Kumar, Rahul,"Cryptanalysis and Improvement of 'A Privacy Enhanced Scheme for Telecare Medical Information Systems'", *J. Med. Syst.,* 2013, 37(4),pp.1-11.

[40] Kim, K.W., and Lee, J.D., On the security of two remote user authentication schemes for telecare medical information systems. *J. Med. Syst.* 38(5):1-11, 2014.

[41] Giri, D., Maitra, T., Amin, R., An efficient and robust RSA-based remote user authentication for telecare medical information systems. *J. Med. Syst.* 39(1):1-9, 2015.

[42] Maitra, T., and Giri, D., An efficient biometric and passwordbased remote user authentication using smart card for telecare medical information systems in multi-server environment. J. Med. Syst. 38(12):1-19, 2014.

[43] Islam, S.K.H., and Khan, M.K., Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems. *J. Med. Syst.* 38(10):1-16, 2014.

[44] Li, X., Xiong, Y., Ma, J., Wang, W., An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards. *J. Netw. Comput. Appl.* 35(2):763-769, 2012.

[45] Sood, S.K., Sarje, A.K., Singh, K., A secure dynamic identity based authentication protocol for multi-server architecture. *J. Netw. Comput. Appl.* 34(2):609-618, 2011.

[46] Wang, B., and Ma, M., A smart card based efficient and secured multi-server authentication scheme. *Wirel. Pers. Commun.* 68(2):361-378, 2013.

[47] Yang, D., and Yang, B., A biometric password-based multi-server authentication scheme with smart card. In: 2010 International Conference on Computer Design and Applications (ICCDA), Vol. 5, pp. 554-559: IEEE, 2010.

[48] Mishra, D., Das, A.K., Mukhopadhyay, S., A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards. *Expert Syst. Appl.* 41(18):8129-8143, 2014.

[49] Amin, R., and Biswas, G.P., A Novel User Authentication and Key Agreement Protocol for Accessing Multi-Medical Server Usable in TMIS. *J. Med. Syst.* 39(3):1-17, 2015.

[50] Das, A. K.,Odelu, V. and Goswami, A., "A Secure and Robust User Authenticated Key Agreement Scheme for Hierarchical Multi-medical Server Environment in TMIS", *J. Med. Syst.*, 39(9),1-24, doi=10.1007/s10916-015-0276-5, 2015.

[51] Chatterjee, S., and Das, A.K., An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks. *Secur. Commun. Netw.* 8(9):1752-1771, 2015.

[52] Das, A.K., A secure user anonymity-preserving three-factor remote user authentication scheme for the telecare medicine information systems. J. Med. Syst. 39(3):1-20, 2015.

[53] Burrows, M., Abadi, M., & Needham, R. A logic of authentication. *ACM Transactions on Computer Systems*, 8(1), 18-36, 1990.

[54] Mir, Omid and Morteza Nikooghadam, A Secure Biometrics Based Authentication with Key Agreement Scheme in Telemedicine Networks for E-Health Services, *Wireless Pers Commun*, 83:2439-2461, 2015.

[55] Chuang, Y.-H., and Tseng, Y.-M., An efficient dynamic group key agreement protocol for imbalanced wireless networks. *Int. J. Netw. Manag.* 20(4):167-180, 2010.

[56] Yanrong Lu, Lixiang Li, Haipeng Peng, Yixian Yang, An Enhanced Biometric-Based Authentication Scheme for Telecare Medicine Information Systems Using Elliptic Curve Cryptosystem, J. Med. Syst. (2015) 39: 32, DOI 10.1007/s10916-015-0221-7.

[57] Xue, K., Hong, P., Ma, C., A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture. *J. Comput. Syst. Sci.* 80(1):195-206, 2014.

[58] AVISPA: Automated Validation of Internet Security Protocols and Applications. http://www.avispa-project.org/. Accessed on January 2016

[59] Von Oheimb, D., The high-level protocol specification language hlpsl developed in the eu project avispa, pp. 1-17: Tallinn, 2005.

[60] H. Lin, F.Wen, and C. Du, An improved anonymous multi-server authenticatedkey agreement scheme using smart cards and biometrics, Wireless Pers. Commun., vol. 84, no. 4, pp. 2351-2362, 2015.

[61] 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.

[62] Reddy AG, Das AK, Odelu V, Yoo K-Y (2016) An Enhanced Biometric Based Authentication with Key-Agreement Protocol for Multi-Server Architecture Based on Elliptic Curve Cryptography. PLoS ONE 11(5): e0154308. doi:10.1371/journal.pone.0154308

[63] Truong, TT., Tran, MT., Duong, AD., Echizen, I. Provable Identity Based User Authentication Scheme on ECC in Multi-server Environment, Wireless Pers Commun (2017) 95(3): 2785-2801.

[64] Chaudhry SA, Naqvi H, Khan MK. An enhanced lightweight anonymous biometric based authentication scheme for TMIS. Multimedia Tools and Applications. 2017; 1-22.

[65] Reddy AG, Yoon EJ, Das AK, Odelu V, Yoo KY. Design of Mutually Authenticated Key Agreement Protocol Resistant to Impersonation Attacks for Multi-Server Environment. IEEE Access. 2017; 5: 3622-3639.

[66] Irshad A, Chaudhry SA, Kumari S, Usman M, Mahmood K, Faisal MS. An improved lightweight multiserver authentication scheme. International Journal of Communication Systems. 2017; 30(17), pp.1-19.

[67] Ali, R. & Pal, A.K. Three-Factor-Based Confidentiality-Preserving Remote User Authentication Scheme in Multi-server Environment, Arab J Sci Eng (2017) 42(8): 3655-3672. https://doi.org/10.1007/s13369-017-2665-1

[68] 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.
[69] Yang L, Zheng Z (2018) Cryptanalysis and improvement of a biometrics-based authentication and key agreement scheme for multi-server environments. PLoS ONE 13(3): e0194093. https://doi.org/10.1371/journal.pone.0194093
[70] Zhao Y, Li S, and Jiang L, Secure and Efficient User Authentication Scheme Based on Password and Smart Card for Multiserver Environment, Security and Communication Networks, Volume 2018, https://doi.org/10.1155/2018/9178941
[71] Qi MP, Chen JH. New robust biometrics-based mutual authentication scheme with key agreement using elliptic curve cryptography. Multimedia Tools and Applications. 2018; 1-17.
[72] 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.
[73] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in International Conference on the Theory and Applications of Cryptographic Techniques" Advances in Cryptology (EUROCRYPT 2001). Innsbruck (Tyrol), Austria: Springer, 2001, pp. 453-474.
[74] R. Canetti and H. Krawczyk, "Universally Composable Notions of Key Exchange and Secure Channels," in International Conference on the Theory and Applications of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT 2002), Amsterdam, The Netherlands, 2002, pp. 337-351.
[75] 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 of Things Journal, vol. 5, no. 1, pp. 269-282,Feb 2018.
[76] J. Srinivas, A. K. Das, N. Kumar, and J. Rodrigues, "Cloud centric authentication for wearable healthcare monitoring system," IEEE Transactions on Dependable and Secure Computing, 2018, DOI: 10.1109/TDSC.2018.2828306.
[77] D. Chattaraj, M. Sarma, and A. K. Das, "A new two-server authentication and key agreement protocol for accessing secure cloud services," Computer Networks, vol. 131, pp. 144-164, 2018.
[78] S. Barman, A. K. Das, D. Samanta, S. Chattopadhyay, J. J. P. C. Rodrigues and Y. Park, "Provably Secure Multi-Server Authentication Protocol Using Fuzzy Commitment," in IEEE Access, vol. 6, pp. 38578-38594, 2018. doi: 10.1109/ACCESS.2018.2854798
[79] D. Wang, H. Cheng, P. Wang, X. Huang and G. Jian, "Zipf's Law in Passwords," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 11, pp. 2776-2791, Nov. 2017. doi: 10.1109/TIFS.2017.2721359
[80] J. Bonneau. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In IEEE Symposium on Security and Privacy (S & P'12), pp. 538-552, San Francisco, California, USA, May 2012.
[81] Sandip Roy, Santanu Chatterjee, Ashok Kumar Das, Samiran Chattopadhyay, Neeraj Kumar, and Athanasios V. Vasilakos. On the Design of Provably Secure Lightweight Remote User Authentication Scheme for Mobile Cloud Computing Services," in IEEE Access, Vol. 5, No. 1, pp. 25808-25825, 2017.
[82] P. Tsai, M. K. Khan, J. Pan and B. Liao, "Interactive Artificial Bee Colony Supported Passive Continuous Authentication System," in IEEE Systems Journal, vol. 8, no. 2, pp. 395-405, June 2014. doi: 10.1109/JSYST.2012.2208153
[83] Siddiqui, Z., Abdullah, A.H., Khan, M.K., Alghamdi, A. S., Smart Environment as a Service: Three Factor Cloud Based User Authentication for Telecare Medical Information System, J Med Syst (2014) 38: 9997. https://doi.org/10.1007/s10916-013-9997-5
[84] Adnan Akhunzada, Mehdi Sookhak, Nor Badrul Anuar, Abdullah Gani, Ejaz Ahmed, Muhammad Shiraz, Steven Furnell, Amir Hayat, Muhammad Khurram Khan, Man-At-The-End attacks: Analysis, taxonomy, human aspects, motivation and future directions, Journal of Network and Computer Applications, Volume 48, 2015,Pages 44-57.
[85] D. Wang, Z. Zhang, P. Wang, J. Yan, and X. Huang, "Targeted online password guessing: An underestimated threat," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS), Vienna, Austria, 2016, pp. 1242-1254.

SUBHAS BARMAN received his B.Tech. degree in Computer Science and Engineering from Kalyani University and M.Tech. degree in Information Technology from IIT Kharagpur, India. He is currently pursuing his Ph.D. in Computer Science and Engineering from Jadavpur University, Kolkata, India. His current research interests include biometrics-based network security. He has authored 8 papers in international journals and conferences in the above areas.

HUBERT P. H. SHUM is an Associate Professor (Reader) at Northumbria University, U.K., as well as the Director of Research and Innovation of the Computer and Information Sciences Department. Before this, he worked as a Senior Lecturer at Northumbria University, U.K., a Lecturer in the University of Worcester, U.K., a post-doctoral researcher in RIKEN, Japan, as well as a research assistant in the City University of Hong Kong. He received his Ph.D. degree from the School of Informatics in the University of Edinburgh, U.K. His research interests include computer graphics, computer vision, motion analysis and machine learning.

SAMIRAN CHATTOPADHYAY is currently working as Professor in the Department of Information Technology, Jadavpur University, Kolkata, India. He has received his Ph.D from Jadavpur University, Kolkata, India, and Masters and Bachelors in computer science and engineering from IIT Kharagpur, India. He is having over 25 years of teaching experience at Jadavpur University, 4 years of industry experience, and 12 years of technical consultancy in the reputed industry houses. He has authored over 110 papers in international journals and conferences.

DEBASIS SAMANTA received his Ph.D. degree in Computer Science and Engineering from IIT Kharagpur, India. He holds M.Tech. and B.Tech. degrees both in Computer Science and Engineering from Jadavpur University, Kolkata, India and Calcutta University, India, respectively. Presently, he is an Associate Professor in 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. For detail, please see http://cse.iitkgp.ac.in/~dsamanta/