ITSSAKA-MS: An Improved Three-Factor Symmetric-Key Based Secure AKA Scheme for Multi-Server Environments

ZEESHAN ALI,1 SAJID HUSSAIN,1 RANA HASEEB UR REHMAN,1 ASMAA MUNSHI,2 MISBAH LIAQAT,3 NEERAJ KUMAR,4,5,7 (Senior Member, IEEE), AND SHEHZAD ASHRAF CHAUDHRY6

1Department of Computer Science, International Islamic University Islamabad, Islamabad 44000, Pakistan
2Cybersecurity Department, University of Jeddah, Jeddah 21959, Saudi Arabia
3College of Computing and Information Technology, University of Jeddah, Khulais 21921, Saudi Arabia
4Computer Science and Engineering Department, Thapar Institute of Engineering and Technology, Patiala 147004, India
5Department of Computer Science and Information Engineering, Asia University, Taichung 41354, Taiwan
6Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul 34310, Turkey
7King Abdulaziz University, Jeddah 22231, Saudi Arabia

Corresponding authors: Misbah Liaqat (mhhaseeb@uj.edu.sa) and Shehzad Ashraf Chaudhry (sashraf@gelisim.edu.tr)

ABSTRACT A variety of three-factor smart-card based schemes, specifically designed for telecare medicine information systems (TMIS) are available for remote user authentication. Most of the existing schemes for TMIS are customarily proposed for the single server-based environments and in a single-server environment. Therefore, there is a need for patients to distinctly register and login with each server to employ distinct services, so it escalates the overhead of keeping the cards and memorizing the passwords for the users. Whereas, in a multi-server environment, users only need to register once to resort various services for exploiting the benefits of a multi-server environment. Recently, Barman et al. proposed an authentication scheme for e-healthcare by employing a fuzzy commitment and asserted that the scheme can endure many known attacks. Nevertheless, after careful analysis, this paper presents the shortcoming related to its design. Furthermore, it proves that the scheme of Barman et al. is prone to many attacks including: server impersonation, session-key leakage, user impersonation, secret temporary parameter leakage attacks as well as its lacks user anonymity. Moreover, their scheme has the scalability issue. In order to mitigate the aforementioned issues, this work proposes an amended three-factor symmetric-key based secure authentication and key agreement scheme for multi-server environments (ITSSAKA-MS). The security of ITSSAKA-MS is proved formally under automated tool AVISPA along with a security feature discussion. Although, the proposed scheme requisites additional communication and computation costs. In contrast, the informal and automated formal security analysis indicate that only proposed scheme withstands several known attacks as compared to recent benchmark schemes.

INDEX TERMS Authentication and key-agreement (AKA), AVISPA tool, e-healthcare, fuzzy commitment scheme, multi-server authentication, telecare medicine information system (TMIS).

I. INTRODUCTION

The use of information and communication technologies (ICT) is increasing day by day not only for the entertainment and related leisure purposes rather its’ becoming a part and parcel of daily life. People are now benefitting through a large number of quality services including e-Health/telemedicine, remote surveillance, online shopping, online banking, and online education etc. With the broad availability of the Internet everywhere and with the cheaper mobile devices, telemedicine and the e-Healthcare services are in the reach to the patients, directly despite being in remote areas [1], [2]. Moreover, e-Health can substitute the traditional clinical medical services [3], [4]. By using TMIS, the physician can access and monitor the live medical condition of the patients within no time by using open channel [5]. It becomes very crucial to block an adversary from deducing the patient’s delicate information.
Furthermore, as the adoption of e-Healthcare increases, the need of patient-privacy should be the first priority as all the communication is taking place through public channel [6], [7]. To prevent various threats, an authentication scheme can be implemented to ensure that TMIS is only accessed by legitimate users [8]–[11]. Recently, Wu et al. [12] introduced a two-factor authentication scheme by employing smart-card and password for TMIS. Debiao et al. [13] identified that Wu et al.’s scheme is prone to insider attack, impersonation attack, and the stolen smart-card attack. He et al. designed an other scheme to solve the flaws of [12]. Zhu [14] also introduced RSA-cryptosystem based authentication scheme. Many other researchers [15]–[18] presented various schemes using password and smart-card, which were later proved weak against one or other attack. Recently, in numerous studies, many researchers proposed three-factor authentication schemes to enhance the security and to ensure user privacy by combining ID/password, biometric (e.g. fingerprint, iris) and smart-card [19]–[24]. Furthermore, some other schemes compromised the users privacy by sending the identity of the user over the insecure channel, directly to the server [12]–[14], [25], [26]. Nevertheless, the privacy of the user should be insured in order to keep the identity secret from the illegal users and privacy is now being taken as a part and parcel of authentication schemes [27], [28].

To ensure user privacy/anonymity Pu et al. [29] presented an elliptic curve cryptography (ECC) based authentication scheme, but the computation, communication and storage demand in Pu et al.’s scheme is very high. An authentication based on dynamic ID with performance efficiency was proposed by Chen et al. [30]. After careful cryptanalysis, it is proved by Jiang et al. [31] that Chen et al.’s scheme is unable to ensure user anonymity and presented a scheme to overcome the flaw. In contrast, Kumari et al. [32] found that Jiang et al.’s [31] scheme is prone to password guessing attack, session-key disclosure attack, Denial-of-Service (DoS) attack and user impersonation attack. Kumari et al. [32] presented an enhanced scheme to overcome the before-mentioned attacks. Chang and Chen [33] proposed another three-factor authentication scheme for multi-server environment. However, Lin et al. [34] and Mishra et al. [35] established that Chuang-Chang’s scheme is unsafe towards several attacks like insider attack, Denial-of-Service (DoS) attack, user impersonation attack, server spoofing attack and lacks user anonymity. Another authentication scheme was proposed by Mishra et al. for expert systems. Nevertheless, Wang et al. [36] & Lu et al. [37] proved that Mishra et al.’s scheme is prone to forgery attack. DoS attack, replay attack as well as lacks user anonymity and perfect forward secrecy.

In 2019, Barman et al. [5] presented a three-factor authentication scheme for e-Healthcare in the multi-server environment by employing fuzzy commitment and stated that the scheme can cope with prominent attacks. But, the carefully analysis conducted in this paper exposes several weaknesses of Barman et al.’s scheme. This manuscript depicts that [5] suffers from design faults, and is prone to stolen verifier attack, which leads to session-key leakage, user and server impersonation attack, secret temporary parameters leakage; moreover, the Barman et al.’s scheme works in absence of user anonymity. Therefore, an improved three-factor symmetric-key based secure authentication and key agreement scheme for multi-server environments (ITSSAKA-MS) is proposed in this paper. Rest of the paper presentation is as follows:

The attack model employed in this paper is outlined in Subsection I-A. Review and cryptanalysis of Barman et al.’s scheme is conducted in Section II and Section III, respectively. In Section IV different phases of the proposed ITSSAKA-MS are discussed. The security analysis of the proposed ITSSAKA-MS is performed in Section V. In Section VI performance analysis of the ITSSAKA-MS is furnished and compared with various schemes. Paper is finally concluded in Section VII.

A. ADVERSARIAL MODEL

In this manuscript, the standard adversarial model is taken into account as stated in [38]–[44] where following considerations are assumed as the power of the adversary $U_A$:

1) $U_A$ can listen the messages exchanged through public channel. $U_A$ have the capability to listen, replay, alter, abolish or can send forges messages.

2) $U_A$ can be a dishonest system user or can be an outsider.

3) $U_A$ can extract information stored into his/stolen smart-card by performing power analysis [38], [40] or from leaked data [41].

4) $U_A$ can be a privileged and legitimate insider, which can expose the verifier table stored in the database of the RC [45]–[48].

5) $U_A$ can not steal the private key of the RC.

II. REVIEW OF THE SCHEME OF BARMAN ET AL.

This section presents the review of the scheme of Barman et al. The three phases of the scheme are described in following subsestions:

A. REGISTRATION PROCESS

Registrations of each of the server and patient are explained in following subsestions:

1) SERVER REGISTRATION PROCESS

All the medical servers ($MS_j$) need to register themselves with RC. A $MS_j$ chooses and transmits an identity $SID_j$ to RC. RC computes $W_j = h(SDJ_j||KRC)$, for $j^{th}$ medical server using its secret key $K_{RC}$ and sends $W_j$ to medical server.

2) PATIENT REGISTRATION PROCESS

In order to register with the RC and avail medical services, every patient/user say $U_i$ selects an identity ($PID_i$), password ($PW_i$), transformation-key ($TP_i$) respectively and imprints his/her fingerprint-biometric ($BM_i$). A cancellable template ($CT_j = f(BM_j, TP_j)$) is generated with a $TP_j$ using a transformation function $f(.)$ from the users $BM_i$. Following are the steps involved in the patients registration process:
1) An error encoding technique $\psi_{enc}$ is utilized to alter the arbitrary picked key $K$ into the code-word $K_{CW} = \psi_{enc}(K)$ and saves it into $LTK_i = K_{CW} \oplus C_{T_i}$. 
2) $U_i$ sends a registration request containing $PID_i$, $PWD_i$ to RC, where $PWD_i = h(PID_i|||K_2|||PW_i)$. 
3) Upon receiving registration request from $U_i$, RC calculates $A_j = PWD_i \oplus h(PID_i|||W_j)$ and $P_j = PWD_i \oplus h(SID_i|||W_j)$. 
4) RC saves the variables $(SID_j, A_j, P_j, h(t_i))$ into the $SC_i$ and $(PID_i, h(PWD_i|||W_j))$ into the database. 
5) $U_i$ calculates the $f_i = h(PID_i|||W_j)||C_{T_i}$ and saves $(LTK_i, T_{P_j}, h(K), f_i, f_i, \psi_{dec}(\cdot), \psi_{enc}(\cdot))$ into the smart-card. 

The $SC_i$ finally holds the subsequent parameters $(A_j, SID_j, P_j) \mid (1 \leq j \leq m + m')$, $T_{P_j}, h(K), LTK_i, f_i, h(K), f_i, \psi_{dec}(\cdot), \psi_{enc}(\cdot))$ into the smart-card.

**B. LOGIN AND KEY-ESTABLISHMENT PROCESS**

In this phase $U_i$ gets authenticated and a session key is shared among the $U_i$ and $S_j$ by executing following steps:

1) $U_i$ enters the $SC_i$ and provides the credentials containing $PID_i$, $PW_i$ and biometric $BM^*_i$. Smart-card $SC_i$ computes $C^*_i = f(BM^*_i, T_P)$, using the transformation function $f(\cdot)$. $SC_i$ regenerates the $K^* = \psi_{dec}(LTK_i \oplus C^*_T) = \psi_{dec}(K^*_i \oplus C^*_T)$. $SC_i$ confirms $h(K^*) = h(K)$, if incorrect session terminates, else continues. $SC_i$ picks $R_{rand_1}$, $T_1$ and calculates $PWD^*_i = h(PID_i|||W_j)||C_{T_i}$. $SC_i$ checks whether $f_i = f_i$, if incorrect session terminates, if not, it proceeds. $SC_i$ computes the subsequent: $V_1 = A_j \oplus PWD^*_i = h(PID_i|||W_j)$, $V_2 = P_j \oplus PWD^*_i = h(SID_i|||W_j)$, $V_3 = PID_i \oplus V_2$, $V_4 = V_1 \oplus R_{rand_1}$, $V_5 = h(V_1|||R_{rand_1}|||T_1)$. $SC_i$ finally sends the login request containing $(T_1, V_3, V_4, V_5)$ to $MS_j$. 

2) Upon getting the login message from $U_i$, $MS_j$ confirms the condition $| T_e - T_1 | \leq \Delta T$ to verify the timeliness of the timestamp $T_1$, if true continue else session terminates. $MS_j$ computes $V_6 = h(SID_i|||W_j)$, $V_7 = V_3 \oplus V_6 = PID_i$, $V_8 = h(V_7 \parallel | W_j = h(PID_i \parallel | W_j)$, $V_9 = V_4 \oplus V_8 = R_{rand_1}$, $V_{10} = h(V_8 \parallel | W_9 = h(D_1|||W_j)||R_{rand_1}|||T_1)$. $MS_j$ picks the arbitrary nonce $R_{rand_2}$ and the present timestamp $T_2$ if $V_{10} \oplus V_5$ is true, else terminates the session. $MS_j$ computes $V_{11} = R_{rand_2} \oplus h(V_8|||R_{rand_2} = R_{rand_2} \oplus h(R_{rand_2}|||W_j)||R_{rand_1}$, $SK_{ij} = h(V_6|||V_8|||V_9|||R_{rand_1}|||T_2) = h(h(SID_i ||| W_j) ||| h(PID_i ||| W_j) ||| R_{rand_1} ||| W_j) ||| V_{12} = h(SK_{ij} ||| V_8||| V_9||| T_2) = h(SK_{ij} ||| h(PID_i ||| W_j) ||| R_{rand_1} ||| T_2)$, $MS_j$ transmits the message containing $(T_2, V_{12}, V_{11})$ to $U_i$ via open channel. 

3) $U_i$ validates the condition $| T_e - T_2 | \leq \Delta T$ to verify the validity of the $T_2$, if false session terminates else continues and $U_i$ computes: $V_{13} = h(V_1|||R_{rand_4} \oplus R_{rand_1} \oplus V_{11}, SK_{ij} = h(V_1|||V_2 ||| R_{rand_4} ||| T_2)$, $V_{14} = h(SK_{ij}|||V_1|||R_{rand_1}|||T_2)$. $U_i$ checks the condition $V_{12} \equiv V_{14}$, if false session is terminated. $SC_i$ generates the new timestamp and calculates: $V_{15} = h(SK_{ij}|||V_1|||V_{13}|||T_3)$ and transmits the message containing $(V_{15}, T_3)$ to $MS_j$ at time $T_3$. Upon getting the message from $U_i$, the server calculates $V_{16} = h(SK_{ij}|||V_8|||R_{rand_2}|||T_3)$, if $| T_e - T_3 | \leq \Delta T$. $MS_j$ checks the condition $V_{16} \equiv V_{15}$, if true, session-key $SK_{ij}$ is established among the $MS_j$ and $U_i$, so that they can communicate securely.

**III. CRYPTOANALYSIS OF THE SCHEME OF BARMAN et al.**

In this section, we demonstrate some of the critical weaknesses of the scheme of Barman et al. It is to substantiate here that a privileged insider $U_A$ having access to RC can impersonate as a legitimate $U_i$ and can launch other attacks under the capabilities mentioned in adversarial model presented in Section I-A:

**A. DESIGN FAULTS**

Barman et al.’s scheme suffers from design fault [49], after login user sends the message $(T_1, V_3, V_4, V_5)$ to a medical server ($MS_j$), as it can be observed that the request message does not include the server ($SID_j$) identity/address, while there are $j$’s $1 \leq j \leq m + m'$ servers. Therefore, for moving further, following two are the possibilities:

*Case 1*: The message is broadcasted, so every server receives it and the intended server processes it completely. In such case, each server partly processes the request, which can cause, unnecessary computation on each server and can cause delay in processing other legitimate requests and hence degrade the quality of service.

*Case 2*: Alternatively, the absence of server address/identity in request message can be treated as a typo. In this case, the scheme can complete working normally but has severe security weaknesses, explained in subsequent subsections.

**B. STOLEN VERIFIER AND USER ANONYMITY VIOLATION ATTACK**

After successfully authenticating the $U_i$, $SC_i$ transmits the message $(V_3, V_4, V_5, SID_i, T_1)$ to $MS_j$ considering III-A in Subsection III-A this message also includes servers identity/address. The message sent by $SC_i$ is transferring over the public channel so a legitimate but wicked user ($U_A$) of the system can intercept it and can compute users identity as follow:

1) The $U_A$ extracts the value $P_j$ from his own smart-card through power-analysis [39], [40] and computes $h(SID_i|||W_j)$ as it is the same for all the users by adopting the following procedure:

$$Z_A = P_j = (h(SID_i|||W_j) \oplus PWD_A) \oplus PWD_A \quad (1)$$

$$Z_A = h(SID_i|||W_j) \quad (2)$$
2) The $U_A$ waits for the $U_i$ to initiate a login request consisting of $<V_3, V_4, V_5, SID_j, T_1>$ where:

$$V_3 = PID_i \oplus h(SID_j||W_j)$$  \hspace{1cm} (3)

3) Then $U_A$ computes the following:

$$PID_i = Z_A \oplus V_3$$  \hspace{1cm} (4)

where $PID_i$ is the identity of $U_i$ and stays similar for all sessions, therefore $U_A$ has successfully launched the traceability attack. Also, $SID_j$ and corresponding key $W_j$ are stored in the verifier table on the $RC$. So a privileged insider can access this table [50] and can compute the corresponding $P_j$ to launch the traceability attack.

C. USER IMPERSONATION ATTACK

Let $U_A$ be a legit user of the system and knows the identity of another legal user $U_i$. Following procedure can be adopted by $U_A$ to impersonate as a $U_i$:

1) The $U_A$ fetches $W_j$ corresponding to $SID_j$ from RC’s verifier table [51], picks an arbitrary nonce $R_{rand_1}^A$ and calculates:

$$V_1^A = h(PID_i||W_j)$$  \hspace{1cm} (5)

$$V_2^A = h(SID_j||W_j)$$  \hspace{1cm} (6)

$$V_3^A = PID_i \oplus V_2^A$$  \hspace{1cm} (7)

$$V_4^A = V_1^A \oplus R_{rand_1}^A$$  \hspace{1cm} (8)

2) $U_A$ generates the current timestamp and computes:

$$V_5^A = h(V_1^A||R_{rand_1}^A||T_1^A)$$  \hspace{1cm} (9)

3) Finally, $U_A$ sends the message containing $(V_3^A, V_4^A, V_5^A, T_1^A)$

4) The server $MS_j$ gets the message forged by the $U_A$, $MS_j$ checks the freshness of time-stamp $T_1^A$, as it is fresh, hence $U_A$ passes this test.

5) $MS_j$ now computes:

$$V_6 = h(SID_j||W_j)$$  \hspace{1cm} (10)

$$V_7 = V_3^A \oplus V_6$$  \hspace{1cm} (11)

$$V_8 = h(V_7||W_j))$$  \hspace{1cm} (12)

$$V_9 = V_4^A \oplus V_8 = R_{rand_1}^A$$  \hspace{1cm} (13)

$$V_{10} = h(V_9||V_9||T_1^A)$$  \hspace{1cm} (14)

6) $MS_j$ now verifies the equality:

$$V_{10} \overset{?}{=} V_5^A$$  \hspace{1cm} (15)

7) $MS_j$ considers $U_A$ as genuine $U_i$ if Eq. 15 holds and process the next steps to complete the authentication process. It can be clearly seen that Eq. 15 holds, as $V_8$ computed by $MS_j$ in Eq. 12 is identical to $V_9^A$ calculated by the $U_A$ in Eq. 5. Similarly, $V_6$ computed in Eq 13 is also the same $R_{rand_1}^A$ generated by $U_A$. Therefore, $U_A$ has successfully launched impersonation attack using the stolen verifier.

D. SECRET TEMPORARY PARAMETER LEAKAGE

1) As described in Subsection III-B and III-C, $U_A$ being insider knows the identity of $U_i$ and secret-key of server $W_j$, and computes:

$$V_1^A = h(PID_i||W_j)$$  \hspace{1cm} (16)

2) $U_A$ can now extract the random number $R_{rand_1}$ in the following way:

$$R_{rand_1} = V_4 \oplus V_1^A$$  \hspace{1cm} (17)

Leakage of users random number leads to the server impersonation attack as described in the next subsection.

E. SESSION-KEY LEAKAGE AND SERVER IMPERSONATION ATTACK

$U_A$ intercepts the message $<V_{11, 12}, T_2>$ from server to user and generates its own message in the following way:

1) As described in Subsection III-B and III-C, that $U_A$ can generate the value $h(SID_j \oplus W_j)$, and $U_A$ also knows the identity of the $U_i$ so he/she computes:

$$V_6^A = h(SID_j||W_j)$$  \hspace{1cm} (18)

$$V_7^A = PID_i \oplus V_6^A$$  \hspace{1cm} (19)

$$V_8^A = h(V_7^A||W_j)$$  \hspace{1cm} (20)

$$V_9^A = V_4 \oplus V_8^A$$  \hspace{1cm} (21)

2) $U_A$ selects an arbitrary nonce $R_{rand_2}^A$, the present timestamps $T_2^A$ and calculates:

$$V_1^A = h(V_6^A||R_{rand_1}^A) \oplus R_{rand_2}^A$$  \hspace{1cm} (22)

$$SK_{ij} = h(V_6^A||V_8^A||V_9^A||R_{rand_2}^A||T_2^A)$$  \hspace{1cm} (23)

$$V_{12}^A = h(SK_{ij}||V_9^A||V_9^A||T_2^A)$$  \hspace{1cm} (24)

Finally, $U_A$ sends the message containing $<V_{11, 12}, V_{12}^A, T_2^A>$ to $U_i$.

3) $U_i$ receives the message forged by the $U_A$, and examines the novelty of time-stamp $T_2^A$, as it is fresh, hence $U_A$ passes this test.

4) Now, $U_i$ computes:

$$V_{13} = V_{11}^A \oplus h(V_1||R_{rand_1}) \oplus R_{rand_1}$$  \hspace{1cm} (25)

$$SK_{ij} = h(V_{11}||V_2||R_{rand_1}||V_{13}||T_2^A)$$  \hspace{1cm} (26)

$$V_{14} = h(SK_{ij}||V_1||R_{rand_1}||T_2^A)$$  \hspace{1cm} (27)

5) $U_i$ now verifies:

$$V_{12} \overset{?}{=} V_{14}$$  \hspace{1cm} (28)

6) $U_i$ considers $U_A$ as genuine $MS_j$ if Eq. 28 holds and process the next steps to complete the authentication process. It can be clearly seen that Eq. 28 holds, as $SK_{ij}$ calculated by $U_i$ in Eq. 26 is identical to that calculated by $U_A$ in Eq. 23. Similarly, $V_1$ is also the same as $V_8^A$ computed by $U_A$ in Eq. 20. Therefore, $U_A$ has successfully launched server impersonation attack using the stolen verifier.
TABLE 1. Notation guide.

| Symbols                  | Representations                          |
|--------------------------|------------------------------------------|
| $U_i, PID_i, PW D_i$     | The patient's name, unique personal identity and password |
| $Gen(.), Rep(.)$         | Probabilistic generation and deterministic reproduction functions of fuzzy extractor, respectively |
| $SC_i, PW D_i$           | The smart-card and pseudo-random-password $U_i$ |
| $RC, K_{RC}$             | The registration center, and its secret key |
| $S_i, S ID_i, S_{priv_i}$| The server, its unique identity and secret key $\tau_i$ |
| $\alpha, \tau_i$         | Error tolerance threshold, Biometric secret-key & public reproduction parameter, respectively |
| $SK_{i, j}$              | Session-key between $U_i$ and $S_j$ |
| $T_i, \Delta T_i$        | Timestamp, Maximum allowable transmission delay |
| $\mathbf{A}, U, T$       | Adversary symbols |

FIGURE 1. Server registration.

IV. PROPOSED SCHEME

This section manifests the improved three-factor symmetric-key based secure AKA scheme for multi-server environments (ITSSAKA-MS), specifically proposed to vanquish the defects exist in [5]. The proposed scheme consists of three phases which are further divided into sub-phases. The notation utilized in the proposed scheme are depicted in Table 1. The scheme is described in the subsequent subsections:

A. REGISTRATION PROCESS

This phase explains the procedure of registering the users and servers:

1) SERVER REGISTRATION PROCESS

All of the medical servers $MS_j (1 \leq j \leq m + m')$ in the proposed scheme have to register with the registration center (RC), where $m$ are the currently registered servers and $m'$ are the servers which may be registered in the future. For registration as presented in Figure 1, each server $S_j(S_j : 1 \leq j \leq m + m')$ selects its identity $S ID_j$ and sends it to the RC and the RC computes $S_{priv_j} = h(S ID_j | K_{RC})$ and sends $S_{priv_j}$ to $S_j$, which saves it in its’ database.

2) USER REGISTRATION PROCESS

All of the users $U_i$ need to register with the $RC$ in order to avail the services. With respect to Figure 2, $U_i$ and $RC$ performs these steps to complete the registration:

RG1: User chooses his/her $PID_i, PW D_i$ and imprints his/her $BIO_i$. $U_i$ now computes $HID_i = h(PID_i)$ and sends registration request containing $HID_i$ to $RC$.

User ($U_i$) \quad Registration centre ($RC$)

+ Selects $PID_i, PW D_i$, inputs $BIO_i$ and computes $HID_i = h(PID_i)$ \quad \rightarrow (U_i \rightarrow RC via secure channel)

RG2: $RC$ selects $R_{rand_i}$ and temporary identity $TPID_i$.

Computes $Auth_i = h(K_{RC} || HID_i || R_{rand_i})$, $K_i = h(HID_i || R_{rand_i})$, $R_i = E_{K_{RC}}( Auth_i, R_{rand_i}, HID_i )$, stores $\{ K_i, R_i, TPID_i \}$ into the $SC_i$.

Finally, $SC_i$ contains $\{ A_i, K_i', TPID_i', h(.), Gen(\cdot), Rep(\cdot), \tau_i, t \}$

FIGURE 2. User registration.

RG3: $User$ computes $Gen(BIO_i) = (\sigma_i, \tau_i)$, $A_i = h(PID_i || PW D_i || \sigma_i)$, $R_i' = R_i \oplus h(PW D_i || \sigma_i)$, $K_i' = K_i \oplus h(PW D_i || \sigma_i)$, $TPID_i' = TPID_i \oplus h(PW D_i || \sigma_i)$. Replicates $R_i, K_i, TID_i$ with $R_i', K_i', TID_i$ and stores $\{ R_i', K_i', TID_i', h(.) , Gen(\cdot), Rep(\cdot), \tau_i, t \}$.

B. LOGIN AND KEY-ESTABLISHMENT PROCESS

Following are the steps performed by $U_i$ to login to $MS_j$ as discussed in Figure 3:

LA1: User $U_i$ inserts $SC_i$, inputs $PID_i, PW D_i$, imprints his/her $BIO_i$. $U_i$ now computes $Rep(BIO_i, \tau_i) = \sigma_i'$, checks if $A_i = h(PID_i || PW D_i || \sigma_i')$, terminate the request if it is in-equation. $U_i$ generates $R_{rand_i}, T_i$ and computes $R_i = R_i' \oplus h(PW D_i || \sigma_i'), K_i = K_i' \oplus h(PW D_i || \sigma_i'), TPID_i = TPID_i' \oplus h(PW D_i || \sigma_i'), HID_i' = h(PID_i)$, $R_{rand_i}' = R_{rand_i} \oplus HID_i', S ID_i = S ID_i \oplus HID_i', TPID_i = TPID_i' \oplus HID_i', W_i = h(HID_i || T_i)$. $U_i$ now transmits the $M_{req} = \{ R_i, S ID_i, R_{rand_i}, W_i, TPID_i, T_i \}$ to $RC$.

LA2: $RC$ receives $M_{req}$, checks the condition $| T_i - T_{c} | \leq \Delta T$, if true computes $Auth_i, R_{rand_i}, HID_i = D_{K_{RC}}( R_i )$, and checks $W_i = h(HID_i || T_i)$, and $Auth_i = h(K_{RC} || HID_i || R_{rand_i})$, terminates if any of these or both are not valid. $RC$ now computes $TPID_i' = TPID_i' \oplus HID_i$, $R_{rand_i} = R_{rand_i} \oplus HID_i$, $S ID_i = S ID_i \oplus HID_i, RC$ generates a timestamp $T_2$ and computes $K_j = h(S ID_i || K_{RC})$, $W_{RC} = h(K_{j} || T_2)$, $Y_{RC} = h(S ID_i || HID_i || R_{rand_i} || T_1)$.
FIGURE 3. Login and Key-establishment.

Patient \((U_i/SC_i)\) | Registration centre \((RC)\) | Server \((S_j)\)
--- | --- | ---
\(U_i\) inserts \(USC_i\), inputs \(PID_i, PW_D_i\), Imprints \(BIO_i\)
Compute \(Rep(BIO_i, \tau_i) = \sigma_i\)
\(A_i = h(PID_i||PW_D_i||\sigma_i)\) else terminate
Generate \(R_{rand_i}, T_1\) and compute
\(R'_i = R'_i \oplus h(PW_D_i||\sigma_i)\)
\(K'_i = K'_i \oplus h(PW_D_i||\sigma_i)\)
\(TPID'_i = TPID'_i \oplus h(PW_D_i||\sigma_i)\)
\(HID'_i = h(PID_i)\)
\(R_{rand_{ij}} = R_{rand_i} \oplus HID'_i\)
\(TPID''_i = TPID'_i \oplus HID'_i\)
\(T_1 = T_1 \oplus HID'_i\)
\(W_i = h(HID'_i||K_i||T_1)\)

\(\frac{M_{reg1}(R_i, SID_i, R_{rand_i}, W_i, TPID''_i, \tau'_i)}{(U_i \rightarrow RC \ via \ open \ channel)}\)

\(RC\) receives \(M_{reg1}\)
\((Auth_i, R_{rand_i}, HID_i) = D_{KRC}(R_i)\)
\(T_1' = T_1' \oplus HID_i\)
\(|T_1' | \leq |T_1| \leq \Delta T\)
\(W_i = h(HID_i||h(HID_i||KRC)||T_1)\)
\(Auth_i = h(KRC)||HID_i||R_{rand_i}\)
\(TPID_i = TPID'_i \oplus HID_i\)
\(R_{rand_{ij}} = R_{rand_i} \oplus HID_i\)
Generate a timestamp \(T_2\)
\(K_j = h(SID_j||KRC)\)
\(W_{RC} = h(K_j||T_2)\)
\(Y_{RC} = h(SID_j||HID_j||R_{rand_i}||T_1)\)
\(G_{RC} = E_{K_j}(TPID_i, W_{RC}, Y_{RC}, T_1, T_2)\)

\(\frac{M_{reg2}(G_{RC}, SID_j)}{(RC \rightarrow S_j \ via \ open \ channel)}\)

\(S_j\) receives \(M_{reg2}\)
\((TPID_i, W_{RC}, Y_{RC}, T_1, T_2) = S_{previ}(G_{RC})\)
\(|T_2 - T_1| \leq \Delta T\)
\(W_{RC} = h(S_{previ}||T_2)\)
Generate \(T_2\) compute
\(SK_{ij} = h(Y_{RC}||SID_j||T_3)\)
\(W_{S_j} = h(SK_{ij}||T_3)\)

\(\frac{M_{reg2}(W_{S_j}, T_2, TPID_i)}{(U_i \rightarrow S_j \ via \ open \ channel)}\)

\(U_i\) receives \(M_{reg2}\)
\(|T_3 - T_c| \leq \Delta T\)
\(Y_i = h(SID_i||HID_i||R_{rand_i}||T_1)\)
\(SK'_{ij} = h(Y_i||SID_i||T_3)\)
\(W_{S_j} = h(SK'_{ij}||T_3)||T_3)\)
If true save the session key

\(\frac{SK'_{ij} = SK_{ij}}{(U_i \rightarrow S_j)}\)

C. UPDATE PROCESS
This phase contains two sub-phases namely i) password and biometric update phase, ii) new user addition, revocation and re-registration phase.

1) PASSWORD AND BIOMETRIC UPDATE PROCESS
To decrease the communication and computation cost, this phase is performed without the involvement of the RC. Following are the actions committed in this phase:

**PBU 1:** \(U_i\) inputs his/her \(SC_i\), enters the old \(PID_i^{old}, PW_D^{old}\) and imprints \(BIO_i^{old}\).

**PBU 2:** \(SC_i\) computes \(Rep(BIO_i^{old}, \tau_i) = \sigma_i^{old}\) and checks \(A_i^{old} \vdash h(PID_i^{old}||PW_D_i^{old}||\sigma_i^{old})\), if true continues else terminate the process.
PBU 3: $SC_i$ prompts the $U_i$ to provide novel password $PWD_{i}^{new}$ and biometric $BIO_{i}^{new}$ and computes $A_i = h(PID_{i}^{old}) \oplus |PWD_{i}^{new}| \oplus |BIO_{i}^{new}| \oplus \sigma_i^{old}$, $R_{i}^{new} = R_i' \oplus h(PWD_{i}^{old}) \oplus |\sigma_i^{old}| \oplus h(PWD_{i}^{new}) \oplus |\sigma_i^{new}|$, $k_i^{new} = K_i^{old} \oplus h(PWD_{i}^{old}) \oplus |\sigma_i^{old}|$ and $TPID_i^{new} = TPID_i \oplus h(PWD_{i}^{old}) || |\sigma_i^{old}| \oplus h(PWD_{i}^{new}) || |\sigma_i^{new}|$.

PBU 4: $SC_i$ replaces the parameters $\{A_i, K_i', R_i'\}$ with $\{A_i^{new}, K_i^{new}, R_i^{new}\}$. $SC_i$ finally contains the following parameters $\{A_i^{new}, K_i^{new}, R_i^{new}, TPID_i^{new}, h(\cdot), Gen(\cdot), Rep(\cdot), t_i^{new}, t\}$.

2) NEW USER ADDITION, REVOCATION AND RE-REGISTRATION PROCESS

If a legal user has misplaced the $SC_i$, stolen by an adversary or some novel user needs to register with the system this can be accomplished in the following manner:

NUARR 1: $U_i^{new}$ enters the identity $PID_i^{new}$ (old user may enter the same old or new identity) and transmits the registration request containing $HID_i = h(PID_i^{new})$ to $RC$ via secure channel.

NUARR 2: $RC$ selects the temporary-identity $TPID_i^{new}$ for $U_i$ and computes the following $A_i^{new} = h(KRC) || |HID_i^{new}| || R_{i rand1}^{new}$, $K_i^{new} = h(HID_i^{new}) || |R_{i rand1}^{new}|$ and $R_{i new} = E_{KRC}(A_i^{new}, R_{i rand1}^{new}, HID_i^{new})$. Finally, $RC$ stores $\{K_i^{new}, R_{i new}^{new}, TPID_i^{new}\}$ into the smart-card $SC_i^{new}$ and then transmits the $SC_i^{new}$ to $U_i^{new}$ over the private/secure channel.

NUARR 3: $U_i^{new}$ receives the smart-card imprints the biometric $BIO_{i}^{new}$ and computes $Gen(BIO_{i}^{new}) = (A_i^{new}, R_{i new}^{new})$, $A_{i new} = h(PID_i^{new}) \oplus |PWD_i^{new}| \oplus |\sigma_i^{new}|$, $R_i' = R_i^{new} \oplus h(PWD_{i}^{new}) \oplus |\sigma_i^{new}|$, $K_i' = K_i^{new} \oplus h(PWD_{i}^{new}) \oplus |\sigma_i^{new}|$ and $TPID_i' = TPID_i^{new} \oplus h(PWD_{i}^{new}) \oplus |\sigma_i^{new}|$.

NUARR 4: $SC_i^{new}$ replaces the $R_{i new}^{new}, K_i^{new}, TPID_i^{new}$ with $R_i', K_i', TPID_i'$. Smart-card finally contains the following parameters $\{A_i^{new}, K_i', R_i', TPID_i', h(\cdot), Gen(\cdot), Rep(\cdot), t_i^{new}, t\}$.

V. SECURITY ANALYSIS

This portion elaborates the formal and informal security discussion:

A. AUTOMATED FORMAL SECURITY VERIFICATION THROUGH AVISPA

This section demonstrates that the scheme can withstand the man-in-the-middle and replay attack verified through widely used AVISPA simulation tool [52]. AVISPA simulation can be performed in the subsequent steps:

Step 1: The role oriented High Level schemes Specification Language (HLPSL) [52] is used to implement the scheme, which is then interpreted into Intermediate Format (IF) through HLPSL2IF translator.

Step 2: Than the translated IF is provided to Output Format (OF) to check either the scheme is secure or not.

The simulation results shown in Figure 4a and Figure 4b exhibit that the proposed scheme is as per to the design properties, and can stand against the man-in-the-middle and replay attacks. In the OFMC backend, a total of 1480 nodes were examined in 12.76 seconds with the depth of 12 piles. The CL-AtSe backend analyzed 3 states the interpretation and computation taken for this backend are 0.40 seconds and 0.00 seconds, individually.

B. SECURITY DISCUSSION

The subsection provides a brief discussion on security features provision of the proposed ITSSAKA-MS:

1) USER ANONYMITY

In proposed ITSSAKA-MS, the user sends $M_{Req} (R_i', SID_i', R_{rand1}, W_i, TPID_i, T_i)$, out of all the sent parameter only $TPID_i$ is related to user identity and it is alias identity stored in smart card, using this alias identity or any other parameter sent on public channel may not benefit the attacker $A$ to reveal original identity of the user, even if $A$ steals the smart-card and tries to recover the identity of the patient, to do this he/she needs to know $PID_i$, $PWD_i$ of the user. Also hashed-identity is stored in $A_i$, but to extract it $A$ needs to know the secret-key of $RC$. Addition to this $U_i$’s identity is never shared with the server, neither is send openly over the public channel. Hence the scheme provides anonymity.

2) PRIVILEGED INSIDER ATTACK

During the registration process identity of the $U_i$ is secured by hash-functions one-way property, so an insider cannot guess the $U_i$’s identity. Also no verifier-table is stored on
the RC, so an insider cannot extract any info. Additionally, if an insider steals the smart-card and tries to extract the $U_i$'s password or identity, yet this is not possible because they are in hashed form. Hence, the said attack is not possible.

3) OFFLINE PASSWORD GUESSING ATTACK
Suppose an adversary $A$ steals the smart-card of a legal user $U_i$, and tries to extract the password from $A_i = h(PID_i)||PWD_i||\sigma_i$ and to be successful, $A$ needs the knowledge of $PID_i$ and $\sigma_i$. Therefore, the offline password guessing attack is not conceivable in the proposed scheme.

4) IMPERSONATION ATTACK
A User ($U_i$) or a server ($S_j$) may try to impersonate as an adversary $A$ in the subsequent ways:

a: USER IMPERSONATION ATTACK
Suppose $U_A$ is a valid but dishonest user and may try to impersonate as a legal user $U_i$. $U_A$ may generate its own random number $R_{\text{rand}}^A$ and current time stamp $T_{3}^A$. Next he/she tries to compute $R_{\text{rand}}^A = R_{\text{rand}}^A \oplus HID_i$, $W_i^A = h(HID_i||K_i||T_{1}^A)$, $TPID_i^A = TPID_i \oplus HID_i$ in order to initiate a genuine login request message. However, $U_A$ needs the knowledge of $PID_i$ and $K_i$ to impersonate as a $U_i$ and form a legal message, so the scheme is secure against the said attack.

b: RESISTS SERVER IMPERSONATION ATTACK
An intruder $A$ may impersonate as an authentic server $S_i$ towards $U_i$. To do this $A$ generates the timestamp $T_{3}^A$ and has to compute $SK_{ij}^A = h(Y_{RC}||SID_i||T_{3}^A)$, $W_{ij}^A = h(SK_{ij}^A||T_{1}||T_{3}^A)$. To produce a legal message $A$ should have the knowledge of $Y_{RC}$ and $T_1$. Hence, the said attack is not possible.

5) MUTUAL AUTHENTICATION
The RC authenticates the user on validation of three conditions: 1) the freshness of timestamp, 2) $W_i = h(HID_i||h(HID_i||K_{RC}||T_{1})$, and 3) $Auth_i = h(K_{RC}||HID_i||R_{\text{rand}})$. The verification of these 3 dependent conditions require the knowledge of $K_{RC}$, $HID_i$ and $R_{\text{rand}}$. In similar way, $S_j$ authenticates $RC$ on validation of two conditions: 1) the freshness of timestamp, and 2) $W_{RC} = h(S_{\text{priv}}||T_2)$, both of these are also dependent on each other and on the knowledge of $S_{\text{priv}}$. Similarly, only valid and legal $S_j$ can generate $M_{s3}(W_S, T_3, TPID_i)$ as described in V-B4b. Hence, the entities of the proposed scheme can mutually authenticate each other.

6) REPLAY ATTACK
Random nonce and timestamp are generated in each session to stop the replay attack in our scheme. If an intruder $A$ intercepts the messages $(M_{s1}, M_{s2}, M_{s3})$ during the login and authentication phase and tries to replay it, the attacker presence can be checked by checking the freshness of the timestamp. Also, timestamp is hashed with other parameters making it hard for the $A$ to replay the old message.

7) MAN-IN-THE-MIDDLE ATTACK
Assume an intruder $A$ captures the message $M_{sg1}(R_i, SID_i, R_{\text{rand}}^i, W_i, TPID_i, T_1)$ and generates its own login message $M_{sg1}(R_i^A, SID_i^A, R_{\text{rand}}^A, W_i^A, TPID_i^A, T_1^A)$, but to do this $A$ needs to know $HID_i$, $R_{\text{rand}}$, and $K_i$. In the same way, $A$ needs to know $Y_{RC}$ and $T_1$ to generate the message $M_{sg3}$, so said attack cannot be employed against the proposed attack.

8) STOLEN SMART-CARD ATTACK
Assume an attacker $A$ steals the smart-card of a legal user $U_i$ and tries to extract his/her $PWD$ or $PID_i$. However, because of hash functions one-way property these parameters cannot be guessed, also $A$ needs to know $\sigma_i$ to correctly guess the $PWD$. Hence scheme is secure against the stolen smart-card attack.

VI. PERFORMANCE ANALYSIS
This section evaluates the proposed scheme with regard to computation, communication costs and security features provision concerning other multi-server authentication schemes.

A. FUNCTIONALITY COMPARISON
The Table 2 depicts the merits and demerits of the proposed scheme associated to related schemes [5], [7], [53], [54]. Different schemes lack various security features. In contrast, our scheme fulfills all the necessary security requirements and is secure against various attacks in multi-server environment.

B. COMPUTATION COST ANALYSIS
For computation costs comparison, different operation timings [55] are depicted in the Table 3. Table 4 depicts that though, the cost of the proposed scheme is slightly higher than [5], [7], [54] and same as [53], but it is evident that the
TABLE 3. Approximate time required for various operations.

| Notation | Description                          | Computation time |
|----------|--------------------------------------|------------------|
| $T_h$    | Hash function                        | $0.00235\text{ms}$ |
| $T_m$    | ECC point multiplication              | $0.0046\text{ms}$ |
| $T_{sym}$| Symmetric enc/dec                     | $2.226\text{ms}$ |
| $T_f$    | Fuzzy extractor function              | $2.226\text{ms}$ |

TABLE 4. Comparison of computation costs.

| Scheme | User | RC | Server | Time (ms) |
|--------|------|----|--------|-----------|
| [7]    | $5T_h$ | $7T_h+2T_{sym}$ | $12T_h$ | $\approx 4.4796\text{ms}$ |
| [53]   | $6T_h+3T_m$ | $9T_h+3T_m$ | $15T_h+4T_m$ | $\approx 8.9385\text{ms}$ |
| [54]   | $8T_h$ | $13T_h+2T_{sym}$ | $21T_h+2T_{sym}$ | $\approx 0.0575\text{ms}$ |
| [5]    | $3T_h+1T_f$ | $11T_h$ | $14T_h+1T_f$ | $\approx 2.2582\text{ms}$ |
| Our    | $6T_h+1T_f$ | $2_{sym}+6T_h$ | $3T_h+1_{sym}$ | $\approx 8.9385\text{ms}$ |

TABLE 5. Comparison of communication costs.

| Scheme | # of bits |
|--------|-----------|
| Chaudhry et al. [7] | 1024 |
| Reddy et al. [53] | 1280 |
| Irshad et al. [54] | 864 |
| Barman et al. [5] | 1116 |
| Proposed | 2144 |

proposed scheme is robust and more secure than the other schemes.

C. COMMUNICATION COST ANALYSIS

The Table 5 shows the communication costs of different schemes in multi-server environment. We assumed that the hash digest (SHA-1), user identity, elliptic curve crypto-based point $(x_p, y_p)$, arbitrary number and timestamp requires respectively $160 − \text{bits}$, $160 − \text{bits}$, $320 − \text{bits}$, $160 − \text{bits}$, and $32 − \text{bits}$. The proposed scheme bears an average computational cost of $2144\text{-bits}$, which is slightly greater than then the other related and compared schemes [5], [7], [53], [54]; but it come up with more security features as compared to other related schemes.

VII. CONCLUSION

In this paper, we have critically analyzed the some shortcomings including vulnerabilities against user impersonation, secret key reveal, lack of anonymity and design flaws of the scheme of Barman et al. proposed specifically for multi-server environments and usable in telecare medical information systems. In contrast, our study presents an improved three-factor symmetric-key based secure authenticated key agreement scheme for multi-server environments (ITSSAKA-MS). The security of ITSSAKA-MS is proved formally through automated tool AVISPA. Moreover, the security discussion argued the robustness of ITSSAKA-MS against the known attacks. The performance analysis is presented keeping the communication and computation costs as metrics. The ITSSAKA-MS incurred slightly additional computation and communication costs, mainly to provide the better security as compared to the recent schemes.

REFERENCES

[1] Y. Zhang, L. Sun, H. Song, and X. Cao, “Ubiquitous WSN for healthcare: Recent advances and future prospects,” IEEE Internet Things J., vol. 1, no. 4, pp. 311–318, Aug. 2014.
[2] U. Gogate and J. Bakal, “Refining healthcare monitoring system using wireless sensor networks based on key design parameters,” in Information and Communication Technology for Intelligent Systems. Singapore: Springer, 2019, pp. 341–349.
[3] S. Gritzalis, C. Lambrinoudakis, D. Lekkas, and S. Deftereos, “Technical guidelines for enhancing privacy and data protection in modern electronic medical environments,” IEEE Trans. Inf. Technol. Biomed., vol. 9, no. 3, pp. 413–423, Sep. 2005.
[4] M. S. Farash, O. Nawaz, K. Mahmood, S. A. Chaudhry, and M. K. Khan, “A provably secure RFID authentication protocol based on elliptic curve for healthcare environments,” J. Med. Syst., vol. 40, no. 7, p. 165, Jul. 2016.
[5] S. Barman, H. P. H. Shum, S. Chattopadhyay, and D. Samanta, “A secure authentication protocol for multi-server-based E-healthcare using a fuzzy commitment scheme,” IEEE Access, vol. 7, pp. 12557–12574, 2019.
[6] S.-H. Li, C.-Y. Wang, W.-H. Lu, Y.-Y. Lin, and D. C. Yen, “Design and implementation of a telecare information platform,” J. Med. Syst., vol. 36, no. 3, pp. 1629–1650, Jun. 2012.
[7] S. A. Chaudhry, H. Naqvi, and M. Khan, “An enhanced lightweight anonymous biometric based authentication scheme for TMIS,” Multimedia Tools Appl., vol. 77, no. 5, pp. 5503–5524, Mar. 2018.
[8] K. Mahmood, J. Arshad, S. A. Chaudhry, and S. Kumari, “An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure,” Int. J. Commun. Syst., vol. 32, no. 16, p. e4137, Nov. 2019.
[9] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Rahman, and M. N. Saqib, “Security and key management in IoT-Based wireless sensor networks: An authentication protocol using symmetric key,” Int. J. Commun. Syst., vol. 32, no. 16, p. e4139, Nov. 2019.
[10] S. Hussain and S. A. Chaudhry, “Comments on biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment,” IEEE Internet Things J., vol. 6, no. 6, pp. 10936–10940, Dec. 2019.
[11] B. A. Alzahrani, S. A. Chaudhry, A. Barnawi, A. Al-Barakati, and T. Shon, “An anonymous device to device authentication protocol using ECC and self-certified public keys usable in Internet of Things based autonomous devices,” Electronics, vol. 9, no. 3, p. 520, Mar. 2020.
[12] Z.-Y. Wu, Y.-C. Lee, F. Lai, H.-C. Lee, and Y. Chung, “A secure authentication scheme for telecare medicine information systems,” J. Med. Syst., vol. 36, no. 3, pp. 1529–1535, Jun. 2012.
[13] H. Debiao, C. Jianhua, and Z. Rui, “A more secure authentication scheme for telecare medicine information systems,” J. Med. Syst., vol. 36, no. 3, pp. 1989–1995, Jun. 2012.
[14] Z. Zhu, “An efficient authentication scheme for telecare medicine information systems,” J. Med. Syst., vol. 36, no. 6, pp. 3833–3838, Dec. 2012.
[15] M.-S. Hwang and L.-H. Li, “A new remote user authentication scheme using smart cards,” IEEE Trans. Consum. Electron., vol. 46, no. 1, pp. 28–30, Feb. 2000.
[16] M. Sandirigama, A. Shimizu, and M. T. Noda, “Simple and secure password authentication protocol (SAP),” IEICE Trans. Commun., vol. 83, no. 6, pp. 1363–1365, 2000.
[17] H. Arshad and M. Nikooghadam, “A scheme and secure authentication and key agreement scheme for session initiation protocol using ECC,” Multimedia Tools Appl., vol. 75, no. 1, pp. 181–197, 2016.
[18] Z. Zhang, Q. Qi, N. Kumar, N. Chilamkurthy, and H.-Y. Jeong, “A secure authentication scheme with anonymity for session initiation protocol using elliptic curve cryptography”, Multimedia Tools Appl., vol. 74, no. 10, pp. 3477–3488, May 2015.
[19] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, “An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks,” Comput. Elect. Eng., vol. 69, pp. 534–554, Jul. 2018.
[20] C.-T. Li and M.-S. Hwang, “An efficient biometrics-based remote user authentication scheme using smart cards,” J. Netw. Comput. Appl., vol. 33, no. 1, pp. 1–5, Jan. 2010.
RANA HASEEB UR REHMAN received the B.S. degree in computer science from COMSATS University, Pakistan, and the M.S. degree from International Islamic University, Islamabad, in 2018. His research interests include computer networking, network security, network communication, information security, cryptography, elliptic/hyper elliptic curve cryptography, encryption, and authentication.

ASMAA MUNSHI received the B.Sc. degree in computer science from King Abdulaziz University, Saudi Arabia, in 2004, and the master’s degree (Hons.) in internet security and forensic, and the Ph.D. degree in information security from Curtin University, Australia, in 2009 and 2014, respectively. She is currently an Associate Professor with the Cybersecurity Department, College of Computer Science and Engineering, University of Jeddah, Saudi Arabia. She is also working as a Supervisor with the Cybersecurity Department, Female Section, College of Computer Science and Engineering, University of Jeddah. She is also the Vice Dean of the Faculty of Computing and Information Technology, Female Section, University of Jeddah, Khulais Branch, Saudi Arabia. Her research interests include educational technology and information security.

MISBAH LIAQAT received the B.S. degree (Hons.) in computer science from COMSATS University, Pakistan, in 2013, and the Ph.D. degree from the University of Malaya, Kuala Lumpur, Malaysia, in 2017. She was associated as a BSP RA with the Center for Mobile Cloud Computing Research (C4MCCR), University of Malaya. She is currently an Assistant Professor with the University of Jeddah, Saudi Arabia. Her research interests include wireless sensor networks, network security, cloud scheduling, cloud resource management, mobile cloud computing, sensor cloud, VM migration, and the Internet of Things. She received the Gold Medal from COMSATS University.

NEERAJ KUMAR (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from Shri Mata Vaishno Devi University, Katra (J&K), India, in 2009. He was a Postdoctoral Research Fellow with Coventry University, Coventry, U.K. He is currently working as a Professor with the Department of Computer Science and Engineering, Thapar University, Patiala, India. He is also a Professor with the Department of Computer Science and Information Engineering, Asia University, Taiwan. He has guided many research scholars leading to Ph.D. and M.E./M.Tech. He has authored more than 170 technical research articles published in leading journals and conferences from the IEEE, Elsevier, Springer, John Wiley, and so on. Some of his research findings are published in top cited journals, such as the IEEE Transactions on Industrial Electronics, the IEEE Transactions on Dependable and Secure Computing, the IEEE Transactions on Intelligent Transportation Systems, the IEEE Transactions on Consumer Electronics, the IEEE Network, the IEEE Communications, the IEEE Wireless Communications, the IEEE Internet of Things Journal, and the IEEE Systems Journal. He is in the editorial board of the Journal of Network and Computer Applications (Elsevier) and the International Journal of Communication Systems (Wiley).

SHEHZAD ASHRAF CHAUDHRY received the master’s and Ph.D. degrees (Hons.) from International Islamic University Islamabad, Pakistan, in 2009 and 2016, respectively. He is currently working as an Associate Professor with the Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey. He has also supervised over 35 graduate students in their research. He has authored over 100 scientific publications appeared in different international journals and proceedings, including 72 in SCI/E journals. With an H-index of 23 and an I-10 index 43, his work has been cited over 1650 times. His current research interests include lightweight cryptography, elliptic/hyper elliptic curve cryptography, multimedia security, e-payment systems, MANETs, SIP authentication, smart grid security, IP multimedia subsystems, and next generation networks. He occasionally writes on issues of higher education in Pakistan. He has served as a TPC member of various international conferences. He was a recipient of the Gold Medal for achieving 4.0/4.0 CGPA in his master’s degree and the Pakistan Council for Science and Technology granted him the Prestigious Research Productivity Award, while affirming him among Top Productive Computer Scientist in Pakistan. He is an Active Reviewer of many ISI indexed journals.

* * *