IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 15, 2020, accepted January 5, 2021, date of publication January 11, 2021, date of current version January 22, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3050402

On the Design of Lightweight and Secure Mutual Authentication System for Global Roaming in Resource-Limited Mobility Networks

R. SHASHIDHARA[1], SANJEET KUMAR NAYAK[1], (Member, IEEE), ASHOK KUMAR DAS[2], (Senior Member, IEEE), AND YOUNGHO PARK[3,4], (Member, IEEE)

[1]Department of Computer Science Engineering, Bennett University, Greater Noida 201310, India
[2]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India
[3]School of Electronics Engineering, Kyungpook National University, Daegu 41566, South Korea
[4]School of Electronic and Electrical Engineering, Kyungpook National University, Daegu 41566, South Korea

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

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant 2020R1I1A3058605.

ABSTRACT A secure authentication protocol plays a crucial role in securing communications over wireless and mobile networks. Due to resource-limitations and the nature of the wireless channel, the global mobile networks are highly susceptible to various attacks. Recently, an efficient authentication system for global roaming has been proposed in the literature. In this article, we first show that the analyzed authentication system is vulnerable man-in-the-middle attack, replay attack and Denial-of-Service (DoS) attack, and it does not ensure untraceability and local password-verification process to identify wrong passwords. To fix these security flaws, we propose a more efficient and robust authentication system for roaming in mobility networks. We use the formal verification tools like ProVerif, Automated Validation of Internet Security Protocols and Applications (AVISPA) and Burrows-Abadi-Needham (BAN) logic to check the regularity of the authentication protocol. Moreover, we prove the secrecy of a session key through the formal security using the random oracle model, known as Real-Or-Random (ROR) model. Finally, a detailed performance evaluation proves that the security protocol not only provides a security strength, but also preserves the low computational overhead. Thus, the proposed authentication protocol is secure and computationally efficient as compared to other relevant schemes.

INDEX TERMS Global roaming, authentication, key establishment, cryptanalysis, security, BAN logic, AVISPA.

I. INTRODUCTION

Global roaming is a basic service for the users who roam across heterogeneous networks. The Mobile User (MU) access the required services from the foreign network by using the mobile devices like smartphones and PDAs. In the mobile network, the registered user can freely roam into foreign networks administrated by the foreign agents and he/she could access ubiquitous services with the assistance of the home network. In the global roaming scenario, the mutual authentication between an *MU* (Mobile User), *HA* (Home Agent) and, *FA* (Foreign Agent) is very crucial to prevent various attacks [1]. The mutual authentication procedure for the global roaming in mobility environments is depicted in Figure 1.

In *MU*'s roaming process, a valid user connects to the foreign network through FA, then it sends an authentic information regarding *MU* and *FA* itself to the home agent HA, in order to validate a identity of valid *MU*. The home agent verifies the received authentication request and transmits the authentic response to shape *FA* and *MU* agents believe in each other. After, a session key is established between *FA* and *MU* to secure communication. Besides authentication, keeping the identity of *MU* being tracked is a further challenging task. In order to ensure the secrecy and privacy in wireless and mobile networks, several security protocols have been

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen.

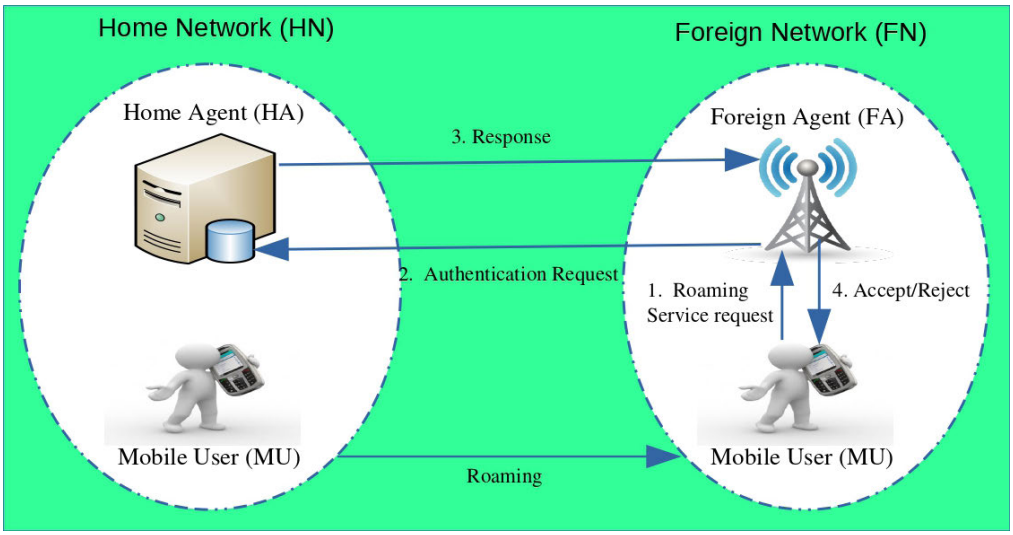

FIGURE 1. User authentication system for global roaming in mobile environments.

proposed [1]–[12]. However, most of the security systems are susceptible to various attacks.

A. MOTIVATION

We analyzed the security strength of numerous mutual authentication systems in literature to provide global roaming in the mobility network. Notably, the existing systems have the following security pitfalls.

1) The authentication systems in the literature are highly vulnerable to impersonation attacks [1]–[3], [7]–[12]. Besides, most of the security protocols in the mobility network make use of static key agreements to deliver the shared secret between a user and service provider networks. In this regard, the entire security system will be compromised when the shared secret-key is deduced by the attacker.
2) Most of the authentication systems make use of timestamps to ensure message freshness, prevent reply attacks. Nevertheless, it require additional clocks which leads to clock synchronization problems since transmission delays are unpredictable in wireless and mobile networks.
3) Furthermore, the existing protocols possesses more communication and computational complexities. These protocols are unfavourable for resource-limited environments like a mobility network.

B. CONTRIBUTIONS

The significant contributions of the paper are summarized as follows:

1) We analyzed the security strength of the protocol in [13] and presented its security pitfalls.
2) A secure mutual authentication protocol has been designed to satisfy all security properties in the context of global roaming in mobile networks. The proposed protocol achieves user privacy, secrecy and computationally efficiency.
3) The formal security-verification and validation of the proposed system is carried out through widely accepted security tools like ProVerif [14] and AVISPA.
4) Consequently, the formal security analysis of the system is measured using BAN logic. Besides, the correctness of the security system has been proved using random oracle model.
5) Finally, a rigorous performance evaluation summarizes the communication and computational gain of the proposed security system under various constraints.

C. PAPER OUTLINE

The sequel of the paper as follows: Section II, covers literature review and cryptographic primitives needed for protocol design. Section III, presents a cryptanalysis of Lee *et al.*'s scheme and its security flaws are derived in Section IV. A robust authentication system with privacy preservation in the mobility network has been presented in Section V. Section VI demonstrates the formal security-analysis of the system using random oracle model and BAN logic, the formal security-verification using ProVerif and AVISPA, and also the informal security analysis. In Section VII, the performance evaluation is summarized. Section VIII concludes the article.

II. BACKGROUND

Authentication and access control are considered as two main security services in various networking environments, such as global mobile network, IoT and wireless sensor network (WSN) [15]–[31].

Recently, several mutual authentication systems have been proposed for the global mobile network. Nevertheless, some of the authentication schemes have been vulnerable to various attacks and suffers with computational inefficiencies.

TABLE 1. Notations and their significance.

Symbol	Description
PW	Password of the user
$ID_{MU}, ID_{HA}, ID_{FA}$	Identity of MU, HA, FA
K_{FH}	Secret-key
S_{HA}	HA's secret
$\mathscr{A}$	The attacker
T_S	Transaction sequence number
$(X)_K$	Private-key cryptosystem
SK	Session-key
R_N, N_{MU}, N_{FA}	Cryptographic nonce
$\|\|$	Concatenation
$h(\cdot)$	Hash operation
$\oplus$	Exclusive-OR

In 2012, Jiang *et al.* [1] proposed a secure user mutual authentication system for roaming in mobile communications. Later, Wen *et al.* [32] analysed the protocol in [1] and proved that the authentication scheme is susceptible is vulnerable to replay attacks and they presented a secure mutual authentication protocol.

Subsequently, Gope and Hwang [33] presented an efficient authentication system for mobility networks. After that, the authors in Wu *et al.* [34] proved that the scheme in [33] does not provides fair-key agreement, and suffers with de-synchronization problem. In addition, they designed a robust mobile user authentication scheme. Later on, many mutual authentication frameworks have been introduced to afford roaming facility in the mobility network [3], [35]–[42]. However, these mutual authentication protocols are computationally inefficient and practically not implementable in resource-constrained environments.

Recently, Lee *et al.* [13] presented an advanced mutual authentication framework for the mobile network and they believed that the protocol in [13] withstand most of the network attacks. In this article, we analyse Lee *et al.*'s the security strength and prove that the security framework is vulnerable to masquerade attacks, denial-of-service attack and replay attacks. Nevertheless, there is local password system to identify the wrong passwords and does not satisfy the untraceable property. In order to over come the flaws in [13], we propose the novel framework for global roaming in the mobile network. The proposed protocol is designed to meet all security requirements, goals and its suitable in resource limited low power mobility terminals.

III. REVIEW OF LEE *et al.*'s AUTHENTICATION SYSTEM

A brief review of Lee *et al.*'s authentication protocol [13] sis presented in this section. It comprises of registration, the authentication and establishment of session key (AESK) and the password-change phase. Various symbols used throughout this article are listed in Table 1.

A. REGISTRATION PHASE

A new mobile user wants to get desired services from the *HA*, he/she should submit the required information to register at the *HA*. The detailed registration procedure of the scheme in [13] is as follows:

1) A new mobile user MU selects ID_{MU}, PW_{MU} and generates the nonce s. After that, MU computes $EID = h(ID_{MU} \oplus PW_{MU}) \oplus s$ and submits registration request to the HA.
2) Upon receiving EID, HA finds $S = h(EID \,||h(SK_{HA}))$. Then, HA sends S to the MU.
3) MU receives S and computes $SPW = S \oplus h(PW_{MU})$. Finally, MU keeps $\{SPW, s\}$ in the device.

B. AUTHENTICATION AND SESSION KEY ESTABLISHMENT PHASE

In this scenario, MU roams into the foreign network (FN) to get services from the service provider network FA. To ensure confidentiality in the system, MU HA, FA must mutually authenticate each other and negotiate the shared secret key SK. AESK phase is described below:

1) MU inputs ID_{MU}, PW_{MU} and the device computes:

$$EID' = h(ID_{MU} \oplus PW_{MU}) \oplus s$$
$$S' = SPW \oplus h(PW_{MU})$$

Then, MU generates random numbers $\{s_{new}, N_M\}$ and computes the following:

$$EID_{new} = h(ID_{MU} \oplus PW_{MU}) \oplus s_{new}$$
$$V_M = EID_{new} \oplus h(S'||N_M)$$
$$Q_M = h(EID_{new}||S'||N_M)$$

After, mobile user sends $M_1 = \{EID', V_M, Q_M, N_M\}$ to the foreign agent FA.

2) Upon receiving M_1 from the user, FA creates the nonce N_F and calculates the following:

$$V_F = N_F \oplus h(SK_{FA})$$
$$Q_F = h(Q_M||N_F||SK_{FA})$$

After that FA submits $M_2 = \{EID', V_M, Q_F, N_M, V_F, ID_{FA}\}$ to the Home agent.

3) HA receives M_2 from FA and computes the following:

$$S' = h(EID'||h(SK_{HA}))$$
$$EID'_{new} = V_M \oplus h(S'||N_M)$$
$$SK_{FA} = h(ID_{FA} \oplus SK_{HA})$$
$$N_F = V_F \oplus h(SK_{FA})$$
$$Q'_F = h(h(EID'_{new}||S'||N_M)||N_F||SK_{FA}).$$

Then, HA verifies $Q'_F \stackrel{?}{=} Q_F$. If the comparison is false, HA ends the session. Otherwise, HA mutually authenticate FA, MU and calculates the following:

$$S_{new} = h(EID'_{new}||h(SK_{HA}))$$
$$V_H = (EID'_{new}||S'||S_{new}) \oplus h(SK_{FA}||N_F).$$

Finally, HA returns $M_3 = \{V_H\}$ to FA.

4) Upon receiving M_3 from HA, *FA* can derive

$$(EID'_{new}||S'||S_{new}) = V_H \oplus h(SK_{FA}||N_F)$$

Then, *FA* examines $Q_M \stackrel{?}{=} h(EID'_{new}||S'||N_M)$. If verification succeeds, *FA* authenticates *MU* and *HA*. Next, *FA* generates the nonce N_{F2} and computes:

$$V_{F2} = S_{new} \oplus h(S'||N_{F2})$$
$$Q_{F2} = h(EID'||S_{new}||N_{F2}).$$

Then, *FA* froms a message $M_4 = \{V_{F2}, Q_{F2}, N_{F2}\}$ to the mobile user.

5) *MU* receives M_4 from *FA* and computes the following:

$$S_{new} = V_{F2} \oplus h(S'||N_{F2}).$$

MU checks $Q_{F2} \stackrel{?}{=} h(EID'||S_{new}||N_{F2})$. If verification successful, *MU* authenticates the *FA*. Finally, mobile user computes a shared secret key $K_{MF} = h(N_M||N_{F2}||S)$ to obtain the desired services provided by the *FA*.

C. PASSWORD CHANGE PHASE

Lee *et al.* [13] password altered phase is described below:

Step 1. *MU* inputs the new password PW_{new}, random nonce s_{new} and the device computes:

$$EID_{new} = h(ID_{MU} \oplus PW_{new}) \oplus s_{new}$$

Step 2. The *MU* use a password PW_{new} to the encryption of S_{new}, computes $SPW_{new} = S_{new} \oplus h(PW_{new})$. Finally, *MU*'s password is successfully changed and the new values of $\{SPW_{new}, s_{new}\}$ are stored in the device.

IV. CRYPTANALYSIS OF LEE *et al.*'s AUTHENTICATION SYSTEM

The threat model and the rigorous security analysis has been accomplished to demonstrate the security weaknesses of the protocol in [13]. In fact, this authentication system is vulnerable to masquerade attacks, replay attack, denial of service attacks, fails to realize untraceability and the wrong passwords cannot be detected at the client side.

A. THREAT MODEL

The intruder $\mathscr{A}$ has control over the channel (insecure channel) between *MU*, *HA* and *FA* in the mobility network [43]. Also, the attacker $\mathscr{A}$ has able to guess the user identities and short passwords in a polynomial time. Notably, an intruder $\mathscr{A}$ has capable to get the authentication details from the lost or stolen smart-card through power analysis techniques [11], [44]. In addition, an adversary may deduce the past session keys to compromise the future session keys [34].

B. VULNERABLE TO MASQUERADE ATTACK

In the mutual authentication process, a valid *MU* sends an authentication request $M_1 = \{EID', V_M, Q_M, N_M\}$ to obtain services of the *FA*. Assume an intruder $\mathscr{A}$ eavesdrops EID' from message M_1, sent through the public network environment. The parameter EID' is a composition of *MU*'s ID_{MU}, PW_{MU} and it's random number s. From registration phase, we can recall that the *MU* submits a registration request *EID* is identical to EID'. Therefore, $\mathscr{A}$ can use this information to re-register with *HA* as a valid user to obtain its services. After, *HA* computes $S = h(EID'||h(SK_{HA}))$ and returns parameter S to the attacker $\mathscr{A}$. Upon receiving S, $\mathscr{A}$ generates a nonce s, inputs his own password PW then computes $SPW = S \oplus h(PW)$ and stores $\{SPW, s\}$ in his device. Next, an adversary use this information to form a valid authentication request messages for *FA* and *HA* to succeed in AESK phase. Therefore, $\mathscr{A}$ can masquerade a valid *MU* to access the services of *HA*.

C. FAILS TO PROVIDE UNTRACEABILITY

The intruder $\mathscr{A}$ neither trace the user identity, nor link the mutual authentication sessions in which the same user has involved. In AESK phase of scheme [13], *MU* submits login request $M_1 = \{EID', V_M, Q_M, N_M\}$ to FA, the authentication request of *FA* $M_2 = \{EID', V_M, Q_F, N_M, V_F, ID_{FA}\}$ to the *HA*. Note that, a user specific value EID' in M_1, M_2 is fixed for all authentication sessions. Further, in this system other communicating parities including valid *FA* knows the identity EID' of *MU*. Therefore, an adversary can easily trace the location of the user by listening to various sessions. Hence, this scheme does not to achieve untraceability.

D. VULNERABLE TO REPLAY ATTACK

In the authentication and session key negotiation process, *MU* submits the authentication request $M_1 = \{EID', V_M, Q_M, N_M\}$ to *FA* through a public network environment. Suppose an adversary $\mathscr{A}$ eavesdrops on message M_1 and sends another message $M'_1 = M_1$ in the next time to *FA*. *FA* creates a nonce N_F then finds $Q_F = h(Q_M||N_F||SK_{FA})$, $V_F = N_F \oplus h(SK_{FA})$. Subsequently, *FA* sends $M_2 = \{EID', V_M, Q_F, N_M, V_F, ID_{FA}\}$ to *HA*. Upon receiving M_2, *HA* processes this authentication requests and confirms that the adversary is a valid *MU*. Although $\mathscr{A}$ may not get session key SK, he/she can impersonates as a legal *MU* to login *FA*. In addition, the above scheme does not use any timestamps, additional clocks synchronization mechanisms and counters to resist with replay attacks, thus an eavesdropper $\mathscr{A}$ replays old messages. Nevertheless, *HA* will not detects a attack. Therefore, the scheme of Lee *et al.* is vulnerable to replay attacks.

E. SUSCEPTIBLE TO DoS ATTACKS

In the above protocol, there is no validation process for the existing password. If $\mathscr{A}$ gets the user's device for a small duration. Then, $\mathscr{A}$ could launch the denial-of-service attack.

1) The intruder $\mathscr{A}$ inputs a random password PW_{new}.
2) *MU* device computes

$$EID' = h(ID_{MU} \oplus PW_{new}) \oplus s$$
$$S' = SPW \oplus h(PW_{new})$$

3) Then, MU generates random numbers $\{s_{new}, N_M\}$ and computes the following:

$$EID_{new} = h(ID_{MU} \oplus PW_{new}) \oplus s_{new}$$

4) Using EID_{new}, SPW, $\mathscr{A}$ has capable to create invalid logins and this would be identified only at the server.
5) The intruder repeats this technique to impose a message traffic and congestion in the authentication system, which restrict the accessibility for the authorised entities and causes distributed denial of service attacks on the home agent.

In addition, an attacker can update false verification information in the password change phase. Later on, an MU is not able to find a session-key. Thus, the authentication framework is susceptible to DoS attacks.

F. SUSCEPTIBLE TO WRONG-PASSWORDS DETECTION

In the above scheme, MU device cannot validate user identity ID_{MU} and password PW_{MU}, before communicating with the FA. An adversary $\mathscr{A}$ can enter the fake login credentials during authentication and establishment of session key phase, this could be detected only by the HA. This makes the security protocol inefficient and there is no local password detection. Thus, the Lee *et al.*'s authentication system is not designed to avoid unauthorized users by validating the password locally.

V. THE PROPOSED SCHEME

The proposed mutual authentication framework for global roaming in the mobility network comprises of the following phases, namely: 1) initialization, 2) registration, 3) mutual authentication, and 4) password change.

The purposes of these phases are briefly summarized below:

- The *initialization phase*, the HA selects the system parameters.
- The *registration phase* allows a legal mobile user MU to be registered with the HA in order to access the services, which occurs in the offline mode (via secure channel). After successful registration, the MU stores the necessary credentials in his/her device.
- The *authentication phase* permits a mobile user MU to mutually authenticate with the foreign agent FA with the help of the HA in order to establish a shared secret key SK.
- During the *password change phase*, an authorized mobile user MU can change the default password without the assistance of the home agent HA at any time.

The detailed description of these phases are provided in the following subsections.

A. INITIALIZATION PHASE

HA issues initialization parameters, when the new mobile user register at the home agent. Assume that HA produces large primes m and n, and computes $r = m * n$. Then, HA chooses an element $g \in G$. Next, HA picks a private key $S_{HA} = a(< n)$, computes its public-key $P_{HA} = g^a \pmod m$ and sends to the FA. Similarly, FA selects a secret-key $S_{FA} = b(< n)$, calculates its public key $P_{FA} = g^b \pmod m$ and sends to the HA. Finally, FA and HA compute the shared secret-key K_{FH} using the secure version of the Diffie-Hellman key exchange protocol [45], known as the station-to-station key exchange protocol.

B. REGISTRATION PHASE

In the registration phase, a mobile user MU freely selects the identity and the password, say $\{ID_{MU}, PW\}$. Then, MU's device produces a random nonce N_M, computes $R_1 = h(ID_{MU}||N_M)$ and sends it to the HA via secure channel. Upon receiving R_1, HA calculates $H_S = h(R_1||S_{HA}||ID_{HA})$. HA then initiates a track sequence number $T_S = 0$ and stores $\{R_1, T_S\}$ in the database. The track sequence number T_S is used to resist against replay attack. Finally, HA returns $R_2 = \{H_S, T_S\}$ to MU via secure channel. MU computes $L_{MU} = h(ID_{MU} ||PW ||N_M)$, $H_M = H_S \oplus h(PW|| N_M)$ and $N'_M = N_M \oplus h(PW||ID_{MU})$, and stores $\{L_{MU}, H_M, T_S, N'_M\}$ in the device.

This phase is then summarized in Figure 2.

C. AUTHENTICATION PHASE

After registration process, a user can roam into foreign networks to obtain ubiquitous services offered by the foreign agent through the assistance of HA. Here, authentication is accomplished in MU, HA and FA to establish the shared secret key SK. The following steps are involved in this phase:

A1:$MU \longrightarrow FA : M_1 = \{V_M, T'_S, R_M\}$

The mobile user MU enters identity ID_{MU} and password PW. Then, MU device calculates $N_M = N'_M \oplus h(PW||ID_{MU})$, $L'_{MU} = h(ID_{MU} ||PW ||N_M)$ and examines whether $L'_{MU} = L_{MU}$ holds or not. If the comparison fails, the authentication session will be terminated. Otherwise, the legitimacy of MU is ensured. Subsequently, MU produces a random nonce R_M and calculates the following parameters:

$$H_S = H_M \oplus h(PW||N_M)$$
$$U_M = h(H_S \oplus R_M)$$
$$V_M = h(ID_{MU}||N_M||U_M||T'_S)$$

Finally, MU sends the message $M_1 = \{V_M, T'_S, R_M\}$ to the FA via public channel.

A2:$FA \rightarrow HA : M_2 = \{ID_{FA}, V_F)\}$

After receiving the message M_1, FA generates a random nonce R_F and encrypts $V_F = E_{K_{FH}}(M_1, R_F)$ using a shared secret key K_{FH} with the help of symmetric encryption function $E(\cdot)$. After that FA submits the encrypted information V_F and its ID_{FA} to the HA via public channel.

A3:$HA \rightarrow FA : M_3 = \{V_H\}$

After receiving the message M_2, the HA device verifies whether received ID_{FA} is the identity of the valid FA. If its satisfies, HA finds the shared key K_{FH} and decrypts V_F to obtain $\{V_M, T'_S, R_M, R_F\}$. Afterwards, HA retrieves R_1, T_S

Mobile User (MU)	Home Agent (HA)
Select identity and password as $\{ID_{MU}, PW\}$ Choose random nonce N_M Compute $R_1 = h(ID_{MU}\|\|N_M)$ $\underrightarrow{\{\boldsymbol{R_1}\}}$ (secure channel)	
	Calculate $H_S = h(R_1\|\|S_{HA}\|\|ID_{HA})$ Initialize track sequence number $T_S = 0$ Store $\{R_1, T_S\}$ in its database $\underleftarrow{\boldsymbol{R_2} = \{\boldsymbol{H_S}, \boldsymbol{T_S}\}}$ (secure channel)
Compute $L_{MU} = h(ID_{MU}\|\|PW\|\|N_M)$, $H_M = H_S \oplus h(PW\|\|N_M)$ and $N'_M = N_M \oplus h(PW\|\|ID_{MU})$ Store $\{L_{MU}, H_M, T_S, N'_M\}$ in the device	

FIGURE 2. Summary of registration phase of the proposed scheme.

from its database and compares $T_S \stackrel{?}{=} T'_S$. If the verification is not true, *HA* declines the authentication request M_2. Otherwise, *HA* proceeds to calculate the following parameters:

$$H'_S = h(R_1||S_{HA}||ID_{HA})$$
$$U^*_M = h(H'_S \oplus R_M)$$
$$V^*_M = h(R_1||U^*_M||T'_S)$$
$$V^*_M \stackrel{?}{=} V_M$$

If the verification fails, *HA* ends the system. Otherwise, the home agent *HA* authenticates *FA* and *MU* successfully, and generates a session key $SK = h(H'_S \oplus R_M \oplus R_F)$. Subsequently, *HA* updates $T_S = T_S + 1$ in its record and encrypts $V_H = E_{K_{FH}}(SK, R_F)$ using its key K_{FH}. Notably, *HA* returns the message $M_3 = \{V_H\}$ to the *FA* via public channel.

A4: $FA \rightarrow MU : M_4 = \{W, R_F\}$ *FA* receives and decrypts the message M_3 to obtain $\{SK, R_F\}$. Then, *FA* checks for correctness of the random nonce R_F. If it fails, *FA* rejects the authentication message M_3. Otherwise, *FA* authenticates *HA* successfully and computes the following parameter:

$$W = h(SK||R_F).$$

Next, *FA* returns the message $M_4 = \{W, R_F\}$ to *MU* via public channel.

A5: After receiving the message M_4, the mobile user *MU* computes a session key as follows:

$$SK^* = h(H_S \oplus R_M \oplus R_F),$$
$$W^* = h(SK^*||R_F).$$

After that *MU* checks whether W^* is same to the received W. If comparison is successful, the *MU* authenticates and believes in *FA*. Otherwise, *MU* device stops the authentication. Finally, *MU* updates $T'_S = T'_S + 1$ in its device.

The procedure of the mutual authentication process is also summarized in Figure 3.

D. PASSWORD CHANGE PROCESS

In this process, the authorized mobile user *MU* can change the default password without the assistance of the home agent *HA* at any time with the help of the following steps:

1) If the registered user *MU* wants to change his/her password, then he/she should select the password change request through the terminal by providing valid credentials ID_{MU} and PW.
2) The device then calculates $N_M = N'_M \oplus h(PW||ID_{MU})$, $H_S = H_M \oplus h(PW||N_M)$ and $L^*_{MU} = h(ID_{MU}||PW||N_M)$, and checks whether $L^*_{MU} \stackrel{?}{=} L_{MU}$. If the comparison is false, the request is aborted. Otherwise, the legality of the user *MU* is proved.
3) Subsequently, the *MU* inputs new password PW^* and the device computes $N^*_M = N_M \oplus h(PW^*||ID_{MU})$, $L^*_{MU} = h(ID_{MU}||PW^*||N_M)$ and $H^*_M = H_S \oplus h(PW^*||N_M)$. Finally, *MU* replaces $\{L_{MU}, H_S, N'_M\}$ with $\{L^*_{MU}, H^*_S, N^*_M\}$.

The summary of password change phase related to the proposed scheme is provided in Figure 4.

VI. SECURITY ANALYSIS

In this section, suppose an intruder $\mathscr{A}$ wants to crack the security system. We trace difficulties that $\mathscr{A}$ encountered to breach the authentication system. In addition, we analyze and demonstrate that the novel mutual authentication framework withstand all security vulnerabilities in global mobile networks.

A. INFORMAL SECURITY ANALYSIS

In this section, we show through non-mathematical (informal) security analysis that the proposed scheme is resilient against the following attacks.

Mobile User (MU)	Foreign Agent (FA)	Home Agent (HA)
MU inputs ID_{MU}, PW $N_M = N'_M \oplus h(PW \| \| ID_{MU})$ $L'_{MU} = h(ID_{MU} \| \| PW \| \| N_M)$ $L'_{MU} \stackrel{?}{=} L_{MU}$ Generate R_M $H_S = H_M \oplus h(PW \| \| N_M)$ $U_M = h(H_S \oplus R_M)$ $V_M = h(ID_{MU} \| \| N_M \| \| U_M \| \| T'_S)$ $\boldsymbol{M_1 = \{V_M, T'_S, R_M\}} \longrightarrow$		
	Generate R_F $V_F = E_{K_{FH}}(M_1, R_F)$ $\boldsymbol{M_2 = \{ID_{FA}, V_F\}} \longrightarrow$	
		Verify ID_{FA} and decrypt V_F $V_F = D_{KFH}(M1, RF)$ $T'_S \stackrel{?}{=} T_S$ $H'_S = h(R_1 \| \| S_{HA} \| \| ID_{HA})$ $U^*_M = h(H'_S \oplus R_M)$ $V^*_M = h(R_1 \| \| U^*_M \| \| T'_S)$ $V^*_M \stackrel{?}{=} V_M$ $SK = h(H'_S \oplus R_M \oplus R_F)$ Update $T_S = T_S + 1$ $V_H = E_{K_{FH}}(SK, R_F)$ $\boldsymbol{M_3 = \{V_H\}} \longleftarrow$
	Decrypt V_H; verifies R_F $W = h(SK \| \| R_F)$ $\boldsymbol{M_4 = \{W, R_F\}} \longleftarrow$	
$SK^* = h(H_S \oplus R_M \oplus R_F)$ $W^* = h(SK^* \| \| R_F)$ $W^* \stackrel{?}{=} W$; Update $T'_S = T'_S + 1$		

FIGURE 3. Summary of login and authentication phases of the proposed scheme.

1) ANONYMITY AND USER UNTRACEABILITY

In registration, user's identity ID_{MU} has associated with the cryptographic nonce that is $R_1 = (ID_{MU} \| N_M)$ and submits to *HA* via a secure channel. As a result, an adversary $\mathscr{A}$, including valid *HA* cannot derive ID_{MU} from registration request R_1. During login and authentication, we assuming that the intruder $\mathscr{A}$ intercepts the authentication message $M_1 = \{V_M, T'_S, R_M\}$, $M_2 = \{ID_{FA}, V_F\}$, $M_3 = \{V_H\}$, $M_4 = \{W, R_F\}$ communicated between the entities *MU*, *HA* and *FA*. Notably the messages $\{M_1, M_2, M_3, M_4\}$ does not provide any user information. In this system, any other communicating parties including valid *FA* does not know the identity of the user. Therefore, the the user privacy and the anonymity is preserved. If $\mathscr{A}$ willing to trace the user using a extracted data in communication, $\mathscr{A}$ should discover a relationship between various sessions. In this system, the messages M_1, M_2, M_3, M_4 shared via *MU*, *HA* and *FA* are dynamic in nature due to the cryptographic nonce values

Mobile User (MU)	MU**'s device**
Enter valid credentials ID_{MU} and PW	
	Compute $N_M = N'_M \oplus h(PW\|\|ID_{MU})$,
	$H_S = H_M \oplus h(PW \|\|N_M)$,
	$L^*_{MU} = h(ID_{MU} \|\|PW \|\|N_M)$
	Check $L^*_{MU} \stackrel{?}{=} L_{MU}$
	If so, input new password PW^*
	Calculate $N^*_M = N_M \oplus h(PW^*\|\|ID_{MU})$
	$L^*_{MU} = h(ID_{MU}\|\|PW^*\|\|N_M)$
	$H^*_M = H_S \oplus h(PW^*\|\| N_M)$
	Replace $\{L_{MU}, H_S, N'_M\}$ with $\{L^*_{MU}, H^*_S, N^*_M\}$ in the device

FIGURE 4. Summary of password change phase of the proposed scheme.

R_M, R_F. As a result, the adversary $\mathscr{A}$ unable trace an MU location.

2) PREVENTION OF REPLAY ATTACKS

In the mutual authentication process, if the attacker $\mathscr{A}$ intercept messages $\{M_1, M_2, M_3, M_4\}$ communicated between MU, FA and HA, these data cannot be replayed to cheat HA. Because the user and FA generates the cryptographic nonce R_M, R_F in each login and authentication sessions to find $M_1 = \{V_M, T'_S, R_M\}$, $M_2 = \{ID_{FA}, V_F\}$. Besides, the protocol makes use of track sequence number based authentication process to withstand replay attack. If the eavesdropper replays a previous login messages, home agent will successfully detects an attack by using a stored sequence number T_S. Assume, if HA receives a replay message $M^*_2 = \{ID_{FA}, V_F\}$, then HA decrypts and uses a stored track sequence number T_M to compare with received T'_M. If the message $M^*_2 = \{ID_{FA}, V_F\}$, is a replay, obviously the comparison will be unsuccessful. Consequently, HA is unable to find V^*_M, since the retrieved value T'_M is not same as the decrypted T_M. Hence, this mechanism prevents the replay attacks.

3) SECURITY AGAINST MASQUERADE ATTACKS

Suppose the attacker $\mathscr{A}$ eavesdrops some sensitive data from the communication sessions and impersonates as the valid FA or HA to cheat the user or $\mathscr{A}$ masquerade as the valid user to obtain the desired services. Here, the attacker could face various challenges:

- MU **masquerade attack:** To masquerade the user, the intruder $\mathscr{A}$ suppose to have ID_{MU} and PW. In this system, user's identity ID_{MU} and passwords PW have been not communicated in authentication sessions $\{M_1, M_2, M_3, M_4\}$ through public channel. Even though, $\mathscr{A}$ gets the MU device and its parameters H_M, T_S, N_M, the attacker $\mathscr{A}$ cannot compute $M_1 = \{V_M, T'_S, R_M\}$ to forge FA and HA.
  $H_S = H_M \oplus h(PW|| N_M)$
  $U_M = h(H_S \oplus R_M)$
  $V_M = h(ID_{MU}||N_M||U_M||T'_S)$.
  Thus, this system withstand mobile user masquerade attacks.
- FA **masquerade attack:** It is highly infeasible for the intruder to find the message $M_2 = \{ID_{FA}, V_F\}$ since the attacker require to break the shared secret value K_{FH}, which practically impossible. Furthermore, without knowing the session-key, its very hard for an attacker to compute the message $M_4 = \{W, R_F\}$. Therefore, the mutual authentication framework resist against FA masquerade attacks.
- HA **masquerade attack:** In order to impersonate HA, the attacker should have the master key S_{HA} and the shared secret K_{FH} to compute the message $M_3 = \{V_H\}$ to cheat FA. However, the master key of HA is non-replayable, unforgeable and the secure authenticated object. Therefore, the proposed system withstand HA impersonation attacks.

4) RESILIENT AGAINST DENIAL-OF-SERVICE ATTACKS

In this attack scenario, the unauthorized user creates the invalid authentication requests to make the server unavailable. To prevent DoS attacks, an MU computes $L'_{MU} = h(ID_{MU}||PW||N_M)$ and checks whether $L'_{MU} = L_{MU}$ or not. If comparison succeeds, legality of the user is provided. Otherwise, login request will be terminated. Thus, the attacker will be not allowed into the system to send the invalid requests to the server. Hence, the mutual authentication framework protects against denial of service attacks.

5) SECURITY AGAINST PASSWORD-GUESSING ATTACKS

Consider, the intruder $\mathscr{A}$ obtains $M_1 = \{V_M, T'_S, R_M\}$, $M_2 = \{ID_{FA}, V_F\}$, $M_3 = \{V_H\}$, $M_4 = \{W, R_F\}$ communicated between MU, HA, FA. Nevertheless, $\mathscr{A}$ cannot deduce user's password information PW from the intercepted messages. Assume that $\mathscr{A}$ inputs the random password PW^* to succeed the login phase. However, the attacker will be not able to compute $L'_{MU} = h(ID^*_{MU}||PW^*||N^*_M)$ and compare L'_{MU} with stored L_{MU} without ID_{MU} and N_M. Thus, our scheme provide security against password guessing attack.

6) IDENTIFY THE WRONG PASSWORDS

In this system, MU device validates the identity ID_{MU} and password PW_{MU}, before sending the messages. The intruder $\mathscr{A}$ cannot computes $L'_{MU} = h(ID_{MU}||PW||N_M)$ without the knowledge of ID_{MU}, PW and random nonce N_M to succeed the verification step $L'_{MU} = L_{MU}$ of the login process. Therefore, the mutual authentication system prevents unauthorized logins by validating the user password locally. In addition, the mutual authentication protocol does not require any additional clocks and timestamps to prevent reply attacks. Hence, the system protect against clock synchronization problems in the mobile network.

B. FORMAL SECURITY ANALYSIS

The security strength of the mutual authentication system using a random oracle model, namely the Real-Or-Random (ROR) model [23], has been presented in this section. Subsequently, we analysed the authentication proof of the proposed system through the BAN Logic. Also, the correctness of the mutual authentication protocol has been verified and validated through Proverif and AVISPA tools.

1) FORMAL SECURITY ANALYSIS USING ROR MODEL

In Theorem 1, we prove that the proposed scheme provides the session key security under the widely-accepted ROR model.

Theorem 1: The advantage of the adversary $\mathbb{A}$ in breaking the security of the shared session-key is given by

$$Adv(\mathbb{A}) \leq \frac{{hash_q}^2}{|\mathbb{H}|} + 2.C'.{send_q}^{s'},$$

where $hash_q$ is a hash queries, $send_q$ is a total number of queries that have been sent in the authentication, and $|\mathbb{H}|$ is a hash operation, respectively. Also, C', s' are Zipf's parameters [46].

Proof: We will prove the security of the session key (SK) using random oracle model. In the proposed scheme, there are three entities, namely, MU, HA and FA. Let ${I_{t_1}}^{MU}$, ${I_{t_1}}^{HA}$ and ${I_{t_1}}^{FA}$ are the instances of the user and server, respectively. Adversary $\mathbb{A}$ can do the following queries [47], [48].

- *Execute(I_{t1}, I_{t2})* query: This query allows the $\mathbb{A}$ to eavesdrop the sessions (M_1, M_2, M_3, M_4) communicated between MU, HA and FA.
- *Test(I_t)* query: A coin is tossed by the Adversary to initiate this Test. $\mathbb{A}$ execute the query and if the shared key among MU and HA is fresh and $c = 0$. Subsequently, I_t returns a nonce if the shared secret between the MU and the HA is fresh and $c = 1$. otherwise of the shared key is not fresh, it returns a null value.
- *Corrupt Mobile Device (${I_{t_1}}^{MU}$)* query: Using this query, $\mathbb{A}$ fetches the personal and confidential information kept on the mobile device. This query is a kind of active attack.
- $h(.)$ query: A coin is tossed by the Adversary to initiate this Test. $\mathbb{A}$ execute the $h(.)$ query and gets the result oif $c = 0$. Besides, I_t returns the nonce if $c = 1$. The oracle maintains a Table to keep track of the input provided by the $\mathbb{A}$.

To prove the above stated theorem, we defined four games, namely, G_I, G_{II}, G_{III}, G_{IV}. Let PS_i be the probability with which an adversary $\mathbb{A}$ wins the game G_i where $i = I, II, III, IV$. Below we discussed the details of the four games.

Game G_I: It is a first game in which the attacker selects a bit c (discussed in the *Test(I_t)* query). As this is the initial game, this game and the proposed scheme are exactly similar. Mathematically,

$$Adv(\mathbb{A}) = [Pr[PS_0] - \frac{1}{2}] \tag{1}$$

Game G_{II}: Here, $\mathbb{A}$ performs the interception. It makes the *Execute()* query as many times as it wants and at the end $\mathbb{A}$ makes a *Test(I_t)* query. Then, output of a *Test(I_t)* query tells that weather the real secret-key SK or the cryptographic nonce. In this mutual authentication framework, the secret-key SK is computed by MU ans FA as $SK = h(H'_S \oplus R_M \oplus R_F)$ where $H'_S = h(R_1||S_{HA}||ID_{HA})$. Here, the secrets R_M and R_F are unknown to the $\mathbb{A}$ even if he eavesdrop the messages communicated between the entities. Hence, the winning probability of the game G_{II} by the $\mathbb{A}$ does not increase using eavesdropping attack and mathematically,

$$Pr[PS_1] = Pr[PS_0] \tag{2}$$

Game G_{III}: This is similar to the previous game, except that $\mathbb{A}$ can issue extra two kinds of queries i.e. *Hash()* query and *send()* query. This game can act as an active attack where $\mathbb{A}$ could eavesdrop M_1, M_2, M_3, and M_4. Random nonce are present in their messages. As a result, no collision in the output of hash function will occur when $\mathbb{A}$ will issue hash queries [49]. Therefore,

$$|Pr[PS_2] - Pr[PS_1]| \leq \frac{{hash_q}^2}{2|\mathbb{H}|} \tag{3}$$

Game G_{IV}: It is the final game which is played by the adversary. In this game, the $\mathbb{A}$ can do one extra query which is known as *Corrupt Mobile Device (${I_t}^{MU}$)* query. In this game, $\mathbb{A}$ can access ID_{MU} and PW of the MU. Note that $H_S = H_M \oplus h(PW||N_M)$, $U_M = h(H_S \oplus R_M)$, and $V_M = h(ID_{MU}||N_M||U_M||T'_S)$. Without knowing a secret-credential of the user i.e. R_M and the master key of HA, i.e. S_{HA}, $\mathbb{A}$ can't guess the password of the system i.e. PW. As a result, G_{IV} and G_{III} are same. Mathematically,

$$|Pr[PS_3] - Pr[PS_2]| \leq C'.{send_q}^{s'} \tag{4}$$

As all games will be completed, $\mathbb{A}$ can guess a right bit c with probability $\frac{1}{2}$. Thus,

$$Pr[PS_3] = \frac{1}{2} \tag{5}$$

Solving Equation (1) and (2), we get

$$\frac{1}{2}.Adv(\mathbb{A}) = |Pr[PS_1] - \frac{1}{2}| \tag{6}$$

Putting Equation (5) in (6),

$$\frac{1}{2}.Adv(\mathbb{A}) = |Pr[PS_1] - Pr[PS_3]| \tag{7}$$

Now, by applying the triangular inequality, we obtain the following relation:

$$\begin{aligned} |Pr[PS_1] - Pr[PS_3]| &= |Pr[PS_1] - Pr[PS_2]| \\ &\quad + |Pr[PS_2] - Pr[PS_3]| \\ &\leq \frac{{hash_q}^2}{2|\mathbb{H}|} + C'.{send_q}^{s'} \\ \implies \frac{1}{2}.Adv(\mathbb{A}) &\leq \frac{{hash_q}^2}{2|\mathbb{H}|} + C'.{send_q}^{s'} \\ \implies Adv(\mathbb{A}) &\leq \frac{{hash_q}^2}{|\mathbb{H}|} + 2.C'.{send_q}^{s'} \end{aligned}$$

□

2) AUTHENTICATION PROOF THROUGH BAN LOGIC

The mutual authentication proof of the protocol anlyzed Burrows-Abadi-Needham (BAN) logic [50], which ensures that the proposed authentication protocol achieves mutual authentication and secure session key establishment. The BAN logic is widely accepted model to analyse the security strength of authentication protocols [50]. The main construction of BAN involves symbols and some rules, which are defined first, after proof of the proposed protocol is described.

Notations Used:

$M| \equiv N$: The entity M believes a message N.
$M \Rightarrow N$: M has jurisdiction on N.
$M \triangle N$: M sees the statement N.
$\#R$: The message N is fresh.
$M| \sim N$: M once said N.
$\{N\}_K$: N encrypted with K.
$M \overset{K}{\longleftrightarrow} N$: The key K is shared between M and N.

BAN Logic Rules:

B1 *Message Meaning Rule:*

$$\frac{M| \equiv M \overset{K}{\longleftrightarrow} N, M \triangle \{N\}_K}{M| \equiv N| \sim N}.$$

B2 *Nonce Verification Rule:*

$$\frac{M| \equiv \#(R), M| \equiv N| \sim R}{M| \equiv N| \equiv N}.$$

B3 *Jurisdiction Rule:*

$$\frac{M| \equiv N| \Rightarrow R, M| \equiv N| \equiv R}{M| \equiv N}.$$

B4 *Session-Key Rule:*

$$\frac{M| \equiv \#(R), M| \equiv N| \equiv R}{M| \equiv M \overset{K}{\longleftrightarrow} N}.$$

B5 *Freshness Concatenation-Rule:*

$$\frac{M| \equiv \#(R)}{M| \equiv \#(R, N)}.$$

The secrecy functionalities of the authentication scheme is analysed and proved through BAN extended-rule:

$$\frac{M| \equiv N \overset{K}{\longleftrightarrow} M, M \triangleleft f(R, N)}{M| \equiv N| \sim R)}.$$

Notably, K is a shared secret between M and N; The originality principal is validated through a function f.

BAN Logic-Based Proof Idealized Form: In the mutual authentication process, the message flows between the mobile terminal (MT), home server (HS), Foreign server (FS) is modelled into the idealized form:

M_1: $MT \rightarrow FN : \{MT \overset{H_S}{\longleftrightarrow} HS, ID_{MU}, R_M, T'_S\}$.
M_2: $FS \rightarrow HS : \{\{MS \overset{H_S}{\longleftrightarrow} HS, ID_{MU}, R_M, T'_S, R_F\}_{KFH}, ID_{FA}\}$.
M_3: $HS \rightarrow FS : \{HS \overset{KFH}{\longleftrightarrow} FS, H_S, R_M, R_F\}$.
M_4: $FS \rightarrow MT : \{FS \overset{SK}{\longleftrightarrow} MT, R_M, H_S, R_F\}$.

The security protocol is analyzed through the subsequent assumptions:

A1: $MT| \equiv MT \overset{H_S}{\longleftrightarrow} HS$;
A2: $HS| \equiv MT \overset{H_S}{\longleftrightarrow} HS$;
A3: $FS| \equiv FS \overset{K_{FH}}{\longleftrightarrow} HS$;
A4: $HS| \equiv FS \overset{K_{FH}}{\longleftrightarrow} HS$;
A5: $MT| \equiv \#R_M$; $FN| \equiv \#R_F$;
A6: $HS| \equiv FS| \Rightarrow FS \overset{SK}{\longleftrightarrow} HS$;
A7: $FS| \equiv HS| \Rightarrow FS \overset{SK}{\longleftrightarrow} HS$;
A8: $FS| \equiv MT| \Rightarrow MT \overset{SK}{\longleftrightarrow} FS$;
A9: $MT| \equiv FS| \Rightarrow MT \overset{SK}{\longleftrightarrow} FS$;

HS Mutual Authentication: according to B1-B5 rules on the proposed scheme:

$$\frac{HS| \equiv MT \overset{H_S}{\longleftrightarrow} HS, HS \triangle f(h(ID_M||H_S||N_M), R_M)}{HN| \equiv MT| \sim V_M}.$$

Hereafter, through freshness-rule B5:

$$\begin{aligned} &(HS| \equiv (R_M, V_M))/(HS| \equiv R_M)); \\ &(HS| \equiv \#(T'_S))/(HS| \equiv \#(T'_S, V_M)); \\ &(HS| \equiv \#(T'_S))/(HS| \equiv \#(T'_S, R_M)). \end{aligned}$$

Likewise, $HS| \equiv FS| \sim V_F$; specifically, according to B1:

$$\frac{HS| \equiv FS \overset{K_{FH}}{\longleftrightarrow} HS, HS \triangle f(ID_{FA}, \{V_F\}_{KFH})}{HS| \equiv FS| \sim V_F}.$$

Using the above statement, we can realize:

$$\frac{HS| \equiv (M_2, V_F)}{HS| \equiv M_2}.$$

FA Mutual Authentication Process: $FS| \equiv HS| \sim V_H$, $FS| \equiv \#(R_F)$ and $((FS| \equiv (M_3, R_F))/(FS| \equiv M_3))$; according to rule B1:

$$\frac{FS| \equiv HS \overset{K_{FH}}{\longleftrightarrow} FS, FS \triangle f\{SK, R_F\}_{KFH}}{FS| \equiv HS| \sim R_F}.$$

Using freshness rule B5:

$$\frac{FS| \equiv \#(R_F)}{FS| \equiv \#(R_F, SK)}; \frac{FS| \equiv \#(SK)}{FS| \equiv \#(M_3, SK)};$$

Using jurisdiction rule B3:

$$\frac{FS| \equiv HS| \Rightarrow SK, FS| \equiv HS| \equiv SK}{FS| \equiv SK}.$$

MT Mutual Authentication Process: $MT| \equiv HS| \sim M_4, MT| \equiv \#(SK)$ and $(MT| \equiv (M_4, SK))/(MT| \equiv M_4)$;

According to message meaning-rule B1:

$$\frac{MT| \equiv HS \overset{H_S}{\longleftrightarrow} MT, MT \triangle f(h(SK||R_F), R_F)}{FS| \equiv HS| \sim R_F}.$$

Here, MS computes and verifies $W^* = h(SK^*||R_F)$, which is meant for shared secret-key establishment. Because in the case of wrong W^*, MS will be not allowed to form the correct secret-key $SK = h(H_S \oplus R_M \oplus R_F)$ to communicate with *FA*. Using belief rules:

$$(MT| \equiv (R_F, H_S))/(MT| \equiv R_F));$$
$$(MT| \equiv (W, R_F))/(MT| \equiv (W));$$
$$(MT| \equiv (SK, W))/(MT| \equiv (SK)).$$

Likewise, the mutual authentication framework in mobility environment satisfies all security functionalities and goals. Consequently, the valid participants mobile subscriber and the foreign network communicates each other using the negotiated session key SK.

3) FORMAL SECURITY-VERIFICATION USING ProVerif

The mutual authentication system has been demonstrated through ProVerif [14]. It is a popular tool for modelling the security protocols and the adversary capabilities using the Horn theory [51]. In ProVerif specification the communication parties like the user and servers have simultaneous execution in the mutual authentication process. The communication parties have capability to send and receive messages over the network.

Notably, *MU*, *HA* and *FA* could verify the authenticity, integrity and secrecy of the transmitted information based on the specified events. Further, the adversary has capability to eavesdrop, modify and reply the messages communicated between the communication agents in the mobility network. Basically, Pi calculus is used to specify the proposed security framework. Later on, it is translated into ''Horn clauses''.

ProVerif result is a verification of all security properties and goals. If the specified protocol is not true, ProVerif tool gives a trace to the cryptographic attack. ProVerif code of functions, channels, private-keys, reduction functions, constants, names, equations, events and the queries are summarized in Figure 5. In this protocol verification process, the operations in the registration and mutual authentication phase is taken into the account. The formal verification model of the mobile user process using ProVerif is described in Figure 6.

```
(*..... Functions.....*)
fun xor(bs,bs):bs (*Xor operation, bs:bitstring*)
fun h(bs):bs (*Hash function*)
fun Concat(bs,bs):bs (*Concatenation operation*)
fun exp(bs, bs): bs (*Exponentiation operation*)
fun En(bs,bs):bs (* Symmetric Encryption process*)
reduc for all a:bs, b:bs; De(En(a,b),b)=a
(*..... Equations.....*)
equation for all a:bs,b:bs; xor(xor(a,b),b)=a.
x: bs,y:bs; exp(exp(g, x),y)=exp
(exp(g, y),x).
(*..... Communication Channels Used.....*)
free C1: channel [public]
free C2: channel [public]
free SC: channel [private]
(*..... Pre-shared Key and Secret Key.....*)
free KFH: bs
free SK: bs [private]
(*.....Free Names and Constants.....*)
free IDM:bs [private]
free PWM:bs [private]
const IDF:bs; const IDH:bs; const p:bs; table db(bs); const g:bs
(*..... Events.....*)
event: evt evt start_MU(bs)
evt end_MU(bs)
evt start_FA(bs)
evt end_FA(bs)
evt start_HA(bs)
evt end_HA(bs)
(*..... Secrecy Queries.....*)
query adversary(SK);
query adversary(SK');
query adversary(IDM);
query weaksecret PWM;
(*..... Authentication Queries.....*)
evt-inj (auth_MU(id)) ==> evt-inj (start_MU(id)).
evt-inj (auth_FA(id))==> evt-inj(start_FA(id)).
```

FIGURE 5. Definitions used in ProVerif.

FA operations consist of reception of message $M_1 = \{V_M, T'_S, R_M\}$ from *MU*, sending message $M_2 = \{ID_{FA}, V_F\}$ to the *HA*, receiving message $M_3 = \{V_H\}$ from *HA* and returns message $M_4 = \{W, R_F\}$ to the *MU* sequentially. The ProVerif code for *FA*'s formal verification process is given in Figure 7. Similarly, formal verification model for *HA* process is presented in Figure 8 and the resultant queries of the system are summarized in Figure 9.

4) FORMAL SECURITY-VERIFICATION USING AVISPA

The proposed security system has been simulated through the formal verification tool called ''Automated Validation of Internet Security Protocols and Applications'' (AVISPA) [52]. It is used to prove the correctness of the cryptographic protocol over an insecure channel. The mutual authentication framework for the mobile network is specified in ''High Level Protocol Specification Language'' (HLPSL). There is a HLPSL2IF translator in AVISPA, which converts the HLPSL source code into Intermediate Format (IF). Later on, the IF can be fed into AVISPA backends like OFMC and

TABLE 2. Comparison of the security requirements and functionalities.

Security requirements	Proposed	Protocol [3]	Protocol [13]	Protocol [39]	Protocol [40]
User anonymity	✓	✓	✓	✓	✓
Mutual authentication	✓	✓	✓	✓	✓
Withstand insider attacks	✓	✓	✓	✓	✓
Withstand impersonation attacks	✓	×	×	✓	✓
Resilience to password guessing	✓	✓	✓	✓	✓
Withstand smartcard loss	✓	✓	✓	✓	✓
Resistance to replay-attacks	✓	✓	×	×	✓
Perfect forward-secrecy	✓	✓	✓	✓	✓
Prevent stolen verifier attacks	✓	×	✓	✓	✓
Local Password-verification	✓	✓	×	✓	×
Fair-Key negotiation	✓	✓	✓	×	✓
Clock-synchronization problem	✓	×	✓	✓	✓
Prevent DoS attacks	✓	✓	×	✓	×
User Friendliness	✓	✓	×	✓	×

```
let MU= new NM:bitstring;
let R1=Concat(IDM, NM) in
out(SC1,(R1));
in(SC1,(HS:bitstring, TS:bitstring));
let LMU=h(IDM, PW, NM) in
let HM=xor(HS, h(PW)) in
let T'S=TS;
insert sc(LMU, HM, T'S, NM);
!
(
evt start_MU(IDM);
let L'MU=h(IDM, PW, NM)
if L'MU=LMU then
new RM:bitstring;
let HS=xor(HM, h(PW)) in
let UM=h(xor(HS, RM)) in
let VM=h(Concat(IDM, NM, UM, T'S)) in
let M1=(VM, T'S, RM) in
out(C1,M1);
in(C1,(W:bitstring, RF:bitstring));
let SKMU=h(xor(HS, RM, RF) in
if W=h(Concat(SKMU, RM)) then
evt end_MU(IDM);
0).
```

FIGURE 6. Formal Verification of *MU* Process.

```
let FA=
!
(
in(C1,(VM:bitstring, T'S:bitstring, RM:bitstring));
evt start_FA(IDF);
new RF:bitstring;
let VF=(En((M1, RF), KFH))) in
let M2=(IDF, VF) in
out(C2, M2);
in(C2, VH);
let De(VH, KFH) in
if haRF=RF then
let W=h(Concat(SK, RF) in
let M4=(W, RF) in
out (C1, M4);
evt end_FA(IDF)
0
).
```

FIGURE 7. Formal Verification of *FA* Process.

CL-AtSe to produce the verification result of the specified protocol [53].

Basically, HLPSL language is role and goal oriented programming language, in which roles of the user, foreign, and the home agents will be specified. Consequently, the security protocol sessions and the adversaries will be modelled using a threat model called Dolev-Yao (DY) [54]. AVISPA is a push button interface, where the security protocol is submitted in HLPSL code and the result is the summary, which displays the protocol status (safe or unsafe) with the details of the security goals and the environment. Besides, if the protocol is unsafe, AVISPA gives the trace to the attack and displays the intruder knowledge about the authentication sessions.

The AVISPA results for the mutual authentication framework using the CL-AtSe as a backend as shown in Figure 10. Notably, the security protocol is safe and satisfied all security goals in the global roaming scenario. Furthermore, the mutual authentication system is simulated through "Security Protocol Animator" (SPAN), which generates the message sequence chart for the specified protocol sessions [55]. If the specified protocol is unsafe, SPAN displays the attack and the intruder simulations through the graphical user interface.

```
let HAReg1=
in(SC1,R1:bitstring);
let HS=h(Concat(R1, SHA, IDH)) in
new TS:bitstring;
let TS=0; in
insert db(R1, TS);
let R2=(HS, TS):bitstring;
out (SC1, R2)
let Auth_HA=
in(C2,(haIDF:bitstring, haVF:bitstring);
evt start_HA(IDH)
if haIDF=IDF then
evt Auth_FA(IDF);
let haVF=De(En(VF), KFH) in
get db(=R1, TS) in
if T'S=TS then
let H'S=h(Concat(R1, SHA, IDH)) in
let U*M=h(xor(H'S, RM)) in
let V*M=h(Concat(R1, U*M, T'S)) in
if V*M = VM then
evt Auth_MU(VM);
let haSK=h(xor(H'S, haRM, haRF)) in
insert db(R1,TS+1);
let VH=En((SK, RF), KFH) in
let M3=VH in
out(C2, M3)
evt end_HA(IDH)
process !MU–!HA–!FA
```

FIGURE 8. Formal Verification of *HA* Process.

```
Q: query; Res: Result; ST: Start; evt: event;
Q not weak_secret(PWM[])
Res not weak_secret (PWM[]) is true.
Q not adversary(SK[])
Res not adversary(SK[]) is true.
Q evt-inj (auth_MU(ID))==> evt-inj (ST_MU(ID))
starting Q evt-inj (auth_MU(ID))==> evt-inj (ST_MU(ID))
Res evt-inj (auth_MU(ID))==> evt-inj (ST_MU(ID)) is true.
Q evt-inj (auth_HA(ID)) ==> evt-inj (ST_HA(ID))
starting Q evt-inj (auth_HA(ID)) ==> evt-inj (ST_HA(ID))
Res evt-inj (auth_HA(ID)) ==> evt-inj (ST_HA(ID)) is true.
Q evt-inj (auth_FA(IDF[])) ==> evt-inj (ST_FA(ID_1280))
starting Q evt-inj (auth_FA(IDF[])) ==> evt-inj (ST_FA(ID_1280))
Res evt-inj (auth_FA(IDF[]))==> evt-inj (ST_FA(ID_1280)) is true.
Q not adversary(ID_MU)
Result not adversary(ID_MU) is true.
query not adversary(SK'[])
Result not adversary(SK'[]) is true.
```

FIGURE 9. ProVerif result analysis.

VII. PERFORMANCE EVALUATION

In this scenario, we could verify security properties and performance of the security system with some other recent authentication schemes [3], [13], [39], [40]. Basically, mobility terminals have limited resources in terms of bandwidth, memory, power, processor and low computing capability. Therefore, an important issue in global mobile network is energy consumption caused by communication and computation operations to establish the secure communication channel. The mutual authentication system is to resist against several security flaws in the existing authentication schemes for global mobile networks.

TABLE 3. Crypto primitives with the execution time (in seconds).

Notations	Description	Execution time (in seconds)
T_h	Hash operation	0.0005
T_m	Modular exponentiation operation	0.522
T_{sym}	Symmetric cryptosystem	0.0087
T_{asym}	Public-key cryptosystem	0.0172
T_p	Elliptic curve point multiplication	0.763

It is clear evident from Table 2 that the security framework satisfies all security properties needed for the mobile user roaming service. In addition, the proposed authentication protocol have to maintain the sensible communication and computational complexities. Notably, the efficiency estimation is performed in terms of the computation and communication cost. To evaluate the performance of the authentication schemes, the computational cost in login and authentication scenario is taken into account because this phase is carried out every time of the roaming process. To evaluate the performance of the security framework in the resource-constrained environments, various security algorithms have been implemented through the Crypto library called MIRACL [56], [57] on the smartphone.

The smartphone runs on Android OS with a frequency of 0.71 GHz. In addition, the mobile device makes use of the Arm Cortex-A8 processor to run various cryptosystems. Consequently, the symmetric and asymmetric cryptosystems are AES (Advanced Encryption Standard) and ECIES (Elliptic Curve Integrated Encryption Scheme), respectively. Besides, the hash function SHA-256 is used to compute the message digest. The experimental results provides the execution time of different cryptographic operations such as hash operation, symmetric/asymmetric computations, modular computation, and elliptic curve point operations are summarized in Table 3.

The computational overhead of various cryptographic primitives in terms of CPU cycles have been demonstrated in [35]. As per the experimental results the hash function take $5.63 * 10^2$. The exponentiation function in Diffie-Hellman algorithm requires $9.52 * 10^6$. In addition, private and public-key cryptosystems take $7.56 * 10^2$ and $12.42 * 10^6$, appropriately. The computational cost (execution time) comparison of the proposed security framework and other recent works [3], [13], [39], [40] are presented in Table 4.

The proposed scheme includes few symmetric operations and the hash functions. Notably, *MU* wants six cryptographic hash functions to form the message M_1. The *FA* wants a hash operation to compute the digest and two symmetric functions to send messages in *HA* and MU, eventually. *HA* require four

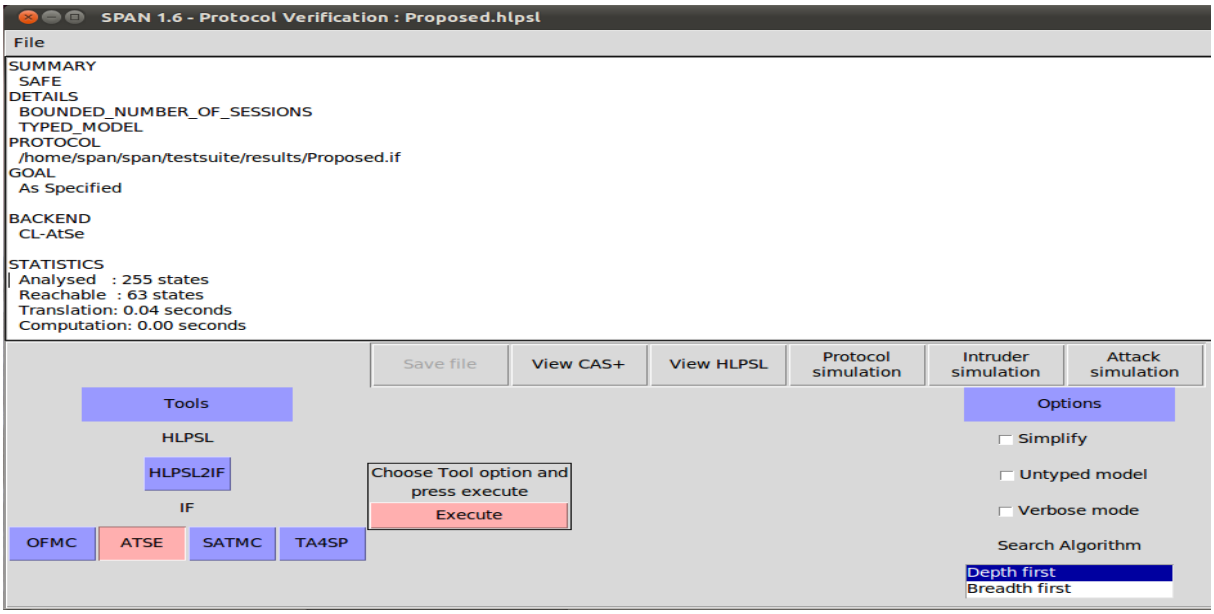

FIGURE 10. Result analysis using CL-AtSe backend.

TABLE 4. Performance analysis on computational overheads.

Computation	Protocol [3]	Protocol [13]	Protocol [39]	Protocol [40]	Proposed
C_{MU}	$8T_h + 3T_m$	$10T_h$	$9t_h + 2T_m + 2T_{sym}$	$2T_p + T_{sym} + 7T_H$	$6T_h$
C_{FA}	$3T_h$	$8T_h$	$3T_h + T_{sym}$	$2T_p + 5T_H$	$T_h + 2T_{sym}$
C_{HA}	$8T_h + T_m + 3T_{sym}$	$8T_h$	$8T_h + T_m + 3T_{sym}$	$3T_{sym} + 6T_H$	$4T_h + 2T_{sym}$
Total	$19T_h + 4T_m + 3T_{sym}$	$26T_h$	$20T_h + 3T_m + 6T_{sym}$	$4T_p + 4T_{sym} + 18T_H$	$11T_h + 4T_{sym}$
Time (s)	2.123	0.013	1.628	3.095	0.040
CPU Cycles	$380929.65 * 10^2$	$146.38 * 10^2$	$285757.96 * 10^2$	$496131.58 * 10^2$	$92.17 * 10^2$

C_{MU} : Computation overhead of MU; C_{FA}: Computation overhead of FA; C_{HA}: Computation overhead of HA

TABLE 5. Analysis of communication overheads (in bits).

Process	Protocol [3]	Protocol [13]	Protocol [39]	Protocol [40]	Proposed
Registration	1120	320	1280	1280	640
User Login	800	640	800	640	480
Authentication & key-negotiation	2400	1600	1600	2080	800
Password change phase	–	800	–	800	–
Total cost	4320	3360	3680	4800	1920

hash values and two symmetric systems to authenticating *MU* and *FA*.

From Table 4, its clear that the security framework is the efficient than the mutual authentication systems in [3], [39], [40]. Notably, the computation overhead of security protocol is slightly increases as compared to the protocol in [13]. Nevertheless, the protocol in [13] has no local password verification mechanism, protection against the masquerade and replay attacks.

Table 5 summarizes the comparison of the communication cost of the systems in [3], [13], [39], [40] and the proposed mutual authentication system. o To estimate the communica-

tion overhead, assume the hash function of length 160 bits. The cryptographic nonce, timestamp, and the data length of 160 bits, appropriately. In addition, the elliptic curve point of length 320 bits is taken into the account. In proposed scheme, the registration messages $R_1 = \{ID_{MU}||N_M\}, R_2 = \{H_S, T_S, h(.)\}$ needs $(160 + 160 + 160 + 160) = 640$ bits, the login message $M_1 = \{V_M, T'_S, R_M\}$ needs $(160 + 160 + 160) = 480$ bits and the messages $M_2 = \{ID_{FA}, V_F\}, M_3 = \{V_H\}, M_4 = \{W, R_F\}$ needs $(320 + 160 + 320) = 800$ bits. Therefore, the proposed scheme requires $(480+ 480+ 800) = 1760$ bits for the communicated messages in between *MU*, *HA* and *FA*.

We can conclude that the security framework has less communication overhead as compared to mutual authentication works in [3], [13], [39], [40]. Thus, the proposed authentication scheme is secure, lightweight and handy for global roaming in mobile networks.

VIII. CONCLUSION

In this research article, the security strength of Lee *et al.*'s mutual authentication system has been analyzed and found that their security system is susceptible to masquerade attacks, replay attacks, denial-of-service attack and cannot provide untraceability service and, local password detection system. Later on, we proposed a lightweight mutual authentication system for global roaming in the mobility network, which provides the possible security services and resist various attacks. The formal security-verification and validation of the proposed system is carried out through widely accepted security tools like ProVerif and AVISPA. Consequently, the formal security analysis of the system is measured using BAN logic. Besides, the correctness of the security system has been proved using random oracle model. Finally, a rigours performance evaluation summarizes the communication and computational gain of the proposed security system under various constraints. The proposed security system is lightweight, secure and practically implementable in the resource-limited mobile environment.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers and an Associate Editor for their invaluable feedback.

REFERENCES

[1] Q. Jiang, J. Ma, G. Li, and L. Yang, "An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks," *Wireless Pers. Commun.*, vol. 68, no. 4, pp. 1477–1491, Feb. 2013.

[2] S. Suzuki and K. Nakada, "An authentication technique based on distributed security management for the global mobility network," *IEEE J. Sel. Areas Commun.*, vol. 15, no. 8, pp. 1608–1617, Oct. 1997.

[3] M. Karuppiah and R. Saravanan, "A secure authentication scheme with user anonymity for roaming service in global mobility networks," *Wireless Pers. Commun.*, vol. 84, no. 3, pp. 2055–2078, Oct. 2015.

[4] D. Samfat, R. Molva, and N. Asokan, "Untraceability in mobile networks," in *Proc. 1st Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, 1995, pp. 26–36.

[5] J. Ha, "An efficient and robust anonymous authentication scheme in global mobility networks," *Int. J. Secur. Appl.*, vol. 9, no. 10, pp. 297–312, Oct. 2015.

[6] E.-J. Yoon, K.-Y. Yoo, and K.-S. Ha, "A user friendly authentication scheme with anonymity for wireless communications," *Comput. Electr. Eng.*, vol. 37, no. 3, pp. 356–364, May 2011.

[7] D. Zhao, H. Peng, L. Li, and Y. Yang, "A secure and effective anonymous authentication scheme for roaming service in global mobility networks," *Wireless Pers. Commun.*, vol. 78, no. 1, pp. 247–269, Sep. 2014.

[8] C.-C. Lee, M.-S. Hwang, and I.-E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," *IEEE Trans. Ind. Electron.*, vol. 53, no. 5, pp. 1683–1687, Oct. 2006.

[9] C.-C. Chang, C.-Y. Lee, and Y.-C. Chiu, "Enhanced authentication scheme with anonymity for roaming service in global mobility networks," *Comput. Commun.*, vol. 32, no. 4, pp. 611–618, Mar. 2009.

[10] T.-Y. Youn, Y.-H. Park, and J. Lim, "Weaknesses in an anonymous authentication scheme for roaming service in global mobility networks," *IEEE Commun. Lett.*, vol. 13, no. 7, pp. 471–473, Jul. 2009.

[11] C.-T. Li and C.-C. Lee, "A novel user authentication and privacy preserving scheme with smart cards for wireless communications," *Math. Comput. Model.*, vol. 55, nos. 1–2, pp. 35–44, Jan. 2012.

[12] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, "A strong user authentication scheme with smart cards for wireless communications," *Comput. Commun.*, vol. 34, no. 3, pp. 367–374, Mar. 2011.

[13] C.-C. Lee, Y.-M. Lai, C.-T. Chen, and S.-D. Chen, "Advanced secure anonymous authentication scheme for roaming service in global mobility networks," *Wireless Pers. Commun.*, vol. 94, no. 3, pp. 1281–1296, Jun. 2017.

[14] M. Abadi, B. Blanchet, and H. Comon-Lundh, "Models and proofs of protocol security: A progress report," in *Computer Aided Verification*. Berlin, Germany: Springer, 2009, pp. 35–49.

[15] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, N. Kumar, Y. Park, and S. Tanwar, "Design of an anonymity-preserving group formation based authentication protocol in global mobility networks," *IEEE Access*, vol. 6, pp. 20673–20693, 2018.

[16] K. Park, Y. Park, Y. Park, A. G. Reddy, and A. K. Das, "Provably secure and efficient authentication protocol for roaming service in global mobility networks," *IEEE Access*, vol. 5, pp. 25110–25125, 2017.

[17] V. Odelu, S. Banerjee, A. K. Das, S. Chattopadhyay, S. Kumari, X. Li, and A. Goswami, "A secure anonymity preserving authentication scheme for roaming service in global mobility networks," *Wireless Pers. Commun.*, vol. 96, no. 2, pp. 2351–2387, Sep. 2017.

[18] M. Wazid, A. K. Das, N. Kumar, and A. V. Vasilakos, "Design of secure key management and user authentication scheme for fog computing services," *Future Gener. Comput. Syst.*, vol. 91, pp. 475–492, Feb. 2019.

[19] M. Wazid, A. K. Das, N. Kumar, V. Odelu, A. G. Reddy, K. Park, and Y. Park, "Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks," *IEEE Access*, vol. 5, pp. 14966–14980, 2017.

[20] A. Dua, N. Kumar, A. K. Das, and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4359–4373, May 2018.

[21] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, "On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services," *IEEE Access*, vol. 5, pp. 25808–25825, 2017.

[22] S. Chatterjee, A. K. Das, and J. K. Sing, "An enhanced access control scheme in wireless sensor networks," *Ad Hoc Sensor Wireless Netw.*, vol. 21, nos. 1–2, pp. 121–149, Jan. 2014.

[23] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 9, pp. 4957–4968, Sep. 2019.

[24] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. P. C. Rodrigues, "Authentication in cloud-driven IoT-based big data environment: Survey and outlook," *J. Syst. Archit.*, vol. 97, pp. 185–196, Aug. 2019.

[25] L. Wu, J. Wang, K.-K.-R. Choo, and D. He, "Secure key agreement and key protection for mobile device user authentication," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 319–330, Feb. 2019.

[26] S. Chatterjee, A. K. Das, and J. K. Sing, "A survey on user access control in wireless sensor networks with formal security verification," *Int. J. Trust Manage. Comput. Commun.*, vol. 2, no. 3, pp. 259–295, 2014.

[27] A. G. Reddy, A. K. Das, E. Yoon, and K. Yoo, "An anonymous authentication with key-agreement protocol for multi-server architecture based on biometrics and smartcards," *KSII Trans. Internet Inf. Syst.*, vol. 10, no. 7, pp. 3371–3396, 2016.

[28] A. K. Das, S. Kumari, V. Odelu, X. Li, F. Wu, and X. Huang, "Provably secure user authentication and key agreement scheme for wireless sensor networks," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3670–3687, Nov. 2016.
[29] V. Odelu, A. K. Das, M. K. Khan, K.-K.-R. Choo, and M. Jo, "Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size keys and ciphertexts," *IEEE Access*, vol. 5, pp. 3273–3283, 2017.
[30] X. Jia, D. He, N. Kumar, and K.-K.-R. Choo, "A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing," *IEEE Syst. J.*, vol. 14, no. 1, pp. 560–571, Mar. 2020.
[31] M. Ma, D. He, H. Wang, N. Kumar, and K.-K.-R. Choo, "An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8065–8075, Oct. 2019.
[32] F. Wen, W. Susilo, and G. Yang, "A secure and effective anonymous user authentication scheme for roaming service in global mobility networks," *Wireless Pers. Commun.*, vol. 73, no. 3, pp. 993–1004, Dec. 2013.
[33] P. Gope and T. Hwang, "Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks," *IEEE Syst. J.*, vol. 10, no. 4, pp. 1370–1379, Dec. 2016.
[34] F. Wu, L. Xu, S. Kumari, X. Li, A. K. Das, M. K. Khan, M. Karuppiah, and R. Baliyan, "A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3527–3542, Nov. 2016.
[35] P. Gope and T. Hwang, "An efficient mutual authentication and key agreement scheme preserving strong anonymity of the mobile user in global mobility networks," *J. Netw. Comput. Appl.*, vol. 62, pp. 1–8, Feb. 2016.
[36] D. Guo and F. Wen, "A more robust authentication scheme for roaming service in global mobility networks using ECC," *IJ Netw. Secur.*, vol. 18, no. 2, pp. 217–223, 2016.
[37] R. Madhusudhan, "An efficient and secure authentication scheme with user anonymity for roaming service in global mobile networks," in *Proc. 6th Int. Conf. Commun. Netw. Secur.*, Nov. 2016, pp. 119–126.
[38] F. Wu, L. Xu, S. Kumari, X. Li, M. K. Khan, and A. K. Das, "An enhanced mutual authentication and key agreement scheme for mobile user roaming service in global mobility networks," *Ann. Telecommun.*, vol. 72, nos. 3–4, pp. 131–144, Apr. 2017.
[39] M. Karuppiah, S. Kumari, X. Li, F. Wu, A. K. Das, M. K. Khan, R. Saravanan, and S. Basu, "A dynamic ID-based generic framework for anonymous authentication scheme for roaming service in global mobility networks," *Wireless Pers. Commun.*, vol. 93, no. 2, pp. 383–407, Mar. 2017.
[40] H. Arshad and A. Rasoolzadegan, "A secure authentication and key agreement scheme for roaming service with user anonymity," *Int. J. Commun. Syst.*, vol. 30, no. 18, p. e3361, Dec. 2017.
[41] F. Wu, X. Li, L. Xu, S. Kumari, and A. K. Sangaiah, "A novel mutual authentication scheme with formal proof for smart healthcare systems under global mobility networks notion," *Comput. Electr. Eng.*, vol. 68, pp. 107–118, May 2018.
[42] R. Madhusudhan, "A secure and lightweight authentication scheme for roaming service in global mobile networks," *J. Inf. Secur. Appl.*, vol. 38, pp. 96–110, Feb. 2018.
[43] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 1999, pp. 388–397.
[44] H. Mun, K. Han, Y. S. Lee, C. Y. Yeun, and H. H. Choi, "Enhanced secure anonymous authentication scheme for roaming service in global mobility networks," *Math. Comput. Model.*, vol. 55, nos. 1–2, pp. 214–222, Jan. 2012.
[45] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.
[46] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2776–2791, Nov. 2017.
[47] 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.
[48] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K.-K.-R. Choo, and Y. Park, "Design of secure and lightweight authentication protocol for wearable devices environment," *IEEE J. Biomed. Health Informat.*, vol. 22, no. 4, pp. 1310–1322, Jul. 2018.
[49] P. Flajolet, D. Gardy, and L. Thimonier, "Birthday paradox, coupon collectors, caching algorithms and self-organizing search," *Discrete Appl. Math.*, vol. 39, no. 3, pp. 207–229, Nov. 1992.
[50] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proc. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 426, no. 1871, pp. 233–271, 1989.
[51] Q. Xie, B. Hu, X. Tan, and D. S. Wong, "Chaotic maps-based strong anonymous authentication scheme for roaming services in global mobility networks," *Wireless Pers. Commun.*, vol. 96, pp. 1–16, May 2017.
[52] A. Armando, D. Basin, J. Cuellar, M. Rusinowitch, and L. Viganò, "AVISPA: Automated validation of Internet security protocols and applications," *ERCIM News*, vol. 64, pp. 66–67, Jan. 2006.
[53] D. Basin, S. Mödersheim, and L. Viganò, "OFMC: A symbolic model checker for security protocols," *Int. J. Inf. Secur.*, vol. 4, no. 3, pp. 181–208, Jun. 2005.
[54] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.
[55] Y. Glouche, T. Genet, O. Heen, and O. Courtay, "A security protocol animator tool for AVISPA," in *Proc. ARTIST Workshop Secur. Specification Verification Embedded Syst.*, Pisa, Italy, May 2006, pp. 1–7.
[56] W. Dai. (2011). *Crypto++ Library 5.1-A Free C++ Class Library of Cryptographic Schemes*. [Online]. Available: http://www.cryptopp.com/
[57] S. Muftic and E. Hatunic, "CISS: Generalized security libraries," *Comput. Secur.*, vol. 11, no. 7, pp. 653–659, Nov. 1992.

R. SHASHIDHARA received the M.Tech. degree in communication and networks from Visvesvaraya Technological University, Belgaum, India, and the Ph.D. degree in cryptography and network security from the National Institute of Technology Karnataka Surathkal, India. He is currently working as an Assistant Professor with the School of Engineering and Applied Sciences, Bennett University (Times of India Group), Greater Noida, India. He has various research publications in conferences indexed in CORE ranking and many journals of international repute, including ACM, Elsevier, Springer, and IEEE. His research interests include design of robust authentication protocols for wireless and mobility environments, Blockchain technology, cross-site scripting attacks, and security in Internet of Things. He is a reviewer of the many reputed international journals.

SANJEET KUMAR NAYAK (Member, IEEE) received the M.Tech. degree in computer science and engineering from the National Institute of Technology Rourkela, India, and the Ph.D. degree in computer science and engineering from the Indian Institute of Technology Patna, India. He is currently working as an Assistant Professor with the Department of Computer Science Engineering, Bennett University (Times of India Group), India. He has published many conferences indexed in CORE ranking and many journals of international repute, including IEEE Transactions, Elsevier, and Springer. His research interests include security and privacy issues in cloud data storage, security and privacy issues in IoT environment, image encryption using lightweight techniques, blind signature schemes, Blockchain, and smart contracts. He is a member of ACM. He serves as a Reviewer for many IEEE Transactions, and Journals of Elsevier and Springer.

ASHOK KUMAR DAS (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering, the M.Tech. degree in computer science and data processing, and the M.Sc. degree in mathematics from IIT Kharagpur, India. He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. His research interests include cryptography, network security, Blockchain, security in the Internet of Things (IoT), Internet of Vehicles (IoV), Internet of Drones (IoD), smart grids, smart city, cloud/fog computing and industrial wireless sensor networks, intrusion detection, and Blockchain and AI/ML security. He has authored over 250 papers in international journals and conferences in the above areas, including over 215 reputed journal articles. Some of his research findings are published in top cited journals, such as the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON SMART GRID, IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS (formerly IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE), IEEE *Consumer Electronics Magazine*, IEEE ACCESS, IEEE *Communications Magazine*, *Future Generation Computer Systems*, *Computers and Electrical Engineering*, *Computer Methods and Programs in Biomedicine*, *Computer Standards and Interfaces*, *Computer Networks*, *Expert Systems with Applications*, and *Journal of Network and Computer Applications*. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He is on the Editorial Board of IEEE SYSTEMS JOURNAL, *Journal of Network and Computer Applications* (Elsevier), *Computer Communications* (Elsevier), IET *Communications*, KSII *Transactions on Internet and Information Systems*, and *International Journal of Internet Technology and Secured Transactions* (Inderscience). He is a Guest Editor for *Computers and Electrical Engineering* (Elsevier) for the Special Issue on Big Data and IoT in E-Healthcare, for ICT *Express* (Elsevier) for the Special Issue on Blockchain Technologies and Applications for 5G Enabled IoT and for *Wireless Communications and Mobile Computing* for the Special Issue on Security and Privacy for Smart Mobile Devices: Attacks, Challenges, and New Designs. He has served as a Program Committee Member for many international conferences. He also severed as one of the Technical Program Committee Chair for the first International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, June 2019, the International Conference on Applied Soft Computing and Communication Networks (ACN'20), October 2020, Chennai, India, and the second International Congress on Blockchain and Applications (BLOCKCHAIN'20), L'Aquila, Italy, October 2020.

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