IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 12, 2018, accepted April 11, 2018, date of publication April 16, 2018, date of current version May 2, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2827027

Design of an Anonymity-Preserving Group Formation Based Authentication Protocol in Global Mobility Networks

SOUMYA BANERJEE[1], VANGA ODELU[2], ASHOK KUMAR DAS[2], (Member, IEEE), SAMIRAN CHATTOPADHYAY[1], NEERAJ KUMAR[3], (Senior Member, IEEE), YOUNGHO PARK[4], (Member, IEEE), AND SUDEEP TANWAR[5]

[1]Department of Information Technology, Jadavpur University, Kolkata 700 098, India
[2]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India
[3]Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Patiala 147 004, India
[4]School of Electronics Engineering, Kyungpook National University, Daegu 41566, South Korea
[5]Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad 382 481, India

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

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea through the Ministry of Science, ICT and Future Planning under Grant 2017R1A2B1002147 and in part by the BK21 Plus project through the Ministry of Education, South Korea, under Grant 21A20131600011.

ABSTRACT Remote user authentication without compromising user anonymity is an emerging area in the last few years. In this paper, we propose a new anonymity preserving mobile user authentication scheme for the global mobility networks (GLOMONETs). We also propose a new anonymity preserving group formation phase for roaming services in GLOMONETs that meets the extended anonymity requirement without compromising any standard security requirements. We provide the security analysis using the widely-accepted Burrows-Abadi-Needham logic and informal analysis for the proposed scheme to show that it is secure against possible well-known attacks, such as replay, man-in-the-middle, impersonation, privileged-insider, stolen smart card, ephemeral secret leakage, and password guessing attacks. In addition, the formal security verification with the help of the broadly accepted automated validation of internet security protocols and applications software simulation tool is tested on the proposed scheme and the simulation results confirm that the proposed scheme is safe. Moreover, the comparative study of the proposed scheme with other relevant schemes reveals that it performs well as compared to other techniques.

INDEX TERMS Global mobility networks, roaming services, authentication, key agreement, security, BAN logic, AVISPA simulation.

I. INTRODUCTION

Global mobility networks (GLOMONETs) provide the ubiquitous services for mobile users while enabling global roaming. Each user belongs to a specific home network (HA) where he/she is registered. When a user is in the domain of a foreign agent (FA), the FA needs to provide service only after authenticating the user (with HA's help). A remote user authentication scheme for GLOMONETs needs to validate that the user who attempts to access the services has rights to do the same. However, with the increasing concern for privacy and anonymity during the authentication it becomes a challenging task due to the high mobility of the users.

The primary challenge is to establish mutual authentication with a low computation and communication overhead in the context of GLOMONETs. The solution to this problem is non-trivial as the resultant scheme also needs to account for various security issues including but not limited to replay, man-in-the-middle, privileged-insider, impersonation, forgery and session key leakage attacks. It is also desirable that the designed scheme should be equipped to handle other issues like smart card loss and user de-registration.

In recent times, the question of right to privacy is a paramount concern with government agencies and privacy activists are actively involved in this process. Regardless, as part of the academic community, we have to acknowledge that if anonymity can be compromised with a simple court order it is not true anonymity. We present the following two scenarios. In the first scenario, a whistle-blower publishes an expose on some governmental malpractice using one of the many security measures available to obscure his/her identity. However, as he/she accesses the anonymity provider through his/her mobile service provider, the provider is aware of the fact that the traffic from a specific user is routed through anonymity service at the specific time. Even if the service provider does not want to expose the whistle-blower, the government can compel them with a court order. In the second scenario, suppose a laboratory has researchers with competing interests. The laboratory has sensitive resources (e.g., equipments and secure information) that can be remotely accessed only after the user is authenticated as an authorized researcher of the laboratory. Therefore, for security and transparency, it is imperative to maintain a log file of each authenticated access available to all authorized researcher of the laboratory. However, at the same time, due the nature of competing interests of the researchers, they should not be able to reconstruct the access history of a competing researcher.

In the first scenario, there is a question of anonymity as we have security against governmental retribution, while in the later case, it is a textbook case of breach of privacy. The similarities lie in the fact that in both the scenarios, the trusted service provider fails to provide the promised anonymity due to external factors. There is a distinct difference between anonymity and privacy. However, one of the means to ensure privacy is through anonymity. Another way to guarantee privacy is through a trusted entity (e.g., server and internet service provider (ISP)). It is customary to make assumptions of implicit trust towards the authentication server while designing an authentication protocol. Nevertheless, as discussed in the above scenarios, sometimes it is advantageous that the authentication server has some plausible deniability regarding its level of knowledge of the users of the system.

Popular acceptance of technologies like onion routing [1] and its popular implementation, the TOR bundle [2] demonstrate the need of service provider independent anonymity. The fact that many current commercial VPN services advertise that they do not maintain any user logs which demonstrates the need of plausible dependability. In this paper, we propose a new anonymity-preserving authentication scheme for roaming services in GLOMONETs such that while authenticating, a roaming mobile user can choose to be anonymous even to his/her home agent (HA), and thus it allows the *HA* plausible deniability.

A. RELATED WORK

In this section, we give an overview of the existing relevant research work on the mobile user authentication in GLOMONETs.

In 1981, Lamport [3] proposed a scheme for remote user authentication over insecure communication channel. Hwang and Li [4] then identified that the password table used in Lamport's scheme is susceptible to verifier modification attacks. In 1999, Yang and Shieh [5] first proposed a smart card based remote that avoids a sensitive verification table to be stored at the server side. Later, several schemes have been proposed and improved by the researchers (for example, the schemes of Wu [6], Tan and Zhu [7] and Chien *et al.* [8]). However, most schemes proposed do not support mutual authentication between the user and the server. The schemes proposed by Ming and Hong [9] and Chien *et al.* [10] were among earliest schemes to support mutual authentication. But in these schemes, the identity of a user used in authenticating himself/herself can be exposed to any or all parties eavesdropping. The remote authentication schemes that obscure the user's identity from an adversary are considered to be anonymous remote authentication schemes.

Das *et al.* [11] first introduced the concept of dynamic ID for users of the system. Their scheme supports user chosen password that could be freely changed at any time. Chien and Chen [12] demonstrated that the dynamic ID can be directly associated with user's actual identity by simply monitoring plaintext variable in the login request message, thus compromising anonymity. Liao *et al.* [13] uncovered that [11] is vulnerable to guessing attack that exposes the user's password to the server and also fails to achieve mutual authentication. They then proposed a modified scheme to overcome the aforementioned drawbacks while retaining its strength of Das *et al.*'s scheme [11]. However, Yoon and Yoo [14] also demonstrated a reflection attack on the improved scheme of Liao *et al.* [13] that breaks the mutual authentication property.

Zhu and Ma [15] in 2004 proposed a scheme which uses a temporary ID to provide user anonymity. But, Lee *et al.* [16] discovered that the scheme described in [15] fails to achieve mutual authentication and it is also susceptible to forgery attacks. Wu *et al.* demonstrated both the schemes [15], [16] fail to achieve user anonymity. They proposed a scheme to remedy the drawbacks found in [16]. Chang *et al.* [17] in 2009 presented an improvement to the scheme [16] as they demonstrated that the scheme [16] fails to provide anonymity when under an forgery attack. Chang *et al.*'s scheme is a lightweight authentication scheme as it only utilized bitwise exclusive (XOR) operation and one-way cryptographic hash function. Young *et al.* [18] cryptanalyzed Cheng *et al.*'s scheme and found that it fails to meet the security requirements.

In 2012, Madhusudan and Mittal [19] refined the criteria in earlier works [20]–[23] and proposed a set of security requirement and a set of desirable attributes for anonymous remote user authentication schemes. They reviewed several existing works [11], [13], [14], [24], [25] and observed none of the schemes meets all the stated criteria. In 2015, Wang *et al.* [26] argued that all the desirable attributes proposed in [19] cannot be simultaneously be satisfied as some of them contradict each other.

In 2014, Gope and Hwang [27] designed a mutual authenticated key agreement protocol. Later, in 2017, Madhusudhan and Suvidha [28] pointed out that Gope-Hwang's scheme is susceptible to replay, stolen smart card, offline password guessing and forgery attacks. In addition, their scheme does not preserve user anonymity. To remedy the security loopholes, they designed another user authentication protocol which can maintain the anonymity property in GLOMONETs.

In 2016, Arshad and Rasoolzadegan [29] analyzed the scheme of Karuppiah *et al.* [30] and showed that their scheme fails to protect off-line password-guessing attack and it does not also provide perfect forward secrecy property.

In 2012, Mun *et al.* [31] proposed a protocol to overcome the weaknesses of existing proposed protocols in GLOMONETs. Later, in Mun et al.'s scheme was shown to be insecure against masquerade as well as man-in-the-middle attacks by Lee *et al.* [32] in 2017. In addition, Lee *et al.* [32] pointed out that Mun *et al.*'s scheme does not preserve the anonymity and prefect forward secrecy properties.

In 2016, Xu and Wu [33] presented a three-factor user authenticated key agreement scheme in GLOMONETs. However, this scheme lacks supporting smart card re-issue phase. Also, Li *et al.* [34] proposed a user authentication protocol for GLOMONETs in smart city environment by enhancing the security of an existing user authentication scheme of Gope and Hwang [27]. Moreover, recently several other authentication schemes have been also proposed in the literature in GLOMONETs [35]–[39].

Samarati and Sweeney [40] introduced the concept k-anonymity for protecting privacy in person specific data. The k-anonymity model was further refined into fore advanced models to provide differential privacy [41], [42]. The k-anonymity property as introduced in [40] is that information about any individual in the released data should be indistinguishable from at least $k-1$ individuals whose information also appears in the same data.

In this paper, we explore a more stringent privacy requirement and consequently adapt the desirable attributes proposed in [19] to account for privacy in form of k-anonymity. All the existing authentication schemes proposed earlier do not consider such property. To the best of our knowledge, the proposed scheme in this paper is the first one to consider the k-anonymity property for privacy in mobile user authentication in GLOMONETs.

TABLE 1. Desirable security requirements.

Resistance against impersonation attacks
Resistance against password guessing attack
Resistance against replay attack
Resistance against man-in-the-middle attack
Resistance against smart card loss attack
Resistance against stolen-verifier attack
Resistance against ephemeral secret leakage (ESL) attack
Resistance against privileged-insider attack

B. SECURITY AND FUNCTIONALITY REQUIREMENTS

While designing a user authentication protocol in GLOMONETs, several security and functionality requirements are necessary. Some security requirements are listed in Table 1 (as described in [19]), while the functionality requirements are also listed in Table 2.

TABLE 2. Desirable functionality attributes.

Attribute	Description
Mutual authentication	All parties (MU, FA and HA) should be able to verify each other's identity
Forward secrecy	Loss of server credentials should not compromise all future sessions
User anonymity	Identity of user obscured such that user cannot be differentiated by any adversary
Elevated anonymity	Users should have the option to validate his/her identity without exposing the same to HA
Multi-factor authentication	User password, biometrics and smart card, all these three factors are required to authenticate MU
Password/ biometrics privacy	User's password/biometrics should be known only to user. No password/biometrics verifier table at HA. Password/biometrics is never transmitted or shared with others
Local password update	Password update by user should be done completely locally
Quick detection of wrong passwords/ biometrics	A wrong password or biometrics needs to be verified quickly in a system
Single registration	User should only register once at his/her HA
Session key security	Even if temporary secrets are compromised, long term keys should not be effected. Leakage of long term secrets should not also compromise previous/future session keys.
Session key composition	Session key should be comprised using both long-term and short-term secrets.

C. THREAT MODEL

It is assumed that any two parties in the network will communicate over insecure (public) channel using the broadly-accepted Dolev-Yao threat (DY) model [43]. According to the DY model, an adversary $\mathcal{A}$ not only can eavesdrop the messages exchanged between the entities, but also can modify or delete the content of the messages or even can insert a fake message during the communication. Moreover, it is assumed that $\mathcal{A}$ can have a lost or stolen smart card of a legal registered user MU and can extract easily all the sensitive data contained in the memory of that smart card using the power analysis attacks [44], [45]. As mentioned in [46], the Canetti and Krawczyk's adversary model (CK-adversary model) [47], [48] is the current *de facto* standard model in modeling authenticated key-exchange protocols. Under the CK-adversary model, $\mathcal{A}$ is not only responsible for delivering messages (as in the DY model), but also can subvert the private keys as well as the session keys and session states. Hence, it is essential that the security of an authenticated key-exchange protocol should assure that the leakage of some forms of secret credentials, such as session ephemeral secrets or session key, will have the minimum possible consequence on the security of other secret credentials of the communicating entities [49].

D. RESEARCH CONTRIBUTIONS

To the best of our knowledge, no existing mobile user authentication schemes in GLOMONETs provide anonymity from the *HA*'s point of view. For plausible deniability of the *HA*, a more stringent privacy model is introduced in the paper. The enhanced privacy model has the following features:

- Anonymity and untraceability for mobile users against a third party observer (e.g., an adversary) as well as the *FA*.
- Optional k-anonymity for mobile users against their home agent (*HA*).

The research contributions of this work are briefed below:

- The proposed authentication scheme allows authentication for both cases: 1) when the *MU* is in a foreign network and 2) when the *MU* is in his/her home network. The proposed scheme supports a group formation of n mobile users. In addition, the proposed scheme provides the integrity check of the group credentials, password update, smart card re-issue when the smart card of the *MU* is lost or compromised.
- With the help of the popular AVISPA tool the proposed scheme is tested for its security, and the the simulation results assume that no replay and man-in-the-middle attacks are found in the scheme.
- The proposed scheme is analyzed for its security using the BAN logic-based proof, and it proves that the proposed scheme provides mutual authentication between the communicating parties in the network. Apart from that, the proposed scheme is also shown to be secure against other possible known attacks using the informal security analysis.
- The proposed scheme also provides session key security, known as the SK-security, under the CK-adversary model. As a result, the proposed scheme also withstands the ephemeral secret leakage (ESL) attack and provides forward secrecy property.
- The comparative analysis of the proposed scheme with the existing relevant schemes in GLOMONETs shows that the proposed scheme performs well as compared to those, specifically by providing better security and more functionality features.

E. ORGANIZATION

The basic mathematical preliminaries needed for discussion and analyzing the proposed scheme are given in Section II. In Section III, the detailed discussion on the proposed scheme is included. The extensive security analysis for various well-known attacks on the proposed scheme is given in Section IV including the formal security verification of the scheme through simulation results in Section V. The performance comparison among the proposed scheme and other relevant schemes is provided in Section VI. The paper is then concluded with some remarks in Section VII.

II. MATHEMATICAL PRELIMINARIES

The necessary mathematical tools are discussed in this section in order to describe and analyze the proposed scheme and other existing schemes.

A. ELLIPTIC CURVE AND ITS PROPERTIES

Consider a set $E_p(a, b)$ of all solutions $(x, y) \in Z_p \times Z_p$ corresponding to a non-singular elliptic curve $y^2 = x^3 + ax + b$ over a prime field $GF(p)$, where p is prime, $a \in Z_p$ and $b \in Z_p$ are constants with fulfilling the condition $4a^3 + 27b^2 \neq 0 \pmod{p}$, and $z_p = \{0, 1, \ldots, p-1\}$. Let $\mathcal{O}$ denote the the point at infinity or zero point in $E_p(a, b)$. Then, $E_p(a, b)$ constitutes an abelian group with respect to addition modulo p operation.

If $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be two points in $E_p(a, b)$, then $R = (x_R, y_R) = P + Q$ is computed by the following rule [50]:

$$x_R = (\mu^2 - x_P - x_Q) \pmod{p},$$
$$y_R = (\mu(x_P - x_R) - y_P) \pmod{p},$$

where $\mu = \begin{cases} \frac{y_Q - y_P}{x_Q - x_P} \pmod{p}, \text{ if } P \neq -Q \\ \frac{3x_P{}^2 + a}{2y_P} \pmod{p}, \text{ if } P = Q. \end{cases}$

The case $P = Q$ is often referred as doubling the point and is represented as $2.P$.

In ECC, the scalar multiplication of an elliptic curve point $P \in E_p(a, b)$ is denoted by $k.P$ where k is a scalar, and it is achieved by using repeated point additions and doubling the point operations. For example, if $P \in E_p(a, b)$, then $23.P$ is computed as $23.P = 2.(2.(2.(2.P) + P) + P) + P$ using three point additions and four doubling the point operations.

Elliptic Curve Discrete Logarithm Problem (ECDLP): Given two points $P, Q \in E_p(a, b)$ where $Q = kP$ and $k \in Z_p^*$ is a scalar. Computing k from P and Q is computationally infeasible if p is sufficiently large (for example, p may be 160 bits prime). This problem is referred to as elliptic curve discrete logarithm problem (ECDLP).

B. COLLISION-RESISTANT ONE-WAY HASH FUNCTION

The one-way hash functions are extremely useful in security-sensitive applications, such as generating digital signature from original data to ensure integrity of data, message authentication code (MAC) along with general practical applications like computing checksum to ensure no data corruption during transmission, and fingerprinting of data in large tables to remove or normalize duplicate data. One of the most prominent properties of a cryptographic one-way hash function is that its message digests (outputs) are very sensitive to inputs even having small perturbations.

The formal definition of a one-way hash function $h(\cdot)$ along with collision-resistant property is given below [51].

Definition 1: A collision-resistant one-way hash function h: $\{0, 1\}^* \rightarrow \{0, 1\}^n$ is a deterministic mathematical function that takes a variable length input and produces a fixed length output, say n bits. Let $Adv^{HASH}_{\mathcal{A}}(rt)$ denote the advantage of an adversary $\mathcal{A}$ in finding a hash collision. Then,

$$Adv^{HASH}_{\mathcal{A}}(rt) = Pr[(i_1, i_2) \in_R \mathcal{A} : i_1 \neq i_2, h(i_1) = h(i_2)],$$

where the probability of a random event X is denoted by $Pr[X]$, and the pair $(i_1, i_2) \in_R \mathcal{A}$ indicates that the inputs i_1 and i_2 are randomly chosen by $\mathcal{A}$. An (ϵ, rt)-adversary $\mathcal{A}$ attacking the collision resistance of $h(\cdot)$ means that the runtime of $\mathcal{A}$ is at most rt and that $Adv^{HASH}_{(A)}(rt) \leq \epsilon$.

An example of a secure collision-resistant hash function $h(\cdot)$ is Secure Hash Standard algorithm (SHA-1) [52] and its more secure version is SHA-256.

C. FUZZY EXTRACTOR FOR BIOMETRIC VERIFICATION

The fuzzy extractor is preferred in biometric verification applied in authentication schemes. A fuzzy extractor is defined as follows [53].

Definition 2: A fuzzy extractor $(\mathcal{M}, m, l, t)$ consists of a pair of two procedures: 1) probabilistic generation function $Gen(\cdot)$ and 2) deterministic reproduction function $Rep(\cdot)$, where $\mathcal{M}$ is a metric space with a distance function $dist$: $\mathcal{M} \times \mathcal{M} \rightarrow [0, \infty)$, m is the minimum entropy, l is the number of bits in the biometric key and t is the maximum error tolerance threshold value. The procedures $Gen(\cdot)$ and $Rep(\cdot)$ have the following properties:

- $Gen(\cdot)$ takes the user biometrics $BIO_{MU} \in \mathcal{M}$ as input string and outputs a biometric secret key $\sigma_{MU} \in \{0, 1\}^l$ and a public reproduction parameter τ_{MU}.
- $Rep(\cdot)$ takes the noisy user biometrics $BIO'_{MU} \in \mathcal{M}$ and the public reproduction parameter τ_{MU} corresponding to $BIO_{MU} \in \mathcal{M}$ as inputs, and then reconstructs the biometric secret key σ_{MU} provided that the Hamming distance $dist(BIO'_{MU}, BIO_{MU}) \leq t$. In other words, $Rep(BIO'_{MU}, \tau_{MU}) = \sigma_{MU}$.

The function $dist$: $\mathcal{M} \times \mathcal{M} \rightarrow [0, \infty)$ gives the Hamming distance between two biometrics with $dist(x, y) = 0$ if and only if $x = y$, and it obeys symmetric property: $dist(x, y) = dist(y, x), \forall x, y \in \mathcal{M}$ as well as triangle inequality: $dist(x, y) + dist(y, z) \geq dist(x, z), \forall x, y, z \in \mathcal{M}$.

The fuzzy extractor $(\mathcal{M}, m, l, t)$ is called efficient if both the $Gen(\cdot)$ and $Rep(\cdot)$ procedures are executed in polynomial time [54].

III. THE PROPOSED AUTHENTICATION SCHEME

A new mobile user authenticated key agreement scheme has been proposed in this section which preserves the anonymity property in GLOMENETs. The scheme is divided into six main phases:

- Setup phase
- Registration phase
- Login and authentication phase
- Group formation phase
- Session key update phase
- Maintenance phase

The detailed description of each phase is provided in the following subsections.

TABLE 3. Notations used in this paper.

Symbol	Description
TA	Trusted authority
MU, FA, HA	Mobile user, foreign agent and home agent, respectively
ID_X	Identity of an entity X
K_{XY}	Shared key between entities X and Y
p	A sufficiently large prime
$E_p(a, b)$	A non-singulars elliptic curve $y^2 = x^3 + ab + b \pmod{p}$ over finite field F_p
G	A base point on $E_p(a, b)$
$k \cdot P$	Scalar multiplication of an ECC point $P \in E_p(a, b)$ with k
$P + Q$	ECC point addition of two points $P, Q \in E_p(a, b)$
$Gen(\cdot), Rep(\cdot)$	Probabilistic generation and reproduction functions for biometric fuzzy extractor, respectively
BIO_{MU}	Personal biometrics of a mobile user MU
σ_{MU}	Secret biometric key associated with BIO_{MU}
τ_{MU}	Public reproduction parameter associated with BIO_{MU}
t	Error tolerance threshold value used in fuzzy extractor $Rep(\cdot)$
$h(\cdot)$	A collision-resistant cryptographic one-way hash function
$E[\cdot]_k/D[\cdot]_k$	Symmetric-key encryption/decryption using key k
(k_x, Q_x)	Private and public key, respectively, $Q_x = k_x \cdot G$
Ω	Secure symmetric-key cryptosystem
$\|\|, \oplus$	String concatenation & bitwise exclusive (XOR) operations, respectively

A. SETUP PHASE

This phase is executed in the offline mode by the trusted authority (TA). During the setup phase, the TA chooses a non-singular elliptic curve $E_p(a, b)$ over a prime finite field $GP(p)$ with a generator G such that the ECDLP becomes intractable with a sufficiently large prime p. After that a cryptographic one-way hash function $h(\cdot)$, probabilistic generation $Gen(\cdot)$ function and deterministic reproduction function $Rep(\cdot)$ for a fuzzy extractor to perform biometric verification, and symmetric cryptosystem Ω are selected by the TA.

After that the TA chooses the private keys k_{HA} and k_{FA} for HA and FA, respectively. The public keys $Q_{HA} = k_{HA} \cdot G$ and $Q_{FA} = k_{FA} \cdot G$ for HA and FA, respectively, are also calculated by the TA. The key $K_{FAHA} = k_{HA} \cdot Q_{FA} = k_{FA} \cdot Q_{HA}$ is then calculated by the TA to be shared between HA and FA in offline mode. The TA then stores the tuple $\{ID_{FA}, K_{FAHA}, 0\}$ in HA's database and the tuple $\{ID_{HA}, K_{FAHA}, 0\}$ in FA's database, called the *key_lookup* table. These steps are also duplicated for all pairs of home and foreign agents in GLOMONETs. Finally, the TA declares the parameters $\{E$, G, $h(\cdot)$, $Gen(\cdot)$, $Rep(\cdot)$, Ω, Q_{HA}, $Q_{FA}\}$ as public.

B. REGISTRATION PHASE

During this phase, each individual mobile user (MU) registers with his/her respective home agent (HA). In order to complete

MU	HA
Select user id ID_{MU} Select password PW_{MU} Imprint biometrics BIO_{MU} Generate random number r Compute $k_{MU} = PW_{MU} \oplus r$, $(\sigma_{MU}, \tau_{MU}) = Gen(BIO_{MU})$, $Q_{MU} = k_{MU} \cdot G$, $PPW = h(PW_{MU} \Vert ID_{MU} \Vert \sigma_{MU})$. $\xrightarrow{\{ID_{MU}, Q_{MU}, PPW\}}$ (secure channel)	
	Calculate $K_{MUHA} = k_{HA} \cdot Q_{MU}$ Store $\{ID_{MU}, K_{MUHA}, 0\}$ in *key_lookup* table Store $\{ID_{MU}, PPW\}$ in its database Calculate $SPW = h(K_{MUHA} \Vert ID_{MU})$, $EID = E[ID_{MU}]_{K_{MUHA}}$ Issue a smart card having information $\{SPW, EID, Q_{HA}, ID_{HA}, G, h(\cdot), \Omega\}$ $\xleftarrow{SmartCard\{SPW, EID, Q_{HA}, ID_{HA}, G, h(\cdot), \Omega\}}$ (secure channel)
Set $count = 0$ Compute $r' = r \oplus h(ID_{MU} \Vert \sigma_{MU} \Vert PW_{MU})$ Add $\tau_{MU}, r', count$ to smart card Finally smart card contains $\{SPW, EID, Q_{HA},$ $ID_{HA}, \tau_{MU}, r', count, G, h(\cdot), \Omega\}$	

FIGURE 1. Summary of registration phase.

the registration process for all pairs of *HA* and *MU*, the following steps need to be executed:

R1: *MU* selects an identity ID_{MU} and a password PW_{MU}, and also imprints his/her biometrics BIO_{MU} at the sensor of a particular terminal. *MU* then generates a random number r and calculates $(\sigma_{MU}, \tau_{MU}) = Gen(BIO_{MU})$, $k_{MU} = PW_{MU} \oplus r$, $Q_{MU} = k_{MU} \cdot G$ and $PPW = h(PW_{MU} \| ID_{MU} \| \sigma_{MU})$. *MU* dispatches the registration request message $\langle ID_{MU}, Q_{MU}, PPW\rangle$ to the *HA* over a secure channel.

R2: *HA* on receiving the registration request message stores the tuple $\{ID_{MU}, PPW\}$ in its database. *HA* then calculates $K_{MUHA} = k_{HA} \cdot Q_{MU}$ and stores the tuple $\{ID_{MU}, K_{MUHA}, 0\}$ in its *key_lookup* table. In addition, *HA* calculates $SPW = h(K_{MUHA} \| ID_{MU})$ and $EID = E[ID_{MU}]_{K_{MUHA}}$ using the symmetric encryption function $E(\cdot)$ with the key K_{MUHA} and issues a smart card containing the credentials $\{SPW, EID, Q_{HA}, ID_{HA}, G, h(\cdot), \Omega\}$ for *MU*. *HA* then sends the smart card to *MU* via a secure channel.

R3: *MU* on receiving the smart card sets *count* to 0 and calculates $r' = r \oplus h(ID_{MU} \| \sigma_{MU} \| PW_{MU})$. Finally, *MU* adds τ_{MU}, r' and *count* to the smart card. Hence, the smart card contains the information $\{SPW, EID, Q_{HA}, ID_{HA}, G, h(\cdot), \Omega, \tau_{MU}, r', count\}$.

Figure 1 summarizes the registration of a mobile user *MU* with his/her home agent (*HA*). Note that the necessity of sending *PPW* during this registration phase by *MU* to the *HA* is to re-issue a new smart card and invalidate the old smart card in case of a loss of smart card or if *MU* suspects that his/her smart card has been compromised. This is performed during the smart card re-issue phase as discussed in Section III-F3.

C. LOGIN AND AUTHENTICATION PHASE

During this phase the mobile user first logins into the network using his/her identity, password and biometrics. The user credential is verified by the smart card. Once the user is verified, through the following steps the *MU* establishes a session key with the *HA* or *FA* depending on the following circumstances.

1) MU IS NOT IN HIS/HER HOME NETWORK

The following steps are executed during this phase:

A1: *MU* provides his/her identity ID_{MU} and password PW_{MU}, and imprints biometric information BIO'_{MU} at the sensor of a particular terminal. The smart card then computes $Rep(BIO_{MU}, \tau_{MU}) = \sigma_{MU}$ provided that the Hamming distance between the registered biometrics BIO_{MU} and current biometrics BIO'_{MU} is less than or equal to the error tolerance threshold value t.

A2: The smart card calculates $r = r' \oplus h(ID_{MU} \| \sigma_{MU} \| PW_{MU})$ and sets the flag *asGroupOrNot* according to whether he/she wants to login as a individual or a group member (through the group formation phase discussed in Section III-D). The smart card calculates $k_{MU} = PW_{MU} \oplus r$ and invokes $K_{MUHA} = getK_{UH}(k_{MU})$, which returns $k_{MU} \cdot Q_{HA}$ or $D[EK_{GRHA}]_{k_{MU}}$ depending on the flag *asGroupOrNot*. *MU* then calculates $SPW' = h(K_{MUHA} \| ID_{MU})$ and checks if $SPW' = SPW$ or $SPW' = SPW_{GR}$. If the condition does not hold, the login fails; otherwise, MU updates *count* to *count* + 1 and generates a random number k_x. After that MU calculates $K_{xHA} = k_x \cdot Q_{HA}$, $Q_x = k_x \cdot G$, $A = h(K_{MUHA} \parallel Q_x)$, $SPWx = h(SPW \parallel Q_x \parallel ID)$, where $ID = ID_{MU}$ or $D[EID_{GR}]_{K_{MUHA}}$ depending on the flag *asGroupOrNot*. Then the smart card sets $EIDx = E[ID]_{K_{xHA}}$ and finally, dispatches the login request message $M_1 = \{A, SPWx, EIDx, ID_{HA}, Q_x\}$ to FA via open channel.

A3: The FA on receiving M_1 generates a random number k_y and looks up K_{FAHA} from its *key_lookup* table with ID_{HA}. The FA then calculates $K_{yHA} = y \cdot Q_{HA}$, $Q_y = k_y \cdot G$ and $EY = E[Q_y]_{K_{FAHA}}$. Then FA sends the authentication request message $M_2 = \{A, EIDx, Q_x, EY, ID_{FA}\}$ to the HA via public channel.

A4: The HA on receiving M_2 looks up K_{FAHA} from its *key_lookup* table with ID_{FA}. It then decrypts Q_y from Ey and then calculates $K'_{xHA} = k_{HA} \cdot Q_x$, $K'_{yHA} = k_{HA} \cdot Q_y$ and $ID_{MU} = D[EIDx]_{K'_{xHA}}$. Next, the HA looks up[1] K_{MUHA} and *loginCount* from its *key_lookup* table with ID_{MU}. Furthermore, the HA calculates $A' = h(K_{MUHA} \parallel Q_x)$. Only if the calculated A' is equal to the received A, the HA validates MU as a valid mobile user (or a valid group member) and calculates EYh as Q_y was encrypted under the key K'_{xHA}, $SPWx' = h(h(K_{MUHA} \parallel ID_{MU}) \parallel Q_x)$ and $authToken = h(ID_{MU} \parallel Q_x \parallel K_{MUHA})$. The HA then updates the tuple $\{ID_{MU}, \sim, loginCount + 1\}$. Finally, the HA composes the message $M_3 = \{E[SPWx', EYh, authToken]_{K'_{yHA}}\}$ and sends it as the authentication reply message to the FA via open channel.

A5: The FA on receiving M_3, it decrypts M_3 using the pre-calculated key K_{yHA} and then checks if the $SPWx$ received from MU is equal to the decrypted received $SPWx'$ from the HA. If the condition is satisfied, the FA assumes that the HA validated MU as a valid mobile user (or a valid group member) and calculates the session key $SK_{xy} = h(k_y \cdot Q_x) \oplus authToken$ shared with MU and $cert = h(Q_x \parallel Q_y \parallel SK_{xy})$. Finally, the FA forwards EYh and $cert$ to MU as the message $M_4 = \{EYh, cert\}$ via open channel.

A6: MU on receiving M_4, the smart card can decrypt EYh using the key K_{xHA} to get Q_y. After that the smart card calculates $authToken = h(ID_{MU} \parallel Q_x \parallel K_{MUHA})$. The smart card calculates the same session key $SK_{xy} = h(k_x \cdot Q_y) \oplus authToken$ shared with the FA. Finally, the smart card calculates $cert' = h(Q_x \parallel Q_y \parallel SK_{xy})$. If the calculated $cert'$ matches with the received $cert$, MU stores SK_{xy} as the session key SK_{xy} for secure communication with the FA. Similarly, the FA also stores the same session key SK_{xy} for secure communication with MU.

Figure 2 summarizes the login and authentication handshake when the user needs to access the services through a foreign agent.

Remark 1: To strengthen the replay attack protection, the following strategy can be adopted [55]. The FA can store the tuple $(EIDx, A)$ in its database. When the next login request message, say $M'_1 = \{A', SPWx', EIDx', ID_{HA}, Q'_x\}$, the FA checks if $EIDx'$ matches with $EIDx$ and also the corresponding A' with A. If both checks are valid, it assures that M'_1 is a replayed message. Otherwise, the FA will add the tuple $(EIDx', A')$ in its database. In a similar way, the HA can also store the tuple (EID_x, Q_y) in its database. When the next message $M'_2 = \{A', EIDx', Q'_x, EY', ID_{FA}\}$ is received, the HA will compute $Q'_y = D[EY']_{K_{FAHA}}$ and checks if $Q'_y = Q_y$. If it holds, M'_2 is also treated as a replay message. Note that these tuples need to be kept in the databases of the FA and the HA for a longer time to provide strong replay attack protection.

2) MU IS IN HIS/HER HOME NETWORK

If the MU is located in his/her home network, the mechanism to establish the session key with the HA is executed using the following steps:

H1: MU operates identically to the steps A1:, A2: discussed in Section III-C1. However, the login request message formed is $M_1 = \{A, EIDx, Q_x\}$ and it is then sent it to the HA by MU via open channel.

H2: The HA on receiving M_1 generates a random number K_y, and calculates $K'_{xHA} = k_{HA} \cdot Q_x$ and $Q_y = K_y \cdot G$. The HA retrieves ID_{MU} by decrypting $EIDx$ with the key K'_{xHA}. Next, the HA looks up K_{MUHA} and *loginCount* from its *key_lookup* table with ID_{MU}. The HA further calculates $A' = h(K_{MUHA} \parallel Q_x)$. Only if the calculated A' is equal to the received A, the HA validates MU as a valid mobile user (or a valid group member), and also calculates EYh as Q_y encrypted under the key K'_{xHA} and $authToken = h(ID_{MU} \parallel Q_x \parallel K_{MUHA})$. In addition, the HA calculates the session key $SK_{xy} = h(k_y \cdot Q_x) \oplus authToken$ shared with MU and $cert = h(Q_x \parallel Q_y \parallel SK_{xy})$, and updates the tuple $\{ID_{MU}, \sim, loginCount + 1\}$. Finally, the HA sends the message $M_2 = \{EYh, cert\}$ to MU via public channel.

H3: MU on receiving M_2 the smart card operates identically to Step A6: and calculates the session key $SK_{xy} = h(k_x \cdot Q_y) \oplus authToken$ shared with the HA and $cert' = h(Q_x \parallel Q_y \parallel SK_{xy})$. If the calculated $cert'$ is equal to the received $cert$, MU stores the session key SK_{xy} shared with the HA. Similarly, the HA also stores the same session key SK_{xy} shared with MU.

Figure 3 summarizes the authentication procedure when MU is located in his/her home network.

D. GROUP FORMATION PHASE

In this section, we discuss the group formation procedure where a registered MU can request the HA for group

[1] Note: If the user MU used group credentials, ID_{MU} and K_{MUHA} hold the values ID_{GR} and K_{GRHA}, respectively.

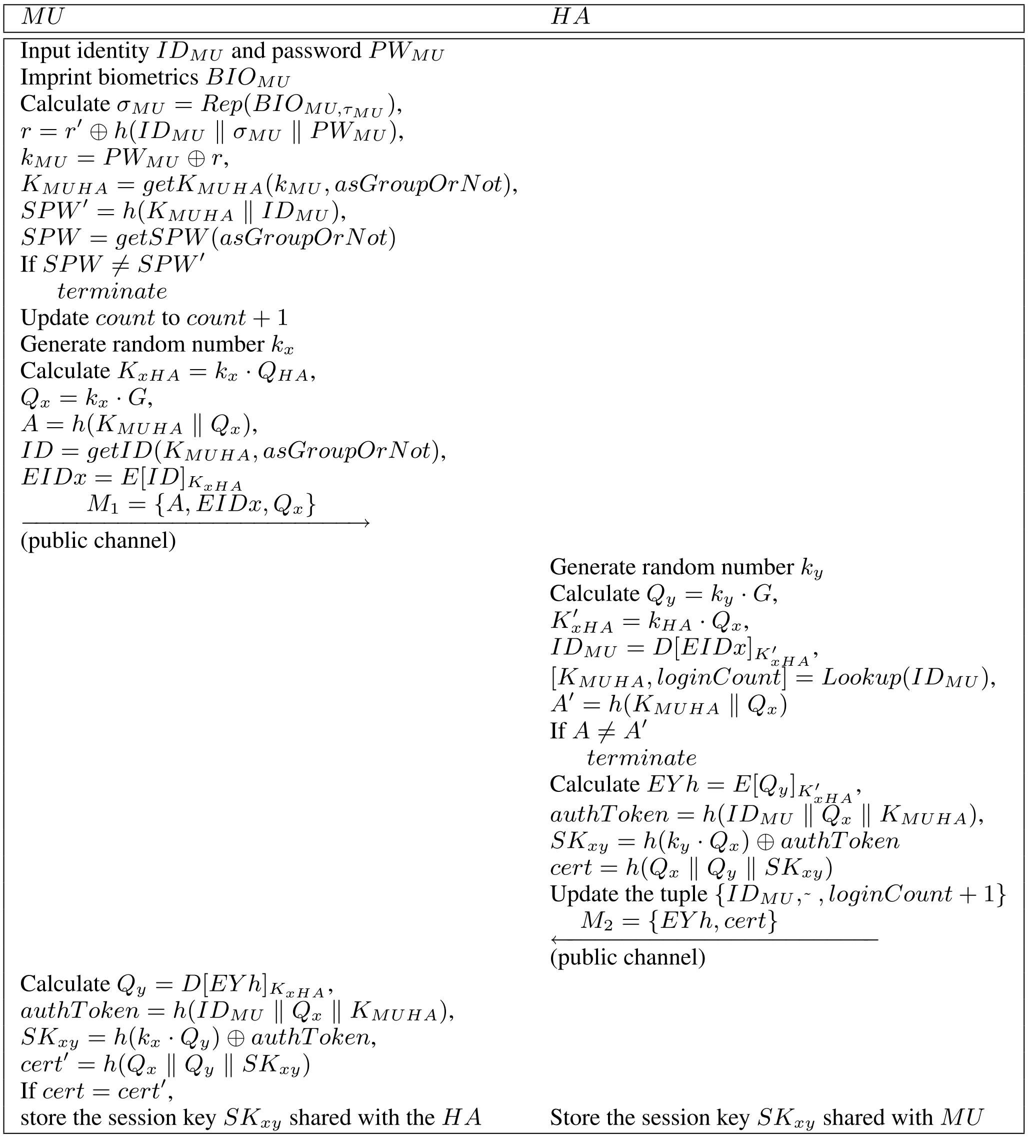
MU	FA	HA
Input identity ID_{MU}, password PW_{MU} Imprint biometrics BIO_{MU} Calculate $\sigma_{MU} = Rep(BIO_{MU,\tau_{MU}})$, $r = r' \oplus h(ID_{MU} \parallel \sigma_{MU} \parallel PW_{MU})$, $k_{MU} = PW_{MU} \oplus r$, $K_{MUHA} = getK_{MUHA}(k_{MU}, asGroupOrNot)$, $SPW' = h(K_{MUHA} \parallel ID_{MU})$, $SPW = getSPW(asGroupOrNot)$. If $SPW \neq SPW'$ $\quad terminate$ Update $count$ to $count + 1$ Generate random number k_x Calculate $K_{xHA} = k_x \cdot Q_{HA}$, $Q_x = k_x \cdot G$, $A = h(K_{MUHA} \parallel Q_x)$, $SPWx = h(SPW \parallel Q_x)$, $ID = getID(K_{MUHA}, asGroupOrNot)$, $EIDx = E[ID]_{K_{xHA}}$ $\xrightarrow{M_1 = \{A, SPWx, EIDx, ID_{HA}, Q_x\}}$ (public channel)		
	Generate random number k_y $[K_{FAHA}, \tilde{}\ ] = Lookup(ID_{HA})$ Calculate $K_{yHA} = k_y \cdot Q_{HA}$, $Q_y = k_y \cdot G$, $EY = E[Q_y]_{K_{FAHA}}$ $\xrightarrow{M_2 = \{A, EIDx, Q_x, EY, ID_{FA}\}}$ (public channel)	
		$[K_{FAHA}, \tilde{}\ ] = Lookup(ID_{FA})$ Calculate $Q_y = D[EY]_{K_{FAHA}}$, $K'_{xHA} = k_{HA} \cdot Q_x$, $K'_{yHA} = k_{HA} \cdot Q_y$, $ID_{MU} = D[EIDx]_{K'_{xHA}}$ $[K_{MUHA}, loginCount] = Lookup(ID_{MU})$ Calculate $A' = h(K_{MUHA} \parallel Q_x)$ If $A \neq A'$ $\quad terminate$ Calculate $EYh = E[Q_y]_{K'_{xHA}}$, $SPWx' = h(h(K_{MUHA} \parallel ID_{MU}) \parallel Q_x)$, $authToken = h(ID_{MU} \parallel Q_x \parallel K_{MUHA})$ Update tuple $\{ID_{MU}, \tilde{}\ , loginCount + 1\}$ $\xleftarrow{M_3 = \{E[SPWx', EYh, authToken]_{K'_{yHA}}\}}$ (public channel)
	Compute $(SPWx', EYh, authToken) = D[M_3]_{K_{yHA}}$ If $SPWx \neq SPWx'$ $\quad terminate$ Compute $SK_{xy} = h(k_y \cdot Q_x) \oplus authToken$, $cert = h(Q_x \parallel Q_y \parallel SK_{xy})$ $\xleftarrow{M_4 = \{EYh, cert\}}$ (public channel)	
Calculate $Q_y = D[EYh]_{K_{xHA}}$, $authToken = h(ID_{MU} \parallel Q_x \parallel K_{MUHA})$, $SK_{xy} = h(k_x \cdot Q_y) \oplus authToken$, $cert' = h(Q_x \parallel Q_y \parallel SK_{xy})$ If $cert = cert'$, store the session key SK_{xy} shared with the FA	Store the session key SK_{xy} shared with MU	

FIGURE 2. Summary of authentication when *MU* is in a foreign network.

credentials. The *HA* initiates and controls the group formation. An k-anonymous user group can be formed through execution of the following steps. The main purpose of the group formation in the proposed scheme is as follows. When a mobile user *MU* visits a foreign agent (*FA*), he/she is always traceable by the *HA*. However, if the *MU* utilizes its group credentials for authentication purpose, he/she will remain untraceable by the *HA*.

G1: The *HA* selects n mobile users who can join the group and establish individual session keys SK_i ($i \in [1, n]$ with each mobile user. The *HA* first requests a mobile user *MU*, say MU_1 for the initial *partialKey*.

G2: A mobile user MU_i on receiving the request for *partialKey* logins with his/her user identity, password and biometrics. If the request for partial key contains $partialKey_{old}$, MU_i replies with



MU | HA

Input identity ID_{MU} and password PW_{MU}
Imprint biometrics BIO_{MU}
Calculate $\sigma_{MU} = Rep(BIO_{MU,\tau_{MU}})$,
$r = r' \oplus h(ID_{MU} \parallel \sigma_{MU} \parallel PW_{MU})$,
$k_{MU} = PW_{MU} \oplus r$,
$K_{MUHA} = getK_{MUHA}(k_{MU}, asGroupOrNot)$,
$SPW' = h(K_{MUHA} \parallel ID_{MU})$,
$SPW = getSPW(asGroupOrNot)$
If $SPW \neq SPW'$
    $terminate$
Update $count$ to $count + 1$
Generate random number k_x
Calculate $K_{xHA} = k_x \cdot Q_{HA}$,
$Q_x = k_x \cdot G$,
$A = h(K_{MUHA} \parallel Q_x)$,
$ID = getID(K_{MUHA}, asGroupOrNot)$,
$EIDx = E[ID]_{K_{xHA}}$

$$\xrightarrow{M_1 = \{A, EIDx, Q_x\}}$$

(public channel)

Generate random number k_y
Calculate $Q_y = k_y \cdot G$,
$K'_{xHA} = k_{HA} \cdot Q_x$,
$ID_{MU} = D[EIDx]_{K'_{xHA}}$,
$[K_{MUHA}, loginCount] = Lookup(ID_{MU})$,
$A' = h(K_{MUHA} \parallel Q_x)$
If $A \neq A'$
    $terminate$
Calculate $EYh = E[Q_y]_{K'_{xHA}}$,
$authToken = h(ID_{MU} \parallel Q_x \parallel K_{MUHA})$,
$SK_{xy} = h(k_y \cdot Q_x) \oplus authToken$
$cert = h(Q_x \parallel Q_y \parallel SK_{xy})$
Update the tuple $\{ID_{MU}, \tilde{}, loginCount + 1\}$

$$\xleftarrow{M_2 = \{EYh, cert\}}$$

(public channel)

Calculate $Q_y = D[EYh]_{K_{xHA}}$,
$authToken = h(ID_{MU} \parallel Q_x \parallel K_{MUHA})$,
$SK_{xy} = h(k_x \cdot Q_y) \oplus authToken$,
$cert' = h(Q_x \parallel Q_y \parallel SK_{xy})$
If $cert = cert'$,
store the session key SK_{xy} shared with the HA | Store the session key SK_{xy} shared with MU

FIGURE 3. Authentication when *MU* is in his/her home network.

$partialKey = partialKey_{old} \oplus h(k_{MU_i})$; otherwise, MU_i replies with $partialKey = h(k_{MU_i})$. The message is then encrypted with its already established session key SK_i and MU_i sends it to the HA via a public channel.

G3: The HA on receiving the partial key from MU_i requests MU_{i+1} with $partialKey_{old}$ for the updated $partialKey$. The message is constructed by encrypting the received $partialKey$ with the key SK_{i+1} and it is then sent to the MU_{i+1} via open channel.

G4: Steps G2: - G3: replete till the HA receives $partialKey$ from n^{th} MU, MU_n. The HA then issues the group identity ID_{GR} and sets group key as $K_{GRHA} = (k_{HA} \oplus partialKey) \cdot G$, and calculates $SPW_{GR} = h(K_{GRHA}) \parallel ID_{GR})$ and $EID_{GR} = E[ID_{GR}]_{K_{GRHA}}$. The HA stores the tuple $\{ID_{GR}, K_{GRHA}, 0\}$ in its key_lookup table. The HA then sends the message $\{K_{GRHA}, SPW_{GR}, EID_{GR}\}$ to each member of the group securely. Note that the message is encrypted with their respective session key.

G5: MU on receiving $\{K_{GRHA}, SPW_{GR}, EID_{GR}\}$ calculates $EK_{GRHA} = E[K_{GRHA}]_{k_{MU}}$ and adds the group credentials $\{EK_{GRHA}, SPW_{GR}, EID_{GR}\}$ to his/her smart card.

When all members MU's of a group update their smart cards with the group credentials, the group formation process is completed. Figure 4 summarizes the formation of a group with n members. It is also worth noticing from this figure that the number of steps towards successful group formation is linearly proportional to the number of group members.

E. SESSION KEY UPDATE PHASE

In this phase, a mobile user MU and the HA/FA negotiate a new session key by leveraging the old session key. The steps to update the session key are given below:

$MU_i, i \in [1,n]$	HA
Smart card $=\{SPW,\ EID,\ Q_{HA},\ ID_{HA},\ \tau_{MU_i},\ r',\ count, G, h(), \Omega\}$	
SK_i is negotiated with HA	SK_i negotiated with MU_i $\vdots$ SK_n is negotiated with MU_n Request MU_1 for initial $partialKey$ Receive $E[Q_{MU_1}]_{SK_1}$ from MU_1 Update $partialKey = D[Q_{MU_1}]_{SK_1}$ Send $E[partialKey]_{SK_2}$ to MU_2 $\vdots$ Receive $E[partialKey]_{SK_{i-1}}$ from MU_{i-1} Set $partialKey_{old} = D[partialKey]_{SK_{i-1}}$ Send $E[partialKey_{old}]_{SK_i}$ to MU_i
Set $partialKey_{old} = D[partialKey_{old}]_{SK_i}$ MU_i enters ID_{MU_i}, password PW_{MU_i} MU_i imprints biometrics BIO_{MU} Calculate $\sigma_{MU_i} = Rep(BIO_{MU_i}, \tau_{MU_i})$, $r = r' \oplus h(ID_{MU_i} \parallel \sigma_{MU_i} \parallel PW_{MU_i})$, $k_{MU_i} = PW_{MU_i} \oplus r$, $SPW' = h(k_{MU_i} \cdot Q_{HA} \parallel ID_{MU_i})$ If $SPW \neq SPW'$ $\quad terminate$ Set $partialKey = h(k_{MU_i}) \oplus partialKey_{old}$	
Send $E[partialKey]_{SK_i}$ to HA	Receive $E[partialKey]_{SK_i}$ from MU_i Set $partialKey_{old} = D[partialKey]_{SK_i}$ Send $E[partialKey_{old}]_{SK_{i+1}}$ to MU_{i+1} $\vdots$ Receive $E[partialKey]_{SK_n}$ from MU_n Set $partialKey = D[partialKey]_{SK_n}$ Issue ID_{GR} Calculate $K_{GRHA} = (k_{HA} \oplus partialKey) \cdot G$ Store $\{ID_{GR}, K_{GRHA}, 0\}$ Compute $SPW_{GR} = h(K_{GRHA} \parallel ID_{GR})$, $EID_{GR} = E[ID_{GR}]_{K_{GRHA}}$ Send $E[K_{GRHA},\ SPW_{GR},\ EID_{GR}]_{SK_p}$ to MU_i for all $i \in [1,n]$
Compute $EK_{GRHA} = E[K_{GRHA}]_{k_{MU}}$ Add $SPW_{GR}, EID_{GR}, EK_{GRHA}$ to smart card Smart card $=\{SPW_{GR},\ EID_{GR},\ EK_{GRHA},\ SPW,\ EID, Q_{HA}, ID_{HA}, \tau_{MU_i}, r', count, G, h(), \Omega\}$	

FIGURE 4. Summary of group formation.

U1: *MU* generates a random number $k_{x_{i+1}}$ and calculates $Q_{x_{i+1}} = k_{x_{i+1}} \cdot G$. *MU* then encrypts the hash of $Q_{x_{i+1}}$ into *EhX* with the old session key SK_i and sends the message $M_1 = \{Q_{x_{i+1}}, EhX\}$ to the *HA* (or the *FA*) via open channel.

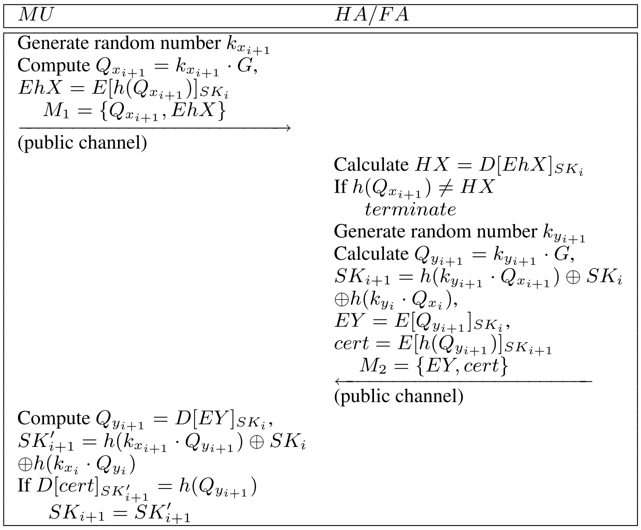
U2: The *HA* (*FA*) on receiving M_1 calculates $HX = D[EhX]_{SK_i}$ and compares it with the hash of the received $Q_{x_{i+1}}$. If the values are equal, *HA* (*FA*) assumes M_1 is non-tampered message and then generates a random number $k_{y_{i+1}}$ to calculate $Q_{y_{i+1}} = k_{y_{i+1}} \cdot G$. The *HA* (*FA*) updates the session key such that $SK_{i+1} = h(k_{y_{i+1}} \cdot Q_{x_{i+1}}) \oplus SK_i \oplus h(k_{y_i} \cdot Q_{x_i})$. Next, the *HA* (*FA*) encrypts $Q_{y_{i+1}}$ with the old session key SK_i to produce *EY* and also encrypts the hash of $Q_{x_{i+1}}$ with the updated session key SK_{i+1} to create *cert*. *HA* (*FA*) finally sends the message $M_2 = \{EY, cert\}$ to *MU* via open channel.

U3: *MU* on receiving M_2 decrypts *EY* with the key SK_i to retrieve $Q_{y_{i+1}}$ and calculates the updated session key $SK'_{i+1} = h(k_{x_{i+1}} \cdot Q_{y_{i+1}}) \oplus SK_i \oplus h(k_{x_i} \cdot Q_{y_i})$. Next, *MU* attempts to decrypt *cert* with SK'_{i+1} and if the result is equal to $h(Q_{y_{i+1}})$, *MU* sets the updated session key SK_{i+1} with SK'_{i+1}.

Figure 5 summarizes the session key update mechanism.

F. MAINTENANCE PHASE

This phase describes the mechanisms for integrity check for the group credentials, password update and smart card reissue phases.



MU — HA/FA

Generate random number $k_{x_{i+1}}$
Compute $Q_{x_{i+1}} = k_{x_{i+1}} \cdot G$,
$EhX = E[h(Q_{x_{i+1}})]_{SK_i}$
$M_1 = \{Q_{x_{i+1}}, EhX\}$
$\xrightarrow{\hspace{6em}}$
(public channel)

Calculate $HX = D[EhX]_{SK_i}$
If $h(Q_{x_{i+1}}) \neq HX$
terminate
Generate random number $k_{y_{i+1}}$
Calculate $Q_{y_{i+1}} = k_{y_{i+1}} \cdot G$,
$SK_{i+1} = h(k_{y_{i+1}} \cdot Q_{x_{i+1}}) \oplus SK_i$
$\oplus h(k_{y_i} \cdot Q_{x_i})$,
$EY = E[Q_{y_{i+1}}]_{SK_i}$,
$cert = E[h(Q_{y_{i+1}})]_{SK_{i+1}}$
$M_2 = \{EY, cert\}$
$\xleftarrow{\hspace{6em}}$
(public channel)

Compute $Q_{y_{i+1}} = D[EY]_{SK_i}$,
$SK'_{i+1} = h(k_{x_{i+1}} \cdot Q_{y_{i+1}}) \oplus SK_i$
$\oplus h(k_{x_i} \cdot Q_{y_i})$
If $D[cert]_{SK'_{i+1}} = h(Q_{y_{i+1}})$
$SK_{i+1} = SK'_{i+1}$

FIGURE 5. **Summary of session key update.**

1) INTEGRITY CHECK FOR GROUP CREDENTIALS

As the group members are anonymous, in order to ensure that no one abuses the group credentials, its integrity needs to be verified regularly. However, this integrity check should not compromise the anonymity of the group members. A procedure that meets such a requirement is presented through the execution of the following steps:

C1: The HA requests all n group members to send the counts of their successful logins. The HA then calculates $totalLogin = \sum loginCount_i + loginCount_g$, where $loginCount_i$ and $loginCount_g$ correspond to the number of times i^{th} mobile user MU_i and an anonymous group member successfully logged in, respectively.

C2: MU_i, the i^{th} group member, on receiving the request sends $Ecount_i = count \cdot G$ to the HA.

C3: The HA, on receiving replies from all the group members, calculates $EtotalLogin = \sum_{i=1}^{n} Ecount_i$. If $EtotalLogin$ matches with $totalLogin \cdot G$, the group credentials are secure and hence, the HA sets $isSecure = True$. However, if that is not the case or if HA fails to receive replies from all n group members, HA deems the group credentials compromised and purges the tuple $\{ID_{grp}, K_{GH}, loginCount\}$ from its key_lookup table, and sets $isSecure = False$. Regardless HA resets all the relevant counters to zero and sends $isSecure$ to all the group members.

C4: MU_i on receiving $isSecure$ sets $count$ to zero. If $isSecure$ is $False$, MU_i removes $\{EK_{GH}, SPW_g, EID_g\}$ from his/her smart card.

This phase is finally briefed in Figure 6.

2) PASSWORD UPDATE

For security reasons, it is a better practice to change the password of any legal registered user MU at any time. The password change phase of the proposed scheme involves the following steps:

P1: MU provides his/her identity ID_{MU} and password PW_{MU}, and imprints biometric information BIO'_{MU} at the sensor of a particular terminal. The smart card then computes $Rep(BIO_{MU}, \tau_{MU}) = \sigma_{MU}$ provided that $dist(BIO_{MU}, BIO'_{MU}) \leq t$ is met.

P2: The smart card calculates $r = r' \oplus h(ID_{MU} \parallel \sigma_{MU} \parallel PW_{MU})$, $k_{MU} = PW_{MU} \oplus r$, $Q_{MU} = k_{MU} \cdot G$, $K_{MUHA} = k_{HA} \cdot Q_{MU}$ and $SPW' = h(K_{MUHA} \parallel ID_{MU})$. If $SPW' = SPW$, the entered credentials of MU are authenticated by the smart card and the smart card asks MU to provide the changed new password.

P3: MU provides the new password PW^{new}_{MU}. The smart card then calculates $k'_{MU} = PW^{new}_{MU} \oplus r$, $Q'_{MU} = k'_{MU} \cdot G$ and $PPW' = h(PW^{new}_{MU} \| ID_{MU} \| \sigma_{MU})$. MU sends the message $\langle ID_{MU}, Q'_{MU}, PPW' \rangle$ to the HA securely.

P4: HA on receiving the message updates PPW with PPW' in the tuple $\{ID_{MU}, PPW\}$. HA then calculates $K'_{MUHA} = k'_{HA} \cdot Q'_{MU}$ and updates K_{MUHA} with K'_{MUHA} in the tuple $\{ID_{MU}, K_{MUHA}, 0\}$ in its key_lookup table. In addition, HA calculates $SPW^{new} = h(K'_{MUHA} \parallel ID_{MU})$ and $EID^{new} = E[ID_{MU}]_{K'_{MUHA}}$ and sends the credentials $\{SPW^{new}, EID^{new}\}$ to MU securely.

P5: Finally, the smart card on receiving the credentials $\{SPW^{new}, EID^{new}\}$ computes $r_{new} = r \oplus h(ID_{MU} \parallel \sigma_{MU} \parallel PW^{new}_{MU})$ and replaces SPW, EID and r with SPW^{new}, EID^{new} and r_{new} in its memory, respectively.

3) SMARTCARD RE-ISSUE

In case of a loss of smart card or if a legal user MU suspects that his/her smart card has been compromised, it is necessary to issue a new smart card and invalidate the old smart card. The steps involved to re-issue a new smart card are as follows:

R1: MU provides his/her user identity ID_{MU}, old password PW_{MU}, new password PW'_{MU} and imprints the biometrics BIO_{MU} at the sensor of a particular terminal. MU then generates a random number r' and calculates $(\sigma_{MU}, \tau_{MU}) = Gen(BIO_{MU})$, $k'_{MU} = PW'_{MU} \oplus r'$, $Q'_{MU} = k'_{MU} \cdot G$, $PPW^{old} = h(PW_{MU} \| ID_{MU} \| \sigma_{MU})$ and $PPW^{new} = h(PW'_{MU} \| ID_{MU} \| \sigma_{MU})$. MU communicates the registration re-issue request message $\{ID_{MU}, Q'_{MU}, PPW^{old}, PPW^{new}\}$ to the HA over a secure channel.

R2: On receiving $\{ID_{MU}, Q'_{MU}, PPW^{old}, PPW^{new}\}$ the HA looks up PPW from its database corresponding to ID_{MU}. If PPW^{old} is equal to PPW, the HA is assured that this is a legitimate request for smart card re-issue. The HA then updates PPW with PPW^{new} in its database, calculates $K'_{MUHA} = k_{HA} \cdot Q'_{MU}$ and updates the tuple $\{ID_{MU}, K'_{MUHA}, -\}$ in its key_lookup table. The HA also calculates $SPW' = h(K'_{MUHA} \parallel ID_{MU})$ and $EID' = E[ID_{MU}]_{K'_{MUHA}}$, and issues a new smart card containing the information $\{SPW', EID', Q'_{HA}, ID_{HA}, G, h(\cdot), \Omega\}$ for MU via a secure channel.

R3: MU on receiving the new smart card sets $count$ to 0 and calculates $r^* = r' \oplus h(ID_{MU} \parallel \sigma_{MU} \parallel PW'_{MU})$.

$MU_i, i \in [1, n]$	HA
	$[\tilde{}, loginCount_i] = Lookup(ID_{MU_i}), i \in [1, n]$ $[\tilde{}, loginCount_g] = Lookup(ID_{grp})$ Calculate $totalLogin = loginCount_g + \sum_{i=1}^{n} loginCount_i$ Request successful login count from $MU_i, i \in [1, n]$
Compute $Ecount_i = count \cdot G$ Communicate $Ecount_i$ with HA	
	Calculate $EtotalLogin = \sum_{i=1}^{n} Ecount_i$ If $(replyReceived < n$ or $EtotalLogin \neq totalLogin \cdot G)$ Delete the tuple $\{ID_{grp}, \tilde{}, loginCount\}$ Set $isSecure = False$ Otherwise Update the tuple $\{ID_{grp}, \tilde{}, 0\}$ Set $isSecure = True$ Update the tuple $\{ID_{MU_i}, \tilde{}, 0\}$ Send $isSecure$ to $MU_i, i \in [1, n]$
Set $count = 0$ If $isSecure = false$ Smart card $=\{SPW, EID, H, ID_{HA}, \tau_{MU}, r', count, G, h(), \Omega\}$	

FIGURE 6. **Summary of integrity check for the group credentials.**

MU	HA
Input ID_{MU}, old password PW_{MU} and new password PW'_{MU} Imprint biometrics BIO_{MU} Compute $(\sigma_{MU}, \tau_{MU}) = Gen(BIO_{MU})$ Generate new random number r' Calculate $k'_{MU} = PW'_{MU} \oplus r'$, $Q'_{MU} = k'_{MU} \cdot G$, $PPW^{old} = h(PW_{MU} \parallel ID_{MU} \parallel \sigma_{MU})$, $PPW^{new} = h(PW'_{MU} \parallel ID_{MU} \parallel \sigma_{MU})$ $\xrightarrow{\{ID_{MU}, Q'_{MU}, PPW^{old}, PPW^{new}\}}$ (secure channel)	
	Retrieve $PPW = Lookup(ID_{MU})$ If $PPW \neq PPW^{old}$ terminate Update PPW with PPW^{new} Calculate $K'_{MUHA} = k_{HA} \cdot Q'_{MU}$ Update the tuple $\{ID_{MU}, K'_{MUHA}, -\}$ Compute $SPW' = h(K'_{MUHA} \parallel ID_{MU})$, $EID' = E[ID_{MU}]_{K'_{MUHA}}$ Issue a new smart card with information $\{SPW', EID', Q_{HA}, ID_{HA}, G, h(\cdot), \Omega\}$ $\xleftarrow{SmartCard\{SPW', EID', Q_{HA}, ID_{HA}, G, h(\cdot), \Omega\}}$ (secure channel)
Set $count = 0$ Calculate $r^* = r' \oplus h(ID_{MU} \parallel \sigma_{MU} \parallel PW^{new}_{MU})$ Add τ_{MU}, r^* and $count$ to smart card Smart card $=\{SPW', EID', Q_{HA}, ID_{HA}, \tau_{MU}, r^*, count, G, h(\cdot), \Omega\}$	

FIGURE 7. **Summary of smart card re-issue.**

MU then adds τ_{MU}, r^* and *count* to the smart card. Finally, the new smart card contains the credentials $\{SPW', EID', Q'_{HA}, ID_{HA}, \tau_{MU}, r^*, count, G, h(\cdot), \Omega\}$.

In Fig. 7, the smart card re-issue process is summarized. It is to be noted that in case of smart card loss, the user loses the privilege to access services as a anonymous member of any group he/she was part of. However, the group is not compromised and if the group was formed with n members, it will currently have $n - 1$ active members.

Remark 2: In case of a smart card loss, the anonymous group is only functional until the next integrity check when the group will be dissolved. This inconvenience can be avoided by appending $E[count]_{k_{MU}}$ to the login request message M_1 in the login and authentication phase, and storing it in the database of the HA.

IV. SECURITY ANALYSIS

In this section, through both the widely accepted Burrows-Abadi-Needham logic (BAN Logic) proof [56] and informal security analysis, we show that the proposed scheme can withstand various known attacks.

A. MUTUAL AUTHENTICATION THROUGH BAN LOGIC

Using the BAN Logic [56], we show that the proposed scheme provides mutual authentication between a legal registered mobile user MU and the FA in presence of the HA.

The notations used in the BAN logic are as follows:

- $P \mid\equiv X$: Principal P believes a statement X, or P is entitled to believe X.
- $\#(X)$: Formula X is considered fresh.
- $P \mid\!\Rightarrow X$: P has jurisdiction over a statement X.
- $P \triangleleft X$: P sees X.
- $P \mid\sim X$: P once said X.
- (X, Y): Formula X or Y is one part of formula (X, Y).
- $\{X\}_K$: X is encrypted using the key K.
- $\langle X\rangle_Y$: X combined with Y.
- $P \overset{K}{\longleftrightarrow} Q$: P and Q may use the shared key K to communicate. K is good in that it will never be discovered by any principal except P and Q.
- $P \overset{X}{\rightleftharpoons} Q$: X is secret that is known only to P and Q, and possibly to principals trusted by them.

The BAN logic is governed by the following four rules:

$Rule(1)$ [Message-meaning rule]: $\frac{P|\equiv P\overset{K}{\longleftrightarrow}Q,P\triangleleft\{X\}_K}{P|\equiv Q|\sim X}$ and $\frac{P|\equiv P\overset{Y}{\rightleftharpoons}Q,P\triangleleft\langle X\rangle_Y}{P|\equiv Q|\sim X}$.

$Rule(2)$ [Nonce-verification rule]: $\frac{P|\equiv\#(X),P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$.

$Rule(3)$ [Jurisdiction rule]: $\frac{P|\equiv Q\mid\!\Rightarrow X,P|\equiv Q|\equiv X}{P|\equiv X}$.

$Rule(4)$ [Freshness-conjuncatenation rule]: $\frac{P|\equiv\#(X)}{P|\equiv\#(X,Y)}$.

We now prove the mutual authentication between MU and the FA with the help of the HA in Theorem 1.

Theorem 1: The proposed scheme provides secure mutual authentication between a legal registered mobile user MU and the FA with the help of the HA during the login and authentication phase of the proposed scheme.

Proof 1: According to the analytic procedures of the BAN logic, the following goals need to be satisfied to prove mutual authentication between MU and FA with the help of HA:

G_1: $FA \mid\equiv MU \overset{authtoken}{\rightleftharpoons} FA$.

G_2: $FA \mid\equiv MU \overset{SK}{\longleftrightarrow} FA$.

G_3: $MU \mid\equiv MU \overset{SK}{\longleftrightarrow} FA$.

The generic forms of the proposed scheme during the login and authentication phase (discussed in Section III-C1) are provided below:

1) From message M_1, we have, $MU \rightarrow FA$: $A = h(K_{MUHA} \parallel Q_x)$, $SPWx = h(h(K_{MUHA} \parallel ID_{MU}) \parallel Q_x)$, $EIDx = \{ID_{MU}\}_{K_{xHA}}, ID_{HA}, Q_x = k_x \cdot G$.
2) From message M_2, we have, $FA \rightarrow HA$: $A = h(K_{MUHA} \parallel Q_x), EIDx = \{ID_{MU}\}_{K_{xHA}}, Q_x = k_x \cdot G, \{Q_y\}_{K_{FAHA}}, ID_{FA}$.
3) From message M_3, we get, $HA \rightarrow FA$: $\{SPWx = h(h(K_{MUHA} \parallel ID_{MU}) \parallel Q_x)$, $EYh = \{Q_y\}_{K_{xHA}}$, $authtoken = h(ID_{MU} \parallel Q_x \parallel K_{MUHA})\}\_{K_{yHA}}$.
4) From message M_4, we get, $FA \rightarrow MU$: $EYh = \{Q_y\}_{K_{xHA}}$ and $MU \rightarrow FA$: $cert = \langle Q_y, SK\rangle_{Q_x}$.

The idealized forms of the above messages can be represented as follows:

M_1: $MU \rightarrow FA$: $\langle ID_{MU}\rangle_{MU \overset{K_{xHA}}{\longleftrightarrow} HA}$.

M_2: $FA \rightarrow HA$: $\langle\langle ID_{MU}\rangle_{MU \overset{K_{xHA}}{\longleftrightarrow} HA}, \langle Y\rangle_{FA \overset{K_{FAHA}}{\longleftrightarrow} HA}\rangle$.

M_3: $HA \rightarrow FA$: $\langle SPWx, EYh, MU \overset{authtoken}{\rightleftharpoons} FA\rangle_{FA \overset{K_{yHA}}{\longleftrightarrow} HA}$.

M_4: $FA \rightarrow MU$: $\langle MU \overset{Q_y}{\rightleftharpoons} FA\rangle_{MU \overset{K_{MUHA}}{\longleftrightarrow} HA}$.

M_5: : $MU \rightarrow FA$: $\langle Y, MU \overset{SK}{\longleftrightarrow} FA\rangle_X$.

The following assumptions regarding the initial states are give below:

H_1: $MU \mid\equiv MU \overset{K_{xHA}}{\rightleftharpoons} HA$.

H_2: $MU \mid\equiv MU \overset{authtoken}{\rightleftharpoons} FA$.

H_3: $MU \mid\equiv HA \mid\!\Rightarrow MU \overset{Q_y}{\rightleftharpoons} FA$.

H_4: $FA \mid\equiv \#(Q_y)$.

H_5: $FA \mid\equiv FA \overset{Q_y}{\rightleftharpoons} HA$.

H_6: $FA \mid\equiv HA \mid\!\Rightarrow MU \overset{authtoken}{\rightleftharpoons} FA$.

H_7: $FA \mid\equiv MU \overset{Q_x}{\rightleftharpoons} FA$.

The idealized forms of the proposed scheme are analyzed based on the BAN logic rules and above stated assumptions. The goals stated above (Goals G_1, G_2, G_3) are proved below.

From H_5: and the fact that K_{yHA} is derived from Q_y, we have the following results:

S_1: $FA \mid\equiv FA \overset{K_{yHA}}{\longleftrightarrow} HA$.

From H_4:, $Rule(4)$, and the fact that K_{yHA} is derived from Q_y, we have:

S_2: $FA \mid\equiv \#(K_{yHA})$.

From M_3:, we obtain,

S_3: $FA \triangleleft \langle SPWx, EYh, MU \overset{authtoken}{\rightleftharpoons} FA\rangle_{FA \overset{K_{yHA}}{\longleftrightarrow} HA}$.

From S_1:,S_3: and $Rule(1)$, it follows that

S_4: $FA \mid\equiv HA \mid\sim \langle SPWx, EYh, MU \overset{authtoken}{\rightleftharpoons} FA\rangle$.

S_2:, S_4:, $Rule(2)$ and $Rule(4)$ lead to the following:

S_5: $FA \mid\equiv HA \mid\equiv MU \overset{authtoken}{\rightleftharpoons} FA$.

From S_5:, H_6:, and $Rule(3)$, we get, $FA \mid\equiv MU \overset{authtoken}{\rightleftharpoons} FA$. (**Goal** G_1:)

From H_7: and the fact that $SK = h(k_x \cdot Q_y) \oplus authtoken$, we obtain, $FA \mid\equiv MU \overset{SK}{\longleftrightarrow} FA$.

(**Goal** G_2:)

M_4: gives the following:

S_6: $MU \lhd \langle MU \overset{Q_y}{\rightleftharpoons} FA \rangle_{MU \overset{K_{xHA}}{\longleftrightarrow} HA}$.

S_6: and $Rule(1)$ lead to the following:

S_7: $MU \mid\equiv HA \mid\sim \langle MU \overset{Q_y}{\rightleftharpoons} FA \rangle$.

From H_4:, S_7:, $Rule(2)$ and $Rule(4)$, it follows that

S_8: $MU \mid\equiv HA \mid\equiv MU \overset{Q_y}{\rightleftharpoons} FA$.

H_3:,S_8:, and $Rule(3)$ give the following result:

S_9: $MU \mid\equiv MU \overset{Q_y}{\rightleftharpoons} FA$.

From S_9:, H_2: and the fact $SK = h(k_x \cdot Q_y) \oplus authtoken$, we have, $MU \mid\equiv MU \overset{SK}{\longleftrightarrow} FA$.

(**Goal** G_3:)

The goals G_1-G_3 assure that both the participants MU and the FA mutually authenticate each other with the help of the HA.

B. INFORMAL SECURITY ANALYSIS

Through informal (non-mathematical) security analysis, we also show that the proposed scheme is resilient against known attacks that are proved in the following propositions.

Proposition 1: Both the user anonymity and untracebility properties are preserved in the proposed scheme.

Proof 2: In the proposed scheme, out of the information transmitted by the messages M_1 through M_4 during the login and authentication phase when MU is not in his/her home network, only A, $SPWx$ and $EDIx$ contains identifiable information, where $A = h(K_{MUHA} \parallel Q_x)$, $SPWx = h(SPW \parallel Q_x \parallel ID)$, where $ID = ID_{MU}$ or $D[EID_{GR}]_{K_{MUHA}}$ depending on the flag $asGroupOrNot$. A and $SPWx$ are the non-invertible hash of $K_{MUHA} \parallel Q_x$ and $h(h(K_{MUHA} \parallel ID_{MU}) \parallel Q_x)$, respectively. Thus, identifying or even differentiating between different MUs is difficult for an adversary. $EIDx$ on the other hand is encrypted with the key K_{xHA} which is shared only between MU and the HA. If $EIDx$ is decrypted, it can be used to identify MU, but neither an adversary nor the FA can decrypt $EIDx$ without having the key K_{xHA}. Furthermore, if MU uses group credentials, the HA only knows that the user MU belongs to the anonymous group with identity ID_{MU} (or ID_{GR} in this case). The similar situation happens for the transmitted messages during the login and authentication phase when MU is in his/her home network. Thus, MU remains also anonymous even to the HA. Hence, it ensures the user anonymity property.

It is also worth noticing that during the login and authentication phase when MU is not in his/her home network the messages $M_1 = \{A, SPWx, EIDx, ID_{HA}, Q_x\}$, $M_2 = \{A, EIDx, Q_x, EY, ID_{FA}\}$, $M_3 = \{E[SPWx', EYh, authToken]_{K'_{yHA}}\}$ and $M_4 = \{EYh, cert\}$ are all dynamic in nature for each session as these messages involve the random nonces. In a similar way, during the login and authentication phase when MU is in his/her home network, the transmitted messages are also dynamic in nature. Due to the dynamic construction of the messages, an adversary could not be able to trace the same user over different sessions even if the same user authenticates with the FA with the help of the HA or directly with the HA. As a result, the proposed scheme is able to preserve untraceability property.

Proposition 2: The proposed scheme is resilient against impersonation attacks.

Proof 3: The proposed scheme can effectively thwart impersonation attacks in the following scenarios:

- An adversary $\mathcal{A}$ cannot impersonate MU to cheat the HA as regardless of whether MU is located in his/her home network or not, his/her identity is verified by the value $A = h(K_{MUHA} \parallel Q_x)$ and K_{MUHA} is only shared between MU and HA.
- $\mathcal{A}$ cannot impersonate MU to cheat the FA as the FA verifies the identity of MU by matching $SPWx$ received from MU with the $SPWx'$ received from the HA.
- $\mathcal{A}$ cannot impersonate the FA to cheat the HA as EY is encrypted by the secret K_{FAHA} that is shared only between the FA and the HA.
- $\mathcal{A}$ cannot impersonate the FA to cheat MU as MU is assured of the FA's authenticity by the message M_4 which is sent by FA but it is encrypted with the secret K_{xHA} which is the key shared between MU and the HA.
- $\mathcal{A}$ cannot also impersonate HA to cheat the FA or MU as through the messages M_3 and M_4, which are encrypted with keys K_{yHA} and K_{xHA}, respectively, are unknown to $\mathcal{A}$.

Considering all the above scenarios, it is derived that the proposed scheme resists the impersonation attacks.

Proposition 3: The proposed scheme is resilient against replay attack.

Proof 4: An adversary $\mathcal{A}$ can replay the message $M_1 = \{A, SPWx, EIDx, ID_{HA}, Q_x\}$ as the login request of a valid user MU to FA and receive the replay message $M_4 = \{EYh, cert\}$ during the login and authentication phase when MU is not in his/her home network (Section III-C1). However, $\mathcal{A}$, lacking access to the key K_{xHA}, can neither decrypt EYh nor calculate the session key $SK_{xy} = h(k_y \cdot Q_x) \oplus authToken$. Furthermore, the FA or HA can easily detect the replayed messages by comparing the transmitted Q_x with previously received Q_x. In addition, the strategy adopted in Remark 1 also prevents $\mathcal{A}$ to perform the replay attack easily on the proposed scheme. The similar situation happens for the login and authentication phase when MU is in his/her home network (Section III-C2). Hence, the proposed scheme resists the replay attack.

Proposition 4: The proposed scheme withstands the man-in-the-middle attack.

Proof 5: In a man-in-the-middle attack, an adversary $\mathcal{A}$ intercepts the transmitted messages and tries to modify the messages in such a way that they are not detected by the respective recipients. In the proposed scheme, assume that $\mathcal{A}$ wishes to modify the messages M_1, M_2, M_3 and M_4 during the login and authentication phase when MU is not in his/her home network. To modify the message $M_1 = \{A, SPWx, EIDx, ID_{HA}, Q_x\}$, $\mathcal{A}$ needs to generate a random number k'_x and calculate $K'_{xHA} = k'_x \cdot Q_{HA}$, $Q'_x = k'_x \cdot G$,

$A' = h(K_{MUHA} \parallel Q'_x)$ and $SPWx' = h(SPW \parallel Q'_x \parallel ID_{MU})$. Note that it is a computationally infeasible task for $\mathcal{A}$ to compute A' and $SPWx'$ without having the secret credentials K_{MUHA}, SPW and ID_{MU}. Thus, $\mathcal{A}$ will not be able to send the modified message M'_1 successfully to the FA. In a similar way, $\mathcal{A}$ can not also modify other messages M_2, M_3 and M_4 as these messages also need the secret credentials. The same argument is valid for the intercepted messages M_1 and M_2 during the login and authentication phase when MU is in his/her home network. Hence, the man-in-the-middle attack is prevented in the proposed scheme.

Proposition 5: The proposed scheme is secure against ephemeral secret leakage (ESL) attack.

Proof 6: We consider the CK-adversary model [47], [48] (as discussed in the threat model in Section I-C) for analysis of ESL attack. In the proposed scheme, the session key is constructed by a legal registered mobile user and the FA during the the login and authentication phase when MU is not in his/her home network is computed as $SK_{xy} = h(k_x \cdot Q_y) \oplus authToken = h(k_y \cdot Q_x) \oplus authToken$, where $authToken = h(ID_{MU} \parallel Q_x \parallel K_{MUHA})$. It is then clear that the session key is composed of both the session-temporary information k_x and k_y as well as long-term secret ID_{MU} and K_{MUHA}. Thus, the session key can be revealed if an adversary $\mathcal{A}$ is able to compromise both the session-temporary and long-term secrets. Again, since the random numbers k_x and k_y are used in construction of the session keys between MU and the FA in different sessions, if a session key is revealed in a particular session it does not lead to compute the other session keys in other sessions due to involvement of long-term secrets. Similarly, $\mathcal{A}$ will not be able to compromise the session keys between MU and the HA during the the login and authentication phase when MU is in his/her home network. Hence, the session-temporary information attack is protected in the proposed scheme and it also provides perfect forward secrecy. As a result, the session key security is preserved and hence, the proposed scheme is also secure against ESL attack.

Proposition 6: The proposed scheme is resilient against the offline password guessing attack through the smart card stolen attack.

Proof 7: Assume that an adversary $\mathcal{A}$ extracts all the information $\{SPW, EID, Q_{HA}, ID_{HA}, G, h(\cdot), \Omega, \tau_{MU}, r', count\}$ stored in the stolen/lost smart card using the power analysis attacks [44], [45] (described in the threat model in Section I-C), where $SPW = h(K_{MUHA} \parallel ID_{MU})$, $EID = E[ID_{MU}]_{K_{MUHA}}$ and $r' = r \oplus h(ID_{MU} \parallel \sigma_{MU} \parallel PW_{MU})$. To guess properly the correct password PW_{MU} from r', the secret credentials, such as the biometric key σ_{MU} and the identity ID_{MU} of MU are necessary to $\mathcal{A}$ apart from random secret r. Also, to derive ID_{MU} from SPW and EID, $\mathcal{A}$ requires the secret key K_{MUHA}. Consequently, it is a computationally infeasible task for guess correctly PW_{MU} as it needs simultaneously guessing another secret credentials K_{MUHA}, ID_{MU} and σ_{MU}. Hence, the proposed scheme is secure against the offline password guessing attack.

Proposition 7: The proposed scheme is resilient against privileged-insider attack.

Proof 8: Though the HA or the TA is trusted entity in the network, a privileged-insider user of that entity may act an insider attacker, say $\mathcal{A}$. At the user registration time, assume that $\mathcal{A}$ has the registration information $\langle ID_{MU}, Q_{MU}, PPW \rangle$, where $k_{MU} = PW_{MU} \oplus r$, $Q_{MU} = k_{MU} \cdot G$ and $PPW = h(PW_{MU} \parallel ID_{MU} \parallel \sigma_{MU})$. In addition, we also assume that the smart card of MU is attained by $\mathcal{A}$ after the registration process is completed. So, $\mathcal{A}$ will have the information $\{SPW, EID, Q_{HA}, ID_{HA}, G, h(\cdot), \Omega, \tau_{MU}, r', count\}$ stored in the stolen/lost smart card. Then, guessing correct password PW_{MU} from PPW needs the biometric key σ_{MU}. To derive the random secret r from r', $\mathcal{A}$ needs σ_{MU}. Hence, without r, it is computationally infeasible task to verify the correct guessed password PW_{MU} of MU. Also, deriving $k_{MU} = PW_{MU} \oplus r$ from $Q_{MU} = k_{MU} \cdot G$ is computational infeasible due to hardness of solving ECDLP (defined in Section II-A). Consequently, the proposed scheme is secure against privileged-insider attack.

Proposition 8: The proposed anonymous group does not compromise the security of the proposed scheme.

Proof 9: The anonymous group, when is used, disallows verification of individual identity. We individually discuss the following cases:

- MU, who has been de-registered, can attempt to access service with group credentials. However, the group credentials are refreshed periodically as well as in event of member de-registration.
- An adversary $\mathcal{A}$ can attempt to impersonate the valid group members. Only valid group members have access to group credentials. Even if the smart card is compromised, the sensitive information is encrypted with k_{MU}.
- A valid group member can voluntarily share the group credentials with $\mathcal{A}$. In this scenario, $\mathcal{A}$ can successfully impersonate an anonymous group member, but only until the integrity of the group is verified. A valid group member will have no motivation to co-operate with $\mathcal{A}$.

Considering the above cases, it is inferred that an anonymous group does not compromise the security of the proposed scheme.

V. FORMAL SECURITY VERIFICATION THROUGH AVISPA TOOL: SIMULATION STUDY

In this section, the proposed scheme is simulated using the AVISPA tool, a widely-accepted tool for the formal security verification. This section demonstrates how the replay and man-in-the-middle attacks against an adversary are protected in the proposed scheme.

AVISPA is an automated validation tool with a high-level language specification for the security sensitive applications and protocols [57]. In recent years, AVISPA becomes a popular and powerful tool for the formal security verification [58]–[64]. The architecture of the AVISPA tool is shown in Figure 8. AVISPA provides various automatic

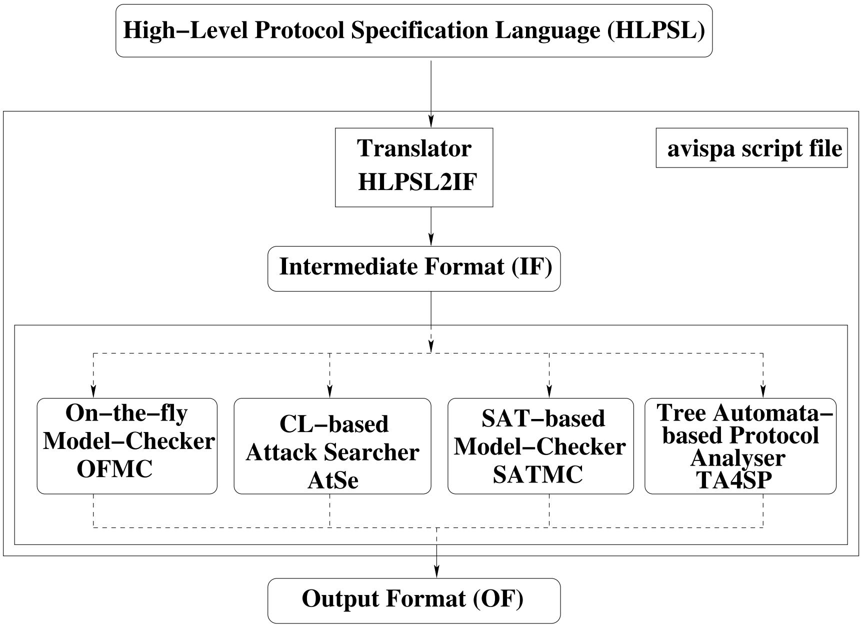

High–Level Protocol Specification Language (HLPSL)
Translator HLPSL2IF
avispa script file
Intermediate Format (IF)
On–the–fly Model–Checker OFMC
CL–based Attack Searcher AtSe
SAT–based Model–Checker SATMC
Tree Automata–based Protocol Analyser TA4SP
Output Format (OF)

FIGURE 8. Architecture of AVISPA [57].

analysis techniques through its four back-ends: 1) On-the-fly Model-Checker (OFMC), 2) Constraint Logic based Attack Searcher (CL-AtSe), 3) SAT-based Model-Checker (SATMC) and 4) Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP). More detailed descriptions on these back-ends can be found in [57].

The security protocols which are to be analyzed for their security part by AVISPA tool need to be implemented in HLPSL (High Level Protocols Specification Language) [65]. HLPSL is a role based language and contains the following roles [57], [65]:

- Basic roles: These roles, in general, represent different participating entities in the protocol.
- Composition roles: These roles represent different scenarios involving basic roles.

In HLPSL, an intruder is represented as one of the basic legitimate roles and is always represented by i. The HLPSL specification of the protocol is translated to its intermediate format (IF) using the HLPSL2IF translator, and then IF is converted to output format (OF) by one of the four back-ends. The OF typically has the following sections [65]:

- SUMMARY: It defines whether the tested protocol is safe, unsafe, or whether the analysis is inconclusive.
- DETAILS: It states a detailed explanation of why the tested protocol is concluded as safe, or under what conditions the test application or protocol is exploitable using an attack, or why the analysis is inconclusive.
- PROTOCOL: It defines the HLPSL specification of the target protocol in intermediate form.
- GOAL: The goal of the analysis which is being performed by AVISPA using HLPSL specification.
- BACKEND: The name of the back-end that is used for the analysis, that is, one of OFMC, CL-AtSe, SATMC and TA4SP.
- Finally, the trace of a possible vulnerability to the target protocol, if any, along with some useful statistics and relevant comments.

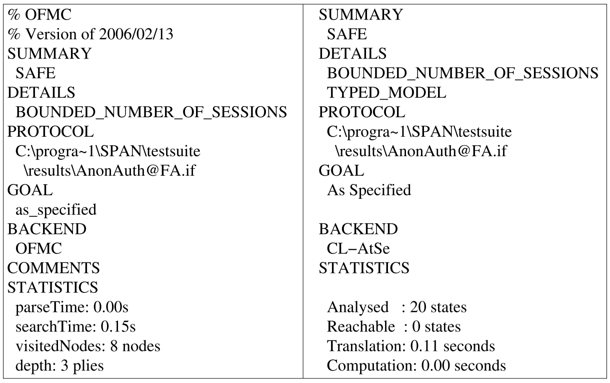
Various basic roles for a mobile user MU), the foreign agent (FA) and the home agent (HA) have been implemented in HLPSL for the proposed scheme. Apart from these roles, the roles for the session, goal and environment for the proposed scheme have been also implemented in HLPSL. For this purpose, the following three cases are considered in implementation:

- Case 1. It simulates the registration phase followed by the login and authentication phase when a mobile user MU is not in his/her home network.
- Case 2. It simulates the registration phase followed by the login and authentication phase when a mobile user MU is in his/her home network.
- Case 3. It simulates the registration phase followed by the group formation phase.

The proposed scheme is simulated for all the cases 1, 2 and 3 under the two broadly-used back-ends, namely OFMC and CL-AtSe, using the SPAN, the Security Protocol ANimator for AVISPA tool [66]. It is worth noticing that the proposed scheme uses the bitwise XOR operations for the cases 1, 2 and 3. At present, other backends, namely SATMC and TA4SP do not support this feature of implementing XOR operations in the roles. As a result, the simulation results of the proposed scheme for all three cases using SATMC and TA4SP backends come as ‘‘inconclusive’’, and hence, we have ignored these results in this paper. The following verifications are essential:

TABLE 4. Computation costs comparison.

Scheme	MU	FA	HA
Proposed	$7T_h + 3T_x + 3T_{E_s} + 4T_m + 1T_b$ ≈ 344.98 ms	$2T_h + 1T_x + 2T_{E_s} + 3T_m$ ≈ 207.63 ms	$4T_h + 3T_{E_s} + 2T_m$ ≈ 154.25 ms
Arshad *et al.* [29]	$7T_h + 1T_x + 1T_{E_s} + 2T_m$ ≈ 138.35 ms	$5T_h + 2T_m$ ≈ 126.65 ms	$6T_h + 3T_{E_s}$ ≈ 29.10 ms
Xu *et al.* [33]	$8T_h + 7T_x + 1T_b + 1T_m$ ≈ 130.16 ms	$6T_h + 2T_{E_s} + 1T_m$ ≈ 66.08 ms	$15T_h + 6T_x$ ≈ 7.51 ms
Lee *et al.* [32]	$10T_h + 8T_x$ ≈ 5.01 ms	$9T_h + 3T_x$ ≈ 4.50 ms	$9T_h + 6T_x$ ≈ 4.01 ms
Memon *et al.* [67]	$7T_h + 6T_x + 2T_m$ ≈ 128.66 ms	$4T_h + 2T_m$ ≈ 128.15 ms	$9T_h + 6T_x$ ≈ 4.51 ms
Zhao *et al.* [68]	$7T_h + 3T_x + 1T_{E_s} + 3T_m$ ≈ 201.428 ms	$3T_h + 3T_{E_s} + 1T_{E_a} + 3T_m$ ≈ 342.98 ms	$5T_h + 2T_x + 2T_{E_s} + 1T_{E_a} + 5T_m$ ≈ 461.43 ms
Mun *et al.* [31]	$4T_h + 2T_x + 2T_m + 1T_{mac}$ ≈ 128.65 ms	$3T_h + 2T_x + 2T_m + 1T_{mac}$ ≈ 128.15 ms	$3T_h + 2T_x$ ≈ 1.51 ms



```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  C:\progra~1\SPAN\testsuite
    \results\AnonAuth@FA.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.15s
  visitedNodes: 8 nodes
  depth: 3 plies
```

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  C:\progra~1\SPAN\testsuite
    \results\AnonAuth@FA.if
GOAL
  As Specified

BACKEND
  CL-AtSe
STATISTICS

  Analysed   : 20 states
  Reachable  : 0 states
  Translation: 0.11 seconds
  Computation: 0.00 seconds
```

FIGURE 9. The result of the analysis using OFMC and CL-AtSe backends (Case 1).

TABLE 5. Approximate time required for various cryptographic operations [69], [70].

Notation	Description (Time to compute)	Rough computation time (in milliseconds)
T_h	One-way hash function	0.5
T_m	ECC point multiplication	63.075
T_{E_s}	Symmetric encryption/decryption	8.7
T_{me}	Modular exponentiation	522
$T_{E_a} \approx T_{me}$	Asymmetric encryption/decryption	522
$T_{mac} \approx T_h$	Message authentication code	0.5
$T_b \approx T_m$	Fuzzy extractor operation	63.075

TABLE 6. Communication costs comparison.

Scheme	No. of bytes	No. of rounds
Proposed	456	4
Arshad *et al.* [29]	304	5
Xu *et al.* [33]	600	4
Lee *et al.* [32]	340	5
Memon *et al.* [67]	460	5
Zhao *et al.* [68]	928	5
Mun *et al.* [31]	340	5

- *Executability check on non-trivial HLPSL specifications:* Due to some modeling mistakes, a protocol can not sometimes execute to completion. Hence, it may be possible that the AVISPA backends will not be able to find an attack, if the protocol model can not reach to a state where an attack can take place. An executability test is then extremely important [65].
- *Replay attack check:* For this check, the OFMC and Cl-AtSe back-ends check whether the legitimate agents can execute the specified protocol by performing a search of a passive intruder. In this case, the back-ends supply the intruder the knowledge of some normal sessions between the legitimate agents. The simulation results shown in Figures 9, 10 and 11 indicate that the proposed scheme is secure against the replay attack.
- *Dolev-Yao model check:* For such a check, the OFMC and Cl-AtSe back-ends also check if any man-in-the-middle attack is possible by an intruder. It is also evident from the simulation results reported in Figures 9, 10 and 11 that the proposed scheme consummates the design goals and it is secure against man-in-the-middle attack under OFMC and Cl-AtSe backends.

VI. PERFORMANCE COMPARISON

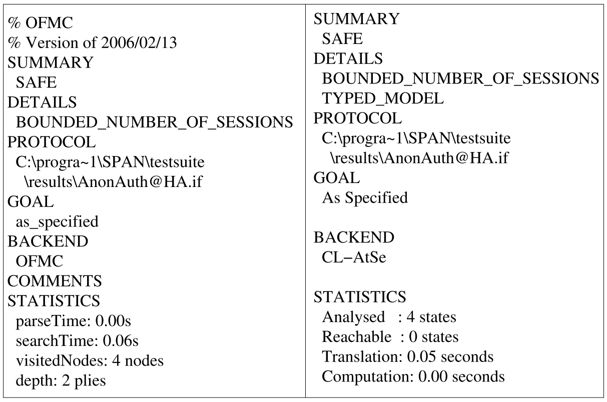
In this section, we compare the merits of the proposed scheme with respect to other existing related schemes, such as the schemes of Arshad and Rasoolzadegan [29], Xu and Wu [33], Lee *et al.* [32], Memon *et al.* [67], Zhao *et al.* [68] and Mun *et al.* [31].

Table 4 shows the computation costs comparison among the proposed scheme and other schemes during the login & authentication and session key agreement phases for MU,

TABLE 7. Security & functionality features comparison.

Feature	Proposed	Arshad *et al.* [29]	Xu *et al.* [33]	Lee *et al.* [32]	Memon *et al.* [67]	Zhao *et al.* [68]	Mun *et al.* [31]
Strong user's anonymity	✓	×	✓	×	✓	×	×
Anonymous user group	✓	×	×	×	×	×	×
Three factor authentication	✓	×	✓	×	×	×	×
Proper mutual authentication	✓	✓	✓	×	✓	✓	×
Resist MU impersonation attack	✓	×	✓	×	✓	✓	×
Resist replay attack	✓	✓	✓	✓	✓	×	×
Resist man-in-the-middle attack	✓	✓	✓	✓	✓	×	×
Perfect forward secrecy	✓	×	✓	×	✓	✓	✓
Resist off-line password guessing attack	✓	✓	✓	×	×	×	×
Resist privileged-insider attack	✓	×	✓	✓	×	×	×
No verifier table	✓	✓	✓	✓	✓	✓	✓
Support password change	✓	✓	✓	✓	✓	✓	×
Resist ESL attack	✓	×	×	×	×	×	×
Re-issue of lost smart card	✓	×	×	×	×	×	×
User untraceability	✓	✓	✓	×	×	✓	×
Support simplified authentication scheme when a user is located in home network	✓	×	×	×	✓	✓	×

Note: ×: the scheme is not secure against an attack or it does not support a feature; ✓: the scheme is resilient against an attack or it supports a feature



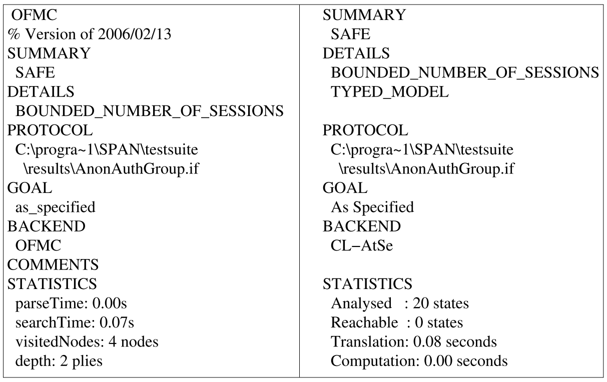
```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  C:\progra~1\SPAN\testsuite
    \results\AnonAuth@HA.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.06s
  visitedNodes: 4 nodes
  depth: 2 plies
```

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  C:\progra~1\SPAN\testsuite
    \results\AnonAuth@HA.if
GOAL
  As Specified

BACKEND
  CL–AtSe

STATISTICS
  Analysed   : 4 states
  Reachable  : 0 states
  Translation: 0.05 seconds
  Computation: 0.00 seconds
```

FIGURE 10. The result of the analysis using OFMC and CL-AtSe backends (Case 2).



```
 OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  C:\progra~1\SPAN\testsuite
    \results\AnonAuthGroup.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.07s
  visitedNodes: 4 nodes
  depth: 2 plies
```

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  C:\progra~1\SPAN\testsuite
    \results\AnonAuthGroup.if
GOAL
  As Specified
BACKEND
  CL–AtSe

STATISTICS
  Analysed   : 20 states
  Reachable  : 0 states
  Translation: 0.08 seconds
  Computation: 0.00 seconds
```

FIGURE 11. The result of the analysis using OFMC and CL-AtSe backends (Case 3).

HA and *FA*. For comparison of computation costs among costs, we apply the following notations provided in Table 5 along with their rough estimated computation time in milliseconds. We have used the existing experimental results reported in [69] and [70]. From Table 4, it is noted that the proposed scheme requires more computation cost as compared to some existing schemes. This is justified because the proposed scheme applies the biometric verification using the fuzzy extractor technique for the mobile user login and authentication and the proposed scheme also offers better security and functionality features as compared to other existing schemes (see Table 7).

In Table 6, we tabulate the communication costs for the authentication and key establishment phase for the proposed scheme and other existing schemes. The bit-length of different parameters are taken as follows: ID_x: 160 bits, random number: 160 bits; $x.P$ (ECC point (x_P, y_P)): 320 bits (assuming 160-bit ECC provides the same level security of 1024-bit RSA public key cryptosystem [71]); output (message digest) of one-way hash function $h(x)$: 160 bits; 128-bit ciphertext for 128-bit plaintext block using symmetric encryption/decryption (using AES-128) [72]. We calculate the communication costs for the proposed scheme as follows. The message $M_1 = \{A, SPWx, EIDx, ID_{HA}, Q_x\}$ needs $(160 + 160 + (\lceil 160/128 \rceil) \times 128 + 160 + 320) = 1056$ bits. Other messages $M_2 = \{A, EIDx, Q_x, EY, ID_{FA}\}$, $M_3 = \{E[SPW', EYh, authToken]_{K'_{yHA}}\}$ and $M_4 = \{EYh, cert\}$ need $(160+(\lceil 160/128\rceil)\times 128+320+(\lceil 320/128\rceil)\times 128+160) = 1280$ bits, $(\lceil (160 + 384 + 160)/128 \rceil) \times 128 = 768$ bits and $(\lceil 320/128 \rceil) \times 128 + 160 = 544$ bits, respectively. Thus, in total, the proposed scheme needs $(1056 + 1280 + 768 + 544) = 3648$ bits, that is, 456 bytes. We can observe the proposed scheme has a significantly lower communication cost as compared to the schemes [33], [67], [68], but it has slightly higher than that of the schemes [29], [31], and [32]. This is justified as the proposed scheme offers better security and functionality features as compared to other existing schemes (see Table 7).

Finally, Table 7 compares the functionality and security features of the proposed scheme along with other schemes. It is apparent that the proposed scheme provides better security, user anonymity and overall more functionality features as compared to other schemes.

VII. CONCLUSION

In this article, we contended that with the ever increasing thrust into monitoring and tracking by government agencies, user anonymity should not dependent on the infallibility of the service provider (*HA*). To this goal, we presented a new anonymous user authentication scheme for roaming in global mobility networks. The proposed authentication scheme allows authentication for both cases: 1) when the *MU* is in a foreign network and 2) when the *MU* is in his/her home network. The proposed scheme supports a group formation of *n* mobile users. In addition, the proposed scheme provides the integrity check of the group credentials, password update, smart card re-issue when the smart card of the *MU* is lost or compromised. Through the BAN logic analysis, we demonstrated that the proposed scheme provides mutual authentication between a mobile user and the foreign/home agent. Further, through informal security analysis, we showed the resistance to various known attacks of the proposed scheme. Additionally, we simulated the proposed scheme using the widely accepted AVISPA tool and the simulation results assure that the scheme is safe. The comparative analysis shows that there is a better trade-off among the computation and communication costs, and security and functionality features among the proposed scheme and other schemes. Overall, the proposed scheme allows the group formation procedure for the mobile users and other features that are not supported by the previous existing schemes.

ACKNOWLEDGMENTS

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

REFERENCES

[1] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, “Anonymous connections and onion routing,” *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 482–494, May 1998.

[2] *Tor*. Accessed: Feb. 2018. [Online]. Available: https://www.torproject.org/

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

[4] 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.

[5] W.-H. Yang and S.-P. Shieh, “Password authentication schemes with smart cards,” *Comput. Secur.*, vol. 18, no. 8, pp. 727–733, 1999.

[6] T.-C. Wu, “Remote login authentication scheme based on a geometric approach,” *Comput. Commun.*, vol. 18, no. 12, pp. 959–963, 1995.

[7] K. Tan and H. Zhu, “Remote password authentication scheme based on cross-product,” *Comput. Commun.*, vol. 22, no. 4, pp. 390–393, 1999.

[8] H.-Y. Chien, J.-K. Jan, and Y.-M. Tseng, “A modified remote login authentication scheme based on geometric approach,” *J. Syst. Softw.*, vol. 55, no. 3, pp. 287–290, 2001.

[9] Y. Sung-Ming and L. Kuo-Hong, “Shared authentication token secure against replay and weak key attacks,” *Inf. Process. Lett.*, vol. 62, no. 2, pp. 77–80, 1997.

[10] H.-Y. Chien, J.-K. Jan, and Y.-M. Tseng, “An efficient and practical solution to remote authentication: Smart card,” *Comput. Secur.*, vol. 21, no. 4, pp. 372–375, 2002.

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

[12] H.-Y. Chien and C.-H. Chen, “A remote authentication scheme preserving user anonymity,” in *Proc. 19th Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, vol. 2. Mar. 2005, pp. 245–248.

[13] I.-E. Liao, C.-C. Lee, and M.-S. Hwang, “Security enhancement for a dynamic ID-based remote user authentication scheme,” in *Proc. Int. Conf. Next Generat. Web Services Pract. (NWeSP)*, Seoul, South Korea, Aug. 2005, pp. 1–4.

[14] E.-J. Yoon and K.-Y. Yoo, “Improving the dynamic ID-based remote mutual authentication scheme,” in *Proc. OTM Conf. Int. Conf.*, Berlin, Germany, 2006, pp. 499–507.

[15] J. Zhu and J. Ma, “A new authentication scheme with anonymity for wireless environments,” *IEEE Trans. Consum. Electron.*, vol. 50, no. 1, pp. 231–235, Feb. 2004.

[16] 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.

[17] 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, 2009.

[18] T.-Y. Youn, Y.-P. 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.

[19] R. Madhusudhan and R. C. Mittal, “Dynamic ID-based remote user password authentication schemes using smart cards: A review,” *Intell. Algorithms Data-Centric Sensor Netw.*, vol. 35, no. 4, pp. 1235–1248, Jul. 2012.

[20] G. Yang, D. S. Wong, H. Wang, and X. Deng, “Two-factor mutual authentication based on smart cards and passwords,” *J. Comput. Syst. Sci.*, vol. 74, no. 7, pp. 1160–1172, 2008.

[21] R.-C. Wang, W.-S. Juang, and C.-L. Lei, “Robust authentication and key agreement scheme preserving the privacy of secret key,” *Comput. Commun.*, vol. 34, no. 3, pp. 274–280, 2011.

[22] I.-E. Liao, C.-C. Lee, and M.-S. Hwang, “A password authentication scheme over insecure networks,” *J. Comput. Syst. Sci.*, vol. 72, no. 4, pp. 727–740, Jun. 2006.

[23] C.-S. Tsai, C.-C. Lee, and M.-S. Hwang, “Password authentication schemes: Current status and key issues,” *Int. J. Netw. Security*, vol. 3, no. 2, pp. 101–115, 2006.

[24] M. K. Khan, S.-K. Kim, and K. Alghathbar, “Cryptanalysis and security enhancement of a ‘more efficient & secure dynamic id-based remote user authentication scheme,’” *Comput. Commun.*, vol. 34, no. 3, pp. 305–309, 2011.

[25] Y.-Y. Wang, J.-Y. Liu, F.-X. Xiao, and J. Dan, “A more efficient and secure dynamic ID-based remote user authentication scheme,” *Comput. Commun.*, vol. 32, no. 4, pp. 583–585, Mar. 2009.

[26] D. Wang, D. He, P. Wang, and C.-H. Chu, “Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment,” *IEEE Trans. Depend. Sec. Comput.*, vol. 12, no. 4, pp. 428–442, Aug. 2015.

[27] 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.

[28] R. Madhusudhan and K. S. Suvidha, “An efficient and secure user authentication scheme with anonymity in global mobility networks,” in *Proc. 31st Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, Mar. 2017, pp. 19–24.

[29] 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, 2017.

[30] M. Karuppiah, S. Kumari, A. K. Das, X. Li, F. Wu, and S. Basu, “A secure lightweight authentication scheme with user anonymity for roaming service in ubiquitous networks,” *Security Commun. Netw.*, vol. 9, no. 17, pp. 4192–4209, 2016.

[31] 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, no. 1, pp. 214–222, 2012.

[32] 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.

[33] L. Xu and F. Wu, "A novel three-factor authentication and key agreement scheme providing anonymity in global mobility networks," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3428–3443, 2016.

[34] X. Li, J. Niu, S. Kumari, F. Wu, and K.-K. R. Choo, "A robust biometrics based three-factor authentication scheme for global mobility networks in smart city," *Future Generat. Comput. Syst.*, vol. 83, pp. 607–618, Jun. 2018, doi: 10.1016/j.future.2017.04.012.

[35] 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.

[36] V. Odelu *et al.*, "A secure anonymity preserving authentication scheme for roaming service in global mobility networks," *Wireless Pers. Commun.*, vol. 96, no. 2, pp. 2351–2387, 2017.

[37] 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, no. 3, pp. 131–144, 2017.

[38] M. Karuppiah *et al.*, "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, 2017.

[39] F. Wu *et al.*, "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, 2016.

[40] P. Samarati and L. Sweeney, "Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression," SRI Int., Menlo Park, CA, USA: Tech. Rep. SRI-CSL-98-04, 1998.

[41] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam, "L-diversity: Privacy beyond k-anonymity," in *Proc. 22nd Int. Conf. Data Eng. (ICDE)*, Atlanta, GA, USA, Apr. 2006, p. 24.

[42] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *Proc. 23rd Int. Conf. Data Eng. (ICDE)*, Istanbul, Turkey, 2007, pp. 106–115.

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

[44] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 1999, pp. 388–397.

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

[46] A. Dua, N. Kumar, A. K. Das, and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Trans. Veh. Technol.*, to be published, doi: 10.1109/TVT.2017.2780183.

[47] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2001, pp. 453–474.

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

[49] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Trans. Smart Grid*, 'to be published, doi: 10.1109/TSG.2016.2602282.

[50] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.

[51] P. Sarkar, "A simple and generic construction of authenticated encryption with associated data," *ACM Trans. Inf. Syst. Secur.*, vol. 13, no. 4, pp. 1–16, 2010.

[52] *Secure Hash Standard*, Standard FIPS PUB 180-1, National Institute of Standards and Technology (NIST), accessed: Feb. 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[53] J.-P. Linnartz and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates," in *Proc. 4th Int. Conf. Audio Video-Based Biometr. Person Authentication (AVBPA)*, Guildford, U.K., 2003, pp. 393–402.

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

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

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

[57] *AVISPA*. Accessed: Jan. 2018. [Online]. Available: http://www.avispa-project.org/

[58] A. K. Das, "A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications," *Netw. Sci.*, vol. 2, nos. 1–2, pp. 12–27, May 2013.

[59] A. K. Das, "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks," *Peer Peer Netw. Appl.*, vol. 9, no. 1, pp. 223–244, 2016.

[60] A. K. Das, "A secure and efficient user anonymity-preserving three-factor authentication protocol for large-scale distributed wireless sensor networks," *Wireless Pers. Commun.*, vol. 82, no. 3, pp. 1377–1404, 2015.

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

[62] V. Odelu, A. K. Das, and A. Goswami, "DMAMA: Dynamic migration access control mechanism for mobile agents in distributed networks," *Wireless Pers. Commun.*, vol. 84, no. 1, pp. 207–230, 2015.

[63] V. Odelu, A. K. Das, and A. Goswami, "An effective and robust secure remote user authenticated key agreement scheme using smart cards in wireless communication systems," *Wireless Pers. Commun.*, vol. 84, no. 4, pp. 2571–2598, 2015.

[64] V. Odelu, A. K. Das, and A. Goswami, "A secure and scalable group access control scheme for wireless sensor networks," *Wireless Pers. Commun.*, vol. 85, no. 4, pp. 1765–1788, 2015.

[65] D. von Oheimb, "The high-level protocol specification language HLPSL developed in the EU project AVISPA," in *Proc. 3rd APPSEM*, Frauenchiemsee, Germany, 2005, pp. 1–17.

[66] AVISPA. *SPAN, the Security Protocol Animator for AVISPA*. Accessed: Feb. 2018. [Online]. Available: http://www.avispa-project.org

[67] I. Memon, I. Hussain, R. Akhtar, and G. Chen, "Enhanced privacy and authentication: An efficient and secure anonymous communication for location based service using asymmetric cryptography scheme," *Wireless Pers. Commun.*, vol. 84, no. 2, pp. 1487–1508, 2015.

[68] 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, 2014.

[69] D. He, N. Kumar, M. Khan, and J.-H. Lee, "Anonymous two-factor authentication for consumer roaming service in global mobility networks," *IEEE Trans. Consum. Electron.*, vol. 59, no. 4, pp. 811–817, Nov. 2013.

[70] Q. Jiang, J. Ma, G. Li, and L. Yang, "An efficient ticket based authentication protocol with unlinkability for wireless access networks," *Wireless Pers. Commun.*, vol. 77, no. 2, pp. 1489–1506, 2014.

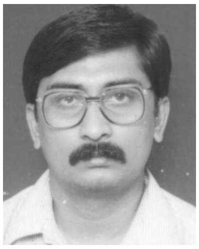
[71] N. Jansma and B. Arrendondo. *Performance Comparison of Elliptic Curve and RSA Digital Signatures*. Accessed: Mar. 2017. [Online]. Available: http://nicj.net/files/performance_comparison_of_elliptic_curve_and_rsa_digital_signatures.pdf

[72] *Advanced Encryption Standard (AES)*, Standard FIPS PUB 197, NIST, accessed: Apr. 2017. [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

SOUMYA BANERJEE received the M.Tech. degree in software engineering from Jadavpur University, Kolkata, India, where he is currently pursuing the Ph.D. degree in computer science and engineering. His current research interests include cryptography and network security. He has authored four papers in international journals and conferences in the above areas.

VANGA ODELU received the M.Tech. and Ph.D. degrees in computer science and data processing from IIT Kharagpur, India. He is currently a Research Assistant with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. He is also associated as a Research Professor with the IoTCoN Laboratory, Korea University, South Korea. Prior to this, he was an Assistant Professor with the Department of Computer Science and Engineering, Indian Institute of Information Technology, Sri City, India. His research interests include cryptography, network security, hierarchical access control, remote user authentication, cloud computing security, and smart grid security. He has authored over 45 papers in international journals and conferences in his area of research.

ASHOK KUMAR DAS (M'17) received the M.Sc. degree in mathematics, the M.Tech. degree in computer science and data processing, and the Ph.D. degree in computer science and engineering from IIT Kharagpur, India. He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. His research interests include cryptography, wireless sensor network security, security in vehicular ad hoc networks, smart grid, smart city, cloud/fog computing, Internet of Things, healthcare applications, and remote user authentication. He has authored over 160 papers in international journals and conferences in the above areas. He has served as a program committee member in many international conferences. He was a recipient of the Institute Silver Medal from IIT Kharagpur. Some of his research findings are published in top cited journals such as the IEEE Transactions on Information Forensics and Security, the IEEE Transactions on Dependable and Secure Computing, the IEEE Transactions on Smart Grid, the IEEE Internet of Things Journal, the IEEE Transactions on Industrial Informatics, the IEEE Transactions on Consumer Electronics, the IEEE Transactions on Vehicular Technology, the IEEE Journal of Biomedical and Health Informatics, the IEEE *Consumer Electronics Magazine*, the IEEE Access, the IEEE *Communications Magazine*, *Future Generation Computer Systems*, *Journal of Network and Computer Applications*, *Computer Networks*, and *Expert Systems with Applications*. He is in the Editorial Board of the *KSII Transactions on Internet and Information Systems*, and the *International Journal of Internet Technology and Secured Transactions* (Inderscience), and a Guest Editor for the *Computers & Electrical Engineering* (Elsevier) for the special issue on Big data and IoT in e-healthcare.



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

NEERAJ KUMAR (M'16–SM'17) received the Ph.D. degree in computer science and engineering from Shri Mata Vaishno Devi University, Katra, India, in 2009. He was a Post-Doctoral Research Fellow with Coventry University, Coventry, U.K. He is currently an Associate Professor with the Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Patiala, India. He has authored over 170 technical research papers published in leading journals and conferences from the IEEE, Elsevier, Springer, and John Wiley. 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 has guided many research scholars leading to M.E./M.Tech. and Ph.D. He is in the Editorial Board of the *Journal of Network and Computer Applications* (Elsevier) and the *International Journal of Communication Systems* (Wiley).

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

SUDEEP TANWAR received the B.Tech. degree in computer engineering from Kurukshetra University, Kurukshetra, Haryana, in 2002, the M.Tech. degree (Hons.) in information technology from Guru Gobing Singh Inderprastha University, Delhi (USIT Campus), in 2009, and the Ph.D. degree in computer science and engineering with specialization in wireless sensor network in 2016. He is currently an Associate Professor with the Computer Engineering Department, Institute of Technology, Nirma University, Ahmedabad, India. His research interests include information security, energy efficiency in WSNs, and integration of sensor with cloud and body area network. He has authored 30 technical research papers in his research areas.