A provably secure and efficient authenticated key agreement scheme for Energy Internet based Vehicle-to-Grid technology framework

Azeem Irshad, Muhammad Usman, Shehzad Ashraf Chaudhry, Husnain Naqvi and Muhammad Shafiq

***Abstract*— The Energy Internet (EI)-based vehicle-to-grid (V2G) technology facilitates the electric vehicles not only to distribute additional electricity into grid systems, but also support receiving back from the power grid in the form of charging. The secure key establishment is quite significant to initiate the bidirectional electricity power delivery into and from the system. To effectively implement any EI-based V2G communication, the authentication protocol must be free from cyber attacks. In this study, we not only explore the drawbacks of several smart grid-based authentication protocols but also bring forth the limitations of a recently presented EI-based V2G scheme by Gope and Sikdar. The examined drawbacks in this protocol may disrupt its proper functioning, since it faces de-synchronization problems while logging into the mobile device bearing registration parameters. The scheme is also vulnerable to replay attack and man-in-the-middle attack. The user is also unable to validate session key in the protocol. Considering these limitations, we propose a novel and efficient V2G protocol framework enabling the vehicles to communicate or recharge at desired recharging stations. The results of proposed framework are compared with several contemporary schemes, and its security features are validated by random oracle model-based formal analysis.**

***Index Terms*—Vehicle-to-grid, authentication, smart grid, energy internet, attacks**

I. Introduction

The paradigm of energy internet (EI) seeks to assimilate the information and communication technologies (ICT), modern cyber systems and the current electrical power systems which could aid in establishing next generation smart grids tremendously [1]. The concept of EI allows the energy to be shared analogous to the information being exchanged on traditional internet. The EI resolves to integrate the element of economics, data information, and energy relying on power grid-based network, resulting in an open framework to exchange the energy and corresponding information. It enables to combine various energy sources with smart grid and contribute to overall efficiency in energy generation, distribution, customer-oriented operations and service provisioning. All of these contributing factors rely on secure communication among the participating entities.

The Vehicle to Grid (V2G) technology allows the bidirectional flow of energy between power grid and the electric vehicles (EV). The electric energy could be transferred from power grid to EV whenever the latter needs to recharge its battery, and from EV to power grid in case of extra energy produced from EV. Hence, in V2G ecosystem, the vehicles also act as the energy asset for the smart grid and this bidirectional charging may contribute significantly in producing the energy. Owing to V2G technology, a single household or an individual EI owner may get into the trade of selling and purchasing of energy from one's electric vehicle, without building a formal power generation and distribution system. The energy produced under EI-based V2G and other renewable energy sources could not only meet high energy requirements at critical times, but also averts wastage of energy produced from renewable sources by real-time injecting of the surplus energy back into the grid. This efficiency of renewable energy leads to its wider adoption in comparison with conventional power energy systems.

Besides the flow of energy, another significant aspect of EI-based V2G network is information exchange among interacting entities. Recently many protocols have been presented for authenticated data flows in energy internet based grid systems. The standard that deals with the EI-based protocols and architectures is ISO/IEC/IEEE 18880 [2]. This standard defines architecture, data storage and application services for various protocols. The security loopholes have been fixed and features enhanced in the later standards such as ISO/IEC/IEEE 18881-3. The V2G network system focus on mere vehicle charging, grid based charging stations, and the power supplying grid system. The charging stations could be simultaneously shared by many users. Different standards of grid are used at various levels of charging. For charging purpose, IEC 15118 standard is used to establish communication between EV and EV charger [3]. Likewise, the electric vehicle supply equipment employs Open Charge

Manuscript received xxxxxxx; revised xxxxxxx; accepted xxxxxxx. Date of publication xxxxxxx; date of current version xxxxxxx. (Corresponding author: Shehzad Ashraf Chaudhry)
A. Irshad is with the Department of Computer Science, University of Sialkot, Pakistan (e-mail: irshadazeem2@gmail.com).
M. Usman is with University of South Wales, United Kingdom (e-mail: muhammad.usman@southwales.ac.uk).
S.A. Chaudhry is with Department of Computer Engineering, Istanbul Gelisim University Istanbul, Turkey (email: ashraf.shahzad.ch@gmail.com)
H. Naqvi is with Department of Computer Science, Muslim Youth University Islamabad, Pakistan (email: husnain.naqvi@myu.edu.pk)
M. Shafiq is with Department of Information and Communication Engineering, Yeungnam University, Gyeongsan, 38541 South Korea (email:shafiq.pu@gmail.com)

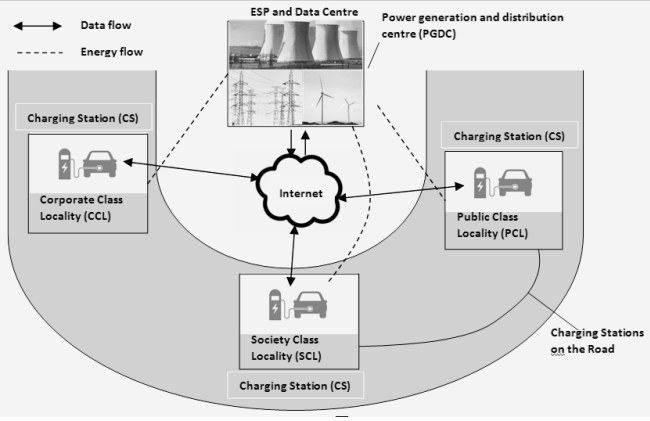

Fig. 1. System model

Point Protocol (OCPP) to communicate with energy management systems [4]. The security of EI-based V2G systems is of significant concern, since the vehicle might be attacked by an attacker affecting not only its operation but also risk its privacy. The privacy threat could be exposure of user's identity, location and driving path of vehicle, etc. Due to mobility of vehicles, the security procedures are getting hard to implement in V2G infrastructure-based environment. We can see several studies, recently, to ensure the vigorous authenticated key agreements in EI-based V2G systems [1-2].

A. Related Work

Many authentication protocols have been presented for Advanced Metering Infrastructure (AMI) with different application objectives, recently. [5] presented two elliptic curve cryptography (ECC) and identity-based authentication protocols. Although, these schemes are resistant to impersonation and de-synchronization attacks and reduced computational cost for smart-meter's end, yet these are prone to man-in-the-middle attack and false data injection attacks. [6] presented a smart grid-oriented protocol relying on both symmetric and ECC-based operations. However, [6] was found to be prone to false injection attacks [7], and high computation cost renders it unfit for smart grid applications. [7] designed a protocol embedding symmetric and public-key operations. Later, [8] demonstrated that [7] does not provide resistance to man in the middle attacks, and proposed another data aggregation scheme. Thereafter, [9] showed that [8] neither resist against forgery attacks nor protects the privacy of user. Later, Tsai et al. presented a key distribution protocol for smart grids by combining identity-based signature and encryption [10]. Then, [10] remarked that does not ensure session key security and privacy of long-term secrets in smart meter and presented an efficient scheme [11]. Thereafter, [12] notices that the scheme [11] suffers man in the middle attack further leading to DoS attack ultimately. In [12], the physical protection of smart meter is considered by employing Physical Uncloneable Functions (PUFs). Here, other than [4-10], many protocols in V2G-based systems can be seen with privacy issues [11-15, 20-23]. Many of these schemes employ group-signatures and sign encryption-based operations. However, these are costly implementations and also the location privacy concerns for EV users remained unsolved in those schemes. In this context, Gope and Sikdar (G & S) presented a lightweight EI-based V2G authentication protocol [12], however, after a careful observation we examined that some limitations in the protocol may disrupt the proper functioning of protocol framework. The G & S's scheme suffers de-synchronization problems while logging into the device bearing registration parameters. The scheme is also vulnerable to replay attack and man-in-the-middle attack, since any adversary may pick a legitimate message from the user request on open channel and forward to service provider by appending that message with the charging station's previous session's message. The service provider is unable to detect this attack and validates the forged message mistakenly, which may lead to serious revenue based concerns on the part of service provider. Besides, the user is unable to evaluate the legitimacy of session key in that protocol if the adversary manipulates public channel and injects false information in the message. Considering the above flaws, we propose a novel and efficient V2G protocol framework enabling the vehicles to communicate or recharge at desired service stations in a secure manner. Besides, the results of the proposed framework are compared with several contemporary schemes, and the feasibility of our scheme is demonstrated under random oracle model-based formal analysis.

B. Our Contribution:

In this scheme, we present a lightweight and secure model for EI-based V2G communication architecture. The subscribers may get their vehicles charged on service stations of different rates depending on the geographical location. The existing schemes for V2G are unable to resist various attacks such as impersonation attacks, forgery and man-in-the-middle attacks. Our scheme ensures resistance from those attacks as well as brings efficiency due to employing lightweight primitives.

C. System Model

The system model for the EI-based V2G technology framework is depicted in Fig. 1, which comprises three main set of entities: a number of EV users having a mobile gadget with access of internet, a number of recharging stations CSj, and a Electricity Service provider (ESP). The ESP comprises two components, 1) Power Generation and Distribution (PGDC) 2) Data Centre (DC). A user gets registered with its electric vehicle from ESP. The ESP stores all of its data in data centre. The ESP procures the electric power from different vendors and distributes to several charging stations in various locations. The charging stations may exist in Corporate Class Locality (CCL), residential Society-based Class Locality (SCL) or any Public Class Locality (PCL). The subscribers may get their vehicles charged from any of the charging stations in a location. The charging rates may vary from location to location. For instance, the stations at corporate locations may charge more than residential society locations, and the stations at residential society may charge more than those in public places. In this context, the identity of location becomes very crucial. In this system, the users having EVs get registered with ESP on secure channel. Subsequently, these users employ public channels to get authenticated on the field from various charging stations.

Table I. Symbols with definitions

Symbols	Definition
Ui/CSj/ESP:	User/ Charging Station/ Electric Service Provider
ID_u, ID_c:	Identities of user and CSj
NID_i:	Pseudo identity of user or subscriber
MID_c:	Masked identity of CSj
φ_i , pwd_i	Biometric value and password of user
q_i:	Shared secret between Ui and ESP
K_{uc}:	Shared secret between CSj and ESP
Gen/Rep:	Generation /Reproduction function:
$\hat{A}$:	*Adversary*
SK:	Session key between Ui and CSj
LRI_u, LRI_{CS}	Location region identifiers for Ui and CSj
⊕, ||, *h()*	XOR, Concatenation, A secure one-way hash function

D. Adversary Model

The subscriber and ESP communicate on a secure channel for registration phase, while the same participants utilize public channel to authenticate one another for converging on a mutually agreed session key. We bring the renowned Dolev-Yao attack model [13] in consideration while developing the proposed model. This model assumes that an attacker is capable of intercepting, replaying, and modifying the message contents recovered on public channel. The chances of forgery, replay and man-in-the middle attacks become even higher on account of wireless communication being used in EI-based V2G network. The privacy of user becomes more significant in EI-based vehicle owners, and the adversary may exploit the open channel to intrude into the users' privacies and impersonate on their behalf to get the services. At the same time, various charging stations could impersonate one another to charge more from the subscribers.

II. PRELIMINARIES

This section briefly presents fuzzy extractor function as follows. Fuzzy extractor modifies the biometric input data into uniform random strings which then serves as a biometric key [14]. Using this algorithm, any random length string L_i could be reformed by merging a generic biometric input (including noise) J_i with the helper string H_i. This algorithm needs two operations to function properly, i.e. *Gen* and *Rep*. The *Gen* operation takes biometric input J_i and generates binary output $L_i \in \{0,1\}^l$ and a helper output $H_i \in \{0,1\}^*$. The L_i string is kept secret, while H_i is also stored. To recover L_i, the second operation *Rep* is employed to use the factors J_i and H_i. To validate the correctness of fuzzy extractor, the function d_s $(J_i, J_i^*) <= t$ and $Gen(Ji) \rightarrow (L_i, H_i)$ is utilized. Then, we get $Rep(Ji^*, H_i) \rightarrow L_i$, where d_s represents distance function and t as error threshold. The Table I shows symbols as used in the scheme.

III. Review of G & S protocol

This section presents the working and drawbacks of G & S protocol.

A. Revisiting G & S's Protocol

This section depicts the review of G & S's authentication protocol for EI-based vehicle to grid communication. In this protocol, the three entities namely, user Ui having a mobile gadget with equipped internet, a charging station CSj, and a electricity service provider ESP, interact to validate the Ui's authenticity so that the latter could get the recharging services from CSj. The G & S's protocol [12] contains two phases 1) user registration 2) mutual authentication.

i. *User registration phase*

A vehicle user needs to register from ESP for getting the recharging services. Its registration procedure is given below:

1. Initially, the user submits its identity ID_u towards ESP as a registration request by using a confidential channel.
2. Next, the ESP records the user's entry into its database and constructs a new pseudo identity NID_i, a secret key q_i and also a set of shadow identities $SID = \{sid_1, sid_2, sid_3, ..., sid_n\}$, which may be used if the participants lose synchronization among themselves. Thereafter, ESP submits the message $\{NID_i, q_i, SID\}$ towards user by utilizing a confidential channel.
3. After receiving the message from ESP, the U_i inputs its biometric factor φ_i, password pwd_i and computes $\gamma_i = h(\varphi_i)$ and $\omega_i = h(\gamma_i || pwd_i)$. After computing ω_i, the user stores the message $\{\omega_i, NID_i, q_i^*, SID\}$ in its mobile gadget to utilize while authenticating with the charging station.

ii. *Login and Authentication phase*

To obtain the services of charging station CSj, Ui must authenticate CSj. Likewise; CSj also authenticates the user with the help of ESP. The steps in mutual authentication phase for Ui and CSj are illustrated below:

1. The user inputs its password pwd_i and biometric factor φ_i. Then, it computes $\gamma_i = h(\varphi_i)$ and $\omega_i' = h(\gamma_i || pwd_i)$ and compares the equality for $\omega_i' ?= \omega_i$. If it is not true, the smart card terminates the session. Otherwise, computes $q_i = q_i \oplus h(\varphi_i || pwd_i)$. Next, it generates a random number R_u and finds the location region identifier LRI_u. Then, it computes $EL = LRI_u \oplus h(q_i || R_u)$ and $B_1 = h(NID_i || R_u || q_i || EL)$. Finally, it submits the message $M_1 = \{NID_i, R_u, EL, B_1\}$ towards charging station.
2. Next, CSj generates a random integer R_c and computes $B_2 = h(ID_c || R_c || K_{uc} || LRI_{CS})$, where LRI_{CS} represents location region identifier for charging station. Then, it submits the message $M_2 = \{M_1, ID_c, R_c, LRI_{CS}, B_2\}$ towards ESP.
3. Next, ESP recovers corresponding NID_i from its repository and verifies message. Then, it computes $ID_c = h(q_i || NID_i) \oplus MID_c$ and verifies B_1 and B_2. Onwards, it decodes and compares LRI_u against LRI_{CS}. If it is validated, it further constructs and generates the novel *SK* and a pseudo identity NID_i^{new}. Thereafter, it further computes $NID_i^{new*} = h(NID_i || q_i) \oplus NID_i^{new}$, $SK_u = h(ID_u || q_i || R_u) \oplus SK$, $SK_{cs} = h(ID_c || K_{uc} || R_c) \oplus SK$, $B_3 = h(SK_{cs} || K_{uc} || R_c)$ and $B_4 = h(ID_u || q_i || NID_i^{new*})$. Finally, it submits the message $M_3 = \{NID_i^{new*}, SK_u, B_4) || (SK_{sp}, B_3)\}$ towards *CSj*.
4. The CSj computes and verifies the validity of parameter B_3 and also calculates the session key as $SK = h(ID_c || K_{uc} || R_c) \oplus SK_{CS}$. Then it sends $M_4 = \{NID_i^{new*}, SK_u, B_4\}$ to Ui for final verification.
5. Ui, finally verifies $B_4 ?= B_4$ after computing B_4. If successful, it further computes $SK = h(ID_u || q_i || R_u) \oplus SK_u$ and $NID_i^{new} = h(NID_i || q_i) \oplus NID_i^{new*}$. This mutually agreed session key is used by Ui and CSj to authenticate and get the required services.

B. Drawbacks in G & S's protocol

The G & S has the following drawbacks: 1) The scheme may suffer biometric de-synchronization problem during the login process; 2) The attacker may initiate replay attack, and owing to this neither user, nor ESP could authenticate the CSj; 3) The user is unable to verify the validity of mutually established

session key; 4) If a single session key is exposed to Â, it might lead to server impersonation attacks in future.

i. ***Biometric de-synchronization****:* One of the drawbacks in G & S's scheme is biometric de-synchronization in which the captured biometric parameters might vary little bit each time it is captured that may result in failure to login attempts repeatedly into mobile device by the user. This may occur even without Â's involvement. This is because of the fact, in G & S, the captured biometric features are stored without any biometric parameters capturing tool such as bio-hashing or fuzzy extractor based functions [14].

ii. ***Replay attack****:* In [12], Â may initiate replay attack which may prevent user and ESP to authenticate the involved CSj. The attack may be initiated by taking the following steps:

1. The attacker intercepts the message $M_1=\{NID_i, R_u, EL, B_1\}$ on its way to a particular charging station CSj. Next, it appends any intercepted message of CSj issued for other subscriber $\{ID_c, R_c, LRI_{CS}, B_2\}$ with Ui's message and forwards $M_2=\{M_1, ID_c, R_c, LRI_{CS}, B_2\}$ towards ESP. Now Â may obstruct the message completely and forwards a new message; or else it may utilize a fast communication channel to forward message towards ESP before original message could reach the server.

2. Upon receiving the message from Â, the ESP verifies all the parameters of legitimate user. However, it may not determine the Â's involvement or non-participation of CSj entity in forwarding the received message. The ESP constructs response message and submits to CSj, which is received by Â. The Â, in return, forwards the message to Ui. The message is validated by the user and recovers agreed session key. The pseudonym is also updated in its repository by Ui. However, the legal CSj is ignorant of the created session key by Ui or ESP. Although, it does not disturb the overall system, yet it makes the participants (user and ESP) erroneously believe that the session key is mutually shared by the intended participants. The user will be kept in waiting position from the CSj for any feedback or response. Similarly, ESP shall be expecting from CSj of any revenue credited to its account, since ESP had verified CSj's authenticity to a particular user.

iii. ***No session key verification****:* In G & S scheme, the user does not verify the authenticity of created session key. An adversary may inject a fake message using XOR function on its way towards user from CSj or ESP. The session key should have been included by ESP in the message B_4. Thus, Â may disrupt the functioning of G & S by manipulating it, which renders scheme inapplicable for practical applications.

iv. ***Key Compromise Impersonation attack****:* The G & S claims that if both the keys q_i and K_{uc} are exposed to Â, then only, the adversary may be able to impersonate as a service provider. However, we observe that if a single shared user secret q_i is revealed by mistake to the Â, then it may impersonate as a service provider by taking the following steps:

1. The Â could guess the identity ID_u by using the intercepted public parameter R_u from intercepted SK_u.

2. Now, Â having q_i, R_u and ID_u may impersonate as a service provider by constructing $M_4= \{NID_i^{new*}, SK_u, B_4\}$ and submitting to user, where R_u is intercepted from Ui's authentication request on real time basis. Here, the factors NID_i^{new} and B_4 may be constructed by Â having q_i, by computing $NID_i^{new*}= h(NID_i||q_i)\oplus NID_i^{new}$ and $B_4=h(ID_u||q_i||\ NID_i^{new*})$, where NID_i^{new} is randomly selected pseudonym number. Now, Â may initiate a successful key compromise impersonation attack against user originating the authentication request.

III. Proposed Model

This section presents an enhanced authentication protocol for EI-based vehicle to grid communication. Our scheme assumes the similar system architecture as G & S has illustrated in its protocol. In this system model, the three entities namely, user Ui with mobile device, a charging station CSj, and a utility service provider ESP, cooperate one another to enable the mutual authenticity between Ui and CSj. In this manner, the user may qualify for the stipulated recharging services. Our scheme comprises two phases; user registration andmutual authentication phase.

A. User registration phase:

A vehicle user needs to register itself from ESP for getting the recharging services. The registration steps are given below:

1. Initially, the user submits its identity ID_u towards ESP as a registration request by using a confidential channel.

2. Next, ESP records the user's entry into its database and constructs a new pseudo identity NID_i, a secret key q_i and also a set of shadow identities $SID = \{sid_1, sid_2, sid_3, ..., sid_n\}$, which may be used if the participants lose the synchronization among themselves. Thereafter, the ESP submits $\{NID_i, q_i, SID\}$ towards user by utilizing a confidential channel.

3. After receiving the message from ESP, the U_i inputs its biometric factor φ_i and password pwd_i. Then it computes $Gen(\varphi_i)\rightarrow(R_i, P_i)$ and stores P_i into the mobile gadget. Next, the gadget computes $\gamma_i=h(R_i)$ and $\omega_i=h(\gamma_i||pwd_i)$. After computing ω_i the U_i stores $\{\omega_i, P_i, NID_i, q_i^*, SID\}$ in its mobile gadget to enable mutual authentication between Ui and CSj/ESP.

B. Login and Authentication phase

To obtain the services of CSj, Ui must authenticate CSj, while CSj must authenticate Ui with the help of ESP. The steps in mutual authentication for Ui and CSj are given below:

1. Ui inputs its password pwd_i and biometric factor φ_i*.Then, it computes $Rep(\varphi_i^*, P_i) \rightarrow R_i$. Next, it computes $\gamma_i = h(R_i)$ and $\omega_i' = h(\gamma_i||\ pwd_i)$ and compares the equality for $\omega_i' ?= \omega_i$. If it is not true, the mobile gadget terminates the session. Otherwise, computes $q_i=q_i\oplus h(\varphi_i||pwd_i)$. Next, it generates a random number R_u and finds location region identifier LRI_u. Then, it computes masked identity as $MID_c=h(q_i||NID_i)\oplus ID_c$, $EL= LRI_u\oplus h(q_i||R_u)$ and $B_1=h(ID_c||NID_i||R_u||q_i||EL)$. Finally, it submits the message $M_1=\{ NID_i, MID_c, R_u, EL, B_1\}$ towards CSj.

2. Next, CSj generates a random integer R_c and computes $B_2=h(B_1||ID_c||R_c||K_{uc}||LRI_{CS})$, where LRI_{CS} represents the location region identifier for charging station and T_c is timestamp. Then, it submits $M_2 = \{M_1, R_c, T_c, LRI_{CS}, B_2\}$ towards ESP.

3. The ESP, upon receiving it, recovers the NID_i and q_i from its repository and computes $ID_c=h(q_i||NID_i)\oplus MID_c$. It then verifies parameters T_c, B_1 and B_2 and location region identities for LRI_u against LRI_{CS}. If it is verified, it further constructs and creates a new SK_c (Current session key) and a pseudo identity NID_i^{new}. Next, it computes $NID_i^{new*}=h(NID_i||q_i)\oplus NID_i^{new}$, $SK_u=h(ID_u||ID_c||SK_p||q_i||R_u)\oplus SK_c$, $SK_{cs}=h(ID_c||\ K_{uc}||R_c)\oplus SK$, $B_3=h(SK_{cs}||K_{uc}||R_c)$ and $B_4=h(ID_u||SK_p||SK_c||q_i||\ NID_i^{new*})$, where SK_p denotes past session key. Then, it submits $M_3=\{(NID_i^{new*}, SK_u, B_4)||(SK_{sp}, B_3)\}$ to *CSj*.

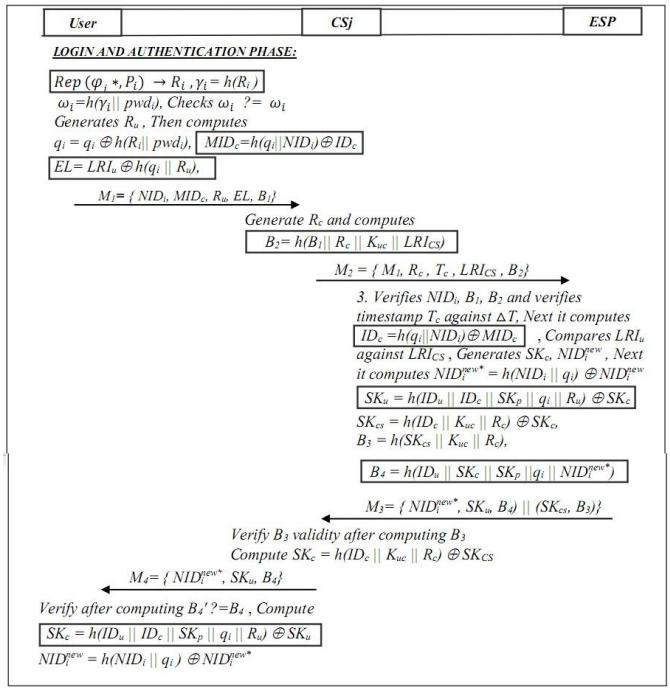

Fig. 2. Proposed model

4. The CSj verifies the validity of B_3 and computes session key as $SK=h(ID_c||K_{uc}||R_c)\oplus SK_{CS}$ and forwards $M_4=\{NID_i^{new*}, SK_u, B_4\}$ to user for final verification as shown in Fig. 2.

5. The user verifies the equation $B_4 ?= B_4$ after computing B_4. If true, it further computes $SK_c=h(ID_u||ID_c||SK_p||q_i||R_u)\oplus SK_u$ and $NID_i^{new}=h(NID_i||q_i)\oplus NID_i^{new*}$. The agreed session key is used by Ui and CSj to authenticate and get the required services.

C. Password revision

In proposed scheme, the password may be revised off and on by the subscriber for safety reasons, without consulting the administrator or server by adopting the following procedure:

1. Initially, Ui inputs its password pwd_i and biometric factor φ_i*. Then, it computes $Rep(\varphi_i*,P_i)\rightarrow R_i$. Further, it calculates $\gamma_i = h(R_i)$ and $\omega_i' = h(\gamma_i|| pwd_i)$ and compares the equality for $\omega_i' ?= \omega_i$. If it does not match, the session is terminated.

2. Otherwise, the mobile device computes $q_i = q_i \oplus h(\varphi_i|| pwd_i)$ and proceeds for inputting new password from subscriber as pwd_i^{new}. The mobile device computes $\omega_i'' = h(\gamma_i|| pwd_i^{new})$ and $q_i' = q_i \oplus h(\varphi_i||pwd_i^{new})$. Lastly, it replaces ω_i with ω_i'' and q_i with q_i' in the mobile device to finalize the password modification.

IV. SECURITY ANALYSIS

This section presents the informal security discussion, demonstrates formal security analysis and security verification using Proverif tool.

A. Informal security analysis

The informal security discussion of our scheme is as under:

i. ***Impersonation or forgery attack:*** The proposed scheme is immune to impersonation attack, since no Â may impersonate as either user, or CSj or ESP. The user and CSj entities, both share secrets q_i and K_{uc} with ESP. Until, these shared secrets are exposed to the Â, the latter could not launch any kind of impersonation attack. If Â attempts to replay or modify parameters to impersonate as a user, this attempt is unmasked at ESP's end while verifying parameters NID_i, B_1, B_2 and location identifiers i.e. LRI_u against LRI_{CS}. Similarly, if Â impersonates as ESP, this unauthorized attempt is unmasked upon the verification of $B_4 = h(ID_u || SK_c || SK_p ||q_i || NID_i^{new*})$.

ii. ***Session key verification:*** The user in proposed scheme verifies mutually established session key between user and CSj with the help of ESP. Earlier, in G & S, the user could not validate the authenticity of fake session key due to the malicious treatment of messages on the way to the user by Â. The verification of parameters by comparing $B_4' ?= B_4$ ensures the authenticity of recovered session key by the user, while $B_4$is computed by embedding various factors including current session key SK_c, where $B_4 = h(ID_u || SK_c || SK_p ||q_i || NID_i^{new*})$.

iii. ***Known-key secrecy and perfect forward secrecy:*** In proposed scheme, if the current session key is revealed to Â, the latter may not compute previous session keys as it does not have the shared long-term secret keys which are necessary to recover the past session keys from SK_u. Similarly, in our scheme if the long term user secret key q_i is revealed to Â, the latter might not be able to compute current session key SK_c, since it has no access to previous session key SK_p. Hence, our scheme adequately provides known-key and forward secrecy.

iv. ***Physical device exposure attack:*** In this scheme we assume that the devices are tamper proof and are capable of implementing Physical Uncloneable Functions (PUFs), which suggests that the devices could hamper any physical exposure to the Â for any leakage of parameters. Any malicious attempt on the device shall be rendered useless due to the embedded hardware design and employed PUFs implementation.

v. ***Key Compromise Impersonation attack:*** In G & S scheme, Â could access all previous session keys if the shared secret q_i is mistakenly exposed. However, in our scheme if q_i is exposed to Â by mistake, Â may not recover current session key SK_c, as it has no access to previous session key SK_p. The shared secret between CSj and ESP is assumed to be protected; however, the subscriber may lose its secret key by accident, as illustrated in the adversary model.

vi. ***Resist unjustified failures of login attempts:*** The failure of login attempts was the limitation in G & S due to the mismatch between stored and captured parameters. This happens when the biometric input is directly applied to compute any parameter in a function. The flaw could be remedied by employing the fuzzy extractor algorithms on captured biometric inputs. In our scheme, we employed fuzzy extractor algorithm on the captured biometric to bring the uniformity in the captured and stored biometric parameters so it may resist unjustified failures to login attempts.

vii. ***Resist DoS attack:*** The denial of service (DoS) attack is not possible in our scheme since the ESP verifies the factors $NIDi$, B_1, and B_2 before accessing the repository. If the $NIDi$, B_1 and B_2 are authenticated using the current time stamp, only then the database will be accessed. Hence, it may resist DoS attack.

B. Formal Security Analysis Using ROM

In this section, we demonstrate the sound security features proposed model by formal security analysis and proofs.

i. Definitions and assumptions

Bellare and Rogaway came forward with a formal security proof for two-party symmetric authentication protocol [15]. Since, the charging station CSj used to forward the message of subscriber, hence the real authentication is between the ESP and subscriber, and it is assumed that the communication between CSj and ESP is secure. In this scenario, CSj and ESP might be deemed as a single member for analyzing formally.

1. Complexity assumptions: Since, the proposed model's security depends largely on one-way hash digest function or alternatively a pseudorandom function [16], it is necessary to define few security terms for pseudorandom functions and the game scenario as utilized in the forthcoming security proof.

Definition 1: We assume r as a polynomial time function and $Adv_J = |Pr[J^r = 1] - Pr[J^{r'} = 1]|$ be the advantage of an algorithm J, if managed by some probabilistic polynomial time Â , while Â could distinguish r function from r' function. Here, r acts as a (g, q^r, ε)-secure pseudorandom function only if there exists no algorithm J distinguishing r from r' having $Adv_J \geq \varepsilon$, that may launch at most q^r oracle queries towards r or any truly random function r' and running at most g times this game.

Initialization: While interacting with Â, a challenger Ĉ chooses some randomly selected bit $b \in \{0, 1\}$ for gauging function r_b, where r_0 represents a pseudo-random function and r_1 represents a perfect random function.

Training phase: Â may issue q^r queries, $z_1, \ldots, z_{qr}$ towards Ĉ, where $z_i \in \{0, 1\}^*$ represent the random length-based binary strings. The Ĉ answers to those queries through submitting $r_b(z_i)$ toward Â such that $i \in (1 \leq i \leq q^r)$, where $r_b(z_i) \in \{0, 1\}^{\ell}$ and ℓ represents the length of the string with positive integer.

Guess: The Â produces $b^* \in \{0, 1\}$ output by guessing b, and wins the game on matching the equality for b* and b. The Â's advantage of winning game is as $Adv_{r0, A} = |Pr[b=b'] - 0.5|$.

2) Security Model and Symbols:

Protocol participants: The oracle $\prod^s_{X,Y}$ represents Â's role in X's interaction with Y for session *s*, and $\prod^t_{Y,X}$ as Â's role for Y's interaction with X for session *t*, where X, Y$\in$ D, s, t $\in$ N, D denotes players' identities, and N is set of positive integers.

Protocols: Our scheme used three entities for establishing the agreed session key between subscriber and service provider. However, this protocol could be condensed as de-factor two party protocol. Hence, we describe the authentication protocol for two interacting members in the following way:

Definition 2: We can formally define a two party authenticated key agreement P by an efficient and computable function $\prod$, using the under-mentioned inputs:

e: denotes the length of parameter as employed in the scheme.
X: denotes the identity of protocol initiator, where X $\in$ D.
Y: denotes identity of other participant in the protocol, where Y $\in$ D.
f: denotes the secret parameter, where f $\in \{0, 1\}^*$.
∂: represents up-to-date exchanged messages in the protocol.
τ: the randomly flipped coins for protocol initiator, while $\tau \in \{0, 1\}^+$.

The output of $\prod(e, X, Y, f, \partial, \tau) = (c, \sigma, \beta)$ can be defined as under:

c: It depicts message that is scheduled to be forwarded next, where $c \in \{0, 1\} \cup \{*\}$, here * indicates blank message sent by initiator.
σ: It shows the "accept" (Ã) or "reject" (Ɍ) decision, or even "no decision" (*) at all, i.e., $\sigma \in$ {Ã, Ɍ, *}.
β: It represents the private output, i.e. $\beta \in \{0, 1\}^* \cup \{*\}$, and {*} shows that the protocol initiator have no private output.

3) Adversary Model: The Â, being a probabilistic polynomial-time Turing machine for the protocol run, might eavesdrop, modify the messages, and fully control the public channel. This activity could be represented by the understated queries:

Execute ($\prod^s_{X,Y}$,$\prod^t_{Y,X}$): The execute query simulates all sort of passive attacks, while a passive attacker may intercept the communication among $\prod^s_{X,Y}$ and $\prod^t_{Y,X}$ for a protocol session.

Send ($\prod^s_{X,Y}$, m): The send query simulates active attacks, in which an attacker could submit the message *m* towards and get the response in accordance with the contributed protocol.

Reveal ($\prod^s_{X,Y}$): The reveal key simulates the revelation of past session key/s regarding any session.

Corrupt ($\prod^s_{X,Y}$): The simulation of corrupt key reveals long term high entropy secrets, while this query simulates the attacks passively.

Test ($\prod^s_{X,Y}$): Upon acceptance and construction of agreed session key by $\prod^s_{X,Y}$, Â may initiate the Test query and could attempt distinguishing a legal session key from any randomly selected string.

4) Security Definitions: Now we define some definitions for a matching conversation below:

Definition 3:We define a protocol session for entity X as (X, Y, s, role) where Y being identity for X's co-partner, s being identifier of session, and role is either initiator or responder. The protocol having two sessions between X and Y is of form (X, Y, s, initiator) and (X, Y, t, responder), respectively, and are called matching conversation sessions engaging X and Y only if session identifiers are same, while the initiator and response entities being X and Y. If P contains more than two sessions while every session pair be a matching conversation, then P is termed as protocol with matching conversations.

The mutual authentication can be defined on the basis of matching conversation as follows: A protocol P complies with mutual authentication if for Â: 1) the matching conversation will be deemed as acceptance and 2) acceptance will be regarded as matching conversation. The first condition suggests that if in P's session of two parties there is matching conversation, both intended parties are said to accept each other. According to second condition, if each entity accepts authenticated session with another entity, then the chances of matching conversation would be negligible. Theoretically, we define mutual authentication (M_uA) as given below:

Definition 4: A protocol satisfies M_uA-secure feature only if:

1. There is matching conversation for $\prod^s_{X,Y}$ and $\prod^t_{Y,X}$, that is, the latter oracles are said to accept each other.
2. The NoMatching^A(k) event occurs and there exist i, j, X, and Y such that $\prod^i_{X,Y}$ is accepted, however there is no other matching conversation-based $\prod^j_{Y,X}$, where the chances of occurring NoMatching^A(k) event is negligible, here k is security parameter. This event may be referred as $Sucs_P^{M_u A}$(Â). This indicates the probability of success about Â's launching impersonation attack towards any one of the two entities in P.

Authentication Key Agreement (AKA) Security: To execute M_uA-secure compliant protocol P, the attacker may interact with two fresh oracles such as $\prod^s_{X,Y}$ and $\prod^t_{Y,X}$. After execution, Â issues Test query to any one of those two oracles. Consequently, either the valid session key or some random string will be sent to Â corresponding to random bit *b*. In the end, Â shall output a bit b^* and ends the game. Now, the AKA-advantage Adv_P^{AKA}(Â) can be described as $|Pr[b^*=b] - 0.5|$. We can lay down the AKA-security theoretically as:

Definition 5: The protocol is deemed to AKA-secure only if it complies with the understated conditions:
1. Â may engage in the authentication protocol's execution with oracles, i.e., $\prod_{X,Y}^{s}$ and $\prod_{Y,X}^{t}$. Both of these oracles may accept and establish an agreed session key between them.
2. The protocol complies with M_uA-secure property
3. The advantage $Adv_{P}^{AKA}(\hat{A})$ is quite negligible for any of the probabilistic polynomial time Â.

ii. Formal Analysis of the proposed protocol

In the formal analysis, it is demonstrated that the contributed scheme as based on hash function-oriented pseudorandom functions, is provably secure of attacks.

Lemma 1: If we assume a function h as a secure pseudorandom function (m_0, u_0, ϑ_0) having negligible ϑ_0, the proposed protocol stands M_uA-secure.

Proof. For proving the lemma 1, it is assumed there is a polynomial time attacker who is capable of breaking M_uA-security of the contributed scheme P with high probability $Sucs_{P}^{M_uA}(\hat{A})$. For this, a polynomial-time algorithm $\mathcal{N}$ is constructed with considerable advantage, and this proves the contradiction. Besides, $Sucs_{P}^{M_uA}(\hat{A}) = \Pr[Sucs_{Ui}] + \Pr[Sucs_{S}] - \Pr[Sucs_{Ui}, Sucs_{S}] \leq \Pr[Sucs_{Ui}] + \Pr[Sucs_{S}]$, where the events $Sucs_{Ui}$ and $Sucs_{S}$ represent the success probabilities of legitimate User and Server's impersonation attempts by the Â. Hence, the proof can be divided in two cases, one for server's impersonation and other as Ui's impersonation.

Case 1 (Server S's impersonation): We suppose that Â may impersonate as S with probability ¢. If the Â wants to get authenticated from Ui successfully by employing $\prod_{Ui,S}^{s}$ controlled by the algorithm $\mathcal{N}$, Â must accurately submit $B_4 = h(ID_u \,||\, SK_c \,||\, SK_p \,||q_i \,||\, NID_i^{new*})$. In the game ahead, $\mathcal{N}$ will take advantage of capable Â for breaking the assumption of pseudorandom function with probability ¢≤$4\vartheta_0+2^{-v}$, where v is a security factor. $\mathcal{N}$ plays game with C̃ as given below:

Initialization: We assume the long term secret key as q_i which is $\mathcal{L}$ bit in length. The C̃ chooses any random bit ъ'ϵ{0, 1}and constructs a secure hash function $h_{b'}$ where $h_0=h_{qi}$ be a pseudo-random function and h_1 a random function. If $\mathcal{N}$ models the game by using h_1 for interaction with Â, we term the game experiment as random experiment. Alternatively, in case the $\mathcal{N}$ utilizes h_0 for modeling the game, it will be termed as a real experiment. The objective lies with guessing the equality for $h_{b'} = h_0$ *or* $h_{b'} = h_1$ i.e guessing the value for ъ' as 0 or 1.

Training: The $\mathcal{N}$ models $\prod_{Ui,S}^{s}$ and $\prod_{Ui,S}^{s}$ for interaction with Â and in return responds to the under-mentioned queries:

- Execute ($\prod_{Ui,S}^{s}$,$\prod_{Ui,GN}^{t}$): $\mathcal{N}$ employs as $h_{b'}$ as provided by C̃ for h_{qi} in protocol P. $\mathcal{N}$ again constructs q_h randomly and $NID_i^{new*}$and calculates $NID_i^{new*}=h(NID_i||q_i)\oplus NID_i^{new}$, $SK_u=h(ID_u||ID_c||SK_p||q_i||R_u)\oplus SK_c$, and $B_4 = h(ID_u \,||\, SK_c \,||\, SK_p \,||q_i \,||\, NID_i^{new*})$. Thereafter, $\mathcal{N}$ models $\prod_{S,Ui}^{s}$ and $\prod_{S,Ui}^{t}$ using $h_{b'}$, NID_i^{new*}, SK_u and B_4.
- Send ($\prod_{Ui,S}^{s}$,m): The oracle $\prod_{Ui,S}^{s}$ submits request $m=\{NID_i, R_u, B_1\}$ to $\prod_{S,Ui}^{t}$ in P. The latter verifies B_1 after querying $h_{b'}$ and checks NID_i in repository and validates B_1 after querying $h_{b'}$.
- Send ($\prod_{S,Ui}^{t}$,m): After getting m=$\{NID_i, R_u, B_1\}$,$\prod_{S,Ui}^{t}$ computes $NID_i^{new*}=h(NID_i||q_i)\oplus NID_i^{new}$, $k_i^{GN}=h(ID_u||ID_c||SK_p||q_i||R_u)\oplus SK_c$ and $B_4=h(SK_u||q_i||NID_i^{new*})$. Then it submits $m=\{NID_i^{new*}, SK_u, B_4\}$ to Â.

Challenge: Â sends the Send ($\prod_{Ui,S}^{s}$, m) to initiate P. Then, the oracle $\prod_{Ui,S}^{s}$ submits $m=\{NID_i, R_u, B_1\}$ to Â. Then, Â computes B_4 with probability Pr [$Sucs_S$] = ¢. Next, Â queries Send ($\prod_{S,Ui}^{t}$, $\{NID_i^{new*}, SK_u, B_4\}$). Upon receiving the query, $\mathcal{N}$ issues the query $z^*=h(SK_u||q_i)$ to $h_{b'}$ and receives $B_4^*=h(SK_u||q_i||NID_i^{new*})$.

Guess: Ultimately, the $\mathcal{N}$ outputs and makes a guess of the bit ъ"ϵ{0, 1}. If the equality $B_4^* = B_4$ holds, $\mathcal{N}$ returns output 0, on the other hand, $\mathcal{N}$ produces any random bit from the set {0, 1}.

The probability analysis regarding $\mathcal{N}$ for successfully distinguishing between $h_{b'}$ may be divided into two parts: one with random experiment (i.e. ъ"=1) and the other with real experiment as (i.e. ъ"=0). For the real experiment case, the Â may submit the accurate information for winning the game with chances ¢, and the $\mathcal{N}$ may output as ъ"=0 having ¢ probability. Otherwise, if Â submits the faulty information, the $\mathcal{N}$ may randomly guess bit ъ", and $\mathcal{N}$ will produce (ъ" = 0) with probability $(1-¢)/2$. For random experiment, Â may submit accurate information by guessing at random, and its probability of guessing is 2^{-e}. Therefore, if b'=1, the $\mathcal{N}$ produces ъ"=1 with probability $(1-2^{-e})/2$. By summing up both probabilities (i.e. b"=1 and b"=0), we get to the result $\{1/2 + ¢/4 - 2^{-(e+2)}\}$. Hence, according to this accumulation result it is proved the probability ¢ cannot exceed $4\vartheta_0 + 2^{-e}$.

Case 2 (Ui's impersonation): Assume that Â may impersonate as a user with chance ¢'. If Â wants to get accepted by$\prod_{S,Ui}^{t}$, then Â needs to submit accurate data. Hence, $\mathcal{N}$ induces a similar game with C̃ as it employs above.

Initialization: To initialize, the challenger chooses a hash digest function h_b, b having the value set {0, 1} to respond the queries from $\mathcal{N}$, where $h_0=h_{qi}$ be a pseudorandom function while h_1 be the random function.

Training: $\mathcal{N}$ initially chooses R_u and NID_i in P, and models $\prod_{Ui,S}^{s}$ and $\prod_{S,Ui}^{t}$ by responding to Execute ($\prod_{Ui,S}^{s}$,$\prod_{S,Ui}^{t}$) and Send($\prod_{Ui,S}^{s}$,m) queries.

Guess: $\mathcal{N}$ produces an output by guessing $b'$with set of values {0, 1} corresponding to NID_i and B_1. If these parameters are validated, the $\mathcal{N}$ produces the output 0, specifying $h_b=h_{qi}$; or else it produces a random bit from the set {0, 1}.

The probability of Â's submitting the accurate parameters NID_i and B_1 is ¢' for the real experiment, while for the random experiment it is 2^{-e}. After combining probabilities for both experiments, we get $\{1/2 + ¢'/4 - 2^{-(e+2)}\}$. Hence, according to this accumulation the probability ¢' is at most $4\vartheta_0 + 2^{-e}$. After summing up the two cases (¢' + ¢), we have

$$Sucs_{P}^{M_uA}(A) \leq \Pr[Sucs_{Ui}] + \Pr[Sucs_{S}] \quad (1)$$
$$\leq 8\vartheta_0 + 2^{-(e-1)} \quad (2)$$

The above equation suggests non-negligibility ofϑ_0, contracting the above lemma about ϑ_0's negligibility. Therefore, the proposed protocol is M_uA-secure.

Lemma 2: If we assume a function h as a secure pseudorandom function (m_0, u_0, ϑ_0) having negligible ϑ_0, the proposed protocol stands AKA-secure.

Proof. We assume an Â that is capable of breaking AKA-security of P with considerable advantage $Adv_{P}^{AKA}(\hat{A})=\vartheta$. Then, a simulator $\mathcal{N}$ is constructed for breaking the assumption of pseudorandom function [17]. The $\mathcal{N}$, according to definition 3, plays the game with C̃ as given below:

```
Completing equations...
Completing equations...
-- Query not attacker(sk[])
Completing...
Starting query not attacker(sk[])
RESULT not attacker(sk[]) is true.
-- Query inj-event(endESP(idu)) ==> inj-event(beginESP(idu))
Completing...
Starting inj-event(endESP(idu)) ==> inj-event(beginESP(idu))
RESULT inj-event(endESP(idu)) ==> inj-event(beginESP(idu)) is true.
-- Query inj-event (endUi(idu_2315)) ==> inj-event(beginUi (idu_2315))
Completing...
Starting query inj-event(endUi(idu_2315)) ==> inj-event(beginUi (idu_2315))
RESULT inj-event(endUi(idu_2315)) ==> inj-event(beginUi (idu_2315)) is true.
```

Fig. 3. Simulation results

Initialization: To initialize, $\hat{C}$ chooses a random bit from the given set {0, 1} and constructs a secure hash-digest function to respond to the queries from $\mathcal{N}$, where $h_0=h_{qi}$ be the pseudorandom function, while h_1 is a random function.

Training: The $\mathcal{N}$ chooses the nonce R_g and NID_i in the protocol, and models $\prod^{s}_{\mathrm{Ui,S}}$ and $\prod^{t}_{\mathrm{S,Ui}}$ by responding the queries, Execute($\prod^{s}_{\mathrm{GN,S}}$,$\prod^{t}_{\mathrm{S,GN}}$) and Send($\prod^{s}_{\mathrm{Ui,S}}$,m), respectively.

- Test ($\prod^{s}_{\mathrm{Ui,S}}$): Using this query, if q_h is constructed, $\mathcal{N}$ selects at random $v \in \{0, 1\}$, then it responds by returning legal session key q_h in case v = 0, or any random string if v =1. Or else, $\mathcal{N}$ returns φ, indicating null string or emptiness.
- Test($\prod^{t}_{\mathrm{R,T}}$): Its modeling is also similar to above query.

Challenge: The Â submits the *Test* query toward $\mathcal{N}$ after having queried the oracle Execute ($\prod^{s}_{\mathrm{GN,S}}$,$\prod^{t}_{\mathrm{S,GN}}$).

Guess: Upon having queried $Test$ ($\prod^{s}_{\mathrm{Ui,S}}$) or $Test$ ($\prod^{t}_{\mathrm{S,Ui}}$), the Â outputs a bit b as 0, if it takes the responded message as valid session key, or else it outputs b as 1. Finally, $\mathcal{N}$ produces the b' as 0 if $b'=b$, or else it will return the output as b'=1.

The probability analysis for $b'=b$ is alike the analysis performed in *Lemma* 1. The Â could win this game if it guesses the equality for $b'=b$ having the real experiment-based probability as $(\vartheta + 1/2)$, i.e. b=0. The Â can only guess under random experiment whether $b'=b$ having probability of 0.5, i.e. b=1. In case, it effectively makes a guess for $b'=b$, the $\mathcal{N}$ produces the output b'=1. Hence, the probability for $\{b'=b$ and $b=0\}$ is calculated as $(\vartheta(1/2) + 1/4)$, while for $\{b'=b$ and $b=1\}$ it is ¼. After accumulating both probabilities for real and random experiments, we get $(\vartheta + 1)/2$. While, the probability for ϑ_0 amounts to at least $\vartheta/2$, which is non-negligible and bears a contradiction. Therefore, the advantage Adv_{P}^{AKA}(Â)is quite negligible for any polynomial time attacker, and in this context our protocol beholds AKA-Secure.

C. Security Verification Using Proverif

The Proverif automated tool [18] is employed to verify the demonstrated protocol's security features including mutual authentication and session key confidentiality. In this section, we develop the corresponding modules to verify the security properties of proposed scheme using Proverif automation tool. The Proverif employs widely accepted laws of π calculus which facilitate many significant cryptographic operations including digital signatures, symmetric or asymmetric encryption/decryption, and hash-digest related operations.

To perform the simulation, we modeled two events for executing the code for Ui and ESP as these are the entities mutually authenticating each other, while CSj performs the forwarding function in general. The event beginUi (bitstring) and event endUi (bitstring) are used by Ui to authenticate ESP.

Table II: Functionality Comparison

	[6]	[7]	[5]	[10]	[8]	[12]	[11]	Ours
F1	×	×	✓	✓	×	✓	✓	✓
F2	×	×	✓	×	✓	✓	✓	✓
F3	×	×	×	✓	✓	✓	✓	✓
F4	✓	✓	✓	✓	✓	×	✓	✓
F5	×	×	×	✓	×	✓	✓	✓
F6	×	×	✓	×	×	✓	✓	✓
F7	×	×	✓	✓	×	×	✓	✓
F8	×	×	×	×	×	✓	×	✓
F9	×	×	×	×	×	✓	×	✓

F1: Anonymity, **F2**: Mutual Authentication, **F3**: Resist Man in the middle Attack, **F4**: Resist unjustified failures of login attempts, **F5**: Supports forward secrecy, **F6**: Resist impersonation attack, **F7**: Supports Session key security, **F8**: Resist Denial of service attack, **F9**: Biometric security (3-factor authentication)

Similarly, the event beginESP (bitstring) and event endESP(bitstring) are employed by ESP to authenticate Ui. We compute the results of queries and the order of the two pair of events remained stable. The results in Fig. 3 depict that our scheme achieves mutual authentication and session key secrecy since the session key is robust against attackers.

VI. PERFORMANCE ANALYSIS

In this section, we examine the performance of proposed scheme with other contemporary authentication schemes for smart grids. Table I depicts the comparative analysis of features and performance efficiency between our scheme and other protocols, which manifests that the schemes [5-8, 10-12] are unable to ensure the requisite security properties of an authentication protocol in general. We focused a few crucial security properties such as session key security, man-in-the-middle attack, DoS and forgery attack, etc. while designing the proposed V2G authentication scheme [21-24]. The scheme [12] affords many security properties; nonetheless, it does not ensure resistance to DoS attacks. Comparatively, our scheme warrants this significant security feature as depicted in Table II. In our scheme, the early decision on the part of ESP against a fake authentication request ensures immunity from DoS attack.

Next, we compute the computational cost of cryptographic operations for proposed and other schemes [5-8, 10-12] as given in Table III using JPBC [19, 20] and JCE library [21]. These operations are implemented on a mobile device (Smartphone Lenovo Zuk Z1 with Quad-core 2.5 Ghz processor having 4GB RAM and Android Operating System V5.1.2), and a personal computer (Virtual machine with HP E8300 Core i5 and 2.93 Ghz processor with 4GB RAM using Ubuntu 16.11 OS). The Table III depicts the communication and computational costs for proposed and compared schemes. It is evident that the performance of our protocol is better in terms of computational and communication delay. There are specifically some standards for smart grid V2G such as OCPP and IEC 15118 protocol, and upon considering these standards we find that the schemes [5-7] adopt costly ECDSA cryptography-based signatures and suffer security weaknesses that render those schemes difficult to fit in V2G applications. Such schemes also involve in exposing useful information such as subscriber's name, identification number of vehicle, location of charging, and other related information affecting the privacy of customer. In this scenario, our proposed scheme finds an effective blend with smart gird standard protocols such as OCPP and IEC 15118 for being lightweight, efficient

Table III. Computational cost

	User (ms)	*Server (ms)*
T_{BP}	*13.662*	*7.318*
T_{ECM}	*10.235*	*5.387*
T_{Exp}	*8.341*	*3.362*
T_M	*5.012*	*2.002*
T_H	*0.019*	*0.012*
T_{SYM}	*0.063*	*0.048*
T_{Bio_Rep}	*0.015*	-
T_{CertG}	*69.326*	-
T_{CertV}	-	*21.257*

Table IV. Operations cost of communication

Primitive operations	***Comm. cost (bits)***
Bilinear Pairing	*320 bits*
Elliptic Curve Point	*320 bits*
User/CSj identity	*60 bits*
Hash function	*160 bits*
Random number	*160 bits*
Time Stamp	*32 bits*
Digital signature	*1024 bits*
Symmetric encryption	*256 bits*

Table V. Comparison of Computational and communication cost

SCHEMES	User's device	ESP/CS	Comm. Cost (bits)
[6]	$3T_{ECM}+T_m+T_{CertG}+T_{sym}+T_h \approx 105.125$	$4T_{ECM}+T_m+T_{CertV}+T_{sym}+4T_h \approx 44.903$	*2590*
[7]	$2T_{ECM}+T_m+T_{CertG}+T_{sym}+T_h \approx 94.89$	$3T_{ECM}+T_m+T_{CertV}+T_{sym}+3T_h$ *39.496*	*4836*
[5]	$2T_{ECM}+T_m+T_{CertG}+3T_h \approx 94.868$	$3T_{ECM}+T_m+T_{CertV}+4T_h \approx 39.468$	*2784*
[10]	$4T_{ECM}+T_{exp}+5T_h \approx 49.376$	$3T_{ECM}+T_{exp}+5T_h+2T_b \approx 34.219$	*8190*
[8]	$T_{sym}+4T_h \approx 0.139$	$T_{sym}+4T_h \approx 0.096$	*3922*
[12]	$6T_h \approx 0.114$	$8T_h \approx 0.096$	*2144*
[11]	$3T_{ECM}+T_{exp}+6T_h \approx 39.16$	$2T_{ECM}+T_{exp}+6T_h+2T_b \approx 28.844$	*3466*
[Ours]	$7T_h+T_{Bio\_Rep} \approx 0.148$	$9T_h \approx 0.108$	*2176*

and secure protocol.

To accommodate the current infrastructure of limited stations for vehicle battery charging, the scalability in the protocol has been considered. In UK, the fuel stations with the largest network are Tesco with 1562 gas stations (operated under supermarket chain), BP with 1228 gas stations, and lastly the Shell and Esso gas stations, both with more than 1000 number of stations. For EVs the prevailing capacity of battery could be categorized as low charging flow rates with 3KW to 6KW and high charging flow rates up to 150KW. We employed GM Spark, Tesla S 85, and Ford focus EV models with battery capacities of 21KWh, 90KWh and 23KWh, respectively. If we consider any instant charging station having the energy flow rate with 50KWh, then the drained tank to full charging for such vehicles may take 25 *min*, 1.8 *hours*, and 28 *min*, respectively. Similarly, the high flow rate-based charger (150KW) takes 36 minutes to charge Tesla S 85 battery. If we assume that the average number of charging points in a charging station is 15, then 15 cars may get charged simultaneously in a CS. This may generate 15 authentication requests every hour from a charging station towards server. Referring to Table V, the communicational cost of our scheme is 2144 bits (268 bytes) excluding TCP/IP and Ethernet overhead. Upon adding this overhead of 64 bytes for each message, the total cost of authentication request including 4 messages, becomes 508 bytes. If verification time of authentication request at ESP is 0.0009s then for 1562 stations of Tesco, the total computation delay on CPU per hour for verifying those requests is calculated as 22 *sec* (1562×15× 0.0009). The bandwidth needed for communicating those requests is computed as (508×1562×15) ≈(26.5Kbps). We used symbols i.e. T_{ECM} for ECC-based point multiplication, T_m for modular multiplication, T_{CertG} for certificate generation, T_h for hash digest, T_{exp} for exponential operation and T_{sym} for symmetric encryption, to calculate communication delay as shown in Table IV. Our scheme takes quite less communication cost of 2176 bits as compared to other related schemes which take from 2590 to 8190 bits to communicate for authentication. Although, communication cost for [12] is less than our scheme as 2144, it is prone to many security problems. These research findings warrant to a large extent that our protocol complies with the claimed security features having low computational and communicational costs which render it quite suitable for EI-based V2G authentication models.

VI. CONCLUSION

To effectively initiate the power transfer among entities in an energy internet-based vehicle-to-grid system, a secure data exchange is very indispensable. For this secure data exchange and communication, the underlying authentication protocol must not only be free from cyber attacks but also ensuring privacy. In this paper, we highlight a few drawbacks of contemporary smart grid-based authentication schemes, and reviewed EI-based V2G scheme by G & S, in particular. G & S demonstrated an efficient EI-based V2G authentication scheme, however, it bears many security loopholes including replay attack, man-in-the-middle attack, and impersonation attack. The scheme is unable to confer session key security to the subscriber and also suffers unjustified failures during login attempts. Considering the said limitations, we propose a novel and efficient V2G protocol framework enabling the vehicles to communicate or recharge at desired recharging stations. Besides, the results of the proposed framework are evaluated and compared against several contemporary schemes and the security properties are validated under rigorous formal analysis employing random oracle model.

REFERENCES

[1] Z. Y. Dong, "Towards an intelligent future energy grid," The University of Sydney, New South Wales, 2016.

[2] V. C. Gungor et al.,"A Survey on Smart Grid Potential Applications and Communication Requirements," IEEE Tran. on Ind. Inf., vol. 9(1), pp. 28-42, 2013.

[3] S. Lee et al., "Study on Analysis of Security Vulnerabilities and Countermeasures in ISO/IEC 15118 Based Electric Vehicle Charging Technology," (ICITCS), doi: 10.1109/ICITCS.2014.7021815, 2014.

[4] C. Alcaraz, J. Lopez and S. Wolthusen, "OCPP Protocol: Security Threats and Challenges," IEEE Trans. Smart Grid, vol. 8, no. 5, pp. 2452–2459, 2017.

[5]Mohd. Ali et al."A Novel ID-Based Key Establishment Method for AMI in Smart Grid," IEEE Trans. on Smart Grid, pp. 1-10, 2016.

[6] H. Nicanfar and V. C. M. Leung, "Multilayer Consensus ECC-Based Password Authenticated Key-Exchange (MCEPAK) Protocol for Smart Grid System," IEEE Transactions on Smart Grid, vol. 4, no. 1, pp. 253-264, 2013.

[7] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," IEEE Trans. Smart Grid, vol. 2 no. 2 pp. 371-378 Jun. 2011.

[8] J. Xia and Y. Wang, "Secure key distribution for the smart grid," IEEE Trans. Smart Grid, vol. 3 no. 3 pp. 1437-1443 Aug. 2012.

[9] J. H. Park, M. Kim, and D. Kwon, "Security weakness in the smart grid key distribution proposed by Xia and Wang" IEEE Trans. Smart Grid, vol. 3 pp. 1613-1614 Sep. 2013.

[10] J.-L. Tsai and N.-W. Lo, "Secure Anonymous Key Distribution Scheme for Smart Grid," IEEE Trans. on Smart Grid, vol. 7, no. 2, pp. 906–914, 2016.

[11] V. Odelu et al., "Provably Secure Authenticated Key Agreement Scheme for Smart Grid," IEEE Trans. on Smart Grid, 2016, DOI: 10.1109/TSG.2016.2602282.
[12] Gope, P., & Sikdar, B. "An Efficient Privacy-preserving Authentication Scheme for Energy Internet-based Vehicle-to-Grid Communication". IEEE Transactions on Smart Grid, pp. 6607 – 6618, Vol. 10 (6), 2019
[13] A. Jindal, N. Kumar and M. Singh, "Internet of energy-based demand response management scheme for smart homes andPHEVs using SVM," Future Generation Computing Systems, doi.org/10.1016/j.future.2018.04.003, 2018.
[14] Dodis Y, Kanukurthi B, Katz J, Reyzin L, Smith A. Robust Fuzzy Extractors and Authenticated Key Agreement From Close Secrets. IEEE Transactions on Information Theory. 2012; 58(9): 6207–6222.
[15] M. Bellare and P. Rogaway, "Entity Authentication and Key Distribution," Advances in Cryptology - Crypto 1993, D. Stinson, ed. pp. 110-125
[16] B. Schneier, Applied Cryptography (2nd edn), pp. 197-211, John Wiley & Sons, New York, 1996.
[17] H. Liu, H. Ning, Y. Zhang and L-T. Yang, "Aggregated-Proofs Based Privacy-Preserving Authentication for V2G Networks in the Smart Grid," IEEE Trans. Smart Grid, vol. 66, no. 3, pp. 1722–1733, 2012.
[18] Blanchet B. ProVerif Automatic Cryptographic Protocol Verifier User Manual. Paris, France: CNRS; 2005.
[19] .Pbc library. Tech. rep. http://crypto.standford.edu/pbc/(Accessed 5-08-2019)
[20] Z. Yang, S. Yu, and C. Liu, "P2 : Privacy-preserving communication and precise reward architecture for V2G networks in smart grid," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 697–706, Dec. 2011.
[21] H. Guo, Y. Wu, and M. Ma, "UBAPV2G: A unique batch authentication protocol for vehicle-to-grid communications," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 707–714, Nov. 2011.
[22] A. Abdallah and X. Shen, "Lightweight Authentication and Privacy Preserving Scheme for V2G Connections," IEEE Transactions on Vehicular Technology vol. 3, no. 4, pp. 2615–2629, 2017.
[23] D. He, S. Chan and M. Guizani, "A Privacy-friendly and efficient secure communication framework for V2G networks" IET Comm. vol. 12(3), pp. 304–309, 2018.
[24] Mahmood, K., Chaudhry, S. A., Naqvi, H., Shon, T., & Ahmad, H. F. (2016). "A lightweight message authentication scheme for Smart Grid communications in power sector". Comp. & Elec. Eng., 52, 114-124

Azeem Irshad received master's degree from Arid Agriculture University, Rawalpindi, Pakistan. Then he completed his PhD from International Islamic University, Islamabad, Pakistan. He has authored more than 60 international journal and conference publications, including 30 SCI-E journal publications. His research work has been cited over 575 times with 12h-index and 13 i-10-index. He received Top Peer-Reviewer Award from Publons in 2018 with 104 verified reviews. He has served as a reviewer for more than 38 reputed journals including IEEE Systems Journal, IEEE Communications Magazine, IEEE Transactions on Industrial Informatics, IEEE Consumer Electronics Magazine, Computer Networks, Information Sciences, CAEE, Cluster Computing, AIHC, Journal of Supercomputing and Wireless Personal Communications, notably. His research interests include strengthening of authenticated key agreements in SIP multimedia, Cloud-IoT, WBAN, TMIS, WSN, Ad hoc Networks, e-health clouds and multi-server architectures

Muhammad Usman received the MS (Computer Science) from the PMAS-AAUR, Pakistan with first class and obtained Ph.D. from School of Information and Communication Technology, Griffith University, Australia. He severed as a Postdoc Research Fellow in Cyber Security and Machine Learning at University of Surrey, UK. He possesses over 16 years of academic and industrial experience in different parts of the world. His current research interests include design and analysis of security and privacy methods for Cyber-Physical Systems, IOT-enabled Systems, Trust & Privacy, Formal and Statistical Modelling, Web Services, and Health Data analytics. He has been recipient of several research and travel grants. He has led, and acted as an associate guest editor, in special issues in IEEE transactions. He has served in different capacities such as organising committee member, TCP member, focal person and/ or publication chair of several international IEEE conferences. His research paper has received the best paper award in IEEE ComTech 2017.

Shehzad Ashraf Chaudhry received the master's and Ph.D. degrees (with Distinction) from International Islamic University, Islamabad, Pakistan, in 2009 and 2016, respectively. Currently working as an Associate Professor with the Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey, he has authored over 75 scientific publications appeared in different international journals and proceedings, including 60 in SCI/E journals. With an H-index of 20 and an I-10 index of 37, his work has been cited over 1375 times. His current research interests include lightweight cryptography, elliptic/hyper elliptic curve cryptography, multimedia security, E-payment systems, MANETs, SIP authentication, smart grid security, IoT Architecture, and next generation networks. He occasionally writes on issues of higher education in Pakistan.
Dr. Chaudhry was a recipient of the Gold Medal for achieving 4.0/4.0CGPA in his Masters. Considering his research, Pakistan Council for Science and Technology granted him the Prestigious Research Productivity Award, while affirming him among Top Productive Computer Scientists in Pakistan. He has served as a TPC member of various international conferences and is an Active Reviewer of many ISI indexed journals.

Syed Husnain Abbas Naqvi received his Ph.D. from The University of Auckland, New Zealand. Currently he is working as Professor at the Department of Computer Science, Muslim Youth University, Islamabad. He authored more than 60 scientific publications appeared indifferent international journals and proceedings. He has vast experience of working in academia and industry throughout the globe. His broad research interests include Sensor Networks, Collaborative Communications, Lightweight Cryptography, Beam forming and Space Time Block Codes.

Muhammad Shafiq received Ph.D. degree in Information and Communication Engineering from the Yeungnam University, South Korea in 2018. He received an M.S. degree in Computer Science from the University Institute of Information Technology, Arid Agriculture University, Rawalpindi, Pakistan. He also received a Master's degree in Information Technology from the University of the Punjab, Gujranwala, Pakistan. Currently, he is a Postdoctoral Fellow at Yeungnam University, South Korea, and also working as Assistant Professor with the Faculty of Computer Science at GC Women University, Sialkot, Pakistan. From 2010-2018, he worked as Lecturer with the Department of Information Technology, University of Gujrat, and formerly held the same position with the Department of Computer Science, Federal Urdu University, Islamabad, Pakistan. His research interests include the design of spectrum management, routing, and medium access control protocols for mobile ad how networks, IoT, and cognitive radio networks.