Energy Reports 8 (2022) 9331–9343

Contents lists available at ScienceDirect

Energy Reports

journal homepage: www.elsevier.com/locate/egyr

Research paper

ABRIS: Anonymous blockchain based revocable and integrity preservation scheme for vehicle to grid network

Arun Sekar Rajasekaran [a,*], Azees Maria [b], Fadi Al-Turjman [c,d], Chadi Altrjman [e], Leonardo Mostarda [f]

[a] Department of ECE, KPR Institute of Engineering and Technology, Coimbatore, Tamil nadu, India
[b] School of Computer Science and Engineering, VIT- AP University, Andhra Pradesh 522 237, India
[c] Artificial Intelligence Engineering Department, Near East University, Mersin 10, Turkey
[d] Research Center for AI and IoT, Faculty of Engineering, University of Kyrenia, Kyrenia, Mersin 10, Turkey
[e] University of Waterloo, Waterloo, Ontario, Canada
[f] Computer Science Division, Camerino University, Italy

ARTICLE INFO

Article history:
Received 11 March 2022
Received in revised form 7 June 2022
Accepted 15 July 2022
Available online 29 July 2022

Keywords:
Authentication
Blockchain
Integrity
Revocation

ABSTRACT

The upcoming development in vehicle to grid network (V2G) allows for the flow of energy from battery powered Electric Vehicle (*EV*) to grid as well as the exchange of information between them. However, during the information exchange, the *EV*'s confidential information should be transferred from one charging station to another in a secure manner. Furthermore, the anonymity of the *EV* and charging station should be preserved. Despite the fact that many works on anonymous authentication and privacy preservation exist, there is an increase in computational cost in existing surveys. In this work, the new charging station authenticates the *EV* using blockchain technology without the involvement of a trusted entity, resulting in a reduction in computational time. Moreover, an efficient revoking mechanism is suggested to block the misbehaving charging station from the V2G network. In addition, security analysis section proves the resistant of our work against several possible well known attacks. Finally, to evaluate the performance of the work, the simulation is performed using CYGWIN platform and the results are proved to be noteworthy.

© 2022 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

1. Introduction

In the upcoming years, to reduce the greenhouse gas emissions, fuel vehicles will be slowly minimized and replaced by alternate energy vehicles which run on electricity are known as electric vehicles (*EVs*). They are also called as zero emission vehicles, as there is outcome of air pollution. The *EV* play a key role and become a significant part of the automobile business. The Electric vehicles (*EVs*) are becoming popular because of their inexpensive valuing, less price in the extended term, and accessibility of charging stations (*CSs*).

Vehicle-to-grid (V2G) technology opens up new possibilities for smart energy management and trading (Rajasekaran et al., 2022a). It releases the energy stored in *EV* batteries and can help the grid when demand is high. In general, *EV* charging is a one-way "Grid-to-Vehicle" energy flow, which means that once the power is transferred to the *EV*, it is only used for driving. However, the recent trend of bi-directional V2G charging stations makes *EV* charging and discharging a two-way street, i.e., whenever the grid's power demand reaches a peak, the *EV*s with sufficient power (discharging *EV*s) can feed stored energy back to the grid, and the owners of these discharging *EV*s will get a reward on their *EV* investment by ensuring that their *EV* has sufficient power (Iqbal et al., 2021). The main advantage of smart grids in this case is that they can maximize their use of renewables while also optimizing their carbon footprint (the total amount of greenhouse gases produced) in real time.

However, there may be a delinquent caused by the rapid increase in *EV*s, namely, the excessive charging load posed on the power grid, which places a burden on charging stations to provide charging services to all *EV*s parked at the *CS*. As a result,

* Corresponding author.
E-mail addresses: rarunsekar007@gmail.com (A.S. Rajasekaran), azeesmm@gmail.com (A. Maria), Fadi.alturjman@neu.edu.tr, Fadi.alturjman@kyrenia.edu.tr (F. Al-Turjman), cmfaltrj@uwaterloo.ca (C. Altrjman), leonardo.mostarda@unicam.it (L. Mostarda).

https://doi.org/10.1016/j.egyr.2022.07.064
2352-4847/© 2022 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

the grid becomes unstable and inefficient. The solution is to use proper scheduling and management of charging services ahead of time. To schedule the charging service, the *EV* should submit critical information to the *CS*, such as the expected time of arrival and the amount of charge required by the *EV*. This data will be used by *CS* and the grid to estimate load, avoid distribution network congestion, and price management. Following receipt of this information, the *CS* responds with its decision to accept or reject charging service to the *EV* based on charge availability. Furthermore, *CS* will reserve the amount of power requested by the *EV*. As a result, the scheduling burden on *CS* and the grid will be reduced. Furthermore, *CS* will be aware of how much power is frequently required by *EV*s in that region. For *EV*s on their way to *CS*, the decision will be clear whether to stop at that specific *CS* to get power (if the *CS* accepted the request) or to search for other *CS* (if request is rejected due to lack of power or excessive load).

When reporting critical information to a nearby *CS*, the *EV* should provide some private information to the untrusted *CS*, such as duration and location. As a result, *CS* may be able to deduce the *EV*'s travel patterns, occupants, and identity information from the reported data. For instance, the service provider at the *CS* can use this private information to track the *EV*, resulting in a significant privacy breach (Wan et al., 2016; Kang et al., 2017). As a result, in order to protect users' privacy, the information provided by *EV* should be anonymous. However, the anonymous system is vulnerable to impersonation and active attacks from external intruders (Arasan et al., 2021). So, the communication between *EV*'s and *CS*'s must be performed only after the authentication of both the entities. Both these goals can be achieved by anonymous authentication.

A significant drawback of anonymous authentication is the possibility of insider attacks, which make the system more vulnerable (Subramani et al., 2021a). When an *EV* sends a charging request to *CS* prior to its arrival, the *CS* accepts it and waits for the *EV* to arrive before providing charge. At that point, a malicious *EV* can take advantage of this opportunity and send a large number of charging requests to that specific *CS*, causing that specific *CS* to reject charging requests from other *EV*s, affecting both the *CS* and other *EV*s in the same area. Similarly, an internal malicious service provider of a specific *CS* can provide erroneous information to nearby *EV*s, such as continuously rejecting their requests and demanding high prices than globally accepted prices and selling the information of *EV*s to external attackers. So, a revocation technique should be used to protect the system from these types of internal attacks from malicious internal *EV* or *CS*. Once a specific *EV* or *CS* is identified as malicious, the duplicate ID of that particular malicious entity is broadcasted to all other entities in the V2G network, allowing them to avoid communication with those malicious users.

In the current existing scenario, *EV* and CS should register with the trusted agent to prove its legitimacy. Further, when the *EV* user moves to another location, the information provided by the *EV* user to the *CS* in an anonymous way is highly confidential (Subramani et al., 2021b; Rajasekaran et al., 2022b). So, these information should be transferred to the subsequent *CS*, if the current *CS* is not able to meet the demand of *EV*. During this transfer of information between the *CS*s, the integrity and authenticity of the information should be preserved. Moreover, in the prevailing works, the new *CS* is required to authenticate the *EV* user once more freshly. As a result, computational time increases, which degrades the performance of the V2G network. But, in our suggested framework, the confidential information of the *EV* user are stored in the blockchain network by *CS*. So, there is no need for the subsequent *CS* to authenticate the *EV* user again, as it gets the data from the blockchain network. Moreover, revoking mechanism is adopted in this work, which prevents the malicious *CS* sending the fake information to subsequent *CS* which cause damage to the V2G system. In V2G network, not only the energy but also the information exchange takes place between the electric vehicle and the charging station. This information exchange should takes place in a confidential way without revealing the true identity of vehicle user. If the privacy of the *EV* user is revealed, it may leads to various security threats. So, integrity of the transferred information should be preserved. Moreover, if any charging station in the network populates fake information, it should be blocklisted and placed in the blockchain to avoid further transaction.

Motivations: Most of the recent works focussed on the efficient energy management in V2G network. They mainly focus on the authentication between the charging station and *EV* user. During the movement of the *EV* user from one *CS* to subsequent *CS*, the *EV* is to be authenticated by new *CS*. This mainly increases the computational overhead. The recent works did not consider this factor. This motivates to propose a novel work to avoid the re-authentication process and to reduce the computational overhead. Moreover, blockchain technology is incorporated to preserve the information and enhance the security.

The contributions are suggested framework are as follows:

- To develop an anonymous authentication protocol to verify the authenticity of *EV* user and *CS*.
- To propose a transfer mechanism protocol based on blockchain between the *CS*s to transfer the confidential information of the *EV*s.
- To propose an efficient revoking mechanism scheme to remove the malicious *CS* from the V2G network.
- To develop a privacy preserving of message integrity scheme in-order to guard the message from message modification and bogus message attacks.

Many authentication schemes were proposed in the recent years based on signature generation to prove the legitimity of the *EV* users. However, the computational cost of validating the *EV* user is significantly high in the prevailing works. But, in our suggested work Elliptic curve cryptography (ECC) based on bilinear pairing of points is used. Since, ECC is used, it is hard to break and provides maximum security. Moreover, authenticity of legitimate *EV* user is preserved by using digital signature and integrity of the confidential information is preserved by using hashing operation.

The manuscript is laid out as trails. Section 2 affords a summary of related similar works. Section 3 deliberates some of the fundamental concepts and system model architecture. Section 4 describes the proposed framework. Section 5 is about our work's security investigation. Section 6 emphases on performance analysis. Conclusion and upcoming work are conferred in Section 7.

2. Related works

Many schemes for *EV* privacy, security, and authenticity have been proposed in existing works. This section discusses some of the relevant schemes. In 2013, Liu et al. (Liu et al., 2013) proposed an anonymous and lightweight data accumulation scheme that protects smart grid users' privacy while also resisting external and internal attackers. The proposed scheme is cost-effective in terms of both communication and computation. However, no revocation technique is provided in this framework to prevent the V2G system from communicating with malicious users by revoking their privacy and revealing their identity. In 2016, Lam et al. (Lam et al., 2016) proposed a smart charging mechanism for V2G networks by modelling a collection of *EV*s with queuing network to estimate the capacities for regulation-up and

regulation-down separately. These estimated capacities are used for creating a new business model, as these capacities can be utilized for launching a regulation contract between an aggregator and the grid operator. The scheme can make the performance of actual system to follow the analytical model in providing charge to the grid. However, it is inefficient due to varying traffic conditions, and there may be instances where a larger number of *EV*s are located at one Charging station or there are insufficient *EV*s located at other Charging stations. Moreover, the transactions are not stored in a secure way as there is a chance to single point of failure and privacy leakage. In 2016, Sabillon et al. (Antunez et al., 2016) proposed a mixed integer linear programming formulation for EV charging coordination in unbalanced electrical distribution systems (EDS). The proposed scheduling technique is based on EDS's steady-state operation, which employs the real and imaginary parts of voltages and currents at nodes and circuits, respectively. Furthermore, the scheme has been tested using a 123-node distribution system. Based on the arrival and leaving times of the *EV*s, this scheme defined an optimal charging schedule. However, there is no guarantee that the information shared by an *EV* that is not at a charging station is genuine, so the proposed scheme fails to preserve privacy and integrity due to a lack of anonymous authentication. In 2018, Abbasinezhad et al. (Abbasinezhad-Mood and Nikooghadam, 2018) proposed an authenticated communication framework between smart metres and neighbour gateways that is resistant to modification, and denial-of-service attacks. It describes the details of control messages sent from neighbourhood gateways to smart metres, and the authors claimed their implementation on ATmega2560 as an appropriate entity to be procured for smart metres. However, they have not included techniques to hide the true identities of the system entities in this scheme, which may leak the privacy of the users while they are communicating, implying that authentication in this scheme is not anonymous.

In 2019, Wang et al. (Wang et al., 2019) suggested a concrete anonymous rewarding scheme in V2G networks using Block chain technology. Using two different efficient public key cryptosystems, the authors proposed a rewarding scheme to give incentive to battery vehicles that act as a source of charge for the grid in this work. The scheme is safe and efficient, and the transactions are unchangeable. However, there is no revocation method in the system. As a result, the malicious user cannot be stopped from participating in energy trading, and will continue to maintain high prices for providing power to the grid, potentially causing the V2G network to become unstable. In 2020, Khan et al. (Khan et al., 2020a) proposed a lightweight password-based key agreement framework using elliptic curve cryptography. It is secure against man-in-the-middle attacks and replay attacks, and the work is validated using the "AVISPA" simulation tool. Data confidentiality, non-traceability, and forward secrecy are achieved as a result of the work. However, they failed to maintain backward secrecy. Furthermore, the 'AVISPA' tool has some drawbacks, such as difficulty in use and the requirement of additional prerequisites.

In 2020, Dariush et al. (Abbasinezhad-Mood et al., 2020) proposed a smart grid key establishment protocol that does not involve an electricity service provider (ESP) during the key agreement, whereas previous works required the smart reader to connect to the ESP via the internet. This work has fewer computational overheads, and there is no overhead on the service provider. The authors used ProVerif, an automatic protocol verifier, to demonstrate the proposed work's security against known attacks. However, the system fails to maintain forward and backward confidentiality, and there is no defence against internal attacks. In 2020, Hassija et al. (Hassija et al., 2020) proposed a lightweight data sharing protocol in V2G network using blockchain based concept called Directed Acyclic Graph-based V2G network (DV2G). A tangle data structure is used in this case to record network transactions in scalable and secure manner. A game theory model (Stackelberg) is used to negotiate between the grid and vehicles at the lowest possible price. This protocol's main advantages include high scalability, low computational cost, and support for micro-transactions in V2G networks. However, the communication does not use anonymous authentication and is not applicable to G2V, G2G, or V2V networks.

In 2020, Irshad et al. (Irshad et al., 2020) proposed a novel framework for allowing vehicles to communicate with one another or recharge at desired charging stations. The work is safe from man-in-the-middle attacks and desynchronization issues. However, the presented scheme is not secure against impersonation or DOS attacks, and there is no anonymity or integrity for communications between *EV*s. In 2020, Luo et al. (Luo et al., 2020) proposed an anonymous communication scheme for delivering charging information in a V2G network. This scheme is appropriate for incorporating identity authentication into key distribution without the involvement of a trusted party. Furthermore, the scheme maintains anonymity by splitting the charging information and forwarding it pseudo-randomly. Furthermore, this scheme ensures anonymity without the involvement of a third party. However, system initialization and entity registration will be difficult without knowing and validating the true credentials of the owners of the *EV*.

In 2020, Iqbal et al. (Iqbal et al., 2020) proposed two controllers for bidirectional power flow in vehicle to grid network namely grid regulation and charge controller by taking various charging profiles, state of charge of electric vehicle batteries, different number of electric vehicles into consideration. In the simulation results, the authors claimed that by adding more electric vehicles in the fleet during V2G mode, can increase frequency of industry microgrid even more and they have used MATLAB and SIMULINK tool for simulation. The scheme is robust and it contributes effectively towards the frequency regulation, when V2G mode is enabled. But, the scheme cannot effectively regulate the frequency of micro grid, when V2G mode is disabled and there is no anonymity and integrity in the communications between internal entities in the system. In 2021, Aggarwal et al. (Aggarwal and Kumar, 2021) proposed a peer-to-peer (P2P) energy trading scheme to manage demand response in a V2G network between *EV*s and service providers (SP). It lacks complex energy-transport meshes and achieves a good balance between demand and response by incentivizing self-interested *EV*s. To avoid third-party intervention between EVs and SPs and to solve traded energy problems, the authors used consortium blockchain technology and a double action mechanism. The primary benefit of this work is that it improves the rate of convergence, standard deviation, scalability metric average latency, and achieves transaction security sustainability. However, there is no anonymity in the system's internal communication, which may result in a major privacy breach.

In 2021, Wang et al. (Wang et al., 2021) proposed a wireless bidirectional grid power interface for *EV*s that allows power to flow between the grid, the *EV*, and homes with nonlinear loads. The authors used a grid-side low frequency to dc converter to set up the two-way energy flows. Furthermore, the authors used the adaptive dc-link voltage controller to improve efficiency. This work is more efficient, as it ensures wireless energy transfer between the grid, *EV*s, and nonlinear household loads while maintaining power quality. However, there is no anonymous authentication protocol between electric vehicles and the grid, which could lead to system instability and a significant privacy breach.

In 2021, Das et al. (Das et al., 2021) proposed a two-part charging service scheme in V2G and G2V networks, the first

being to assign appropriate charging stations to *EV*s based on a linear optimization problem, and the second of it is to schedule charging. The authors proposed an intelligent charging scheduling algorithm that incorporates henry gas solubility optimization in this paper. The total daily cost incurred by the *CS* operator is minimized, and the scheme is robust. However, there is no efficiency in charging scheduling because traffic analysis may deviate from designed traffic, and there is no anonymity or integrity for communications in this V2G framework.

3. Preliminaries

The basic concepts regarding elliptic curve cryptography, blockchain, system model of our suggested framework are conferred in this section.

3.1. Elliptic curve cryptography (ECC)

Let us consider an elliptic curve over a finite field is demarcated by $E(a,b): s^2 = r^3 + ar + b \ mod \ q$ which satisfies the condition $4a^3 + 27b^2 \neq 0$ where $a, b \in Z_q^*$ under the group $G = \{(r,s): r,s \in Z_q^*, (r,s) \in E\} \cup \{\circledcirc\}$. Here $\circledcirc$ represents the identity element under additive group. In addition, the scalar multiplication in ECC is represented as $nX = X + X + X + X + \cdots X(n - times)$. The scalar point addition is represented as $X + Y = (r_3, s_3)$ such that $X = (r_1, s_1) \in G$, $Y = (r_2, s_2) \in G$, where the values of r_3 and s_3 are calculated as follows. $r_3 = \lambda^2 - r_1 - r_2 \ mod \ q$, $s_3 = (\lambda\,(r_1 - r_3) - s_1) \ \ mod \ q$ and

$$\lambda = \begin{cases} \dfrac{s_2 - s_1}{r_2 - r_1} \text{ mod q if X} \neq Y \\ \dfrac{3r_1^2 + a}{2s_1} \text{ mod q if X} = Y \end{cases}$$

3.2. Blockchain

The blockchain is a collection of blocks that are linked together. The block is a distributed ledger and the transactions recorded in the block are immutable and unchangeable. Each block in the blockchain contains the previous block's cryptographic hash value, a unique timestamp, and transaction data. Since, the blockchain is decentralized and distributed, the blocks in the blockchain cannot be modified selectively without impacting all subsequent blocks. Security, transparency, decentralization, and immutability are some of the key characteristics of blockchain technology. To prevent tampering, the data in the blocks is cryptographically secured. To achieve this security level, the contents of the blocks are hashed and added to the block's header. Finally, the blocks are chained together in such a way that the previous block's secured hash value is linked with the current block. As a result, each block is dependent not only on its own data content, but also on the hash value of the previous block. Furthermore, it does not rely on any centralized trusted authorities to process data transactions. Moreover, no third-party intermediary is required to verify and validate data transactions. This phenomenon enables users to independently verify and review transactions. Once the data transactions are successfully completed, the valid transactions are hashed and encoded into the merkle tree. The transactions are viewed in the form of SHA256 code.

3.3. Blockchain in V2G network

The Charging stations are responsible for providing service to the *EV*. There may be a possibility that the *CS* may be corrupted and send false information to subsequent *CS* regarding the charging/discharging status of *EV*s. This may disrupts and degrades the performance of the system. But, the introduction of blockchain technology has created possibilities for V2G to address the aforementioned challenges. As a result, in our proposed work, blockchain is integrated with V2G network, which enables integrity and authenticity without the intervention of Federated trust entity, thereby reducing EVs computation time.

3.4. System model

The system model for the proposed privacy-preserving anonymous authentication framework consists of three main entities namely Electric Vehicles (EV_i), Charging Stations (CS_i) and a Federated Trust Entity (*FTE*), which in-turn contains three sub departments i.e., Financial Department (*FD*), Validation Department (*VD*), and Department of Service Providers (*DSP*). Every entity have its own Endorsement and Duplicate IDs. Moreover, these entities have their own Endorsement and Duplicate IDs which is unique in our suggested work. Further, each department performs their own functional role independently but finally the results are combined to authenticate the end users. In addition, the integrity of information regarding the *EV* are stored in blockchain which is immutable and untamperable. Thus, the system is unique in nature. Fig. 1 shows the basic architecture of V2G network.

Federated Trust entity (***FTE***) *FTE* is the heart of our proposed V2G framework. It is a fully trusted single entity, which internally consists of separate departments for performing different functions in the V2G network, to maintain the stability of the system. Since, it is fully trusted entity and it is difficult for anyone to compromise *FTE*. Financial department of *FTE* work is to monitor the financial activities in the system, i.e., it will fix the price for charging at charging stations and it act as separate entity, such as bank or financial institution. Validation department of *FTE* is used to verify the true identities of users, at the time of offline registration. Moreover, it will be associated with government agency to validate the identity of the users and service providers of charging station. The Department of service providers (*DSP*) of *FTE* work is to monitor the behaviours of EVs and *CS*s, and to block the malicious users. Moreover, it will provide the true genuine identity (*EID*) and dummy identity (*DID*) for EVs and *CS*s. There are some examples for *VD* in real-world namely Symantec, DigiCert, and Verisign.

Charging Station (***CS***)**:** *CS* is used to provide charging to the nearby EVs. Initially, the service provider of *CS* has to go to *FTE* and register at trusted party by providing its true credentials like address, phone number, Identification card, etc., After successful authentication, the *FTE* will provide security parameters to service provider of *CS* like dummy identity (DID_{c_i}) and real identity (EID_{c_i}), which are used to communicate with EVs in a wireless manner. Moreover, the service provider of *CS* have On-Board Device (*OBD*) which is used to store the security parameters and to compute the required communication parameters during authentication. Before the arrival of the EV to the particular *CS*, the corresponding EV will send its demand information to *CS*. Once the EV is anonymously authenticated, the *CS* will reply with acceptance or rejection message, based on the charge available at grid and the number of slots available at *CS*. If any *CS* is corrupted or broadcasted false information into the system, than its identity will be tracked by *FTE* and its duplicate ID will be shared to the other entities, thereby protecting system from further damage.

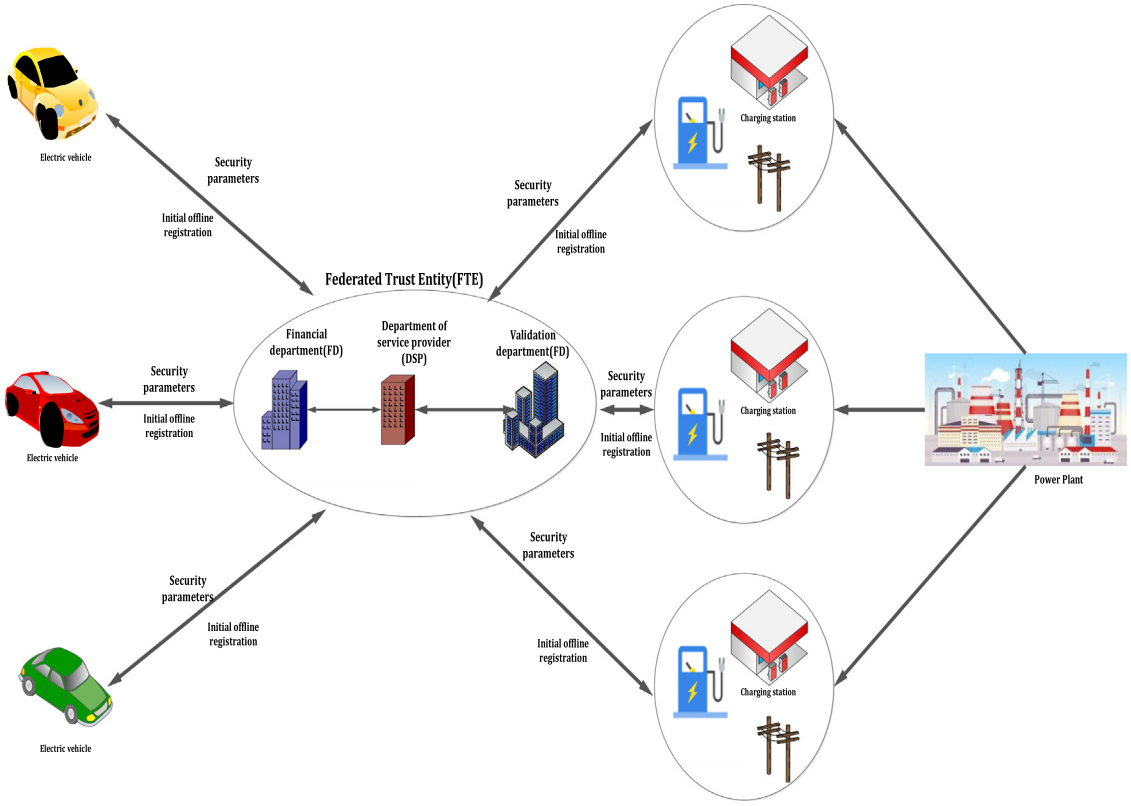

Fig. 1. Basic architecture of V2G network.

Dummy IDs are used for anonymous authentication to preserve the privacy of the end users. During registration, the FTE will map these duplicate IDs of EVs to their true Identities for the purpose of revocation. As a result, even if the duplicate ID is disclosed to anyone, they provide zero knowledge about the true identity of EV.

***Electric Vehicle* (EV):** EVs are also provided with On-Board Device (*OBD*) unit, which is used to store the security parameters and to compute the communication parameters at the time of authentication. The on-board devices are installed in every EV and charging station. They have high computation capability. The OBD of EV act as a smart device, collects the various parameters like (v_i, x, f, EID_{v_i}) from FTE and store them. Similarly, the OBD of CS, store the values of $(EID_{c_i}, DID_{c_i}, x, f)$ provided by FTE. Initially, the EV owner should register at *FTE* by providing his true credentials like vehicle number, phone number, address, etc., Then, the *VD* in *FTE* will validate EV credentials and provide two parameters to EV namely dummy identity for EV (DID_{v_i}) and true genuine identity for EV (EID_{v_i}). Whenever, charge is required by EV, it will communicate to nearby *CS* in advance. At that instant, both EV and *CS* will authenticate each other in an anonymous and secure way. Once authenticated, EV will send its request to *CS*. When the EV request is accepted by *CS*, the EV gets its service. If the *CS* is completely occupied or there is no charge, it will reject to provide the charging service to EV. Then, the EV will request to other *CS* for the required service. In our proposed system, there is no need of re-authentication, since "Transfer mechanism and Integrity preservation" technique is used. Moreover, revocation technique is used to revoke the malicious EVs from the V2G network.

4. Proposed work

In V2G network, for secure and efficient transmission of data between EV's and *CS*, a Blockchain based revocable integrity preservation scheme is proposed in this work. To achieve anonymous authentication between EVs and *CS*, the following processes are involved in this work. This includes System initialization, EV's and *CS*'s registration, Anonymous authentication of both EV's and *CS*'s in a secure way, and finally revocation and Integrity preservation techniques. The notations used in our suggested framework are shown in Table 1.

4.1. System initialization

In this proposed system, the main entity is *FTE* which is responsible for performing various activities like finance, registration etc., through its sub-departments. Initially *FTE* chooses a finite elliptic curve of $y^2 = (\alpha^3 + \vartheta\alpha + \beta)\ mod\ a$, where a is the large prime number. Let us consider two points on elliptic curve R and . *FTE* chooses three random numbers $e, f, x \in Z_a^*$. Let Z_a^* be the multiplicative group of size a. Then, *FTE* chooses public and authentication parameters as $\theta = eR$, $\phi = fR$ and $\psi = x^2R$. Finally, *FTE* broadcasts the parameters $(\theta, \phi, \psi, H, R, T, e\,(R, T), a)$ to all the *EV*'s and *CS*'s present in the network. Here, the hash function is given by $H: \{0, 1\}^*$. Fig. 2 shows the schematic representation of the proposed framework. Initial registration process takes place in an offline manner. Since, if the registration takes place in an online manner, due to the open platform, there may be a possibility of information to be hacked. So, to have a better security, in our suggested work both *CS* and *EV* user registration takes place in an offline way. After successful registration, required security parameters are issued to *CS* and *EV* user by *FTE* in an offline way.

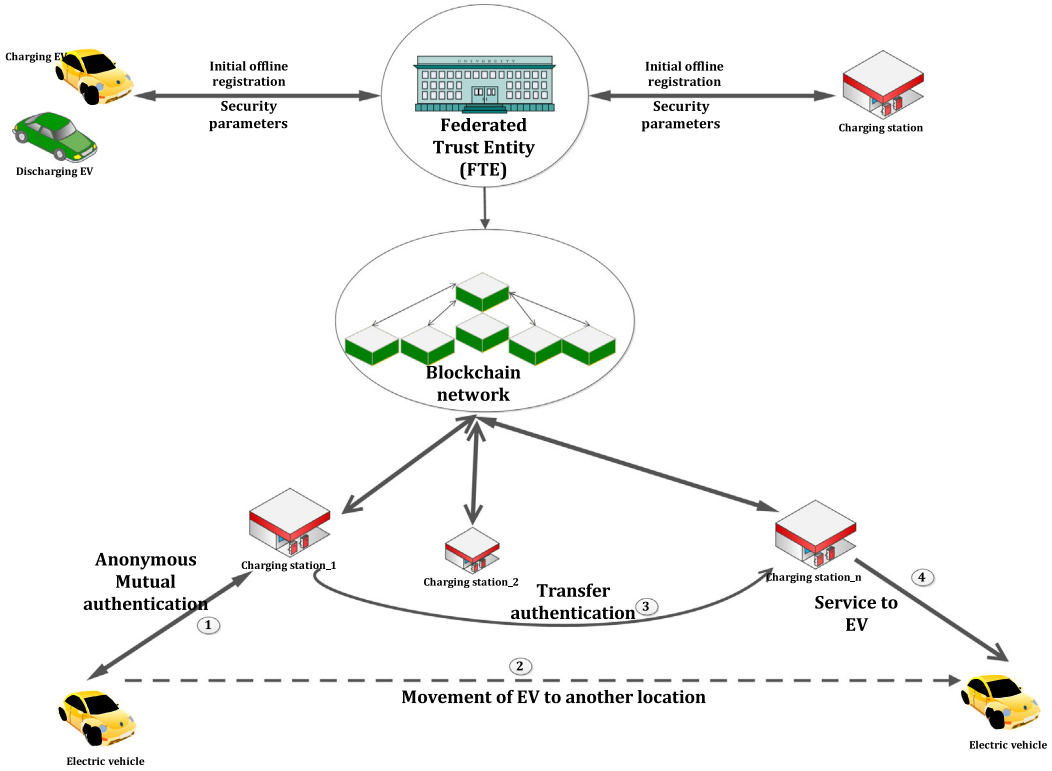

Fig. 2. Schematic representation of proposed work.

Table 1
List of notations and abbreviations.

Notations	Explanation
EV	Electric vehicle
CS	Control station
FTE	Federated trust entity
$y^2 = (\alpha^3 + \vartheta\alpha + \beta) mod\ a$	Finite elliptic curve equation
R and T	Finite points of elliptic curve
Z_a^*	Multiplicative group of size a
a	Large prime number
e, f, x, v_i	Random numbers chosen from Z_a^* by *FTE*
θ, ϕ, ψ	public parameters
H	Hash function
EID_{v_i}	Endorsement ID for *EV* user
DID_{v_i}	Duplicate/dummy ID for *EV* user
EID_{c_i}	Endorsement ID for *CS*
DID_{c_i}	Duplicate/dummy ID for *CS*
AA	Authentication acknowledgement of *CS*
b_i, r_i, s_i, q_i	Random numbers chosen from Z_a^* by *CS*
i_i	Confidential information
i_i^*	Fake information
σ_i	Signature of a confidential information
t_i	Timestamp
O_1, O_2	Short life keys of *CS*
$\oplus$	Exclusive OR operation

4.2. EV's Registration

Initially, the owner of EV should register at *FTE* by providing his confidential information like mobile number, address and Identification card etc., to *FTE* in an offline manner. Then, the *FTE* validates those credentials and it chooses a random number $v_i \in Z_a^*$ and computes the Endorsement ID and duplicate/dummy ID for every EV as EID_{v_i} and DID_{v_i}, where $EID_{v_i} = v_i\,(e+f)\,x$. Moreover, *FTE* will map these duplicate IDs of EVs to their true Identities for the purpose of revocation. Here, even if the duplicate ID is disclosed to anyone, they provide zero knowledge about the true identity of EV. Then, *FTE* securely provides (v_i, x, f, EID_{v_i}) to all the corresponding EVs in an offline manner i.e., these credentials will be stored inside the *OBD* of the EV. Moreover, the *FTE* stores (DID_{v_i}, Z) in the blockchain network, where $Z = e(R,T)^{v_i.x^2}$.

4.3. CS registration

Similar to EV's registration, the service providers in every *CS* should mandatorily register at *FTE* by providing their required credentials. The Endorsement ID of a particular *CS* will be computed as $EID_{c_i} = \left(\frac{x}{e+f}\right)T$ and the duplicate ID will be selected as DID_{c_i} such that $DID_{c_i} \in Z_a^*$. Finally, the *FTE* provides the $(EID_{c_i}, DID_{c_i}, x, f)$ to the corresponding service provider of *CS* i.e., the service provider will store those credentials in the *OBD* of particular charging Station.

4.4. EV's Anonymous authentication

The process of validating the credentials of EV's and *CS*'s in an anonymous way in order to ensure security is known as anonymous authentication. i.e., this process authenticates EV's and *CS*'s without revealing their true identities to preserve their privacy. In V2G network, the entities should anonymously authenticate with each other to communicate in a secure and efficient way and the authentication steps are listed below. Here, the charging services at *CS* will be scheduled in advance i.e., the EV will provide its critical information like amount of charge needed/excess, time of

arrival to the charging station in advance. So, during this time both entities should mutually authenticate with each other.

1. The *OBD* of EV will send $v_i xf$ to the *OBD* of the charging station.
2. Similarly, the *OBD* of the *CS* computes $DID_{c_i} xf$ and sends it to EV's on-board device.
3. Then, EVs on-board device computes $l = DID_{c_i} xf\, v_i R$. Similarly, the *CS*'s on-board device also computes l as $l = v_i xf DID_{c_i} R$.
4. Moreover, the EVs *OBD* calculates $l_1 = EID_{v_i} \bigoplus H(l)$ and sends it to *OBD* of *CS*. Once, l_1 is received, the *CS* find the Endorsement ID of EV by the following equation $EID_{v_i} = l_1 \bigoplus H(l)$.
5. After computing the Endorsement ID of EV, the *OBD* of the *CS* will check whether $e\left(EID_{v_i} R, EID_{c_i}\right) = Z$ in the blockchain network. As blockchain network is used in this work, the *CS* can access the Z value without any association with *FTE*, which results in reduction of computation time at the time of re-authentication.

Proof of correctness

$$\begin{aligned} e\left(EID_{v_i} R, EID_{c_i}\right) &= e\left(v_i\,(e+f)\,xR, \frac{x}{(e+f)} T\right) \\ &= e(R, T)^{v_i x^2 (e+f)/(e+f)} \\ &= e(R, T)^{v_i x^2} \\ &= Z \end{aligned}$$

Finally, the *OBD* of the *CS* picks the duplicate ID of EV (DID_{v_i}) from the blockchain network and computes the authentication acknowledgement as $AA = (DID_{v_i}, DID_{c_i}, H(DID_{v_i}, DID_{c_i}))$ which is transmitted to all other *CS* in the network to prevent EV from re-authentication at another charging station. Moreover, *CS* on-board device computes $l_2 = EID_{v_i} \bigoplus DID_{c_i}$ and this value of l_2 is given to the EV's on-board device, so that the EV computes the duplicate ID of *CS* as $DID_{c_i} = EID_{v_i} \bigoplus l_2$, which is used to authenticate charging station anonymously. Authentication receipt is used to avoid the re-authentication process and to reduce the computational overhead. This *AA* is transferred to all other *CS* in the network. Thus the re-authentication time of *EV* by the subsequent *CS* is avoided. Moreover, the authentication receipt uses only the dummy identity which helps to preserve the anonymity of the entities.

4.5. CS'S anonymous authentication

The *CS* provides the service information like its acceptance to provide charge, price etc., to EV in advance. So, this information should be transmitted to EV in a secure and efficient way. Because, any malicious entity can send another faulty information to EV, so the EV should authenticate the *CS* in an anonymous way, before receiving any information from the charging station. In this procedure, the *CS* on-board device chooses $b_i \in Z_a^*$ and computes the following parameters $h_i = b_i R$, $k_i = H(EID_{v_i} \times (\theta + \phi))$ and $m_i = \left(b_i + k_i f + h_i x^2\right) \ mod\ a$. Based on these values, on-board device of *CS* computes $O_1 = DID_{c_i} \bigoplus m_i$ and $O_2 = EID_{v_i} \bigoplus k_i$. Finally, the values of O_1, O_2 and b_i will be sent to the EVs on-board device. Once, these values are received, the EV find the values of h_i, k_i, m_i and checks whether $m_i R = (h_i + k_i \phi + h_i \psi)$. If this condition satisfies, then the EV accepts the near by charging station's information about charging service.

Proof of correctness

$$\begin{aligned} m_i R &= \left(b_i + k_i f + h_i x^2\right) R \\ &= \left(b_i R + k_i f R + h_i x^2 R\right) \\ &= (h_i + k_i \phi + h_i \psi) \end{aligned}$$

4.6. Transfer mechanism and integrity preservation

To send the confidential information of EV like charging request, EV number etc., to other *CS*, the current *CS* will choose three random numbers $r_i, s_i, q_i \in Z_a^*$ and computes the following values $V = r_i\theta$, $W = (m_i + q_i)\theta$, $u_i = s_i\theta$, $\Omega = (u_i + V + W)$ and $M_i = D_i\,(s_i + r_i + m_i + q_i) \ mod\ a$, where $D_i = H(r_i \times (i_i + \Omega))$ and i_i is the confidential information to be shared.

Then, the current *CS* sets $\sigma_i = (u_i, i_i)$ as the signature of a confidential information. Here, the integrity of message will be preserved, as this signature is unique and no one can alter or modify the signature. Then, the current *CS*'s on-board device sends $(M_i, t_i, i_i, \sigma_i, \Omega, DID_{v_i}, DID_{c_i})$ to another charging station's *OBD* in the network. Here, t_i represents the time stamp at which the confidential message is created. Once this message is received by new *CS*, it will compute $D_i = H(i_i \times (u_i + \Omega))$ and checks the condition $M_i\theta = D_i\Omega$. If the condition gratifies, then the confidential information (i_i) is accepted by new *CS*, otherwise it will be rejected.

Proof of correctness

$$\begin{aligned} M_i\theta &= D_i(s_i\theta + r_i\theta + m_i\theta + q_i\theta) \\ &= D_i(u_i + V + W) \\ &= D_i\Omega \end{aligned}$$

4.7. Revocation

Even if there is a successful anonymous authentication, there may be a possibility, where the *CS*'s in the network may become corrupt and transmit false information into the network (i.e., to other *CS*). In those cases, the *FTE* revokes the current malicious *CS* from the V2G network and mark that *CS* identity in the block list. Thus, the *CS* cannot communicate further to any other *CS* or EV in V2G network. For instance, if a faulty message i_i^* is sent by a malicious *CS* to other *CS* in the network i.e., $(M_i, t_i, i_i^*, \sigma_i, \Omega, DID_{v_i}, DID_{c_i})$. After receiving of this message, if new *CS* found that the information is fake, it will report these credentials to *FTE*. Then, the *FTE* will remove the identity of malicious *CS* by using these credentials. Moreover, the *FTE* sends $(DID_{c_i}, H\left(DID_{c_i}, f, x\right))$ to all the *CS*'s in the V2G network. On receiving this, the on-board device of all the *CS* computes $ss = H\left(DID_{c_i}, f, x\right)$.

If ss is equal to the received $H\left(DID_{c_i}, f, x\right)$, then the DID_{c_i} will be stored in the block list. Hence, the *CS* with duplicate identity DID_{c_i} will not be allowed to perform any further communications with other entities in the V2G network.

5. Security analysis

In this section, identity privacy preserving, message integrity and ensuring security using revocation techniques are discussed. In our suggested scheme, the signature σ_i and D_i are the required parameters to ensure security against various attacks. Moreover, the values of l *and* l_1 are useful to ensure protection against unauthorized access, while communicating with the charging station in the network. In our scheme, it is an impossible task for an external attacker to compute the values of l *and* l_1 and to perform impersonation attacks, because he cannot compute the values of x *and* f which are provided to authorized users by *FTE* in an offline manner. Moreover, the intruder cannot compromise the registration, as it will be performed in an offline manner with the trusted *FTE*. Proposed system's defence procedure against various threats and attacks is explained below.

5.1. Defence against impersonation attack

In order to execute an impersonation attack by pretending to be an authorized user, the external attacker has to find the secret parameters of authorized entities i.e., the values of x, f *and* v_i. But, these values are sent to EV and *CS* in an offline manner, which are used in *EV's* registration to compute the values of $l = v_i x f DID_{c_i} R$ and $l_1 = EID_{v_i} \bigoplus H(l)$. So, an external attacker cannot access these values and to pretend as a fake *EV* to participate in the authentication procedure, which is performed at charging station. Moreover, at the time of *CS's* registration, the value of b_i is selected randomly by *OBD* of *CS*, which is used to calculate the values of $h_i = b_i R$, $k_i = H(EID_{v_i} \times (\theta + \phi))$ and $m_i = \left(b_i + k_i f + h_i x^2\right)$ *mod a*. So, the values of h_i, k_i and m_i also random and it is difficult for an intruder to access these random numbers and calculate the authentication parameters. So, it is difficult for an attacker to compromise the anonymous authentication step to perform impersonation attack either by pretending to be an *EV* or an *CS*. Hence, our authentication procedure can withstand against the impersonation attack.

5.2. Defence against bogus message attack

An intruder has to find the value of signature σ_i and the value of D_i of the *CS* to send bogus messages to other charging station. Moreover, the values of $= r_i\theta$, $W = (m_i + q_i)\theta$, $u_i = s_i\theta$, $\Omega = (u_i + V + W)$ and $M_i = D_i\,(s_i + r_i + m_i + q_i)$ *mod a* depends on the values of r_i, s_i, q_i which are chosen randomly by the current *CS*. Moreover, here $D_i = H(r_i \times (i_i + \Omega))$, $m_i = \left(b_i + k_i f + h_i x^2\right)$ and the values of r_i, s_i, q_i are chosen by current *CS* randomly and it involves Elliptic curve discrete logarithmic problem (ECDLP). It is impossible for an external attacker to crack the values of r_i, s_i, q_i. So, it is difficult to execute bogus message attack.

5.3. Defence against message modification attack

In our suggested scheme, every current *CS* transfer the message to new *CS* as $(M_i, t_i, i_i, \sigma_i, \Omega, DID_{v_i}, DID_{c_i})$. Sometimes, external attacker will try to modify this message, such as changing the content of the broadcasted message before it reaches the receiver. But, in our scheme, to preserve message integrity, *CS's* signature is generated based on signature $\sigma_i = (u_i, i_i)$ where i_i is confidential information about *EV* and $u_i = s_i\theta$. The value of s_i is only known to current charging station, as it is chosen randomly by *CS*. So, an external attacker cannot find the values of s_i and u_i. Moreover, the random number s_i is for short duration and its value changes for every new communication of current *CS* with other *CS*. So, even though, if the intruder crack the current value of s_i, he cannot follow the subsequent communication of that particular charging station. Thus, the external attackers cannot forge the signatures of internal charging stations. As a result, the proposed scheme is safe against the message modification attack.

5.4. Revocation mechanism

In our suggested scheme, the users will communicate with each other anonymously using anonymous signatures to hide their real identity to ensure privacy and integrity. But, if any *CS* is compromised and sends a false information to other *CS*, then the *FTE* block that particular malicious *CS* by using his duplicate ID (DID_{c_i}). Moreover, when the new *CS* identifies the information sent by a current *CS* as fake, it will submit these credentials $(M_i, t_i, i_i^*, \sigma_i, \Omega, DID_{v_i}, DID_{c_i})$ to *FTE* where, i_i^* is a fake information content. Then, the *FTE* will remove the identity of malicious *CS* by using these credentials. Moreover, the *FTE* sends $(DID_{c_i}, H\left(DID_{c_i}, f, x\right))$ to all the *CS*'s in the V2G network. On receiving this, the on-board device of remaining *CS* in the network computes $ss = H\left(DID_{c_i}, f, x\right)$. Thus, the remaining charging stations in the network use this DID_{c_i} to restrict the communication with that particular malicious *CS*.

5.5. Defence against non-repudiation attack.

In our suggested scheme, the charging station cannot repudiate after receiving the charging request from the *EV* or after receiving a transfer information from other *CS* about particular *EV*. Moreover, when the information is received from the *EV*, the authenticity of the *EV* is checked by the *CS* using anonymous authentication process. So, repudiation of the *EV* is not acceptable. In addition, while sending the transfer information to new *CS* by current *CS*, the request can be accepted only, if the current *CS* is authenticated. Moreover, the users give their credentials and registered in offline to the *FTE*. As a result, after sending the demand request, the user cannot repudiate.

5.6. Anonymity and privacy preserving.

In our suggested scheme, the *EV* and *CS* uses a valid signature and dummy identities provided to them by *FTE* to communicate between each other. Moreover, the authentication parameters like l, l_1, M_i and D_i are computed using dummy identities of *EV*/*CS* and random numbers which are chosen by the entities. As a result, external attacker have zero knowledge about the sender of the message. Even though, if these dummy identities are revealed, the external attacker get zero knowledge about the true identity of *EV* or *CS*. As a result, anonymity and privacy of the users are preserved in our scheme.

5.7. Unlinkability.

In our work, the signature is computed as $\sigma_i = (u_i, i_i)$, where i_i is information content and $u_i = s_i\theta$, where s_i is random number chosen by current *CS* which will be changed periodically. In *CS* anonymous authentication, the authentication parameter $m_i = \left(b_i + k_i f + h_i x^2\right)$ *mod a* is calculated based on the value of b_i, which is randomly chosen by *CS*, whose value will be changed periodically. During information exchange, these random numbers are used for computing authentication keys and signature. As a result, once the information is exchanged after validating the identity of both parties, the validity of these random numbers will be expired and entities will use new random numbers for further communication. So, there is a complete unlinkability during the information exchange.

5.8. Defence against sybil attack.

In this attack, a particular *EV* will send multiple fake requests to a charging station to make the charging station busy. As a result, the corresponding *CS* will not accept any request from other *EV*. But, in our suggested scheme, if an external attacker wishes to sends a single fake message, he has to crack the values of x, f, v_i to compute the values of l *and* l_1, where $l = v_i x f DID_{c_i} R$ and $l_1 = EID_{v_i} \bigoplus H(l)$. But, the values of v_i, x and f are known only to authorized *EV*, as they are provided to them in an offline manner by *FTE* at the time of registration. So, it is impossible for an external attacker to create multiple identities without knowing x, f, v_i values. So, it is difficult for an external entity to send multiple fake request messages to the charging station. Thus, our proposed scheme can withstand against the sybil attack.

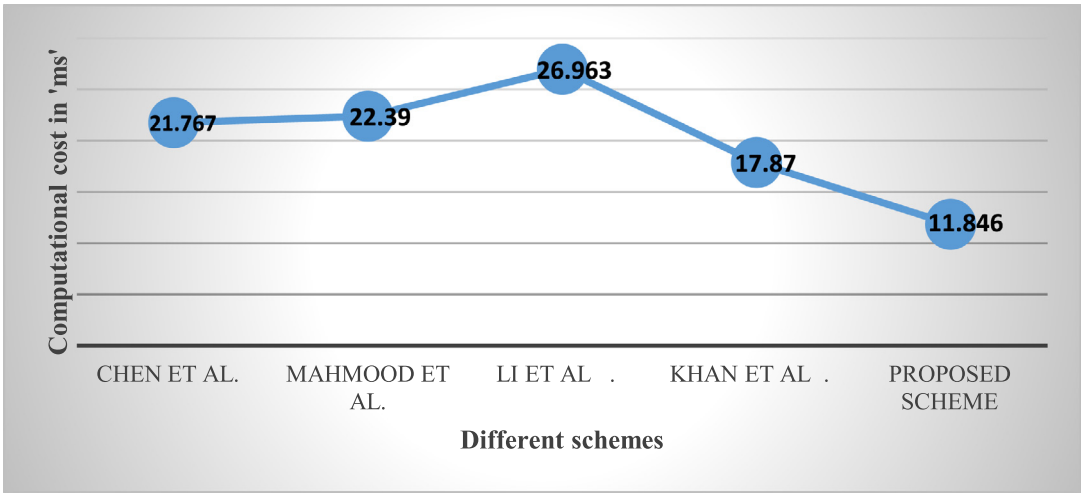

Fig. 3. Computational time for single *EV* and single *CS*.

Table 2
Authentication time of different schemes.

S.no	Schemes	Verification time for single EV and single *CS* in '*ms*'	Verification time for n EV and n *CS* in '*ms*'
1.	Chen et al.	$5ET_m + ET_p + 2ET_e + 12ET_h$	$5nET_m + nET_p + (n+1)ET_e + 12nET_h$
2.	Mahmood et al.	$10ET_m + 4ET_a + 8ET_h$	$10nET_m + 4nET_a + 8nET_h$
3.	Li et al.	$7ET_e + 6ET_h$	$7nET_e + 6nET_h$
4.	Khan et al.	$4ET_{ed} + 8ET_m + 19ET_h$	$4nET_{ed} + 8nET_m + 19nET_h$
5.	Proposed scheme	$4ET_m + ET_p + ET_a + 4ET_{xor}$	$4nET_m + nET_p + nET_a + 4nET_{xor}$

5.9. Defence against replay attack

In this attack, an external attacker captures a message at the time of transmission and retransmit it at a later time. In our scheme, to avoid the replay attack, the timestamp t_i is attached to the message $(M_i, t_i, i_i, \sigma_i, \Omega, DID_{v_i}, DID_{c_i})$, which is sent by the current *CS* to new *CS* at the time of transfer mechanism. So, once the message is received, the new *CS* checks whether $\left|t_j - t_i\right| < \triangle t$, where $\triangle t$ is the mutually agreed time delay between internal users. If this time delay is not reasonable, then new *CS* simply rejects the message. Thus, our proposed scheme can withstand against the Replay attacks.

6. Performance analysis

Performance investigation is evaluated in terms of computational cost, communication cost, security assessments, and *CS* serving ratio.

6.1. Computational cost

The time required to perform the cryptographic operations involved for the verification of authenticity of EV and *CS* is referred as computational cost. Nearly 100 random simulations are computed and average value is taken for the calculation of computational cost. The suggested scheme is compared with the related similar schemes like Chen et al. (Chen et al., 2017), Mahmood et al. (Mahmood et al., 2018), Li et al. (Li et al., 2019) and Khan et al. (Khan et al., 2020b) respectively and proved to be noteworthy in terms of computational analysis. Several cryptographic operations like one point multiplication (ET_m), point addition (ET_a), symmetric encryption and decryption operation (ET_{ed}), secure hashing operation (ET_h), bilinear pairing operation (ET_{bp}), modular exponential operation (ET_e) and E-xor operation (ET_{xor}) are involved in the analysis of computational cost. The computation time required to perform the above mentioned cryptographic operations are calculated as 2.226 ms, 0.028 ms, 0.0046 ms, 0.0023 ms, 2.91 ms, 3.85 ms, 0.001 ms, where 'ms' symbolizes milliseconds. In order to perform the simulation, core i7 processor with 8 GB RAM is used. The simulation tool used for the implementation is Cygwin platform using PBC library (Anon, 2021). Table clearly displays the execution time required for the verification of single *CS* and single EV user. The proposed scheme involves four point multiplication operations, four E-xor operations, one bilinear pairing and one point addition operation for the verification of single *CS* and single EV user. The total computation time of our suggested scheme is computed as 11.846 ms, whereas the prevailing schemes like Chen et al. (2017), Mahmood et al. (2018), Li et al. (2019), and Khan et al. (2020b) consumes 21.767 ms, 22.390 ms, 26.963 ms and 17.870 ms respectively. The proposed work consumes only simple point multiplication operation, point addition operation and xor operation. The time involved for performing these cryptographic operations are minimum. The suggested scheme consumes only four point multiplication operation, four xor operations, one pairing and one point addition operation for the verification of *EV* user. Thus for authenticating a single vehicle user, the suggested scheme consumes 11.846 ms, which shows the suggested scheme has less computational time when compared the related schemes. Moreover, Table 2 displays the computation time involved for the verification of n EV users and *CS* respectively. Fig. 3 portrays the computational overhead for single *EV* and *CS* in a graphical notation. Fig. 4 portrays the graphical representation based on the increase in number of EV users and *CS*. From the graph,

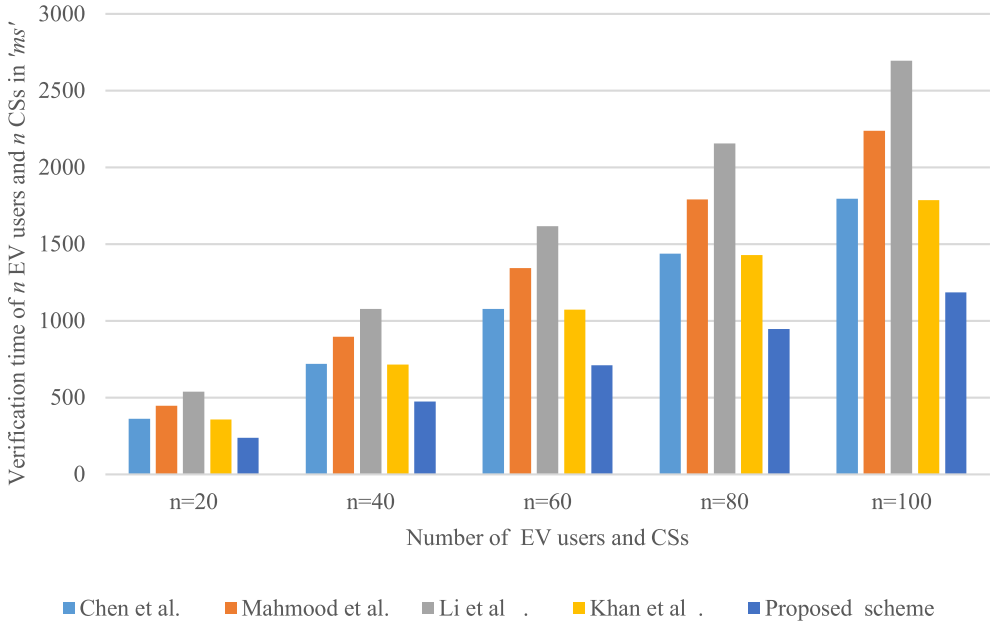

Fig. 4. Computational time for *n EV*s and *n CS*s.

it clearly indicates that our suggested scheme outperforms the related prevailing schemes. In our suggested work, whenever, the *EV* user requests the charging/discharging from charging station. The *CS* authenticates the *EV* user. Once the authentication is successful, the request is accepted. But when the same *EV* user moves from one *CS* to subsequent *CS*, there is no requirement for the new *CS* to authenticate the *EV* user once again. Instead, the new *CS* takes the data from blockchain and authenticate the *EV* user. In our proposed work, when there 20 *EV* users at the *CS*, then the computational overhead required for authenticating the *EV*s is 236.92 ms only, whereas, the relevant schemes requires more than 350 ms.

Table 3
Communication time for different schemes.

Schemes	Single EV user verification (bits)	'***n***' EV user verification (bits)
Chen et al.	2848	2848*n*
Mahmood et al.	1792	1792*n*
Li et al.	2752	2752*n*
Khan et al.	1184	1184*n*
Proposed work	992	992*n*

6.2. Communication cost

Communication cost refers to the number of bits required for the transfer of information between the end users. In our suggested framework, when the EV user moves from one location to another location, the confidential information regarding the EV user is transferred by the current *CS* to the subsequent *CS*. Here, the re-authentication of EV user is completely avoided by the subsequent *CS*. During the exchange of data, the output of the hash function is 160 bits, the timestamp requires 32 bits, information, signature and the dummy identities which belongs to Z_a^* consumes 160 bits. Therefore, the total communication cost is computed as 992 bits. The suggested scheme communication cost is compared with the prevailing existing schemes like Chen et al. (Chen et al., 2017), Mahmood et al. (Mahmood et al., 2018), Li et al. (Li et al., 2019) and Khan et al. (Khan et al., 2020b) respectively as shown in Table 3. Fig. 5 portrays the graphical depiction of communication analysis for different schemes. In our suggested work, blockchain technology is used for storing the information of EV. So, there is no possibility for an intruder to hack the data and modify it. Since, if any modification or alteration in the data affects the block in the blockchain. As all the blocks are interconnected, the modification will subsequently affects all the blocks in the blockchain. As a results, hacking can be easily identified. Moreover, the proposed scheme involves only simple cryptographic addition and Xor operation which consumes less computational time. Further, during the exchange of information, the communication overhead is only 992 bits. Thus our proposed algorithm has good performance over other schemes.

6.3. Security assessment

The security strength of our suggested scheme is analysed in this section. Table 4 shows the security strength of different prevailing related schemes with our suggested scheme. From the table, it is clear that our proposed scheme can provide complete security strength against different security parameters, when compared to the existing frameworks like Chen et al. (Chen et al., 2017), Mahmood et al. (Mahmood et al., 2018), Li et al. (Li et al., 2019) and Khan et al. (Khan et al., 2020b) respectively. Moreover, the symbol '$\surd$' indicates that the particular scheme can resist specific security aspects and the symbol '$\times$' indicates that the particular scheme cannot resist against specific security aspects.

6.4. CS Serving ratio

CS serving ratio represents the service providing capability of the *CS* to the EV user. When number of EV users reaches the particular *CS*, the *CS* should have the capability to provide the required service the EV user. For instance, if $\mathbb{N}$ be the number of authenticated EV user arriving at the particular *CS* and p be the probability of the service provided by the *CS* to the EV users. The

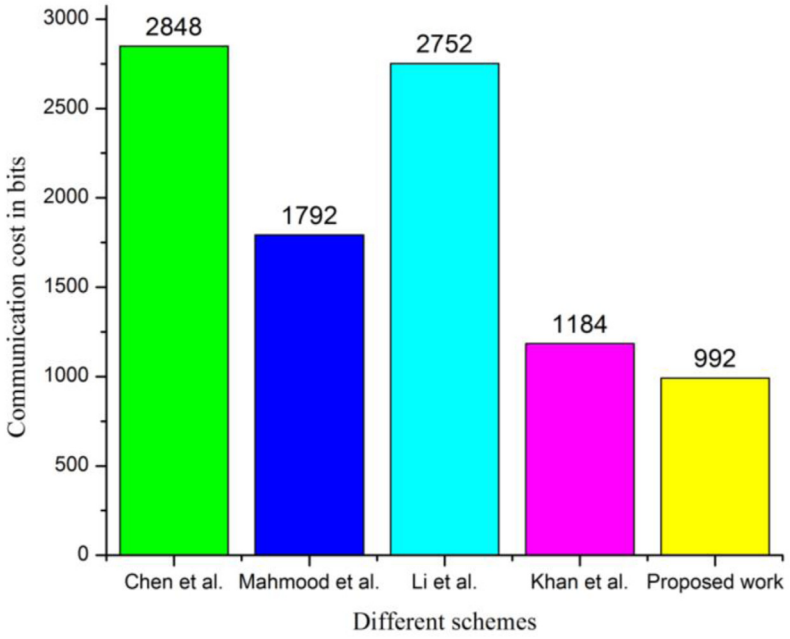

Fig. 5. Communication cost for different schemes.

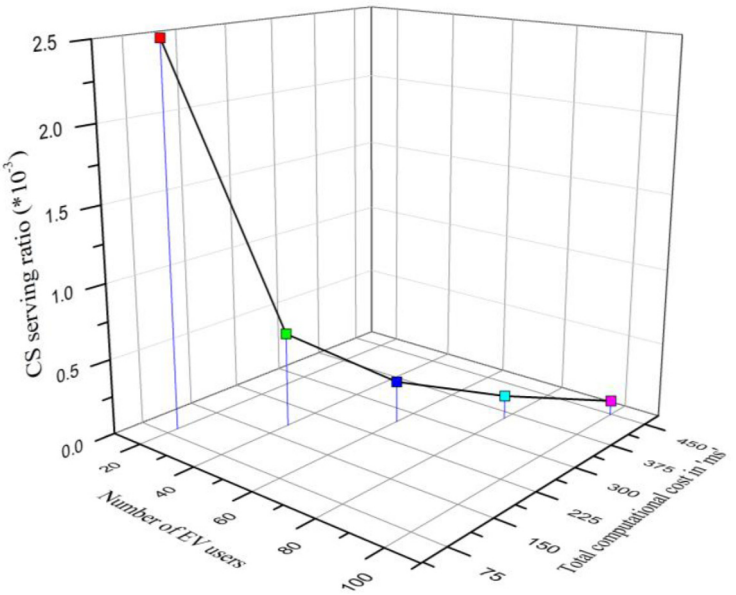

Fig. 6. *CS* serving ratio.

Table 4
Security aspects for different schemes.

Security features	Different schemes				
	[]	[]	[]	[]	Proposed
Anonymity	√	×	×	√	√
Authentication	×	√	√	√	√
Confidentiality	×	√	×	×	√
Data integrity	×	√	√	√	√
Privacy preservation	×	×	√	√	√
Impersonation	×	×	√	√	√
Non-repudiation	√	√	×	√	√
Replay attack	×	×	×	√	√
Transfer authentication	×	×	×	×	√
Revocation	×	×	×	×	√

verification time required for authenticating a single EV user is computed as $\Im_{tot} = 2ET_m + ET_a + 2ET_{xor} = 4.482$ ms. Therefore, the serving ratio for authenticating $\mathbb{N}$ number of EV is given by $CS_{ser} = \frac{p}{\mathbb{N} * \Im_{tot} * \mathbb{N}}$. Fig. 6 portrays the graphical representation of *CS* serving ratio. From the figure, it clearly indicates, as the number of EV users increases at the particular *CS*, the computational time increases with the decrease in the serving ratio.

7. Conclusion

Initially, anonymous authentication of EV user and CS is suggested in this manuscript. Blockchain technology is used to authenticate the EV user without the involvement of FTE. As a result, re-authentication of the EV user is completely avoided. Moreover, the confidential information of the EV user is transferred from current CS to the subsequent CS based on transfer mechanism. Thus, the computational cost is greatly reduced. The signature and timestamp contribute to the integrity and resistance to reply attacks. In addition, the security section describes the resistance of our scheme against well-known possible attacks. Lastly, the performance is assessed in terms of computational time, communication bits, security parameters and CS serving ratio. Future research could include batch authentication integrated with artificial intelligence to achieve low computational cost. Furthermore, security problems pertaining to 6G and edge computing will be addressed in the future. In addition, future study will focus on an identity-based verification mechanism for a group of *EV* users, message delay, and message transmission failure.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

Abbasinezhad-Mood, D., Nikooghadam, M., 2018. Efficient design and hardware implementation of a secure communication scheme for smart grid. Int. J. Commun. Syst. 31 (10), http://dx.doi.org/10.1002/dac.3575.

Abbasinezhad-Mood, D. Dariush, Ostad-Sharif, A., Nikooghadam, M., 2020. Novel anonymous key establishment protocol for isolated smart meters. IEEE Trans. Ind. Electron. 67 (4), 2844–2851. http://dx.doi.org/10.1109/tie.2019.2912789.

Aggarwal, S., Kumar, N., 2021. A consortium blockchain-based energy trading for demand response management in vehicle-to-grid. IEEE Trans. Veh. Technol. 70 (9), 9480–9494. http://dx.doi.org/10.1109/tvt.2021.3100681.

Anon, https://www.cygwin.com/install.html. (Accessed 3 December 2021).

Antunez, C. Sabillon, Franco, J.F., Rider, M.J., Romero, R., 2016. A new methodology for the optimal charging coordination of electric vehicles considering vehicle-to-grid technology. IEEE Trans. Sustain. Energy 7 (2), 596–607. http://dx.doi.org/10.1109/tste.2015.2505502.

Arasan, A., Sadaiyandi, R., Al-Turjman, F., Rajasekaran, A.S., Karuppuswamy, K.Selvi., 2021. Computationally efficient and secure anonymous authentication scheme for cloud users. Pers. Ubiquitous Comput. 25, http://dx.doi.org/10.1007/s00779-021-01566-9.

Chen, Y., Martínez, J.-F., Castillejo, P., López, L., 2017. An anonymous authentication and key establish scheme for smart grid: Fauth. Energies 10 (9), 1354. http://dx.doi.org/10.3390/en10091354.

Das, S., Acharjee, P., Bhattacharya, A., 2021. Charging scheduling of electric vehicle incorporating grid-to-vehicle and vehicle-to-grid technology considering in smart grid. IEEE Trans. Ind. Appl. 57 (2), 1688–1702. http://dx.doi.org/10.1109/tia.2020.3041808.

Hassija, V., Chamola, V., Garg, S., Krishna, D.N., Kaddoum, G., Jayakody, D.N., 2020. A blockchain-based framework for lightweight data sharing and energy trading in V2G network. IEEE Trans. Veh. Technol. 69 (6), 5799–5812. http://dx.doi.org/10.1109/tvt.2020.2967052.

Iqbal, A., Rajasekaran, A.S., Nikhil, G.S., Azees, M., 2021. A secure and decentralized blockchain based EV energy trading model using smart contract in V2G network. IEEE Access 9, 75761–75777. http://dx.doi.org/10.1109/access.2021.3081506.

Iqbal, S., Xin, A., Jan, M.U., Abdelbaky, M.A., Rehman, H.U., Salman, S., Rizvi, S.A., Aurangzeb, M., 2020. Aggregation of evs for primary frequency control of an industrial microgrid by implementing GRID regulation & charger controller. IEEE Access 8, 141977–141989. http://dx.doi.org/10.1109/access.2020.3013762.

Irshad, A., Usman, M., Chaudhry, S. Ashraf, Naqvi, H., Shafiq, M., 2020. A provably secure and efficient authenticated key agreement scheme for energy internet based vehicle-to-grid technology framework. IEEE Trans. Ind. Appl. 1. http://dx.doi.org/10.1109/tia.2020.2966160.

Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., Hossain, E., 2017. Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. IEEE Trans. Ind. Inf. 13 (6), 3154–3164.

Khan, A.A., Kumar, V., Ahmad, M., Rana, S., Mishra, D., 2020a. Palk: Password-based anonymous lightweight key agreement framework for smart grid. Int. J. Electr. Power Energy Syst. 121, 106121. http://dx.doi.org/10.1016/j.ijepes.2020.106121.

Khan, A.A., Kumar, V., Ahmad, M., Rana, S., Mishra, D., 2020b. Palk: Password-based anonymous lightweight key agreement framework for smart grid. Int. J. Electr. Power Energy Syst. 121, 106121. http://dx.doi.org/10.1016/j.ijepes.2020.106121.

Lam, A.Y., Leung, K.-C., Li, V.O., 2016. Capacity estimation for vehicle-to-grid frequency regulation services with smart charging mechanism. IEEE Trans. Smart Grid 7 (1), 156–166. http://dx.doi.org/10.1109/tsg.2015.2436901.

Li, X., Wu, F., Kumari, S., Xu, L., Sangaiah, A.K., Choo, K.-K.R., 2019. A provably secure and anonymous message authentication scheme for smart grids. J. Parallel Distrib. Comput. 132, 242–249. http://dx.doi.org/10.1016/j.jpdc.2017.11.008.

Liu, X., Zhang, Y., Wang, B., Wang, H., 2013. An anonymous data aggregation scheme for smart grid systems. Secur. Commun. Netw. 7 (3), 602–610. http://dx.doi.org/10.1002/sec.761.

Luo, J., Yao, S., Zhang, J., Xu, W., He, Y., Zhang, M., 2020. A secure and anonymous communication scheme for charging information in vehicle-to-grid. IEEE Access 8, 126733–126742. http://dx.doi.org/10.1109/access.2020.3005400.

Mahmood, K., Chaudhry, S.A., Naqvi, H., Kumari, S., Li, X., Sangaiah, A.K., 2018. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. Future Gener. Comput. Syst. 81, 557–565. http://dx.doi.org/10.1016/j.future.2017.05.002.

Rajasekaran, A.S., Azees, M., Al-Turjman, F., 2022a. A comprehensive survey on security issues in vehicle-to-grid networks. J. Control Decis. 1–10. http://dx.doi.org/10.1080/23307706.2021.2021113.

Rajasekaran, A.S., Maria, A., Al-Turjman, F., Altrjman, C., Mostarda, L., 2022b. Anonymous mutual and batch authentication with location privacy of UAV in FANET. In: Drones. Vol. 6. p. 14. http://dx.doi.org/10.3390/drones6010014.

Subramani, J., Azees, M., Sekar, A., Al-Turjman, F., 2021a. Lightweight privacy and confidentiality preserving anonymous authentication scheme for WBANs. IEEE Trans. Ind. Inf. http://dx.doi.org/10.1109/TII.2021.3097759, (Early access).

Subramani, J., Nguyen, T.N., Maria, A., Rajasekaran, A.S., Cengiz, K., 2021b. Lightweight batch authentication and privacy-preserving scheme for online education system. Comput. Electr. Eng. 96, 107532. http://dx.doi.org/10.1016/j.compeleceng.2021.107532.

Wan, Z., Zhu, W.T., Wang, G., 2016. PRAC: Efficient privacy protection for vehicle-to-grid communications in the smart grid. Comput. Secur. 62, 246–256.

Wang, L., Madawala, U.K., Wong, M.-C., 2021. A wireless vehicle-to-grid-to-home power interface with an adaptive DC link. IEEE J. Emerg. Sel. Top. Power Electron. 9 (2), 2373–2383. http://dx.doi.org/10.1109/jestpe.2020.2992776.

Wang, H., Wang, Q., He, D., Li, Q., Liu, Z., 2019. BBARS: Blockchain-based anonymous rewarding scheme for V2G networks. IEEE Internet Things J. 6 (2), 3676–3687. http://dx.doi.org/10.1109/jiot.2018.2890213.