
Article:
Aggarwal, S., Kumar, N. and Gope, P. orcid.org/0000-0003-2786-0273 (2021) An efficient blockchain-based authentication scheme for energy-trading in V2G networks. IEEE Transactions on Industrial Informatics, 17 (10). pp. 6971-6980. ISSN 1551-3203

https://doi.org/10.1109/tii.2020.3030949

An Efficient Blockchain-based Authentication Scheme for Energy-Trading in V2G Networks

Shubhani Aggarwal, Neeraj Kumar, *Senior Member, IEEE*, and Prosanta Gope, *Senior Member, IEEE*

***Abstract*—Vehicle-to-Grid (V2G) networks have been emerged as a new technology in the smart grid (SG). These networks allow a two-way flow of energy-trading between electric vehicles (EVs) and charging stations (CSs) in the SG. EVs are regarded as one of the most effective tools to reduce energy demands. It will bring a great impact on our society and human life. Thus, during energy-trading between EVs and CSs, various security and privacy challenges occur in V2G networks. Although several proposals have been proposed, still there are many issues like lack of integrity, mutual authentication, identity privacy-preservation makes the system more vulnerable. Researchers have used the centralized system in V2G networks which may act as a single point of failure. So, for deploying secure V2G networks in the SG, we propose an energy-trading scheme having blockchain between three communicating parties, *i.e.*, EVs, CSs, utility center (UC). The proposed system is divided into three phases, (1) the registration process provides identity privacy-preservation to the EVs and CSs (2) the searching process makes the registration and key-generation steps faster, and (3) the authentication process provides mutual authentication between them and a blockchain network is used to execute transactions using Merkle Root Hash (MRH). The security analysis result shows that the proposed scheme is secure for energy-trading in V2G networks. The performance evaluation results illustrate that our scheme has less communication cost and computation time as compared to the existing proposals.**

***Index Terms*—Vehicle-to-Grid, Smart Grid, Blockchain, Mutual Authentication, Merkle Root Hash, Electric Vehicles, Charging Stations.**

I. Introduction

WITH the fast development and growth of Information and Communication Technologies (ICT), smart grid (SG) is gaining wide popularity from the past few years [1]. It is widely used for an efficient and smart transmission system. It consists of all type of operational and energy measures such as- smart meters, smart appliances, advanced metering infrastructure (AMI), renewable energy resources, *etc*. It can enhance the scalability of the power grid using intelligent energy management. From the wireless mesh networks in the SG [2], vehicle-to-grid (V2G) has developed and evolved as an important network. As an automated energy network, it uses the two-way flow of electrical energy between electric vehicles (EVs) and charging stations (CSs). The benefit of this network is to generate, distribute, transmit the energy and can interact with the SG for demand response management, energy-trading, and dynamic pricing.

S. Aggarwal, N. Kumar are with the Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, India, Patiala, 147004 and P. Gope is with Department of Computer Science, University of Sheffield, United Kingdom , e-mail: (shubhaniaggarwal529@gmail.com, neeraj.kumar@thapar.edu, and p.gope@sheffield.ac.uk).

From the above-mentioned discussion, energy-trading is one of the major problems in V2G networks. It is a mechanism that uses charging/discharging operations across EVs and other V2G entities to regulate and manage the demand response [3]. However, due to the cooperation of network communications, charging and discharging operations, and vehicle mobility, EVs can face many privacy and security risks. Thus, they may not be active for participating in energy trade-offs but, they play a major role in energy management. So, to encourage EVs, it is needed to design a reliable, secure, and efficient mechanism for energy-trading in V2G networks. The pictorial representation of energy-trading in V2G networks as shown in Fig 1.

Traditionally, there is a number of protocols, for example,

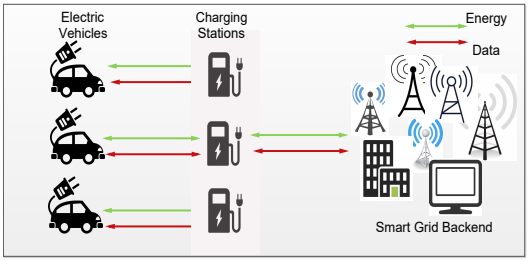

Fig. 1: Energy Trading in Vehicle-to-Grid environment

ISO/IEC/IEEE 18880 standard protocol that defines communication architecture in the SG. It also defines the network infrastructure and data exchange protocols to integrate the various components, data information, data storage, application services, *etc*. These standard protocols are used for communication in a wide area network (WAN) using transmission control protocol/Internet protocol (TCP/IP). But, it has some security and network management issues that can be solved by other protocols such as- ISO/IEC/IEEE 18881 and ISO/IEC/IEEE 18883. These protocols are non-TCP/IP that connects with the multiple Gateways. Earlier, in V2G networks, IEC 15118 and open charge point protocol (OCPP) have been used for communication between the EVs, CSs and the management system [4]. But recently, there is a number of cryptographic methods and functions that have been used for energy-trading in V2G networks. For example, in [5], authors proposed a secure authenticated key-agreement scheme for SG. They have provided the various security services that include session-key security and smart meter privacy under the Canetti-Krawczyk adversary model. Similarly, in [6], authors proposed a lightweight key-agreement scheme based on elliptical curve cryptography (ECC). In the same way, Gope and Sikdar [7]

proposed a key-agreement scheme that provides privacy and security to smart meters and service providers. Abdallah and Shel [8] presented a lightweight V2G connection scheme that provides security and privacy-preserving to the power grid. They have also provided confidentiality and integrity to the EVs during the exchange of information. Similarly, the authors in [9] presented an authentication scheme to provide trust, integrity, and anonymity to the smart meters. Shen *et al.* [10] proposed a protocol based on mutual authentication using hash and bitwise EX-OR functions. Bansal *et al.* [11] proposed a lightweight, secure, and privacy-preserving based secure user key-exchange authentication protocol for V2G systems, which uses a two-step mutual authentication between an EV and the grid server.

From the above-mentioned survey, we observe that cyber security and privacy of the V2G components and data are major concern [12]. The various security attacks and privacy issues like EVs identity, eavesdropping, man-in-the-middle (mitm) attack, replay attack, impersonation attack, *etc.* are still present in V2G networks. Thus, there are several challenges present for designing a secure and efficient mechanism for V2G networks in the SG. For their security solutions, advancements and development of V2G networks and large number of organizations are working on energy-trading in the SG [13], [14]. For example, Hassija *et al.* [15] proposed a lightweight blockchain-based protocol, which is called a directed acyclic graph-based in the V2G network. They have used game theory to perform negotiation between the grid and vehicles at an optimized cost. Their proposed model is highly scalable and supports the micro-transactions required in V2G networks. In the same way, the authors in [16] proposed a blockchain-based energy transaction model for EVs in V2G network, which enables peer-to-peer (P2P) energy transactions between EVs and power grid without need of trusted third party. However, with the development of EVs, smart grid, and V2G, the existing energy sector started shifting towards distributed and decentralized solutions. Moreover, security and privacy issues because of centralization is another major concern in V2G networks. In this context, Blockchain technology with the features of automation, immutability, public ledger facility, irreversibility, decentralization, consensus, and security has been adopted that motivates for solving the prevailing problems like identity privacy-preservation, entity authentication for energy trading in V2G networks.

A. Contributions

In this paper, firstly, we introduce the blockchain-based system model in V2G networks. Subsequently, we present a registration, searching, and authentication process between EVs, CSs, and Utility Center (UC) for V2G networks in the SG. The key contributions of this paper are as follows.

- We present an effective blockchain-based system model for secure and anonymous energy trading in V2G networks. Here, blockchain's distributed ledger is employed for transaction execution in distributed V2G environments while digital signatures are used for mutual authentication.
- The mutual authentication mechanism has been designed to preserve the identity of EVs and CSs and support mutual authentication between the EVs, CSs, and UC. Additionally, it also supports minimal communicational and computational overheads on resource-constrained EVs.
- We presented security and performance analysis of our proposed system model, which shows our authentication scheme is secure with less computation time and communication cost as compared to the existing proposals. We also justify the performance of the proposed scheme on the widely acceptable AVISPA tool.

B. Organization

The rest of the paper is organized with the following sequence. Section II describes the related work in V2G networks. Section III represents the system model. The description of the proposed scheme is presented in Section IV. The security and performance analysis of the proposed scheme is done in Section V. Section VI concludes the paper.

II. Related Work

Secure communication is one of the important concern in V2G networks for exchanging of energy and data. So, for security and privacy in the communication of V2G components, high performance and security protocols are required. To address these issues, many research proposals have been proposed based on authentication protocols and key establishment protocols. For example, Gope and Sikdar [17] proposed an efficient privacy-preserving authentication scheme for energy Internet-based V2G communication. Similarly, Mohammadali *et al.* [18] proposed an identity-based two key establishment protocols that employs ECC. These protocols have been used to reduce the computational overhead on AMI. In the same way, authors in [19] proposed two key-exchange protocols based on ECC and symmetric key algorithms. Wu and Zhou [20] proposed a management scheme that combines the symmetric key technique and ECC-based public key technique. These techniques are based on Needham Schroeder authentication protocol that eliminates replay and mitm attacks. Similarly, Xia and Wang [21] proposed an efficient key distribution protocol that eliminates the mitm attack and ensures security in V2G networks. Park *et al.* [22] presented a key-generation and key-distribution scheme which is not secure from impersonation attacks. With this issue, it does not address the customer's privacy requirements. So, to improve these issues, Tsai *et al.* [23] represented a combined identity-based signature and identity-based encryption scheme for key-distribution in the SG. But these schemes do not guarantee the security and privacy of the session-key and smart meter. In [24]–[26], authors proposed an authentication protocol and privacy-preserving scheme that ensures the communication in V2G networks. In this paper [24], the authors show that their authentication scheme provides less delay, less computational cost, and less communication traffic.

Despite having several cryptographic solutions, V2G communication faces privacy and security issues. Moreover, these

solutions give high communication and computation cost, lack of anonymity, and rely on a centralized system which may act as a single point of failure [27]. So, to remove these problems in V2G networks, an emerging and distributed technology called *"Blockchain"* has been used. It is a P2P technology in which cryptographically secured blocks are combined to form a chain in a verifiable and manageable manner. It provides high integrity, security, and reliability to the system by adopting multiple methods such as- data encryption, consensus agreement, time-stamping. It improves the problem of high costs, data storage, and data inefficiency that are commonly present in traditional centralized systems. In this context, many authors used this technology to solve the problems of security and privacy in V2G networks. For example, in [28], authors proposed a privacy-preserving and data aggregation scheme based on blockchain for secure SG environment. They have adopted the Bloom filter for fast authentication. Similarly, Wang *et al.* [29] proposed a blockchain-based anonymous rewarding scheme for V2G networks. They have used the public-key cryptosystem for security and performance analysis. In the same way, Li *et al.* [30] proposed a consortium blockchain-based solution in Industrial Internet of Things (IIoT) for secure energy-trading. They have also proposed the payment scheme based on a credit system using Stackelberg game theory for optimal pricing. Similarly, Kang *et al.* [31] proposed this technology to improve transaction security and privacy protection in energy-trading among Plug-in Hybrid Vehicles (PHEVs).

From the literature survey, we observed that most of the researchers have used the authentication schemes, which is based on blockchain technology for energy-trading in V2G networks. But still, these schemes do not ensure identity privacy-preservation and mutual authentication among communicating parties such as- EVs, CSs and the management system. So, in this paper, we propose a blockchain-based secure energy-trading scheme that provides identity privacy-preservation and mutual authentication in V2G networks. The relative comparison of the existing proposals is as shown in Table I.

TABLE I: Relative comparison of the existing proposals

Reference	Primitive used	1	2	3	4
Odelu *et al.* [5]	Bilinear, Hash function	✓	✓	x	✓
Shen *et al.* [10]	Hash function, Bitwise EX-OR	✓	✓	✓	✓
Gope and Sikdar [17]	Hash and EX-OR function	✓	✓	✓	✓
Mohammadali *et al.* [18]	ECC, Bilinear pairing	✓	✓	x	x
Nicanfar *et al.* [19]	ECC, Bilinear pairing	x	x	x	x
Wu and Jhou [20]	Bilinear pairing	x	✓	x	x
Xia and Wang [21]	AES-CBL, Hash function	x	x	x	x
Park *et al.* [22]	Bilinear pairing, Hash function	x	x	x	x
Tsai *et al.* [23]	Bilinear pairing, Hash function	✓	✓	x	x
Guan *et al.* [28]	Blockchain	✓	x	x	x
Wang *et al.* [29]	Blockchain, Public-key cryptography	✓	x	x	x
Li *et al.* [30]	Blockchain	✓	x	x	x
Kang *et al.* [31]	Blockchain	✓	x	x	x
IEC15118 scheme	ECDSA	x	x	x	x
OCPP scheme	ECDSA	x	x	x	x
Proposed Scheme	Blockchain, Hash function	✓	✓	✓	✓

1: Identity-Privacy of the EVs; 2: Protection against Eavesdropper; 3: Protection against Replay attack; 4: Protection against Impersonation attack; ✓: considered; x: not considered

III. System Model

This section describes the high-level view of V2G networks with different components such as- EVs, CSs, and UC. These components help in making and maintaining the global distributed ledger in the blockchain network. Fig 2. shows that the systematic model of the proposed scheme with different entities. The brief description of these entities is as follows.

- **Electric Vehicles:** EVs with bidirectional energy-trading capabilities that helps in maintaining the stability of the SG. They can act as energy producers by discharging their battery during peak time. They can also act as energy consumers by charging their battery during off-peak time. They charge or discharge their battery at particular CSs that can be available at the UC level. Hence, the blockchain network provides incentives to the EVs for participating in the regulatory and managing process.
- **Charging Stations:** CSs are equipped with sufficient communicational and computational resources for the EVs. They are also equipped with smart meters. These meters are used to keep track of the energy stored or energy withdrawn from the CSs. They store the current electricity consumption bills. They also keep track of the rewards that need to be given to the EVs for participating in the regulatory process. They are also responsible for generating transactions between the EVs and CSs.
- **Utility Center:** UC is the central authority which is being used to validate the transactions created by the CS and maintains in the blockchain network. With this, it is used to take responsibility for registering the legal and illegal identities of EVs and CSs. It is also responsible to take care of all the transactions that are being created between EVs and CSs. At this level, registration, searching and authentication process between EVs and CSs are done over the secure channel.
- **Blockchain Network:** Blockchain network is used to verify the transactions that are being generated by the UC between EVs and CSs. It also helps in sending the rewards to the EVs in an anonymous and secure manner.

In the proposed V2G energy-trading process as shown in Fig. 2, the step 1 defines the initialization, which is used to initialize the system where UC releases the public parameters to implement the cryptographic hash functions. In the next step 2, EVs and CSs register their identities with a key pointer at the UC level. The key pointers of EVs and CSs return

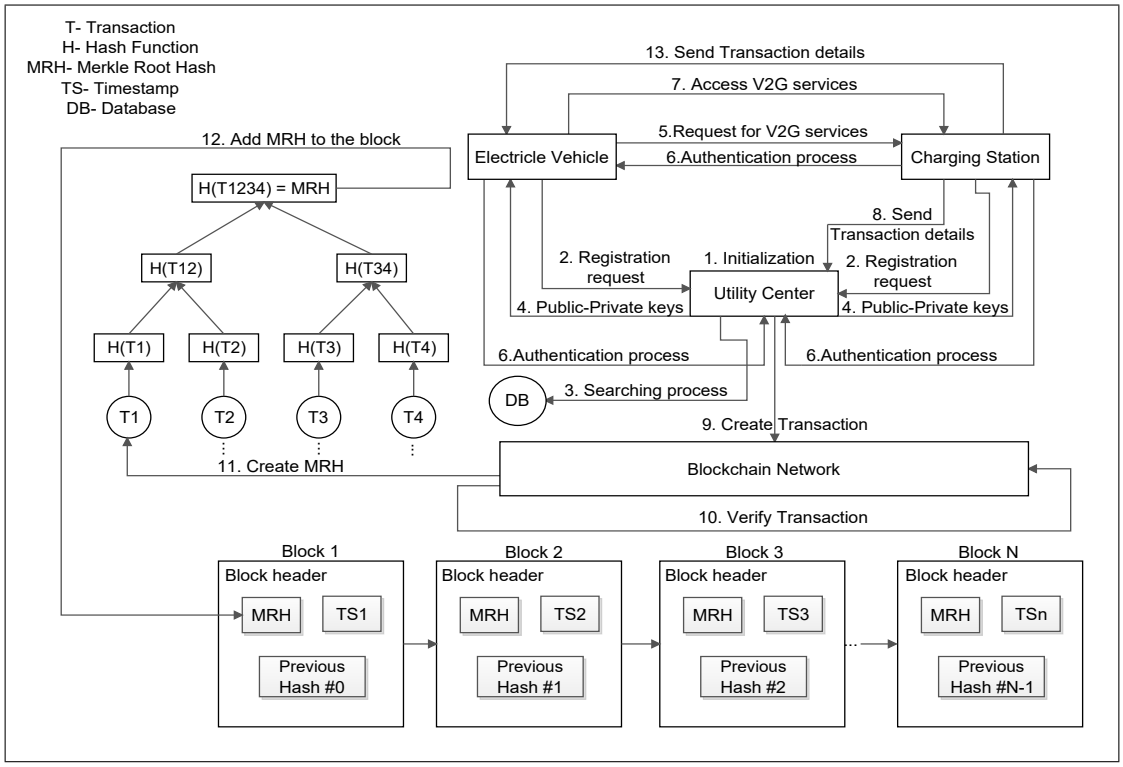

Fig. 2: System model

the pointer to an entity if these are present at the UC level, else it returns no value. In step 3, after successful searching of these entities in the database, UC generates the public-private key pairs for EVs, CSs and itself for identity privacy-preservation in step 4. In step 5, for secure energy-trading in V2G networks, CSs accepts the service request of EVs and to participate in post successful authentication process among these three communicating parties as defined in step 6. Once the authentication process completes, in step 7 CSs provide V2G services to the EVs and generates the corresponding rewards. In step 8, the transaction details are transferred to the UC, which further transmits these to the blockchain network for creating a valid transaction in step 9. Then, the blockchain network verifies the transaction using MRH and writes it into the distributed ledgers of the blockchain as defined in step 10, 11, and 12. At the end in step 13, with the help of Proof-of-Work (PoW) consensus among three communicating parties, the rewards are transferred to the designated EVs and a receipt is sent to the EVs by the CSs.

A. Adversary Model

During EVs and CSs registration, both EVs and CSs interact with UC through a secure channel. On the other hand, in the proposed authentication process, all three parties communicate through an insecure channel. In this context, we consider the Dolev-Yao threat model (DY model) [32], where an adversary may eavesdrop, modify, or change the messages exchanged during transmission. Now, due to the usage of public networks and wireless communication in blockchain-based V2G networks, there is a possibility of several attacks, such as- impersonation attack, man-in-the-middle, replay attacks, *etc*. Therefore, the privacy of EVs and CSs are another important concern in V2G networks. Hence, there is a need for an authentication process by which the legitimacy of the entities can be verified, and also both can establish a secure energy-trading in V2G networks.

IV. Proposed Scheme

The proposed system model based on blockchain technology is classified into three phases. (1) the registration process involves the identity privacy-preservation of EVs and CSs (2) the searching process having B+ tree for fast key-generation and registration steps, and (3) the authentication process involves the mutual authentication between EVs and CSs having UC. After the authentication between three communication parties, UC sent the transaction details to the blockchain network. After the successful verification and validation of the transaction using MRH, it is added to the blocks of the blockchain. The system is initialized by UC which prepares the V2G network for other phases. UC defines the public parameter for cryptographic hash function such as- SHA-1 (H()). The detailed information of the subsequent phases is as follows.

A. Registration Process

In this phase, the EVs and CSs are involved at the UC level over the secure channel. The process of registering the identification of EVs and CSs is indistinguishable that provides identity privacy-preservation to system model. This

process is done through hashing, *i.e.*, collision avoidance based one-way hash function such as- SHA-1 while digital signatures are used for mutual authentication. The step-wise functionalities of the registration process of EVs are as follows.

- EVs selects an identity (ID_{EV}) to uniquely present itself. It also generates the timestamp (TS_{EV}) and key pointer (KP_{EV}) for registering itself at the UC. Next, it computes the hash $H_2 = H(ID_{EV}||TS_{EV}||KP_{EV})$. Further, it computes the digital signatures (DS) with its private key (PK_{EV}) as $DS = PK_{EV}(H_2)$.
- Then, the DS and public key of EVs (PU_{EV}) is transmitted to the UC over the secure channel for identification.
- After receiving the hash value from EVs, the UC extracts all parameters from the hash such as- ID_{EV}, TS_{EV}, and KP_{EV} with the help of PU_{EV}. It validates the TS_{EV} of the EVs and proceeds further as it is within the range value.
- The UC verifies the presence of ID_{EV} in its database repository as described in the searching process. If the match is found, UC allocates the unique identity ID_{EV1} to the EVs, else terminate the connection.
- The UC accepts the EV's registration request and generates the key-pair on the basis of unique identity, *i.e.*, Private key (PK_{EV1}) and Public key (PU_{EV1}) for energy-trading.
- Next at the UC level, compute the hash for pseudo-identity of $EV1$ as $H_3 = H(PK_{EV1}||ID_{EV1})$ and transmitted it to the EVs with PK_{EV1} over the secure channel.
- Further, the UC stores the H_3 and PU_{EV1} values, while EVs stores the H_3 and PK_{EV1} values for secure energy-trading process in V2G networks.

Similarly, the step-wise functionalities of the registration process of CSs are as follows.

- CSs selects an identity (ID_{CS}) to uniquely present itself. It also generates the timestamp (TS_{CS}) and key pointer (KP_{CS})for registering itself at the UC. Next, it computes the hash $H_4 = H(ID_{CS}||TS_{CS}||KP_{CS})$. Further, it computes the digital signatures (DS1) with its private key (PK_{CS}) as $DS1 = PK_{CS}(H_4)$.
- Then, the $DS1$ and public key of CSs (PU_{CS}) is transmitted to the UC over the secure channel for identification.
- After receiving the hash value, the UC extracts the parameters of CSs such as- ID_{CS}, TS_{CS}, and KP_{CS} with the help PU_{CS}. Then, it validates the TS_{CS} and proceeds further as it is within the range value.
- The UC verifies the presence of ID_{CS} in its database repository as described in the searching process. If the match is found in the repository, UC allocates the unique identity ID_{CS1} to the CSs, else terminate the connection.
- The UC accepts the CS's registration request and generates the key-pair on the basis of unique identity, *i.e.*, Private key (PK_{CS1}) and Public key (PU_{CS1}) for energy-trading.
- Next at the UC level, compute the hash for pseudo-identity of $CS1$ as $H_5 = H(PK_{CS1}||ID_{CS1})$ and transmitted it to the CSs with PK_{CS1} over the secure channel.
- Then, the UC stores the H_5 and PU_{CS1} values, while CSs store the H_5 and PK_{CS1} values for secure energy-trading process in V2G networks.

In the same way, UC selects an identity ID_{UC} to uniquely present itself. Then, it generates the timestamp TS_{UC} and computes the hash $H_0 = H(ID_{UC}||TS_{UC})$ for identification. The step-wise description of above-mentioned registration process of EVs and CSs at the UC is described as shown in Fig 3.

To show the implementation of the registration process, we presented a case study on EVs for energy-trading in V2G networks. Researchers in [17], [33] presented a systematic review of existing blockchain-based solutions, particularly for energy-trading in V2G networks. From the study, we observed that EVs in India could represent Rs 500 billion opportunities by 2025 with the present and projected level of EV penetration as described in the report [34]. The proposed case study mainly focused on the EVs for energy-trading in V2G networks. To implement the above-mentioned use case, there is a need for a strong and reliable network that manages the energy-trading transactions. With the adoption of blockchain technology in V2G networks, the energy-trading transactions are secure, transparent, and immutable [35]. Hence, the proposed system model (Fig. 2) for energy-trading in V2G networks shows the registration and authentication process among EVs, CSs, and UC. The blockchain network maintains all energy-trading transactions and store it into the public ledgers of the network. In this model, we use permissionless or public blockchain, which gives a high level of transparency by providing a copy of the distributed ledger to each node, and the ability to perform consensus and validation of data. [36]. In addition, we have used PoW consensus mechanism having bitcoin to confirm transactions and produce new blocks to the chain. With this mechanism, EVs are responsible to complete energy-trading transactions on the network and gets rewarded. This mechanism is also used to securely sequence Bitcoin's transaction history while increasing the difficulty of altering data over time.

B. Searching Process

For searching an EVs and CSs identity at the UC level, the UC is used the B+ tree. It is a balanced tree in which every path from the root of the tree to a leaf is of the same length. Each non-leaf node of the B+ tree has between [n/2] and [n] children. During the searching process, no structure has been changed or rearranged in the B+ tree. So, just compare the key pointers of the EVs and CSs with the key pointers of the tree and give back the results to the UC at the UC level. UC compare the data of the EVs and CSs with the data present in the database repository of the tree. If the data matches, then EVs and CSs are marked as an authentic and represented with a unique identity by UC, else terminate the connection.

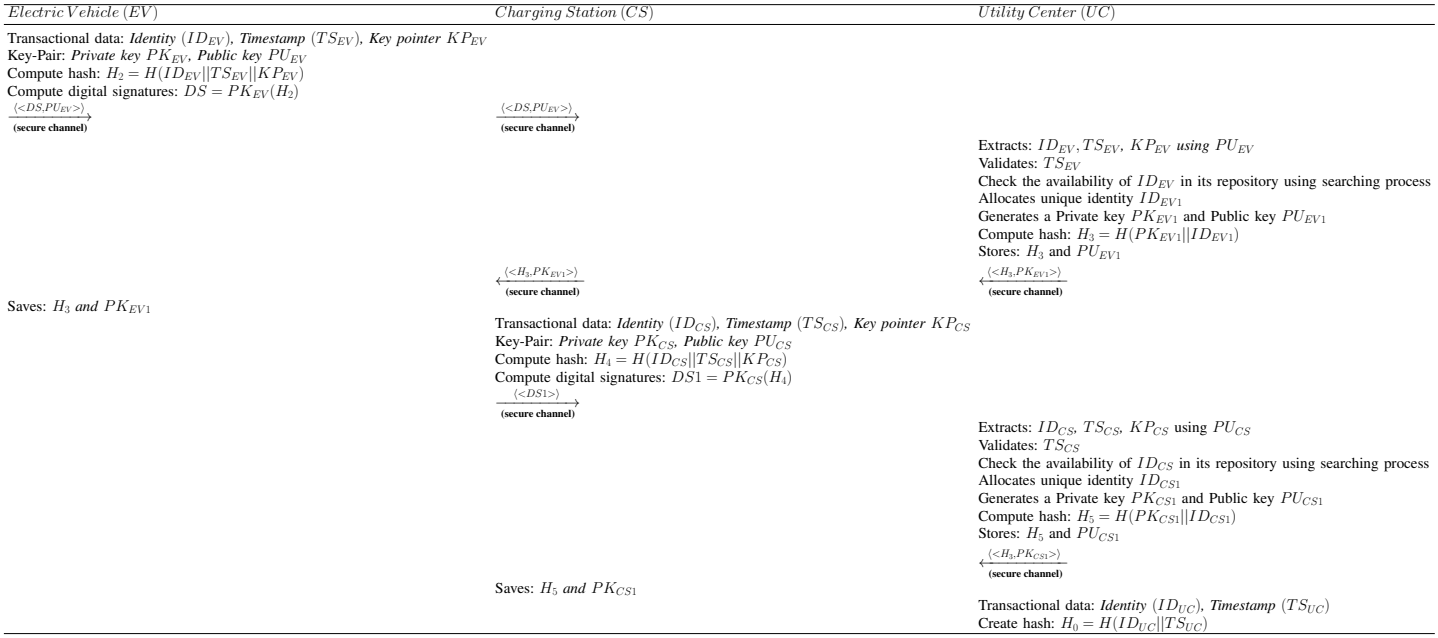

Fig. 3: Registration process

The main benefit of the B+ tree is that its searching time is much shorter than most of the other kind of trees like B-tree, red-black tree, *etc*. It fastens the key-generation and registration steps at the UC level. By using this process in the system model, the verification and validation automatically fast due to the fast searching in the database repository. For example, to search a data in one million key-values, a binary tree requires 20 block reads in contrast to B+ tree requires only 4 block reads. Hence, there is no need to check the balancing factor because it is inherently balanced. Instead of this, it is very easy to maintain and manipulate the data in the tree. But, when two values hash to the same array location then, there occurs a collision. There are two broad ways of collision resolution *i.e.,* separate chaining (an array of linked list implementation), and open addressing (array-based implementation such as- Linear probing, quadratic probing, and double hashing) as described in [37]. In the proposed model, we auume that there is no collision occurs to find an entity in the database. Here, UC finds the entities on first search if it is present in the database and represented as an authentic otherwise that entity is not present in the database.

C. Authentication Process

In this phase, the mutually authentication between EVs and CSs is done using UC before doing any transaction. The proposed authentication mechanism follows one-way hash function and append operation. The step-wise flow of the authentication process is as shown in Fig. 4 and their detail description is as follows.

- The phase is started from the CS level as the EVs connect to the CSs for charging or discharging their battery according to the demand response services. To start the process, $CS1$ (as computed in the registration process Fig. 3) generates the timestamp TS_1 and computes the hash message with its unique identity (H_5) is $M_1 = H(H_5||TS_1)$ and send this message to the $EV1$.
- To receive M_1 from the $CS1$, $EV1$ extracts the H_5 and TS_1 from M_1 and validates the TS_1 as it is in within the permissible range. After this, EVs itself generates the timestamp TS_2 for authentication and computes two hash values with its unique identity (H_3) (as computed in the registration process Fig. 3) for mutual authentication, *i.e.*, $Auth_{EV1-CS1} = H(H_3||H_5||TS_2||PK_{EV1})$ and $Auth_{EV1-UC} = H(H_3||H_0||TS_2||PK_{EV1})$.
- Finally, $EV1$ transmits the message $< M_2 >=< Auth_{EV1-CS1}, Auth_{EV1-UC}, H_3, TS_2 >$ to the $CS1$ at the CS level for authentication.
- The $CS1$ starts checking the authenticity of the $EV1$ by validating the TS_2. It computes the $Auth*_{EV1-CS1} = H(H_3||H_5||TS_2||PU_{EV1})$ and check that $Auth*_{EV-CS} = Auth_{EV1-CS1}$ is same or not. If same, $EV1$ is marked as an authentic, else terminate the connection.
- The $CS1$ continues do the authentication process and generates the timestamp TS_3 and hash value for authenticity, *i.e.*, $Auth_{CS1-UC} = H(H_5||H_0||TS_3||PK_{CS1})$. It transmits the message $< M_3 >=< Auth_{CS1-UC}, H_5, H_3, TS_2, TS_3 >$ to the UC at the UC level for mutual authentication.
- After receiving the message, the UC validates the timestamp TS_2, TS_3 and computes the authentication hash for $CS1$ and $EV1$, *i.e.*, $Auth*_{CS1-UC} = H(H_5||H_0||TS_3||PU_{CS1})$ and $Auth*_{EV1-UC} = H(H_3||H_0||TS_2||PU_{EV1})$. It checks that $Auth*_{CS1-UC} = Auth_{CS1-UC}$ and $Auth*_{EV1-UC} = Auth_{EV1-UC}$ are same or not. If same, $CS1$ and $EV1$ are marked as an authentic, else

terminate the connection.

- Now, the UC itself generates the timestamp TS_4 and computes the authentication hash as $Auth_{UC} = H(H_5||H_3||H_0||TS_4)$. It transmits the message $< M_4 >=< Auth_{UC}, TS_4 >$ to the $CS1$ at the CS level for authentication.
- The $CS1$ validates the timestamp TS_4 and compute the hash $Auth*_{UC}$= $H(H_0||H_3||H_5||TS_4||PU_{UC})$. It check s that $Auth*_{UC} = Auth_{UC}$ is equal or not. If same, UC is marked as an authentic, else terminate the connection. It generates the timestamp TS_5 and transmits the message $< M_5 >=< Auth_{UC}, TS_4, TS_5 >$ to the $EV1$ at the EV level.
- After receiving the message from $CS1$, $EV1$ validates the timestamp TS_4, TS_5 as it is in the permissible range value. It computes the hash $Auth*_{UC} = H(H_0||H_3||H_5||TS_4||TS_5||PU_{UC})$ and check that $Auth*_{UC} = Auth_{UC}$, If they are same, UC is marked as an authentic, else terminate the connection.
- In this way, $EV1$ and $CS1$ mutually validates the authenticity of UC.
  In this way, mutual authentication between three communicating parties, *i.e.,* EVs, CSs, and UC have been done.

D. Blockchain Network

The proposed secure and anonymous energy-trading scheme employs the advantages of MRH to maintain the global ledger. In the considered scenario, it is assumed that the CSs are equipped with sufficient computational and communicational resources. EVs can charge/discharge their batteries at particular CSs. UC creates a transaction between EVs and CSs. It also provides mutual authentication between three communicating parties. Here, the blockchain network is used for executing the transactions using MRH, which is the fundamental part of the blockchain technology. It is used to secure the verification and validation of the transaction content. It helps to make consistency in the nodes of the network. It is created by the repeated hashing pair of all the nodes until there is only one hash left at the end called MRH. It is binary in nature. Therefore, leaf nodes of the MRH are even in number. Each leaf node is a hash of the transactional data and each non-leaf node is a hash of its previous hashes. It summarizes all the transactions in a block by creating a hash of the entire set of transactions. It encodes the blockchain data efficiently and securely. It enables the quick verification of blockchain data, as well as the quick movement of large amounts of data from one node to the other on the P2P blockchain network. Due to the tree-like linkage of hashes, it contains all the information about every single transaction hash that exists on the block. It offers a single-point hash value that enables validating everything present on that block.

MRH maintains the integrity of the data in the tree. It is used in cryptocurrency to make sure data blocks passed between peers on a P2P network are whole, undamaged, and unaltered. If any single change in the input data, the output of the MRH also changes. For example, if an adversary can change the transaction details then, the MRH of that transaction also changes. So, it prevents the transaction from impersonation attack, modification of data, replay attack, *etc*. Moreover, it requires a very little memory as their proofs are computationally fast and easy. After computing the hash of the tree, it is added to the blocks of the blockchain as MRH. The block header of the blockchain contains previous hash and timestamp which will be combined with the MRH of all the transactions in the current block, called the *block*. This mechanism significantly reduces the levels of hashing to be performed, enabling faster verification and transactions. Then, after the verification and validation of the block, this block is added to the blockchain and the process still goes on. Then, the blockchain network gives some rewards to the EVs. This is done for the secure participation of the EVs in the regulatory and managing process.

V. Discussion

In this section, the security and performance analysis of the proposed system model is evaluated in terms of security analysis, communication cost and computation time. The blockchain-based authentication scheme supports mutual authentication of the EVs and CSs having UC and identity privacy-preservation of the EVs and CSs. Further, it also provides protection against replay attacks, impersonation attack, and eavesdropping. The detailed evaluation of the system model is discussed below.

A. Security Analysis

In this subsection, we represent the security analysis of our proposed system model. It shows that this model ensures the given security properties that are necessary for blockchain-based V2G networks in the SG.

- **Identity privacy-preservation of the EVs and CSs:** In the proposed system model, the EVs need to use a valid identity ID_{EV} for each new timestamp TS_{EV} which can never be reused. Except the UC, no one can recognize the privacy information and activity of the EVs. Therefore, changing the timestamp of the EVs in each session provides identity privacy-preservation to the EVs. It also ensures the EVs from intractability. Similarly, we provide the identity privacy-preservation to the CSs.
- **Protection against impersonation attack:** In the proposed system model, if an adversary tries to show as a legal EV then, it needs to send an authentication and valid message request $< M_{EV} = (ID_{EV}||TS_{EV}) >$ to the UC. On the other hand, if it tries to impersonate as a legitimate EVs then, it must know its own public-private key-pair (PU_{EV}, PK_{EV}). Without knowing these keys, it cannot generate a hash message $< Hash = H(PK_{EV}||TD_{EV}) >$. In V2G networks, if EVs can try to cheat by providing wrong or duplicate identity to the CSs and UC. Then, this model is able to find this by detecting the wrong identities of the EVs. Only the authenticated EVs will proceed to the registration and

Electric Vehicle (EV)	*Charging Station (CS)*	*Utility Center (UC)*
	Generate timestamp: TS_1 Compute message: $M_1 = (H_5 \| \| TS_1)$ $\xleftarrow{<M_1>}$	
Extracts: H_5, TS_1 Validate timestamp: TS_1 Generate timestamp: TS_2 Compute hash: $Auth_{EV1-CS1} = H(H_3 \| \| H_5 \| \| TS_2 \| \| PK_{EV1})$ Compute hash: $Auth_{EV1-UC} = H(H_3 \| \| H_0 \| \| TS_2 \| \| PK_{EV1})$ $\xrightarrow{<M_2>=<Auth_{EV1-CS1}, Auth_{EV1-UC}, H_3, TS_2>}$		
	Validate timestamp: TS_2 Compute hash: $Auth*_{EV1-CS1} = H(H_3 \| \| H_5 \| \| TS_2 \| \| PU_{EV1})$ Check: $Auth*_{EV1-CS1} = Auth_{EV1-CS1}$ If same, $EV1$ is marked authentic, else terminate the connection Generate timestamp: TS_3 Compute hash: $Auth_{CS1-UC} = H(H_5 \| \| H_0 \| \| TS_3 \| \| PK_{CS1})$ $\xrightarrow{<M_3>=<Auth_{CS1-UC}, Auth_{EV1-UC}, H_5, H_3, TS_2, TS_3>}$	
		Validate timestamp: TS_2, TS_3 Compute: $Auth*_{CS1-UC} = H(H_5 \| \| H_0 \| \| TS_3 \| \| PU_{CS1})$ Compute: $Auth*_{EV1-UC} = H(H_3 \| \| H_0 \| \| TS_2 \| \| PU_{EV1})$ Check: $Auth*_{CS1-UC} = Auth_{CS1-UC}$ Check: $Auth*_{EV1-UC} = Auth_{EV1-UC}$ If same, $CS1$ and $EV1$ are marked authentic, else terminate the connection Generate timestamp: TS_4 Compute: $Auth_{UC} = H(H_5 \| \| H_3 \| \| H_0 \| \| TS_4)$ $\xleftarrow{<M_4>=<Auth_{UC}, TS_4>}$
	Validate timestamp: TS_4 Compute hash: $Auth*_{UC} = H(H_0 \| \| H_3 \| \| H_5 \| \| TS_4 \| \| PU_{UC})$ Check: $Auth*_{UC} = Auth_{UC}$ If same, UC is marked authentic, else terminate the connection Generate timestamp: TS_5 $\xleftarrow{<M_5>=<Auth_{UC}, TS_4, TS_5>}$	
Validate timestamp: TS_4, TS_5 Compute: $Auth*_{UC} = H(H_0 \| \| H_3 \| \| H_5 \| \| TS_4 \| \| TS_5 \| \| PU_{UC})$ Check: $Auth*_{UC} = Auth_{UC}$ If same, UC is marked authentic, else terminate the connection		

Fig. 4: Authentication process

TABLE II: Relative comparison of the existing proposals

Level	**Registration Process**		**Authentication Process**	
	Communication Cost	Computation Time	Communication Cost	Computation Time
EVs level	$H_2 = H(128 + 32 + 32) = H(192) = 160bits$	$(2append + 1hash) = 3.7ms$	$[Auth_{EV1-CS1} = H(160 + 160 + 32 + 32) = 160bits]$ + $[Auth_{EV1-UC} = H(160 + 160 + 32 + 32) = 160bits]$ + $[Auth*_{UC} = H(160 + 160 + 160+32+32+32) = 160bits]$= $480bits$	$[(3append+1hash)+(3append+1hash)+(5append+1hash)] = 13.6ms$
CSs level	$H_4 = H(128 + 32 + 32) = H(192) = 160bits$	$(2append + 1hash) = 3.7ms$	$[Auth_{EV1-CS1} = H(160 + 160 + 32 + 32) = 160bits]$ + $[Auth_{CS1-UC} = H(160 + 160 + 32 + 32) = 160bits]$ + $[Auth*_{UC} = H(160 + 160 + 160 + 32 + 32) = 160bits]$= $480bits$	$[(3append+1hash)+(3append+1hash)+(4append+1hash)] = 13.1ms$
UC level	$H_3 + H_5 = H(64 + 128) + H(64 + 128) = 160 + 160 = 320bits$	$[(1hash + 1append) + (1hash + 1append)+(1hash+1append)] = 9.6ms$	$[Auth*_{CS1-UC} = H(160 + 160 + 32 + 32) = 160bits]$ + $[Auth_{UC} = H(160 + 160 + 160+32) = 160bits]$= $320bits$	$[(4append+1hash)+(4append+1hash)] = 9.4ms$
Total	$(160 + 160 + 320) = 640bits$	$(3.7 + 3.7 + 9.6) = 17ms$	$(480 + 480 + 320) = 1680bits$	$(13.6 + 13.1 + 9.4) = 36.1ms$

key-generation steps. In this way, our system model can ensure the security against impersonation attack.

- **Protection against replay attack:** In the proposed system model, an adversary cannot reuse the message $< M_{EV} = (ID_{EV} \| \| TS_{EV} \| \| KP_{EV}) >$ because of timestamp of the EVs changes in each session. Similarly, he/she cannot resend the hash message $< Hash = H(PK_{EV} \| \| TD_{EV}) >$ because it also changes with the session. These hash messages are generated on the basis of timestamp. So, every new hash message brings the new TS. In this way, our model ensures security against replay attacks.
- **Protection against eavesdropping:** In the proposed system model, EVs need to use an unique identity that can be allocated by the UC. This unique identity is valid only for a single session because of timestamp used in the model. Except the UC, no one can find the personal details of the EVs. So, changing the timestamp of the EVs in each session ensures the privacy and protection against eavesdropper. In this way, our proposed model provides security against eavesdropping.

TABLE III: Relative comparison of the existing proposals

Reference	Communication Cost in Authentication Process	Computation Time in Authentication Process
Odelu *et al.* [5]	2912 bits	15.32 seconds
Gope and Sikdar [17]	1802 bits	.88 seconds
Mohammadali *et al.* [18]	2340 bits	57.87 seconds
Nicanfar *et al.* [19]	2176 bits	63.77 seconds
Wu and Jhou [20]	4064 bits	57.88 seconds
Xia and Wang [21]	3296 bits	0.085 seconds
Tsai *et al.* [23]	6880 bits	23.22 seconds
Guan *et al.* [28]	-	1.5 seconds
Proposed Scheme	1680 bits	.0361 seconds

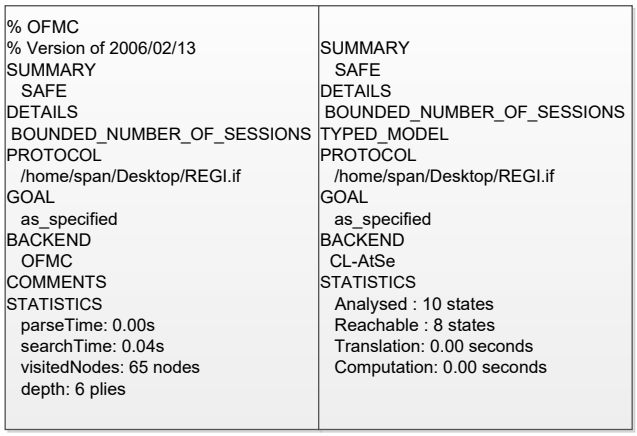

Fig. 5: Evaluation of mutual authentication on AVISPA

B. Performance Analysis

In this subsection, we represent the performance analysis of our proposed system model. Let us suppose that each identity of the three communicating parties EVs, CSs and UC is of 128 bits and the message digest of the SHA-1 (hash output) generated is of 160 bits. Using this, the communication cost of the registration and authentication process at three levels is shown in Table II. In computation time, we use the append operation and hash (SHA-1) function are used. The average time of these two is 0.5 ms and 2.7ms respectively. So, the computation time of the registration and authentication process at three levels is shown in Table II. The relative comparison of the communication cost and computation time in the authentication process with the existing proposals is as shown in Table III. From the table, we observed that our proposed authentication scheme has less communication cost and computation time as compared to the existing proposals. The reason is that our authentication scheme uses SHA-1 hash function and append operation that has a very less average time to process each block with respect to the other time-consuming operations like XOR, Bitwise EX-OR, *etc.* Hence, we conclude that our scheme can provide all the security properties and is suitable for V2G networks in the SG. In addition, The result of executing the transactions on AVISPA using OFMC and CL-AtSe back-ends which leads to the "SAFE" results as shown in Fig. 5. It provides a suite of applications to build and analyze the formal models of security protocols. These protocols have been written in the High-Level Protocol Specification Language (HLPSL). This tool is used to verify and validate the security attacks of any designed model by providing the AVISPA's back-ends. It also provide many solutions to remove the security attacks and flaws in the designed model.

With this, we analyze the computation and communication overhead across the three entities involved in the mutual authentication process. It is evident from the description given in Section IV that EVs, CSs, and UC participate in the authentication process for mutually authenticating each other. In the overall process, the considered entities incur computational and communicational expenses. The computational expenses incurred by the EVs, CSs, and UC could be attributed to the number of cryptographic hash operations performed in the overall process as shown in Fig. 6. On the other hand, the communication overhead is expressed in terms of the number of incoming tokens. The higher the number of incoming tokens, the higher is the communicational cost of an entity. The results are shown in Fig. refgraph, which indicates that the EVs experience the least communication overhead followed by CSs, and UC. Thus, it can be summarized that the mutual authentication mechanism not only guarantees enhanced security but also imposes less overhead on the battery-powered EVs.

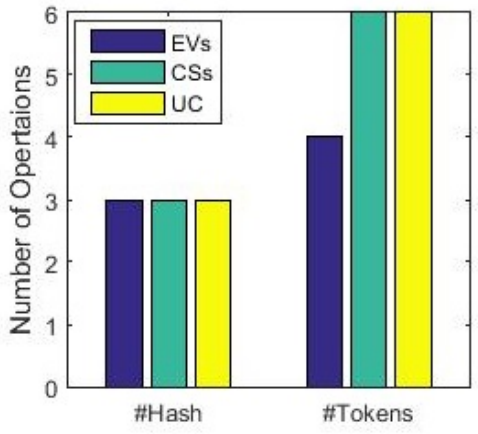

Fig. 6: Overhead analysis of mutual authentication process

VI. Conclusion

Secure and key-exchange communication in V2G networks is an important aspect. To aim at the problem of secure communication between EVs, CSs, and UC, this paper proposed a blockchain-based efficient authentication scheme in V2G networks. On the other hand, this scheme provides

identity privacy-preservation and mutual authentication between three communicating parties. In this order, a lightweight cryptographically one-way hash function has been considered. Further, the results obtained from the security evaluation shows that our proposed scheme is suitable for V2G networks. It also leads to reduce security attacks and an efficient model in terms of communication cost and computation time as compared to the existing proposals.

REFERENCES

[1] J. Rifkin, "The third industrial revolution," *Engineering & Technology*, vol. 3, no. 7, pp. 26–27, 2008.

[2] P. Guo, J. Wang, X. H. Geng, C. S. Kim, and J.-U. Kim, "A variable threshold-value authentication architecture for wireless mesh networks," *J.Internet Technol*, vol. 15, no. 6, pp. 929–935, 2014.

[3] K. Kaur, S. Garg, N. Kumar, and A. Y. Zomaya, "A game of incentives: An efficient demand response mechanism using fleet of electric vehicles," in *Proceedings of the 1st International Workshop on Future Industrial Communication Networks*. ACM, 2018, pp. 27–32.

[4] C. Alcaraz, J. Lopez, and S. Wolthusen, "Ocpp protocol: Security threats and challenges," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2452–2459, 2017.

[5] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1900–1910, 2018.

[6] F. Wu, L. Xu, X. Li, S. Kumari, M. Karuppiah, and M. S. Obaidat, "A lightweight and provably secure key agreement system for a smart grid with elliptic curve cryptography," *IEEE Systems Journal*, 2018.

[7] P. Gope and B. Sikdar, "Privacy-aware authenticated key agreement scheme for secure smart grid communication," *IEEE Transactions on Smart Grid*, 2018.

[8] A. Abdallah and X. S. Shen, "Lightweight authentication and privacy-preserving scheme for v2g connections," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2615–2629, 2017.

[9] P. Kumar, A. Gurtov, M. Sain, A. Martin, and P. H. Ha, "Lightweight authentication and key agreement for smart metering in smart energy networks," *IEEE Transactions on Smart Grid*, 2018.

[10] J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "Privacy-preserving and lightweight key agreement protocol for v2g in the social internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2526–2536, 2018.

[11] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani, "Lightweight mutual authentication protocol for v2g using physical unclonable function," *IEEE Transactions on Vehicular Technology*, 2020.

[12] A. S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, and Z. Y. Dong, "Cyber security framework for internet of things-based energy internet," *Future Generation Computer Systems*, vol. 93, pp. 849–859, 2019.

[13] J. Dong, "Towards an intelligent future energy grid," *School of Electrical & Information Engineering, The University of Sydney, New South Wales*, 2016.

[14] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "A survey on smart grid potential applications and communication requirements," *IEEE Transactions on industrial informatics*, vol. 9, no. 1, pp. 28–42, 2013.

[15] V. Hassija, V. Chamola, S. Garg, N. G. K. Dara, G. Kaddoum, and D. N. K. Jayakody, "A blockchain-based framework for lightweight data sharing and energy trading in v2g network," *IEEE Transactions on Vehicular Technology*, 2020.

[16] M. M. Islam, M. Shahjalal, M. K. Hasan, and Y. M. Jang, "Blockchain-based energy transaction model for electric vehicles in v2g network," in *2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*. IEEE, 2020, pp. 628–630.

[17] P. Gope and B. Sikdar, "An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication," *IEEE Transactions on Smart Grid*, 2019.

[18] A. Mohammadali, M. S. Haghighi, M. H. Tadayon, and A. Mohammadi-Nodooshan, "A novel identity-based key establishment method for advanced metering infrastructure in smart grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2834–2842, 2018.

[19] H. Nicanfar and V. C. 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.

[20] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 375–381, 2011.

[21] J. Xia and Y. Wang, "Secure key distribution for the smart grid," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1437–1443, 2012.

[22] J. H. Park, M. Kim, and D. Kwon, "Security weakness in the smart grid key distribution scheme proposed by xia and wang," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1613–1614, 2013.

[23] J.-L. Tsai and N.-W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE transactions on smart grid*, vol. 7, no. 2, pp. 906–914, 2016.

[24] H. Guo, Y. Wu, F. Bao, H. Chen, and M. Ma, "Ubapv2g: A unique batch authentication protocol for vehicle-to-grid communications," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 707–714, 2011.

[25] H. Liu, H. Ning, Y. Zhang, Q. Xiong, and L. T. Yang, "Role-dependent privacy preservation for secure v2g networks in the smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, pp. 208–220, 2014.

[26] Z. Yang, S. Yu, W. Lou, and C. Liu, "P2: Privacy-preserving communication and precise reward architecture for v2g networks in smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 697–706, 2011.

[27] K. Kaur, N. Kumar, M. Singh, and M. S. Obaidat, "Lightweight authentication protocol for rfid-enabled systems based on ecc," in *2016 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2016, pp. 1–6.

[28] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 82–88, 2018.

[29] H. Wang, Q. Wang, D. He, Q. Li, and Z. Liu, "Bbars: Blockchain-based anonymous rewarding scheme for v2g networks," *IEEE Internet of Things Journal*, 2019.

[30] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE transactions on industrial informatics*, vol. 14, no. 8, pp. 3690–3700, 2018.

[31] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3154–3164, 2017.

[32] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.

[33] S. Garg, K. Kaur, G. Kaddoum, F. Gagnon, and J. J. Rodrigues, "An efficient blockchain-based hierarchical authentication mechanism for energy trading in v2g environment," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2019, pp. 1–6.

[34] "Indian ev industry to represent rs 500 billion opportunity by 2025, covid notwithstanding: Report," ET Auto.com, From the Economic Times, accessed 31 August 2020, Available:https://auto.economictimes.indiatimes.com/news/industry/indian-ev-industry-to-represent-rs-500-billion-opportunity-by-2025-covid-notwithstan 77127688.

[35] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K. R. Choo, and A. Y. Zomaya, "Blockchain for smart communities: Applications, challenges and opportunities," *Journal of Network and Computer Applications*, vol. 144, pp. 13–48, 2019.

[36] A. S. Yahaya, N. Javaid, F. A. Alzahrani, A. Rehman, I. Ullah, A. Shahid, and M. Shafiq, "Blockchain based sustainable local energy trading considering home energy management and demurrage mechanism," *Sustainability*, vol. 12, no. 8, p. 3385, 2020.

[37] M. Patel, *Data Structure and Algorithm With C*. Educreation Publishing, 2018.

Shubhani Aggarwal is pursuing a Ph.D. from Thapar Institute of Engineering and Technology (Deemed to be University), Patiala, Punjab, India. She received the B.Tech degree in Computer Science and Engineering from Punjabi University, Patiala, Punjab India, in 2015, and the M.E. degree in Computer Science from Panjab University, Chandigarh, India, in 2017. She has many research interests in the area of Blockchain, cryptography, Internet of Drones, and information security. Some of her research findings are published in top-cited journals such as IEEE IoTJ, Elsevier JNCA, Computers and Security, Mobile Networks and Applications, Computer Communications.

Neeraj Kumar (M'16, SM'17) received his Ph.D. in CSE from SMVD University, Katra (J & K), India, and was a postdoctoral research fellow in Coventry University, Coventry, UK. He is working as a full Professor in the CSED, Thapar Institute of Engineering and Technology, Patiala (Punjab), India. He has published more than 300 technical research papers in leading journals and conferences from IEEE, Elsevier, Springer, John Wiley, etc. Some of his research findings are published in top-cited journals such as IEEE TKDE, IEEE TIE, IEEE TDSC, IEEE TITS, IEEE TCE, IEEE TII, IEEE TVT, IEEE ITS. He has also published four books from Springer and CRC Press. He is an Associate Technical Editor of IEEE Communication Magazine, IEEE Network Magazine, Elsevier JNCA, and ComCom. He is in the 2019 list of highly cited researcher in WOS. He has won many prestigious awards from IEEE.

Prosanta Gope (M-18, SM-20) is currently working as an Assistant Professor in the Department of Computer Science (Cyber Security) at the University of Sheffield, UK. Dr. Gope served as a Research Fellow in the Department of Computer Science at National University of Singapore (NUS). Primarily driven by tackling challenging real-world security problems, he has expertise in lightweight anonymous authentication, authenticated encryption, access control, security of mobile communications, healthcare, Internet of Things, Cloud, RFIDs, WSNs, Smart-Grid and hardware security of IoT devices. He has authored more than 75 peer-reviewed articles in several reputable international journals and conferences and has four filed patents. He received the Distinguished Ph.D. Scholar Award 2014 by National Cheng Kung University (Taiwan). Dr. Gope received the Best Performing Associate Editor Award from the IEEE Sensors Journal. Several of his papers have been published in high impact journals such as IEEE TIFS, IEEE TDSC, IEEE TIE, IEEE TII, IEEE TSG, IEEE JBHI, IEEE TVT, etc. Dr. Gope has served as TPC member in several international conferences such as IEEE GLOBECOM, ARES, etc. He currently serves as an Associate Editor for the IEEE INTERNET OF THINGS JOURNAL, IEEE SYSTEMS JOURNAL, IEEE SENSORS JOURNAL, the Security and Communication Networks, and the Mobile Information Systems Journal.