A Privacy-Preserving Secure Framework for Electric Vehicles in IoT using Matching Market and Signcryption

Gulshan Kumar, Rahul Saha, Mritunjay Kumar Rai, William J. Buchanan, Reji Thomas, G. Geetha, Tai Hoon-Kim and Joel J. P. C. Rodrigues, *Fellow, IEEE,*

***Abstract*—The present world of vehicle technology is inclined to develop Electric Vehicles (EVs) with various optimized features. These vehicles need frequent charging which takes a longer time to charge up. Therefore, scheduling of vehicles in charging stations is required. Besides, the information of the EVs and its location is also stored by the charging stations and therefore creates a concern of EV privacy. Various researches are going on to solve these problems; however, an efficient privacy-preserving solution is less practiced till date. In this paper, a framework for Electric Vehicle (EV) charging is discussed. The framework uses the concept of Matching Market to identify a charging station and uses the lattice-based cryptography for secure communications. The matching market considers multiple factors to provide the best allocation of charging station and cryptography ensures security and privacy preservation. The use of lattice-based cryptographic hash SWIFFT avoids heavy computation. This usage of matching market and lattice cryptography, more specifically signcryption for EV charging framework are the highlights of the solution and add-ons to the novel features. Overall, the presented framework is efficient in terms of computation and communication cost, satisfaction ratio, slot ratio, charging latency and load balancing index. The performance metrics are compared with recent developments in this field.**

***Index Terms*—Electric Vehicle, privacy, signcryption, lattice, cryptography, security**

I. Introduction

Electricity is preferred for motor-vehicle propulsion as it provides more comfort, simplicity in design and efficiency in operation. Proof of the existence of Electric Vehicles (EVs) is known since the mid of 19^{th} century and the present interest in 21^{st} century is mainly due to environmental concern [1]. Previously except a few cars and small electric trains with distance restrictions, EVs were unable to gather much interest due to the unavailability of batteries' high power and energy density with large cycleability and high rate capability. This allowed fossil fuel to dominate the transportation sector. However, the introduction of high-density Li-ion batteries towards the end of 20^{th} century rejuvenated the interest in EVs once again. In fact, transportation technology and the renewable energy sector with Li-ion batteries are going to be the hope for a gasoline-free 21^{st} century to address all environmental concerns. Increasing demand for EVs has been predicted; a giant leap from 2% of the global share in 2016 to 22% in 2030 as environmentally benign and cheap Li-ion technology with desirable properties are expected to fulfill the requirements of the transportation sector [2].

To strengthen the deployment of EVs worldwide, charging centres like present gas stations should be made more available and the locations should be mapped [3][4]. This has made EVs to get connected with the distributed electric grid and networks. The Grid-to-Vehicle (G2V) and Vehicle-to-Grid (V2G) communication technology help in the process of selecting the electric grid for efficient charging of the EVs [5][6]. In future, this G2V and V2G are going to be consolidated with Internet-of-Things (IoTs) to make the total infrastructure functioning in a smoother way with the least human intervention and less time consumption [7]. The main objective for connecting the vehicle to the electric grid is to charge the vehicle when required without wasting time in waiting as charging a battery takes much more time than filling a gas tank of gasoline vehicles. However, the EVs provide load balancing through 'valley filling' and 'peak shaving', frequency regulation, and back-up power. Various researches are getting conducted on these services in the G2V and V2G technology [8][9]. Furthermore, to execute these services various Transport System Models (TSM) are closely connected with electric grids or smart grids through various means of Information and Communication Technology (ICT) [10][11]. The advent of IoT with the goal of smoother and easier processing of the system modeling and functioning has made the ICT an adhesive component of TSM. Figure 1 shows a logical representation of the connections among TSM, EV and grids extending to the IoT. The figure depicts that EVs are one of the components of vehicular networks which are based on IoT; on the other side, the extension of electric grid systems, "the smart grid",is controlled through IoT. Therefore, IoT is a prominent enabler of EVs and gaining popularity in EV research community.

The continuous functioning of EV depends on the identification of the charging station in the vicinity before the

G. Kumar, R. Saha and G. Geetha are with the School of Computer Science and Engineering, Lovely Professional University, Punjab, India. e-mail: (gulshan3971@gmail.com, rsahaaot@gmail.com, gitaskumar@yahoo.com).

M. K. Rai is with Department of Electronics and Electrical Engineering, Lovely Professional University, India. e-mail: (raimritunjay@gmail.com).

William J. Buchanan is with Blockpass ID Lab, Edinburgh Napier University, Edinburgh, United Kingdom. e-mail: (B.Buchanan@napier.ac.uk).

R. Thomas is with Divison of Research and Development, Lovely Professional University, India. e-mail: (rthomas.eyyalil@gmail.com).

T. H. Kim is with Beijing Jiaotong University, Beijing, 100044, P.R. China e-mail: (taihoonn@daum.net).

Joel J. P. C. Rodrigues is with Federal University of Piauí, Teresina - PI, Brazil and Instituto de Telecomunicações, Portugal e-mail: (joeljr@ieee.org).

Corresponding Author: R. Saha (email: rsahaaot@gmail.com) and T. H. Kim (taihoonn@daum.net)

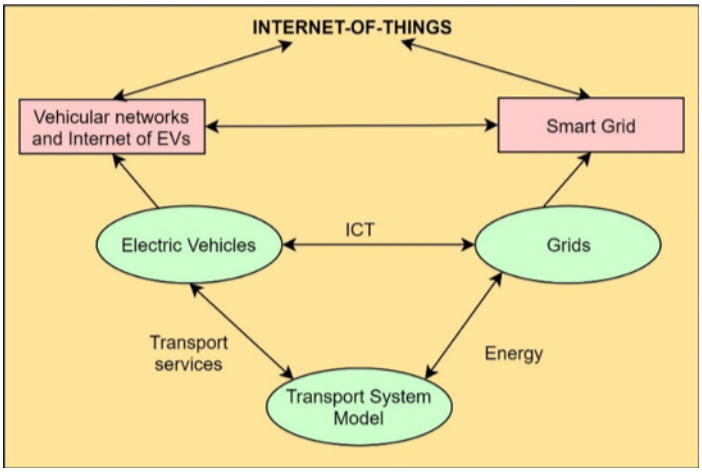

Fig. 1. Logical representation of IoT enabling EVs

battery gets exhausted[12]. The EV charging infrastructure also considers the controlling mechanism of the charging station and accommodating the EV for a charging point. Various researches are executed in this field at present and some are efficient to be considered in the near future [13][14]. Moreover, various energy management methods are executed by the charging points for the ease of EV charging process and some of the recent significant developments in this direction are published elsewhere[15][16][17]. Along with these comforts which came with this technology, security and privacy of EV infrastructure are at threats. There are different active entities in V2G network viz., the owner of the EV, the EV battery, the power company, and the payment management company. The EVs communicate with the electric grid through a collector or data aggregator for charging their batteries at the charging stations with minimum queuing time or to have an optimum distance-time product. A data aggregator is a device or set of devices that acts as a collector of available power information of the vehicles. An aggregator also offers power supply information to the EVs through the charging stations based on various energy management and resource scheduling algorithms. They are also enabled to access the authentication and communication servers to coordinate the charging. Figure 2 explains the architecture of the overall V2G communication process.

The use of Electric Vehicle (EV) is growing due to its environmental benefits and easy technical maintenance and obviously cost[18][19]. However, the limitation of battery exhaustion, cycleability and rate capability (longer recharge time) are the major concerns. As EVs are now the component of IoT and smart grid, security has been attributed to the concerning factors as well. An overall summary of attacks has been shown in Table I for the V2G and G2V communication architecture by considering the Internet of Electric Vehicles (IoEV) [20][21].

From the table, it is clear that EVs are vulnerable more for attacks when they communicate with the charging infrastructure networks. The critical security requirements of the charging infrastructure are data maintenance and user authentication, data confidentiality, and finally the privacy of EVs. Therefore, a solution has been provided for the secure and privacy-preserving framework for EVs in the present paper. It is comprised of a matching market concept used with multi-payoff convergence as a payoff. The lattice cryptography is also used for a less complex cryptographic process for accomplishing security requirements. The literature background of these two concepts, matching market concept and lattice cryptography along with the recent developments are discussed in the next section. The contribution and novelty of the proposed work are:

- A solution is provided for the optimization of EV allocation to a charging station.
- Multi-factor payoff-based matching market is used for the best allocation of charging stations.
- Lattice signcryption is applied for EV infrastructure communication to reduce time consumption of the cryptographic procedures and to withstand the quantum attacks.
- Thus, system stability and robustness against security attacks are ensured.

The rest of the paper is organized as follows. Section II explains shows the recent state of the art. Section III explains the proposed framework. Section IV discusses the experimental results and finally, the major conclusion drawn from the presented study is given in Section V.

II. Background and Recent Developments

In this section, a basic understanding of the matching market concept and signcryption and its applications are discussed first. Recent security-privacy solutions for EVs are also given in this section.

A. Matching market

The matching theory is a mathematical framework generally used for the economic understanding of the problem to design a particular 'market' (considered as group of nodes to generalize the concept). It deals with the analysis of the formation of the beneficial relationships mutually developed between the parties over a period of time. A matching function is scientifically represented as a mathematical relationship

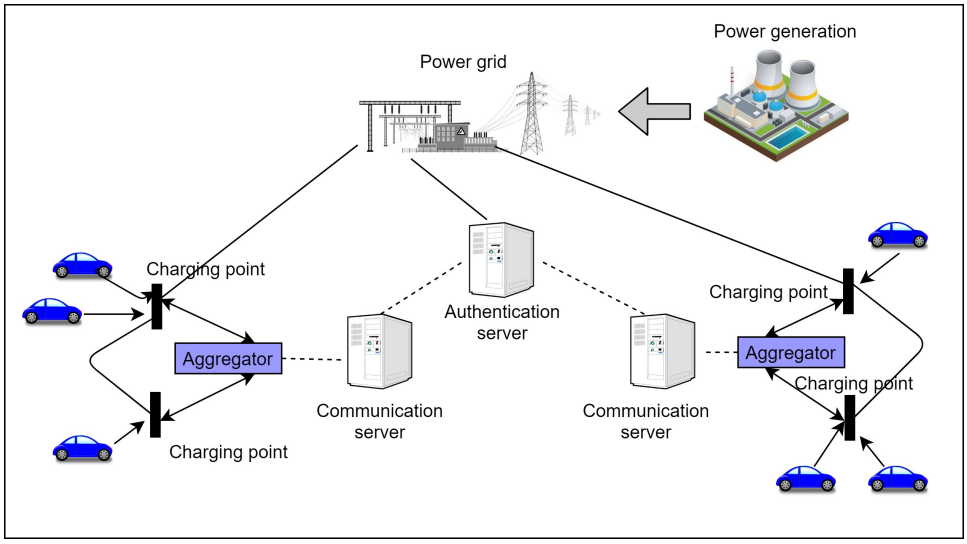

Fig. 2. V2G and G2V communication architecture

TABLE I
ATTACKS ON EVS AND RELATED COMMUNICATION

Category	Attack name	Attack on
Vehicle-to-Sensor communication	Jamming	User Authentication, data availability
	False data injection	Data integrity
	GPS deception	Data integrity, confidentiality, privacy
	Denial of Service	Data availability
Vehicle-to-Vehicle communication	Modification	Data integrity, confidentiality
	Sybil	User Authentication
	False data injection	Data and user authentication, confidentiality, privacy
	Eavesdropping	Data availability
	Black hole	Data integrity, data authentication
	Grey hole	Data integrity, data authentication
	Worm hole	Data authentication, User authentication
	Denial of Service	Data availability
Vehicle-to-Infrastructure communication	Replay	Non-repudiation
	Route information forgery	Data integrity, confidentiality
	Privacy	Privacy
	RSU spoofing	Authentication
	Duplicate Address Detection	Authentication
Vehicle to Network communication	DoS, MiTM, Spoofing	Authentication
	Physical Attacks	Data integrity, privacy, confidentiality
	Eavesdropping	Data availability
	Configuration Attacks	Data integrity, confidentiality

between unmatched agents dealing with the same service. The agents are classified into two types; the requester and the acceptor. With a wide extension and feasibility of the application, matching functions can be assumed to follow the 'Cobb–Douglas' form [22]:

$$m_t = M(u_t, v_t) = c u_t^a v_t^b \tag{1}$$

where c, a and b are positive constants. In this equation, u_t represents the number of requesters in a matching system at a given time t, v_t is the number of acceptors trying to fill the requests of the requesters. The number of new relationships (matches) created between requesters and acceptors (per unit of time) is given by m_t. The above theory can be expressed as a bipartite graph as shown in Figure 3 for observing the perfect matching with individual preferences.

Figure 3 shows an example with five requesters and five acceptors with their preferences (indicating, for instance, that the requester R1 has preferred allocators A1, A2 as acceptable options, while the requester R4 only prefers acceptor A4). The allocation or the relationship between a requester and an acceptor should be formed in such a way that the acceptor must be in the preference list of a requester. Since the edges represent acceptable options for requesters, assigning an acceptor to each requester is preferred in the present case. This allows each requester is assigned an acceptor to which the requester is connected by an edge. Figure 3 shows such an assignment with the darkened edges indicating who gets which acceptor. Such an assignment is considered as a perfect matching [23]. Extending the concept of this perfect matching with some valuations, prices associated with each of the preference and allocation in the matching outcomes, a payoff need to be maximized from the overall matching system. For example, suppose that each acceptor i puts the accepted relationship with a price $p_i > 0$. If a requester j

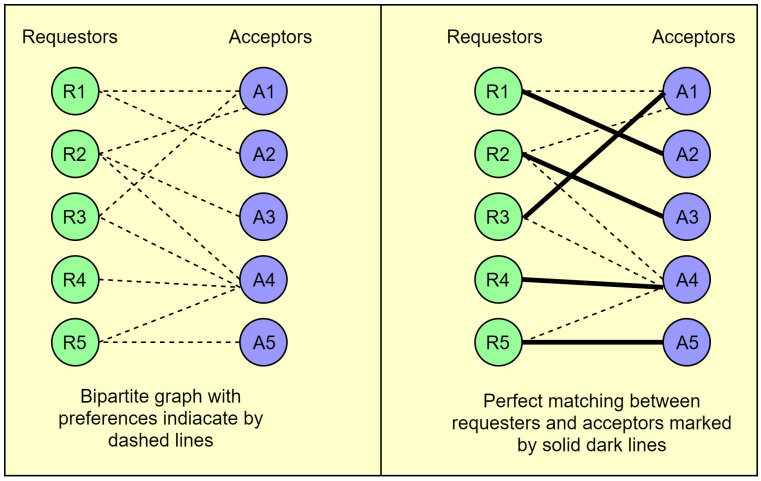

Fig. 3. Example of perfect matching

requests the acceptor i at this price, the requester's payoff is the valuation for this acceptor minus the amount of price the requester has to pay: $v_{ij} - p_i$, where v_{ij} is the valuation for the acceptor i by the requester j. So, with a given a set of valuations and prices, if requester j wants to maximize its payoff, it will be waiting to be allocated to the acceptor i for which $v_{ij} - p_i$ is maximized. Therefore, Nash equilibrium is calculated for both the requester and accepter for which they have maximized the payoff [24]. This nash equilibrium leads to maximum payoff for acceptor and requester with their respective preferences providing the solution stability. Therefore, we have chosen this method in the present work for allocating the best option of charging stations.

This matching market concept has been used in the present study and customized as per the requirement of the proposed framework. The allocation of an EV (requester) to a charging station (acceptor) is based on the maximized payoff' for both the requester and the acceptor. Therefore developing a market matching allocation scheme for EVs is considered here. Generally, in matching market bipartite graph the number of acceptors and requesters are to be equal; however, the presented customized use of matching market is applicable to any number of the acceptors and requesters which also adds on to the novelty.

B. Signcryption

The security aspects are critical for any type of networking applications and so with EV charging networks. Generally, for all the security services, encryption and digital signature are the two fundamental cryptographic tools that ensure the security viz., confidentiality, integrity, and non-repudiation [25].

Previously, a traditional method "signature-then-encryption" involving public key has been used in which the message is signed digitally and is then followed by encryption. However, this method faces problems of low efficiency and high cost of the combination. Besides, arbitrary combinations are questionable sometimes for providing appropriate security provisions. To overcome these problems, signcryption has been introduced in 1997 [25].]. It has been developed as a cryptographic primitive for performing the digital signature and encryption functions simultaneously. Any signcryption scheme should have some certain properties such as correctness, efficiency in terms of computational cost and communication overhead, security in terms of confidentiality, forward secrecy, unforgeability, non-repudiation, integrity and public verifiability. The generic and logical functioning of signcryption are shown in Figure 4. It shows a Public Key Generator (PKG) and involvement of keys and other components for the signcryption and unsigncryption process. Pu_A, Pr_A are the public and private keys of the sender A and Pu_B, Pr_B are the public and private keys of the receiver B.

Various researchers have developed efficient signcryption schemes and extensions of the same are still in progress for improving the security features. Some of the significant usage of signcryption for IoT based applications have been discussed in the literature [26][27][28]. Moreover, the advanced signcryption schemes are also introduced recently in the form of lightweight signcryption schemes [29][30] [31] [32][33].

In the proposed framework, a lattice based signcryption for providing more security has been considered as lattice cryptography is able to withstand against quantum attacks [34]. It has been observed that the advent of quantum computers makes the existing cryptographic algorithms vulnerable if factorization of large primes and other mathematical processes are used. To make the security algorithms sustainable against attacks, lattice-based cryptography is introduced. It constructs cryptographic primitives involving lattices of data points calculated by the integer linear combination basis vectors, either in the construction itself or in the security proof. Such constructions are currently important for post-quantum cryptography as the Shortest Vector Problem (SVP) is hard to solve. Lattice cryptography has shown successful derivations of hash functions, public key systems and even signcryptions that produce less computational cost and message overhead. It provides lightness to the system's complexity and hence, chosen for the present work.

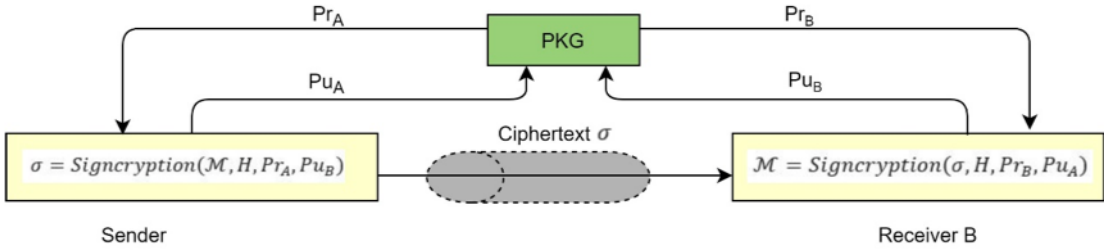

Fig. 4. Logical representation of signcryption process

C. Recent developments

In this subsection, some significant recent development of security solutions for EVs have been reviewed. The pros and cons are notified for the selected existing security solutions and the steps taken in the present study to solve the problems are mentioned. The objective of the present work is to provide a secure and privacy-preserving framework for electric vehicles with the best suit charging point. Existing works related to security and privacy, the energy distribution and the management systems have been considered for this purpose.

Mutual authentication and blockchain-based secure framework for EV charging has been recently introduced [35]. Burrows–Abadi–Needham logic is used in this framework to provide anonymity and forward secrecy with efficient charging. It also prevents the replay and the man-in-the-middle attacks using automated validation of internet security protocols. With the aforementioned advantages, the method suffers mainly from latency with the increasing number of EVs and does not provide the best option for a charging station recommendation. Another blockchain-based solution that considers mobile charging concepts also came in recently [36]. The authors propose an algorithm based on a double-objective optimization model that maximizes the user's satisfaction and minimizes users' cost. The method considers diverse metrics like the location of charging centres, the time of waiting, and the driving speed of EVs, etc. Though the blockchain provides security, the method is unable to protect EVs' privacy in a suitable way. A reliable, automated blockchain-based protocol that ensures privacy for EVs has been developed [37]. The approach is reliable, automated and ensures privacy. The selection of stations is based on pricing and distance; however, the load balance is not included. It also uses blockchain comprised of EV's demand and charging station's bids. A priority-based privacy-preserving solution has experimented with [38]. In this third method, the selection of stations is based on pricing and distance without considering the load balance. It also considers of EV's demand and charging station's bids. A priority-based privacy-preserving solution has been developed based on three schemes, namely, multiauthority attribute-based prioritization, e-payment and hierarchical authentication. [39]. Though privacy of the EVs is maintained the compromised authority has not been addressed well enough to avoid false priority claiming. The lightweight scheme is used for the authentication process in this method and the hierarchical construction for authentication may provide a bottleneck for the performance with a huge number of EVs. Another recent development using Lightweight Privacy-aware Power injection and Communication (LPPC) scheme is applicable to V2G architecture [40]. In this case, EVs use bids and secret keys for different time slots. Elliptic Curve Cryptography (ECC) is used for the data aggregation and the hash function-based technique is used for authenticity or/and integrity of the aggregated bid. A privacy-preserving supplier matching EV charging system is also considered in which the problem of information leakage is handled by the solution using Biochromatic Mutual Nearest Neighbour (BMNN) assignments of suppliers [41].In this method, homomorphic encryption is used for hiding EV information and dynamic environments are considered for the simulation. The results are satisfactory, but the problem is with assignments where the supplier and user profit need to be maximized. A similar privacy-preserving approach applicable for vehicle-to-grid uses anonymous credentials for privacy [42].

Control on the usage of the third party and the fine-grained hash chain based rewarding mechanism are beneficial for fair exchange and non-repudiation. The certificate process needs to be explored more for EVs as they are resource-constrained. EVs are now also become part of the Intelligent Transport System (ITS) and therefore their autonomous controlling is another important research work. Such a significant work for ITS ensuring privacy has been studied [43].

The privacy is provided by using location pseudonyms of the EVs where they contact the trusted authority once and then update their pseudonyms by themselves. It provides less communication overhead in the network; however, the approach fails to address the known pseudonyms attacks where some compromised EVs may update the pseudonyms with a predefined set of attack base[44].

Charging station allocation and energy management are significant factors that affect EV charging systems. Such developments with a hybrid power system have been studied recently based on the combination of three control methods; a fuzzy logic control, a flatness control and a rule-based algorithm.Though energy management is addressed in this method, the load balancing is not considered. Another energy control model considers the decentralized system and flexible charging demand uses the Lagrangian method and the alternating direction multiplier [44]. With this technique, EVs are able to decide their charging plan locally but the algorithm faces the problem of load balancing. Some other distributed control strategy for congestion control and other services for EVs have been experimented for various aspects that affect

the EV charging process [45][46][47].

A more recent development provides a scheduling mechanism in the Charging Station (CS) with an economic cost and reduced charging time for the EV [13]. Moreover, it avoids third-party inclusion and ensures EV's privacy and complex information exchange between the EV and CS. The privacy and security section of the approach needs to be explored more.

The above discussion of the existing developments for EV charging framework suggests that the research in this field is still in infancy. The overall problems identified from the recent literatures are: i) enery efficient charging station allocation and optimization, ii) privacy preservation of EV information and, iii) less complex cryptograhic processes. As EVs are energy resource-constrained, an adaptable solution in the near future is required to address the aforementioned problems. Therefore, a novel framework using the matching market scheme and lattice cryptography/signcryption for security services for future EVs in IoT is presented here.

III. Proposed framework

The proposed framework (Figure 5) in the present study is an extension from the basic network generally used, which is discussed in the introduction with the help of Figure 2. At first, EVs communicate with the aggregators and the aggregators propagate the messages to the operators. This operator includes communication servers, authentication server and the processing server. It is this 'operator' which is responsible for the allocation of the appropriate charging station to an EV based on the market matching scheme with defined payoff function. The aggregator knows only the pseudo-identity of the EV to deliver privacy to the EV. The other information like location, charging-discharging data and traceroute are encrypted while communicating with the aggregator and the charging station; however, operators are able to get the location of EVs via GPS systems configured in the vehicles.

All operations start as EVs broadcast charge request messages $CHRG : P_{ID}, RES, V$. This message is encrypted by the appropriate keys of the EVs and forwarded towards the operator via aggregators and that EVs' authentication is then validated by the operator. As the message passes through aggregators, aggregators' authentication is also required for the operator and then only the messages from EVs are processed further for allocating a charging station. After the verification, the operator executes the market matching and then allocates the EV to a charging station having the defined preference and maximum payoff. In this process aggregators' identity is verified at the EVs and messages are accepted accordingly. Once the EV reaches the charging station and plugs in for charging all the information are hashed and shared with the charging station. The charging station stores the hashed information and EV stores the charging station id and time stamp.

In the process considered here, a vehicle is in the moving mode with an average speed of 35-40 km/h and dynamic decision from the operator is required. As per the schematics shown in Figure 5, the EV broadcasts the message when it is near to charging station 1, however, the operator allocates charging station is 4 as per the moving direction and speed of the vehicle. The overall functionalities are classified into following subsections like initialization and registration, authentication, allocation and charging. In the present case, processing of the request from the EV to finally allocate a charging station considers the assumption as:

- Operator centre is secured enough.
- Operator uses a secret channel for distributing keys.
- EVs and aggregators are non-secure and therefore need proper authentication process.

A. Initialization Phase

The operator initializes the system and sets up the network by configuring EV charging aggregators registered. The process steps for the initialization and the algorithm for the key generation are given below.

Step 1: The operator selects a base point G of order n on the selected elliptic curve F over finite field q which is transformed into a polynomial form $F = (x, y) : y^2 = (x^3 + ax + b) \pmod q$. The order of n must be greater than 2^{160} and satisfying $n \times G = I$, where I is a point on F at infinity.

Step 2: The polynomial of degree n $(poly(n))$ calculated in the previous step is then transformed into a vector $\mathcal{B}$. A random basis $\aleph_{ag}$ is calculated by hashing of the vector $\mathcal{B}$ appended with aggregator's ID and then randomly choosing m bits; $\aleph_{ag} = (rand_m(hash(\mathcal{B}||ID_{aggr}))$. ID_{aggr} is generated by the ICMetrics of the aggregator device.

Step 3: The lattice of the vector $\mathcal{B}$ is also calculated as: $\mathcal{L} = \sum_{i=1}^{m} a_i v_i$, where $a_i \in R$ and $v_i \in \mathcal{B}$.

Step 4: SETLA key generation process is followed to calculate the public-private keys for the aggregators [48]. The key generation process is shown in Algorithm 1.

Algorithm 1 Key generation for Aggregators

1: **Data** $\aleph_{ag}, \mathcal{L}$
2: **Result** $K_{ag+} = (t_1, t_2), K_{ag-} = (s, e_1, e_2)$
3: $(s, e_1, e_2) \leftarrow R_{q,[1]}$
4: $t_1 \leftarrow \aleph_{ag}.s + e_1$
5: $t_2 \leftarrow \mathcal{L}.s + e_2$
6: **return** K_{ag+} and K_{ag-}

In the Algorithm 1, K_{ag+} is the public key and K_{ag-} is the private key of the EV aggregator communication. $R_{q,[1]}$ is the well-known ring $R_q = Z_q[\mathcal{B}]/[\mathcal{B}_m + 1]$ with $q = 1 \pmod{2n}$ and have the set of elements in the range of $[-1, 1]$. $s \in Z_q^m$ such that $s \in R_q$ and $e_i \in R = Z[\mathcal{B}]/[p(\mathcal{B})]$ with coefficients sampled from X with Gaussian distribution. Here, Z_q denotes residue class $\pmod q$.

Step 5: Operator calculates its private-public key pair as: $K_{opagg+} = K_{ag+}.G$ and $K_{opagg-} = K_{ag-}.G$ where K_{opagg+} is the public key and K_{opagg-} is the private key established between the operator and an aggregator.

Step 6: Operator then sends the key pair: K_{ag+} and K_{ag-} and its own public key K_{op+} to the aggregator.

The registration phase is executed once an EV wants to access a charging system and wants to be part of the EV network. In

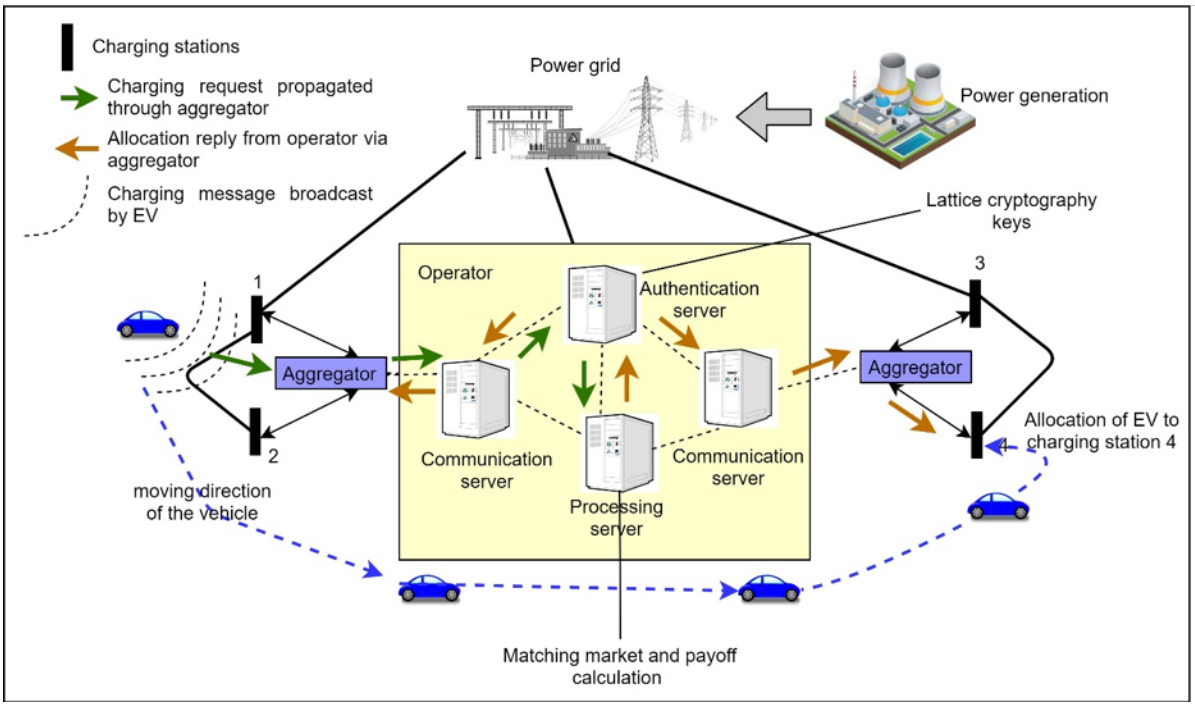

Fig. 5. Proposed framework for EV charging

this case, EVs are also parts of vehicular networks. The steps of registration are as followed.

Step 1: EV sends its own id EV_{ID} to the operator.

Step 2: The operator calculates $H(EV_{ID})$ and maps with EV_{ID} and stores them in mapping repository.

Step 3: Operator generates two random numbers r_1 and r_2.

Step 4: Operator calculates $K_{op-} = H(EV_ID||r_1)$ and $K_{ev-} = H(EV_{ID}||r_2)$. $H()$ is the family of SWIFFT hash which is based on lattice cryptography as shown in [49]. The use of SWIFFT is more powerful as compared to generic hash functions and is able to withstand quantum key attacks. This private key is also stored by the operator in hashed format for verification process in later stage. The functioning of SWIFFT is shown in Algorithm 2.

Algorithm 2 Private key generation for EVs

1: **Data** $EV_{ID}||r_i; Output : K_{op-}, K_{ev-}$
2: **Result** (K_{op-}, K_{ev-})
3: Convert $EV_{ID}||r_i$ into a collection of m polynomials p_i in a certain polynomial ring R with binary coefficients
4: Calculate Fourier coefficients for each p_i
5: Define Fourier coefficients for each a_i where a_i is dependent of on SWIFFT family
6: Point-wise multiply the Fourier coefficients of p_i and a_i
7: Use inverse Fast Fourier Transform (FFT) to obtain m polynomials f_i of degree $< 2n$
8: Compute $f = \sum_{i=1}^{m} f_i \pmod p$ $K_{op-}, K_{ev-} \leftarrow$ Convert f to $nlog(p)$ bits

Step 5: Operator calculates the public keys: $K_{op+} = Lr_1.G$ and $K_{ev+} = Lr_2.G$.

Step 6: Operator sends $K_{op+}, K_{ev-} K_{ev+}$ to EV for further communication using secret channel.

Therefore, we can say that, before the authentication phase, two sets of operator keys are initiated: one set is working between operator and aggregator, i.e. $[K_{opagg+}, K_{opagg-}, K_{ag+}, K_{ag-}]$ and another set is working between operator and EV, i.e. $[K_{op+}, K_{op-}, K_{ev-}, K_{ev+}]$.

B. Authentication Phase

Authentication phase is executed between an EV and aggregator when EV wants to access a charging system. A common session key is generated after both the parties are authenticated.

Step 1: EV generates a charging request message $CHRG$: $H(EV_{Id}), EV_{loc}, E_r, V, H(K_{ev-})$, where $H(EV_{Id})$ is hash of the electric vehicle id, EV_{loc} is the location of the EV given by two-dimensional coordinates (x_{ev}, y_{ev}), E_r is the residual charge of the EV and V is the velocity of the EV. $H()$ is the lattice based SWIFFT hash function as shown in Algorithm 2. The vehicle encrypts the $CHRG$ message with operator's public key K_{op+},and broadcast it.

Step 2: The suitable aggregator in the vicinity of the EV receives the encrypted CHRG message and sends to the operator through signcryption process along with its id ID_{aggr}. Aggregator is not able to see the message due to the unavailbility of the operator private key. The signcryption process for aggregator is shown below in algorithm 3. The aggregator generates a digital signature (R, s), of the message $[CHRG]_{K_{ev-}}$ and finally sends the signcrypted message (R, s, c).

Step 3: Operation centre executes the unsigncryption process as shown in Algorithm 4.

Algorithm 3 Signcryption for aggregator

1: **Data** $CHRG_{K_{op+}}, H_1, H_2, G$
2: **Result** $y = (R, s, c)$
3: Select $k \xleftarrow{random} R_q \tilde{P-}$, where R_q is the ring and $\tilde{P-}$ is the generator of the ring
4: Calculate $k_1 = k.P-$ and $k_2 = k.K_{opagg+}$
5: Compute $c = CHRG_{K_{op+}} \oplus H_1(k_1, k_2)$, where $H_1 : R_q \times R_q \rightarrow Z_q$
6: Compute $h = H_2(c, k_2)$, where H_2 is a hash function in SWIFFT family
7: Compute $s = k/(h + K_{ag-}) \pmod q)$
8: Compute $R = h\tilde{P-}$

Algorithm 4 Unsigncryption at operation centre

1: **Data** $y = (R, s, c), K_{opagg-}$
2: **Result** $CHRG_{K_{op+}}$
3: Compute $k_1 = (K_{opagg-}).s.R$
4: Find the aggregator identity and use the corresponding public key K_{ag+}
5: Compute $k_2 = (K_{opagg-}).s.(K_{ag+})$
6: Compute $\sigma = (c, k_2)$
7: **if** $(\sigma.K_{ag+} = R)$ **then**
8: accept the message
9: $CHRG_{K_{op+}} = c \oplus H_1(k_1, k_2)$
10: **end if**

Note that, till the process described above aggregator is unable to see the identity of the EV and also deals with an encrypted version of the CHRG. Thus, privacy is preserved in the proposed system from the aggregators.

Step 4: Operator decrypts the message $[CHRG_{K_{op+}}$ with the its corresponding private key K_{op-}. It verifies the hashed key and the hashed vehicle ID in its mapping repository; if there is match, it considers the message as authenticated with aggregator and EV and processes it further for allocation calculation.

Step 5: It may happen that different aggregators have communicated the signcrypted message of CHRG to the operator due to the dynamic location of EV. All such messages are accounted by the operator to estimate the allocation of the charging station as aggregators positions (Assuming Road Side Units) are prefixed and under the observation of the operator.

C. Charging station allocation

The operator is responsible for the allocation of EV to a particular charging point for every registered EV in the network that requested charging. The operator executes the charging station allocation based on distance, residual charge, load at the charging station and waiting time at the charging station. The allocated charging station must satisfy the requirements of minimum distance, minimum residual charge, load balance and less waiting time. For this, the operator executes an allocation scheme, notifies the best suitable charging station to the aggregator and finally aggregator shares the information with EV.

The transmission range of the EV and aggregator is considered as r_1 and r_2 respectively, assuming that $r_1 < r_2$. The minimum distance between the two entities (EV and aggregator) should be less than $d = r_2 + r_1$. Figure 6 shows the geometrical configuration considering the transmission range to be as circle area. The distance payoff is given by:

$$\wp_D = \bigvee_{j=1}^{m} min(d) \tag{2}$$

where, d is the distance between an EV and aggregator and m is the number of aggregators' messages arrived for the same CHRG.

The residual charge is another parameter to be considered. If residual charge is too low, the EV is granted a priority. In the proposed system 20% residual charge is considered as a threshold value (E_{th}) after which the EV starts charging request. The selection of 20% is based on experiment which have been found sufficient for charging station to be allocated to the EV. If an EV is having E_{res} too low (assuming that the rate of charge discharge per unit distance is β), the discharged charge for covering the $min(d)$ distance must be less than E_{res}. Therefore, the condition for energy payoff is calculated as:

$$\wp_E = min[(E_{th} - E_{res}) - (d \times \beta)] \tag{3}$$

The charging time for EV is generally more as compared to other charging systems. Considering the charging rate μ per unit time and x is the total charge capacity of the vehicle, the time taken for full charging is $\frac{x}{\mu}$ time unit. A charging station having the capacity of α number of vehicles. Suppose, α vehicles are in process of charging simultaneously and when they are filled up with ρ amount of charge the other vehicle comes. So, the total charging time T_{chrg} for the new vehicle becomes:

$$T_{chrg} = \frac{x}{\mu} + \frac{x - \rho}{\mu} = \frac{2x - \rho}{\mu} \; unit \; time \tag{4}$$

For the θth vehicle therefore, the waiting time increases as:

$$T_{wait} = \frac{x - \rho}{\mu} + \frac{x}{\mu} + \frac{x}{\mu} + ... \; up \; to \; \theta^{th} \; vehicle = \frac{\theta x - \rho}{\mu} \tag{5}$$

The time of charging for θ^{th} vehicle, i.e. $\frac{\theta x - \rho}{\mu}$ is inversely proportional to α which is the capacity of the charging station. More the capacity, less the time for charging as waiting time is reduced. The above equation suggests that if θ is more and ρ is less then T_{wait} increases significantly and thus generating more congestion at a particular charging station and reducing the overall system's performance. Therefore, T_{wait} should be minimum for the vehicle going to be allocated to a charging station.

These parameters are used by the operator for conceptualizing the matching market scheme as shown in the following steps.

Step 1: For every aggregator forwarding the signed CHRG message operator calculates:

$$d = \sqrt{(x_{ev} - x_{agg})^2 + (y_{ev} - y_{agg})^2} \tag{6a}$$

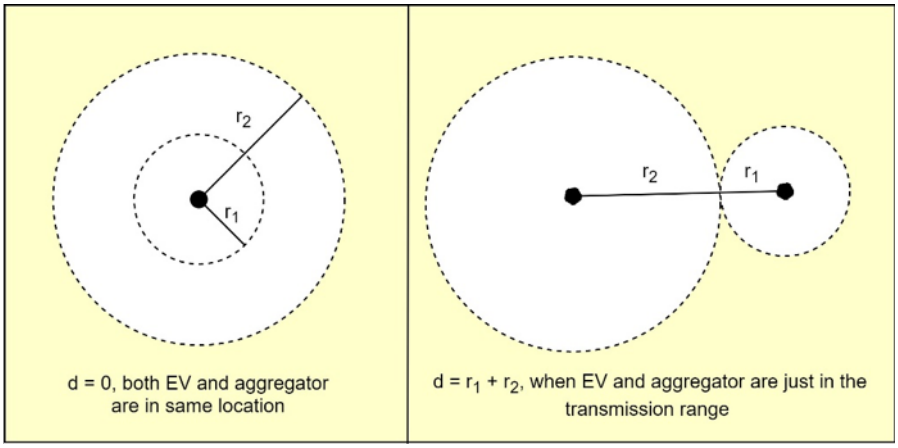

Fig. 6. Geometrical representation of distance variation between aggregator and EV

TABLE II
PAYOFF MATRIX FORMAT

	EV1	EV2	EV3
A1	d_{11}, E_{11}, t_{11}	NA	d_{13}, E_{13}, t_{13}
A2	d_{21}, E_{21}, t_{21}	d_{22}, E_{22}, t_{22}	NA
A3	d_{31}, E_{31}, t_{31}	d_{32}, E_{32}, t_{32}	d_{33}, E_{33}, t_{33}

$$E_{con} = (E_{th} - E_{res}) - (d \times \beta) \tag{6b}$$

$$T_{wait} = \frac{\theta x - \rho}{\mu} \tag{7}$$

Step 2: Operator creates a payoff matrix at time instant t as shown in Table II.

Table II shows the format of the payoff matrix. For example, A1, A2 and A3 are the aggregators and EV1, EV2 and EV3 are the electric vehicles. d_{ij} is the distance between an aggregator i and vehicle j, E_{ij} is the calculated charge consumption between an aggregator i and vehicle j; and t_{ij} is the waiting time for the j assigned to a charging station by aggregator i .

Step 3: Operator calculates two payoff functions (one for EV $\wp_p$ and one for charging station $\wp_{chrg_{st}}$) as:

$$\wp_p = d_p + C_p + W_p \tag{8}$$

where the priority for distance d_p and priority for charge consumption C_p are proportional to each other and the priority for waiting W_p is the secondary. For the same d_p and C_p, W_p works as an enabler of allocation. These priorities are calculated as:

$$d_p = min(d) \tag{9}$$

$$C_p = min(E_{con}) \tag{10}$$

$$W_p = min(T_{wait}) \tag{11}$$

$$\wp_{chrg_{st}} = max[(x - E_{con})] \times \mathrm{p}] \tag{12}$$

where, p is the price of charging per unit. The priority values are either 0 or 1 to denote whether a particular EV is having minimum distance, minimum energy and minimum waiting time. The cumulative score of $\wp_p$ lies between 0 and 3. For $\wp_{chrg_{st}}$ the maximum value is given priority of 1.

The cost of charging per unit p can be varied and dynamic depending upon operators' regulations and can be calculated as: $\mathrm{p} = \mathrm{p}_{cst} - \mathrm{v}_{EV}$ where, p_{cst} is the price by charging station and v_{EV} is the EV cost valuation which depends upon the EV owner.

Step 4: Operator finally calculates the payoff of overall allocation as:

$$\wp_{\mathrm{a}} = max(\wp_p + \wp_{chrg_{st}}) \tag{13}$$

Following the above explanation, the $\wp_{\mathrm{a}}$ becomes within range of 0 to 4 overall. This priority checking is an iterative process.

Step 5: Allocation in confirmed.

Step 6: Operator sends ALLOC : $[CS_{ID},\ Agg_{loc},\ CS_{payoff}]$ message signcrypted to the EV via aggregator.

Let us consider a bipartite graph following the above payoff matrix to understand the charging station allocation process. In the example, aggregators A1 and A2 have forwarded the message of signed CHRG and A3 has been added by the operator based on the location of the vehicle received in the message and velocity of the vehicle. Similarly, for EV2 vehicle, A2 is the aggregator that sends the signed message of EV2 and for EV3 vehicle, A2 is the aggregator that sends the signed message of EV3. A3 and A1 have been added by the operator respectively, for EV2 and EV3. The bipartite graph explains the preferences with respect to distance, charge and waiting time as shown in Figure 7.

Note that, when we consider the parameters individually, the allocation changes, but as per priority-based parameters the final allocation may be the same or different. The allocation of EV2 to A2 is static for every parameter; however, other allocation has been changed. Individual parametric allocations are not optimal and therefore, this proposed priority-based matching market scheme for allocation is beneficial for getting multi-factor allocation.

D. Charging phase

While transmitting of signcrypted ALLOC message, aggregator works only as a forwarder without having the provision of unsigncryption. The unsigncryption of the ALLOC message

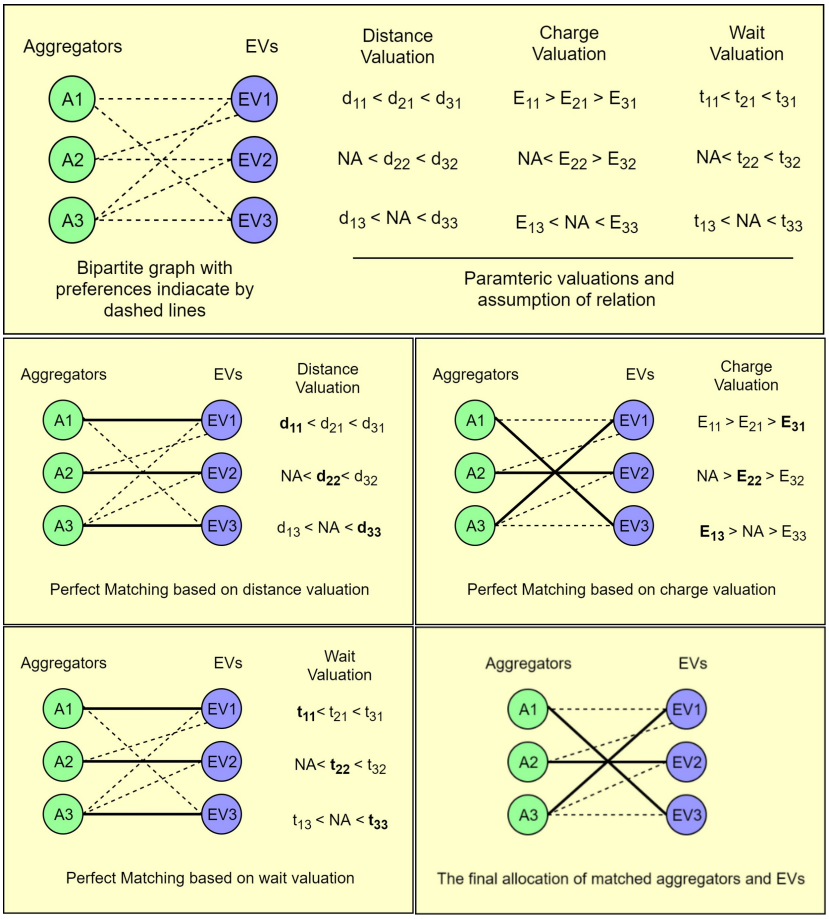

Fig. 7. Bipartite graph representation for proposed allocation scheme

is only possible for EVs which authenticates the source of the message and checks the validity of it in the same process of signcryption and unsigncryption followed previously. Once the EV plugins into a charging station, the charging station logs the hash of the EV's identity and sent it to the operator on a regular basis with batch processing. While charging all the information of the EV is encrypted and saved by itself.

IV. Performance and Analysis

Performance of the proposed system based on computation cost, communication cost, satisfaction ratio, and slot ratio are discussed. The performance metrics are compared with the existing approaches [35][37][38][40]. The selection of these candidate algorithms for comparison is due to the similar kind of framework orientation and privacy-preserving work with the proposed method. Moreover, dynamic tariff decision, priority and supplier matching are also considered in [37][38][40], respectively, which gives the base of comparison with the presented solution. In the following subsections performance metrics, experiment environment, and results are discussed.

A. Performance metrics

Parameters considered for the evaluation of the secured framework for EVs are computation cost, communication cost, satisfaction ratio, slot ratio, charging latency, and load balancing index. These performance evaluation parameters are defined first for clarity as below.

1) Computation and communication costs: : Computation and communications costs are defined in terms of time and bits, respectively. In the case of computation, each of the operations in the cryptographic approach consumes some amount of time and therefore, computation cost measures the cumulative time whereas the communication represents the message overhead criteria for any network-based framework development.

2) Satisfaction Ratio: : This metric is introduced to calculate the satisfaction of the allocation in terms of payoff. Satisfaction Ratio (SR) is calculated as:

$$SR = \frac{Payoff_{alloc}}{Maximum\ payoff} \tag{14}$$

where, Maximum payoff is the probable maximum payoff amount from the overall system's execution. The range of SR is in between of 0 to 1 with maximum value of $SR = 1$ where the payoff of the allocation is actually providing the maximum payoff to the system.

3) Slot ratio:: This metric is introduced to identify the congestion in charging stations. The slot ratio (SL) is calculated as:

$$SL = \frac{No.\ of\ charging\ stations}{No.\ of\ vehicles} \tag{15}$$

For a fix the number of charging stations (practically it is fixed), the increasing number of EVs make the SL ratio decreasing. It is not practically feasible that $SL = 0$ as the number of charging stations cannot be zero. At a certain point of time $SL = 1$ where the number of charging stations and the number of vehicles is equal, optimally balanced load in the framework. With the increasing number of EVs, SL starts decreasing further.

4) Charging latency: This metric is an extended one from the computation cost. In computation cost, only the time for the message exchange processing is only considered; whereas, in charging latency the overall time from initiating charging message to charge completion is measured. Assuming all the EVs charging capacity is x and charging per unit time μ the Charging Latency *(CL)* for a void charged EV is given by,

$$CL = message\ exchange\ time + T_{wait} + T_{chrg} \quad (16)$$

where, message exchange time is actually the communication cost occurred during the process or verification and authentication.

5) Load Balancing Index (LBI): : It plays an important role in the framework, as the overall EV charging time is depending upon this metric. If load balance is not proper, T_{wait} increases and as a result charging latency increases. Therefore, load balancing has been observed and Average Charging Station Allocation (ACSA) calculated as:

$$ACSA = \frac{Total\ number\ of\ EVs}{Total\ number\ of\ charging\ station} \quad (17)$$

B. Experimental environment

In order to evaluate the computation overhead of the proposed scheme and the comparison with existing approaches, Python charm cryptographic library [50] is used. The computing machine runs with Intel Core i7-4765T 2.00 GHz and 16 GB RAM. Lattice and bilinear pairing are used with a super singular elliptic curve with the symmetric Type 1 of size 512 bits (SS512 curve) [51]. 512 bits for an elliptic curve is the experimented value. The specifications of the EV, aggregator and operator are inherited from the recent work on EV charging based on blockchain sensors [35]. However, customization in the security feature and asymmetric cryptography has been included additionally in the present framework discussed here. A High-Level Protocol Specification Language (HLPSL) in the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool has been used for the same. The specifications are shown in Figure 8.

The above-mentioned specification of the entities are involved in the experimentation and additional system parameters are given in Table III.

C. Results

In this subsection, the performance metrics discussed in the preceding section are compared with the existing framework already available and analysed the pros and cons of the framework presented here. First, the computation cost on average (in time) for individual function associated with a security mechanism through the lattice framework has been measured and is listed in Table IV. These measurements are iterated 100 times to obtain the average value of the functions.

TABLE III
EXPERIMENTAL PARAMETERS

Parameter	Value
Transmission range of aggregator	50 meters
Transmission range of EV	20-35 meter
Velocity of the EVs (average)	35-40 km/hour
Number of EVs	20
Number of aggregators	10
Number of charging stations	10
SWIFFT hash function bits	512 bits
Lattice encryption bits	512 bits
Keys bits	512 bits

TABLE IV
COMPUTATION COST FOR INDIVIDUAL FUNCTION IN THE PROPOSED APPROACH

Function Name	Time
Bilinear pairing for Elliptic curve selection (T_ecc)	2.80 ms
Scalar multiplication (T_mul)	1.63 ms
Point addition with bilinear pairing (T_addbp)	0.007 ms
Scalar multiplication with lattice (T_mull)	0.012 ms
Point addition with lattice (T_addl)	0.0010 ms
Encryption (T_enc)	0.43 ms
Decryption (T_dec)	0.28 ms
Hash lattice based (T_hash)	0.0002 ms

Table V compares the computation cost of the presented framework with the four existing schemes. It shows that the encryption-decryption process in other schemes is computationally costlier as compared to the presented work. This better performance id due to the use of lattice cryptography in the solution that makes the process less computing. Also, signcryption mechanism employed further reduces the computation time as signature and encryption are logically done in a single step. For initial setup the computation cost is $(T\_ecc) + (T\_mul) + (T\_addbp) = 4.437ms$. The time for key establishment between aggregator and EV becomes $(T\_mull) + (T\_addl) = 0.0130ms$. Table V classifies the cost in five parts: initialization, key establishment, authentication, encryption and decryption. It also shows the cumulative complexity of the overall proposed algorithms and existing algorithms in comparison.

The complexities are calculated as the initial set up with key establishments, authentication-verification and encryption-decryption where m is the number of aggregators and n is the number of EV users.

Table V shows an interesting fact that the cost of initial set up for the proposed scheme is more than the other approaches in comparison, however, the lattice framework for keys and signcryption-unsigncryption processes has significantly reduced the cumulative computation cost by 11.63% on average. The comparison of the 'order of complexity' for all schemes is also shown and the proposed scheme is less complex compared to others. The communication cost for EVs is charge constrained and hence requires more consideration for communication cost as compared to other modules. Table

role vehicle (EV, OP, EAG: aggregator, ASK_{ev} : asymmetric_key, H: hash_function, lattice_function( ), signcrypt ( ), m: message , SND,RCV: channel (dy))

played_by EV
def =
local state: all the initial parameters
init state: 0
transition:
1. State = 0 to SND(channel(dy))
2. State = 1 to lattice_function( )
3. State = 2 to ASK_{ev} ()
4. State = 2 to { H || ASKev (m)}
5. State = 2 to RCV (channel (dy))

end role

Specification of electric vehicle

role aggregator (EV,OP,EAG: aggregator, ASK_{ev} : asymmetric_key, H: hash_function, lattice_function( ), signcrypt ( ), EV_params, mktmtch: market_matching_function, m: message , SND,RCV: channel (dy))

played_by EAG
def =
local state: all the initial parameters
init state: 0
transition:
1. State = 0 to RCV(channel(dy)){EV_params}
2. State = 1 to lattice_function( )
3. State = 2 to ASK_{ev} ()
4. State = 2 to signcrypt ()
5. State = 2 to mktmtch(EV params)
6. State = 2 to SND

end role

Specification of aggregator

role operator (EV, OP, EAG: aggregator, ASK_{ev} : asymmetric_key, H: hash_function, lattice_function( ), signcrypt ( ), EV_params, mktmtch: market_matching_function, m: message , SND,RCV: channel (dy))

played_by OP
def =
local state: all the initial parameters
init state: 0
transition:
1. State = 0 to RCV(channel(dy)){EAG}
2. State = 1 to lattice_function( )
3. State = 2 to ASK_{ev} () to EAG and EV
4. State = 2 to signcrypt ()
5. State = 2 to mktmtch(EV params)
6. State = 2 to SND

end role

Specification of operator

Fig. 8. Specifications of EV, aggregator and operator

TABLE V
COMPUTATION COST COMPARISON

	Initial set up	Key establishment	Authentication	Encryption	Decryption	Order of Complexity of the overall scheme
Kim et. al. [35]	4.397	0.011	0.677	1.771	1.180	$\mathcal{O}$(n^4+m^2 log(n)
Knirsch et. al. [37]	4.270	0.097	1.233	3.877	2.333	$\mathcal{O}$(n^4 m^2 log(n+m logn)
Nabil et. al. [38]	4.383	0.763	1.447	2.463	2.403	$\mathcal{O}$((n^4+m^2)+m log(n))
Yucel et. al. [40]	4.377	0.134	0.976	4.500	4.124	$\mathcal{O}$(nm^2+n)^4 m log(n)
Proposed scheme	4.437	0.013	0.16	1.43	0.98	$\mathcal{O}$(mn^2+nm log(nm)

VI compares the communication cost of all the considered schemes. For this comparison, ECC of 512 bits, the random number is 128 bits, the message of 128 bits, identity of 128 bits and timestamp of 32 bits have been considered. It is observed that the proposed scheme significantly reduces the communication overhead by 22.6% , 15.4% , 83.% and 55.8% respectively as compared to the approaches depicted in [35][37][38][40].

Next, the satisfaction ratio by increasing the number of EVs from 1 to 20 and aggregators with a fixed number of 10 is measured. Figure 9 shows the results for the satisfaction ratio. The presented approach initially starts with a high (maximum) satisfaction ratio and gradually reduces after 4 EVs in the network; after 10 EVs it follows a constant satisfaction ration of approximately 0.58. As the experimental network has 10 aggregators and 10 charging points, with more 10 EVs the waiting time increases for every EV and therefore, satisfaction ratio achieves a constant value. It depicts that the proposed approach is better than the other approaches by increasing the satisfaction of the EV users by 43.33% on average. The matching market theory and the payoff observation have helped in this regard significantly

Moreover, to observe the system's behaviour in congestion or waiting state, the satisfaction ratio with respect to the slot ratio has been considered and is shown in Figure 10. It shows that up to the slot ratio 1, the satisfaction ratio is 1 and it decreases after that due to the increased congestion leading to the decreased average slot ratio. However, other works, except for the scheme in [40], show a low satisfaction ratio all over irrespective of the slot ratio as they do not follow a strict matching strategy. Slot ratio is below 1 when there are a greater number of vehicles exists as compared with the number of the charging stations. So, whenever, the slot ratio goes below 1 there is the probability that the vehicles allocation payoff decreases as a result satisfaction

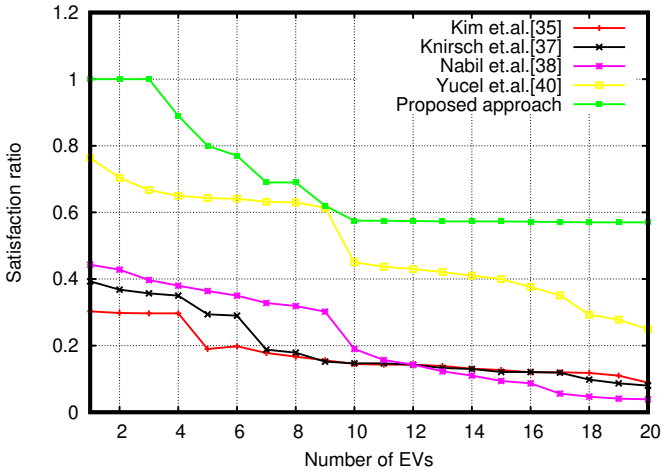

Fig. 9. Comparison of satisfaction ratio with increasing number of EVs

ratio decrease. The graph actually shows this relationship between that two factors. Therefore, the proposed approach is beneficial in gaining the overall payoff of satisfaction and also provides load stability. The constant straight line also suggests the system's stability in congestion for matching with charging stations for the maximized payoff.

The evaluation for charging latency has been calculated with average values for all the scenarios of 20 EVs, 10 aggregators, and 10 charging points. These results are shown in Figure 11. It shows that the proposed approach initially faces a low latency of 42 minutes and increases up to 124 minutes with the increasing number of vehicles. The other algorithms also initially start with low latency and gradually latency increases. In this case all the EVs are considered to have a constant time of charge filled up. The fact behind the variable latency for EVs is depending upon less number of EVs at the start and therefore message exchange time is reduced initially which

TABLE VI
COMPARISON OF COMMUNICATION COST

Schemes	No. of message exchanges with EV	Communication cost
Kim et. al. [35]	4	1824 bits
Knirsch et. al. [37]	5	1670 bits
Nabil et. al. [38]	11	8737 bits
Yucel et. al. [40]	7	3200 bits
Proposed scheme	4	1412 bits

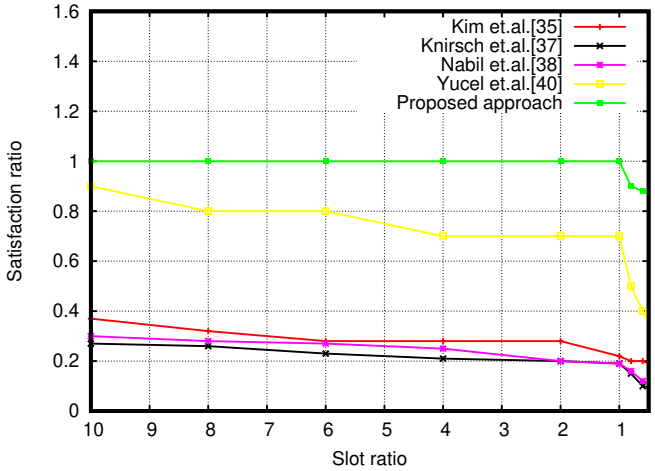

Fig. 10. Comparison of slot ratio vs. satisfaction ratio

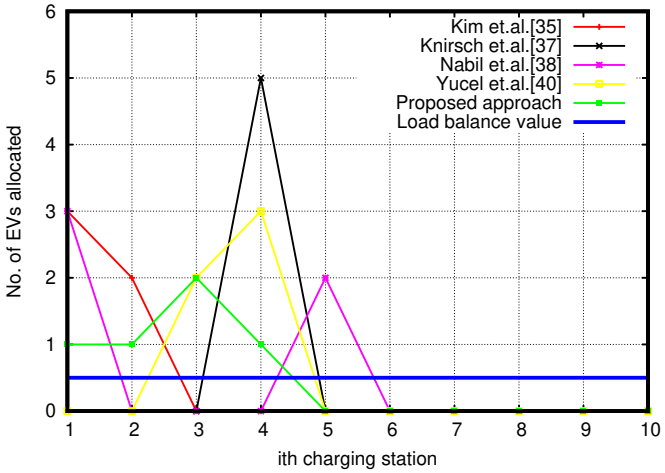

Fig. 12. Comparison of load balance with increasing number of charging stations and average load balance = 0.5

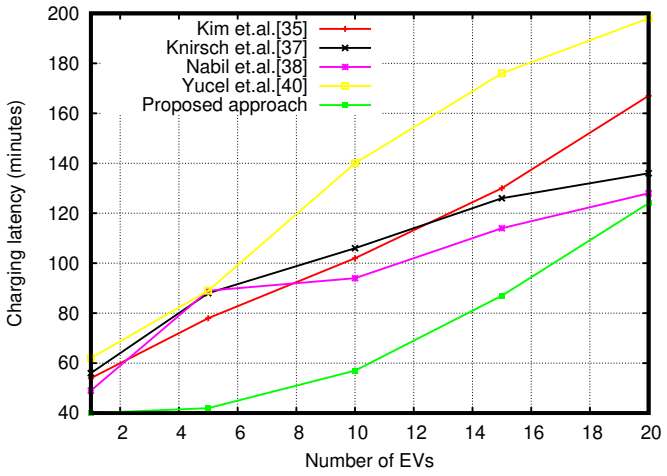

Fig. 11. Comparison of charging latency with the increasing Number of EVs

leads to overall reduced latency. However, with the increasing number of EVs message exchange increases and latency also increases accordingly. Moreover, the perfect matching factors in the presented approach also help in reducing the overall latency. Statistically, the proposed approach is having 34.7% reduced latency as compared to the existing approaches.

The purpose of using the matching market and payoff generation is to balance the load of charging stations leading to reduced waiting time and hence overall reduction in latency. Therefore, loads of the charging stations have been compared to evaluate the efficiency of the proposed approach. Figure 12-15 depicts the comparison of the existing algorithms based on the load balancing factor. The number of charging stations is fixed at 10 and varied the EVs from 5 to 20. Therefore, the average load of the charging stations ranges from 0.5 to 2.0. The load for each of the charging stations is measured and shown in Figure 12-15 with the comparison of other approaches.

Figure 12-15 shows four different scenarios (in terms of average load balance) with a number of EVs ranging from 5 to 20. The load balance data for each of the charging stations is plotted and blue solid lines in the figures represent the average load balance value. The observation from each of the figures depicts that the load in the proposed system is more balanced compared to the other approaches. The peaks in the graphs show the deviation of the systems from the balanced load. The market matching and maximum payoff calculation significantly contribute to this load balance and hence, the proposed system is suitable for IoT based EV charging framework. It is clear from the experimental results that the efficiency of the proposed work better and the feasibility of the method in an EV charging infrastructure perspective.

D. Security Analysis

The use of lattice cryptography in the proposed work significantly enhances the security and privacy of the EV charging framework. For privacy, the presented work provides anonymity through signcryption by hiding the EVs information while charging as the charging station is only able to record the pseudoidentity of the EVs for log purpose. The security proof and related analysis of basic lattice-based

TABLE VII
COMPARISON OF SECURITY FEATURES

	Kim et. al. [35]	Knirsch et. al. [37]	Nabil et. al.[38]	Yucel et. al. [40]	Proposed scheme
Confidentiality	Yes	No	Yes	No	Yes
Authentication	Yes	No	No	Yes	Yes
Digital signature	Yes	No	No	No	Yes
Integrity	Yes	No	No	No	Yes
Non-repudiation	Yes	No	No	No	Yes
Privacy	Yes	Yes	Yes	Yes	Yes

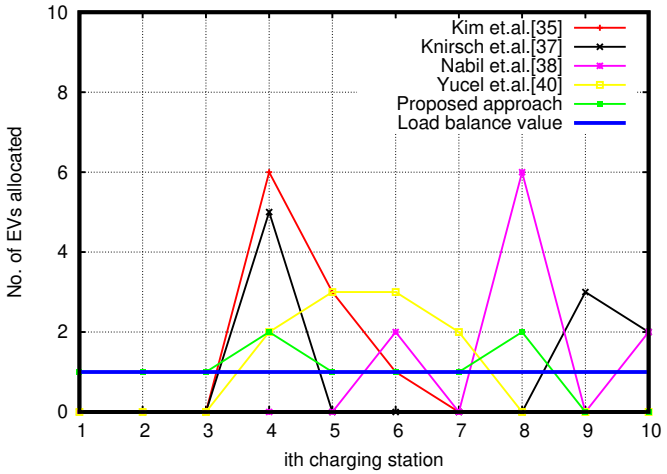

Fig. 13. Comparison of load balance with increasing number of charging stations and average load balance = 1.0

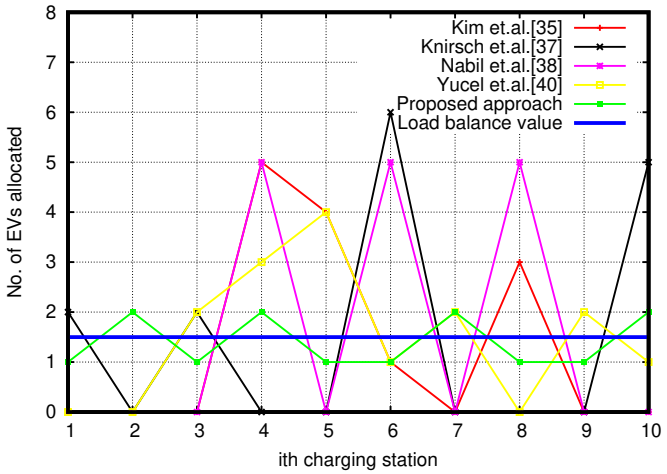

Fig. 14. Comparison of load balance with increasing number of charging stations and average load balance = 1.5

cryptography are already shown in many recent publications [52][53][54].Therefore, the contribution on the basis of security services, viz., confidentiality, authentication and hash, non-repudiation and privacy has been discussed here. It is worth to mention that no separate attacker module is used for security analysis in the study. Rather, lattice signcryption is emphasized and security is measured in terms of security services. This shows the proposed work is robust against security attacks in the above said services. EVs and aggregators are considered to be non-secure which means they are not trustable and

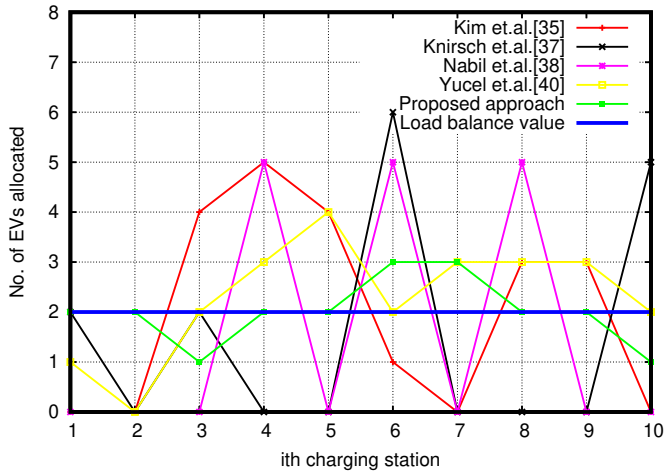

Fig. 15. Comparison of load balance with increasing number of charging stations and average load balance = 2.0

therefore any communication to and fro among them need authentication.

Confidentiality: This security service is provided by using the signcryption method. It uses a hash of 512 bits, encryption-decryption keys of 512 bits, message size of 128 bits block and a random number of 128 bits. The keys are generated using the random basis of 512 bits. Therefore, an attack for a key bit of disclosure, the bit costs becomes:

$$Bit\_cost_{confidentiality} = \prod_{512}^{(0,1)} perm(hashed\ bits) \times perm(message\ bits)$$

where, $\prod_{512}^{(0,1)} perm()$ is the selection of a random bit out of 512 bits with value 0 or 1. The probability of identifying a single bit in the signcryption process is $1/Bit_{cost_{confidentiality}}$ and which is approximately equal to zero. Therefore, it is observed that confidentiality is ensured in the presented work.

Digital signature: Authentication has been ensured by the use of a digital signature. However, the signature is not executed as a separate step; rather, it has been included in a single logical step of signcryption. The probability of two signatures are same to be forged is given as:

$$P_{sign1=sign2} = \frac{1}{\prod_{512}^{(0,1)} k \times \prod_{512}^{(0,1)} k') \times P(H1 = H2)} \quad (18)$$

This approximately equals to 0.000000000034 as $P(H1 = H2) \rightarrow 0, P_{sign1=sign2} \rightarrow 0$ eventually.

Non-repudiation: The message exchange between the entities uses signcryption and therefore, each message transmission ensures non-repudiation with its signature.
Privacy: EVs or aggregators are prone to get controlled by the attackers to perform malicious tasks. Moreover, the location of the EVs and other information need to be secured in the process. To achieve, this aspect, hash of the EV information is used before transmission and hashed value and the mapping is stored by the operator. Aggregators are customized for provisioning only with a forward mechanism to the operator so that the privacy and confidentiality can be maintained. The security features of the existing works of [35][37][38][40] are compared, as shown in Table VII.

Table VII shows that Kim et. al. [35] possesses the similar features; however, the computational complexity on the blockchain is higher as compared to lattice-based signcryption techniques. The other existing approaches are able to provide privacy but unable to execute other security services as required. Therefore, from the security point of view also, the proposed solution is efficient as a secure framework for EV charging in IoT infrastructure. The description of symbols and variables used are listed in Table VIII.

V. Conclusion

In the present work, a framework for electric vehicle charging in IoT infrastructure has been developed with lattice cryptography. The signcryption has been used to generate the keys for convenience and simplicity. Moreover, the market matching theory with maximum payoff calculation has been additionally considered on multi-parameters viz., distance, remaining charge and waiting time. Furthermore, two new performance metrics are identified to locate EV charging stations to the vehicles. The experimental and comparative analysis based on latency, satisfaction and load balance have significantly improved with this framework. The security analysis in this aspect also confirms that the presented solution is able to withstand against any post-quantum computing attacks. In short, the proposed method is able to handle confidentiality-authentication attacks in terms of security. The allocation of blockchain to this framework to check some specific attacks is an interesting step forward and will be considered in the future.The trust management in aggregators is another extended future research problem.

Acknowledgments

This work was partially supported FCT/MCTES through national funds and when applicable co-funded EU funds under the project UIDB/EEA/50008/2020; and by Brazilian National Council for Scientific and Technological Development (CNPq) via Grant No. 309335/2017-5.

References

[1] A. Faiz, C. S. Weaver, and M. P. Walsh, *Air pollution from motor vehicles: standards and technologies for controlling emissions*. The World Bank, 1996.
[2] Cbinsights, "Auto and Mobility Trends In 2019," https://www.cbinsights.com/research/report/auto-mobility-trends-2019/, 2019, [Online; accessed 12-Dec-2019].
[3] M. Huda, M. Aziz, and K. Tokimatsu, "The future of electric vehicles to grid integration in indonesia," *Energy Procedia*, vol. 158, pp. 4592–4597, 2019.
[4] M. Li and M. Lenzen, "How many electric vehicles can the current australian electricity grid support?" *International Journal of Electrical Power & Energy Systems*, vol. 117, p. 105586, 2020.
[5] M. R. Khalid, M. S. Alam, A. Sarwar, and M. J. Asghar, "A comprehensive review on electric vehicles charging infrastructures and their impacts on power-quality of the utility grid," *eTransportation*, vol. 1, p. 100006, 2019.
[6] F. Kupzog, H. J. Bacher, M. Glatz, W. Prüggler, A. Adegbite, and G. Kienesberger, "Architectural options for vehicle to grid communication," *e & i Elektrotechnik und Informationstechnik*, vol. 128, no. 1-2, pp. 47–52, 2011.
[7] F. Al-Turjman and M. Abujubbeh, "Iot-enabled smart grid via sm: An overview," *Future Generation Computer Systems*, vol. 96, pp. 579–590, 2019.
[8] Z.-k. Feng, W.-j. Niu, C.-t. Cheng, and J.-z. Zhou, "Peak shaving operation of hydro-thermal-nuclear plants serving multiple power grids by linear programming," *Energy*, vol. 135, pp. 210–219, 2017.
[9] K. Zhan, Z. Hu, Y. Song, N. Lu, Z. Xu, and L. Jia, "A probability transition matrix based decentralized electric vehicle charging method for load valley filling," *Electric Power Systems Research*, vol. 125, pp. 1–7, 2015.
[10] E. Cascetta, *Transportation systems analysis: models and applications*. Springer Science & Business Media, 2009, vol. 29.
[11] W. Jifeng, L. Huapu, and P. Hu, "System dynamics model of urban transportation system and its application," *Journal of Transportation Systems engineering and information technology*, vol. 8, no. 3, pp. 83–89, 2008.
[12] S. Dhameja, "Electric vehicle battery charging."
[13] G. F. Savari, V. Krishnasamy, J. Sathik, Z. M. Ali, and S. H. A. Aleem, "Internet of things based real-time electric vehicle load forecasting and charging station recommendation," *ISA transactions*, 2019.
[14] B. Csonka and C. Csiszár, "Determination of charging infrastructure location for electric vehicles," *Transportation Research Procedia*, vol. 27, pp. 768–775, 2017.
[15] M. Yue, S. Jemei, R. Gouriveau, and N. Zerhouni, "Review on health-conscious energy management strategies for fuel cell hybrid electric vehicles: Degradation models and strategies," *International Journal of Hydrogen Energy*, 2019.
[16] Z. Li, A. Khajepour, and J. Song, "A comprehensive review of the key technologies for pure electric vehicles," *Energy*, 2019.
[17] S.-Y. Chen, C.-H. Wu, Y.-H. Hung, and C.-T. Chung, "Optimal strategies of energy management integrated with transmission control for a hybrid electric vehicle using dynamic particle swarm optimization," *Energy*, vol. 160, pp. 154–170, 2018.
[18] Z. Gelmanova, G. Zhabalova, G. Sivyakova, O. Lelikova, O. Onishchenko, A. Smailova, and S. Kamarova, "Electric cars. advantages and disadvantages," in *Journal of Physics: Conference Series*, vol. 1015, no. 5. IOP Publishing, 2018, p. 052029.
[19] Ergon, "Benefits of Electric Vehicles," https://www.ergon.com.au/network/smarter-energy/electric-vehicles/benefits-of-electric-vehicles, 2019, [Online; accessed 12-Dec-2019].
[20] Y. Fraiji, L. B. Azzouz, W. Trojet, and L. A. Saidane, "Cyber security issues of internet of electric vehicles," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2018, pp. 1–6.
[21] N. Saxena, S. Grijalva, V. Chukwuka, and A. V. Vasilakos, "Network security and privacy challenges in smart vehicle-to-grid," *IEEE Wireless Communications*, vol. 24, no. 4, pp. 88–98, 2017.
[22] C. W. Cobb and P. H. Douglas, "A theory of production," *The American Economic Review*, vol. 18, no. 1, pp. 139–165, 1928.
[23] S. Networking, "Not known," Notknown, 2019, [Online; accessed 12-Dec-2019].
[24] W. Stallings, *Cryptography and network security: principles and practice*. Pearson Upper Saddle River, 2017.
[25] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) - cost (signature)+ cost (encryption)," in *Annual International Cryptology Conference*. Springer, 1997, pp. 165–179.
[26] X. Fan, T. Wu, Q. Zheng, Y. Chen, M. Alam, and X. Xiao, "Hse-voting: A secure high-efficiency electronic voting scheme based on homomorphic signcryption," *Future Generation Computer Systems*, 2019.
[27] Y. Wang, H. Pang, R. H. Deng, Y. Ding, Q. Wu, and B. Qin, "Securing messaging services through efficient signcryption with designated equality test," *Information Sciences*, vol. 490, pp. 146–165, 2019.

TABLE VIII
LIST OF SYMBOLS

Symbol	Definition
G	A base point of order n on the selected elliptic curve F
$F = (x, y)$	A polynomial form of elliptical curve F
$\mathcal{B}$	A vector calculated from $(poly(n))$
$\aleph_{ag}$	Random basis
$\mathcal{L}$	Lattice of the vector $\mathcal{B}$
K_{ag+}, K_{ag-}	Public key and private key of the EV aggregator.
K_{opagg+}, K_{opagg-}	Public key and private key established between the operator and an aggregator.
EV_{ID}	Id of EV
(R, s)	Digital signature
H, H_1, H_2	Hash functions
d	The distance between an EV and aggregator
m	The number of aggregators' messages arrived for the same CHRG.
E_{th}	Threshold value of charging for CHRG message
E_{res}	Residual charge of EV while initiating charging request
μ	Charging rate of an EV
x	Charge Capacity (full charge) of an EV
α	Number of vehicles allowed in a charging station
ρ	Fraction of charge in process

[28] P. Datta, R. Dutta, and S. Mukhopadhyay, "Functional signcryption," *Journal of information security and applications*, vol. 42, pp. 118–134, 2018.

[29] C. Zhou, "An improved lightweight certificateless generalized signcryption scheme for mobile-health system," *International Journal of Distributed Sensor Networks*, vol. 15, no. 1, p. 1550147718824465, 2019.

[30] D. K. Vaisla, "A lightweight signcryption scheme based on elliptic curve cryptography," *Proceedings of First International Conference on Advances in Computing & Communication Engineering (ICACCE-2014)*, 2014.

[31] V. Rajasekar, S. Varadhaganapathy, K. Sathya, and J. Premalatha, "An efficient lightweight cryptographic scheme of signcryption based on hyperelliptic curve," in *2016 3rd International Conference on Recent Advances in Information Technology (RAIT)*. IEEE, 2016, pp. 394–397.

[32] P.-Y. Ting, J.-L. Tsai, and T.-S. Wu, "Signcryption method suitable for low-power iot devices in a wireless sensor network," *IEEE Systems Journal*, vol. 12, no. 3, pp. 2385–2394, 2017.

[33] M. Nikravan, A. Movaghar, and M. Hosseinzadeh, "A lightweight signcryption scheme for defense against fragment duplication attack in the 6lowpan networks," *Peer-to-Peer Networking and Applications*, vol. 12, no. 1, pp. 209–226, 2019.

[34] J. Yan, L. Wang, L. Wang, Y. Yang, and W. Yao, "Efficient lattice-based signcryption in standard model," *Mathematical Problems in Engineering*, vol. 2013, 2013.

[35] M. Kim, K. Park, S. Yu, J. Lee, Y. Park, S.-W. Lee, and B. Chung, "A secure charging system for electric vehicles based on blockchain," *Sensors*, vol. 19, no. 13, p. 3028, 2019.

[36] X. Huang, Y. Zhang, D. Li, and L. Han, "An optimal scheduling algorithm for hybrid ev charging scenario using consortium blockchains," *Future Generation Computer Systems*, vol. 91, pp. 555–562, 2019.

[37] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," *Computer Science-Research and Development*, vol. 33, no. 1-2, pp. 71–79, 2018.

[38] M. Nabil, M. Bima, A. Alsharif, W. Johnson, S. Gunukula, M. Mahmoud, and M. Abdallah, "Priority-based and privacy-preserving electric vehicle dynamic charging system with divisible e-payment," in *Smart Cities Cybersecurity and Privacy*. Elsevier, 2019, pp. 165–186.

[39] I. A. Kamil and S. O. Ogundoyin, "Lightweight privacy-preserving power injection and communication over vehicular networks and 5g smart grid slice with provable security," *Internet of Things*, vol. 8, p. 100116, 2019.

[40] F. Yucel, K. Akkaya, and E. Bulut, "Efficient and privacy preserving supplier matching for electric vehicle charging," *Ad Hoc Networks*, vol. 90, p. 101730, 2019.

[41] Z. Wan, W.-T. Zhu, and G. Wang, "Prac: Efficient privacy protection for vehicle-to-grid communications in the smart grid," *Computers & security*, vol. 62, pp. 246–256, 2016.

[42] V. Sucasas, G. Mantas, F. B. Saghezchi, A. Radwan, and J. Rodriguez, "An autonomous privacy-preserving authentication scheme for intelligent transportation systems," *Computers & Security*, vol. 60, pp. 193–205, 2016.

[43] H. Marzougui, A. Kadri, J.-P. Martin, M. Amari, S. Pierfederici, and F. Bacha, "Implementation of energy management strategy of hybrid power source for electrical vehicle," *Energy Conversion and Management*, vol. 195, pp. 830–843, 2019.

[44] S. Xu, Z. Yan, D. Feng, and X. Zhao, "Decentralized charging control strategy of the electric vehicle aggregator based on augmented lagrangian method," *International Journal of Electrical Power & Energy Systems*, vol. 104, pp. 673–679, 2019.

[45] R. Carli and M. Dotoli, "A distributed control algorithm for optimal charging of electric vehicle fleets with congestion management," *IFAC-PapersOnLine*, vol. 51, no. 9, pp. 373–378, 2018.

[46] Y. R. Rodrigues, A. Z. de Souza, and P. Ribeiro, "An inclusive methodology for plug-in electrical vehicle operation with g2v and v2g in smart microgrid environments," *International Journal of Electrical Power & Energy Systems*, vol. 102, pp. 312–323, 2018.

[47] M. Liu, P. K. Phanivong, Y. Shi, and D. S. Callaway, "Decentralized charging control of electric vehicles in residential distribution networks," *IEEE Transactions on Control Systems Technology*, vol. 27, no. 1, pp. 266–281, 2017.

[48] F. Gérard and K. Merckx, "Setla: Signature and encryption from lattices," in *International Conference on Cryptology and Network Security*. Springer, 2018, pp. 299–320.

[49] V. Lyubashevsky, D. Micciancio, C. Peikert, and A. Rosen, "Swifft: A modest proposal for fft hashing," in *International Workshop on Fast Software Encryption*. Springer, 2008, pp. 54–72.

[50] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, "Charm: a framework for rapidly prototyping cryptosystems," *Journal of Cryptographic Engineering*, vol. 3, no. 2, pp. 111–128, 2013.

[51] T. Teruya, K. Saito, N. Kanayama, Y. Kawahara, T. Kobayashi, and E. Okamoto, "Constructing symmetric pairings over supersingular elliptic curves with embedding degree three," in *International Conference on Pairing-Based Cryptography*. Springer, 2013, pp. 97–112.

[52] C. Peikert, "Lattice cryptography for the internet," in *international workshop on post-quantum cryptography*. Springer, 2014, pp. 197–219.

[53] S. Okumura, S. Sugiyama, M. Yasuda, and T. Takagi, "Security analysis of cryptosystems using short generators over ideal lattices," *Japan Journal of Industrial and Applied Mathematics*, vol. 35, no. 2, pp. 739–771, 2018.

[54] G. Barthe, X. Fan, J. Gancher, B. Grégoire, C. Jacomme, and E. Shi, "Symbolic proofs for lattice-based cryptography," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2018, pp. 538–555.