# Electric Vehicles Privacy Preserving Using Blockchain in Smart Community

Omaji Samuel[1], Nadeem Javaid[1(✉)], Faisal Shehzad[1], Muhammad Sohaib Iftikhar[1], Muhammad Zohaib Iftikhar[1], Hassan Farooq[1], and Muhammad Ramzan[2,3]

[1] Department of Computer Science, COMSATS University, Islamabad 44000, Pakistan
omajiman1@gmail.com, nadeemjavaidqau@gmail.com
[2] Department of Computer Science and IT, University of Sargodha, Sargodha, Pakistan
[3] Pakistan School of Systems & Technology, University of Management and Technology, Lahore, Pakistan

**Abstract.** During the process of charging, electric vehicle's location is usually revealed when making payment. This brings about the potential risk to privacy of electric vehicle. We observe that the trade information recorded on blockchain may raise privacy concern and therefore, we propose a blockchain oriented approach to resolve the privacy issue without restricting trading activities through $(\epsilon, \delta)$-differential privacy. The proposed scheme does not only preserve the electric vehicle's location; however, prevents semantic, linking and data mining based attacks. Simulation results show that as the privacy level increases, the risk revealing decreases as well.

**Keywords:** Blockchain · Demand side management · Electric vehicle · Energy trading and privacy preserving

## 1 Introduction

Presently, there has been a tremendous advancement in the development of electric vehicles (EVs). EVs as part of demand-side management provide more benefits and environmental advantages [1]. Several countries of the world have started adopting EVs for de-carbonization and mobile energy storage to achieve a green city [2]. As the number of EV continues to increase, there is a need to create a charging infrastructure. Authors in [3] and [4] have proposed an optimal settings of charging station (CS) and optimal scheduling to minimize vehicular resources and time. However, authors do not give emphasis on privacy related issues of EV such as location, price and consumption. Traditionally, EV is controlled and monitored by a centralized system [5]. Besides, the centralized system also faces issues of privacy and security like other known centralized schemes [6]. Also, the centralized system lacks the ability to enforce the decision-making process


L. Barolli et al. (Eds.): BWCCA 2019, LNNS 97, pp. 67–80, 2020.
https://doi.org/10.1007/978-3-030-33506-9_7

on autonomous EVs. Solutions for aforementioned problem include peer-to-peer and decentralization via blockchain [7]. The Table 1 provides description of the parameters or variables used throughout this paper.

**Table 1.** Parameters and variables

| Notations | Descriptions |
|---|---|
| $A^p_{\min}$ | Minimum acceptance probability |
| $A^p_k$ | The $kth$ charging station's (CS) assignment probability |
| $A^p_n$ | The $nth$ electric vehicle's (EV) acceptance probability |
| $b_{i,j}$ and $z_{j,i}$ | Row and column stochastic matrices |
| $Pr_b$ | The $bth$ blockchain offered price by CS |
| $CS^{sel}_k$ | The $kth$ CS's selection probability based on $Pr_b$ and $d^k_n$ |
| $d^k_n$ | Distances of $nth$ EV from the $kth$ CS |
| $g_b$ and $pr_b$ | The broadcast parameters of distance and offered price, respectively |
| $lap(y)$ | Cumulative Laplace distribution for the given input $y$ |
| $N^-$ and $N^+$ | Cardinality of the out-bound and in-bound flow for $ith$ nodes and $jth$ vertices |
| $P^{req}_n$ | Energy the $nth$ EV required from CS |

The concept of blockchain is introduced in 2008 by Satoshi Nakamoto [8] and Bitcoin is its first application. Blockchain is a shared ledger that facilitates the process of recording transaction and tracking assets in a distributed network. Within the last decade, blockchain is now the focus of many researchers, stakeholders and industries spanning from voting, healthcare, finance, real estate, utilities [9], Internet of Things [10,11], wireless sensor network [12,13]. Blockchain provides decentralization, immutability, trustfulness [14], traceability, secure environment and data storage. Advantages of blockchain include real-time transaction and payment; quick response time; avoids duplication; prevents fraud and cyber attacks; minimizes time-consuming vetting process and provides transparency.

Several studies in [15–21] used blockchain as a privacy-preserving mechanism for data aggregation; privacy protection and energy storage; secure classification of multiple data; incentive announcement network for a smart vehicle; crowdsensing applications; dynamic tariff decision, payment mechanism for vehicle-to-grid, data right management [22], and incentive for lightweight clients [23]. However, blockchain solution is inefficient to tackle data mining and linking attacks [24]. These attacks take advantage of exposed information stored in a block and privacy is disclosed by linking records of other datasets.

From the literature above and the inspiration obtained from the work of [25], we derive our problem statement based on the following analogies: assuming we have a setup of centralized server coordinating the trading between EVs and CSs. The server publishes CSs with offered prices and locations and EVs autonomously choose the preferred CSs. The benefit is that the EVs do not need to disclose their exact locations and the server does not know the CSs which EVs

have selected. The disadvantage is that the server has no control over the assignment of CSs and the EVs can select CSs based on their distances and offered prices. In contrast to the centralized approach, we have a setup of blockchain-based energy trading between EVs and CSs. The EVs send their locations and the required quantity of energy to the blockchain. The blockchain controls and allocates nearby CSs to the EVs while maximizes EVs' acceptance rates. However, EVs' private information such as locations are revealed to the blockchain during the payment process, which raise privacy concerns to the owners of EV.

In a privacy-preserving perspective, information recorded on blockchain may raise privacy concern [26]. Nevertheless, the traditional system cannot protect EVs' information within this scenario. Hence, we propose a system that protects EVs' location while ensuring fair energy trading. The proposed system will prevent re-identification attack via private blockchain since EVs' transaction records are stored across different networks. Thus, honest-but-curious EVs cannot infer the identity of EVs through observational studies.

The organization of the paper is as follows: Sect. 2 provides the paper contributions while Sect. 3 discusses the proposed system model as well as problem formulations. Simulation results are discussed in Sects. 4 and 5 provides the conclusion and future work.

## 2 Contributions

In this section, the contributions of this paper are as follows.

1. We protect EV's privacy from future blockchain based data transmission by defending EV against a possible breach. Our proposed scheme ensures complete accuracy since it is implemented using real dataset and it is efficiently adoptable since all computations are done off-chain, thereby reducing the number of computing resources on the chain.
2. Differential privacy is proposed by using the consensus energy management algorithm [27] to conceal the broadcast information.
3. Two types of blockchain are proposed: private blockchain located at rural area achieves the following: prevents re-identification and data mining attacks due to membership restrictions and provides subsidy for charging; and public blockchain located in urban area resolves the scalability issue.

## 3 Proposed System Model and Problem Formulations

### 3.1 System Overview

In the proposed system in Fig. 1, three fundamental entities with distinct functionalities are studied. Firstly, the EV as an entity that requires energy for charging, secondly, CS as an entity that acts as an energy provider. However, CS gets charged by the main grid if its internal generated energy is insufficient. In addition, the CS charged EV on the basis of the offered price [1]. Lastly, the

aggregator (blockchain) acts as a broker between the EV and CS for fair energy transactions. EVs send charging request and location to the aggregator; aggregator broadcasts this information to the blockchain network. CSs who meet this requirement response back with offered price and location to the aggregator. Aggregator reports this information to the requesting EV and CS is assigned to EV on the basis of price and location.

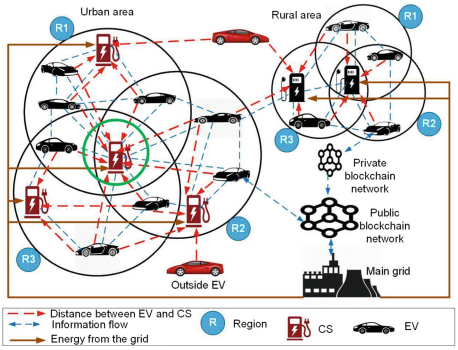


**Fig. 1.** Proposed system. EV: electric vehicle, and CS: charging station.

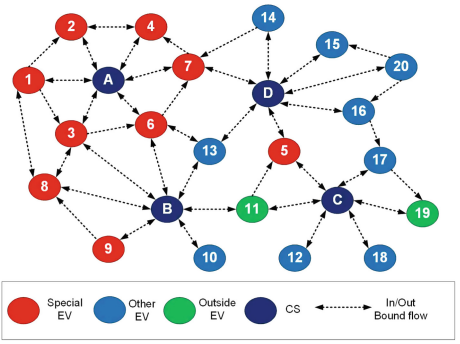


**Fig. 2.** Illustration of the system network.

### 3.2 Blockchain Based Location Privacy Preserving with Differential Privacy

In energy trading, the EV's charging request task is denoted as RDT, while CS's discharging response task given as RST. Thus, the rationality of RDT and RST are as follows:

RDT: In the blockchain, EVs addresses are anonymous; hence, the blockchain receives all RDT from EVs and broadcast them. However, blockchain is unaware of the locations and charging request of EVs. In addition, EVs choose charging locations based on reduced $Pr_b$ and $d_n^k$, to minimize traveling costs. Thus, blockchain has no control over the activities of EVs [25].
RST: CSs send $l_k$ and $Pr_b$ to the blockchain. Blockchain assigns CS to EV based on $d_n^k$. Thus, the blockchain controls activities of EVs. Since RDT and RST are known to the blockchain, which may raise privacy concerns [25]. A blockchain knowledge base ($BKB$) that stores all records of CSs and EVs, respectively is proposed.

$$BKB = \{EV_n, CS_k, d_n^k, A_k^p, CS_k^{sel}, l_n, l_k, H_n\{l_n, P_n^{req}\}, H_k\{l_k, Pr_b\}\}, \quad (1)$$

where $EV_n$ and $CS_k$ are lists of EVs and CSs, respectively. $H_n$ and $H_k$ are the histories of EVs and CSs; while, $l_n$ and $l_k$ are the locations of EVs and CSs, respectively.

### 3.2.1 Adversary Model

We assume that there are honest-but-curious aggregators on the blockchain network. These curious aggregators disclose information of EVs for selfish interest or financial benefits. Also, the curious aggregator known as $CurAg$ can join the public or private blockchain to gain information [25]. Moreover, the EV's current, past, and future location can be leaked by $CurAg$ during charging and payment process. The attacker can be any participant in the blockchain network. Although, an attacker in the public blockchain can access transactional records of EVs, while attacker as EV can join the private blockchain to get transaction records of other EVs. Besides, access to other private blockchain is hindered due to membership restrictions [25]. Attacker as an aggregator may have access to transactional records of his own dataset. However, it is impossible to access records of other aggregators [25].

### 3.2.2 Privacy-Preserving in Blockchain

The use of blockchain provides anonymization, ensures that EV fulfilled an agreement with the CSs and decentralized the system to prevent a single point of failure. Also, private blockchain prevents the re-identification attack since each aggregator has distinct transactional history. Thus, it is infeasible for an attacker to access transactional records of all aggregators without poisoning their records [25].

Process of blockchain:

1. Registration: EVs and CSs are required to register with their private $sk$ and public $pk$ key for verification and authentication.
2. CS price mechanism: the price offered to EV is determined by CS.
3. Smart contract: CSs and EVs are required to make an initial token deposit which prevents double spending and false declaration of information.
4. EV's assignment: EV prefers CS on the basis of $l_n$ and $Pr_b$, and make requests accordingly. However, EV is validated based on uploaded $l_n$ in the urban area; thereby, granting access to a specific CS.
5. CS's selection: Blockchain ensures that CSs have the available discharging capacities from the urban area to charge EVs. Otherwise, a new block is created with deduction of the deposited token from CS's account.
6. Consensus: EVs make charging request to the blockchain. Miner validates the authenticity of the request. In this paper, proof of authority (PoA) is used [28]. If requests are accepted, then payment transfer is made to CS's wallet account. Otherwise, if the claim is falsified, the token deposit is used as a penalty.

Payment process: EVs wish to get charged at the closest possible distance to their locations. Assuming all CSs sell energy at a fixed price, the acceptance probability of EV will drop. Thus, the acceptance of EV is enhanced if CSs discharge at different offered prices. Hence, acceptance probability of EV is calculated in Eq. (2) [25].

$$A_n^p = \frac{d_{n,k}^{\max} - A_{min}^p}{d_{n,k}^{\max}};\ 0 \leq A_k^p \leq 1, \tag{2}$$

$$A_k^p = 1 - (1 - A_n^p)^R. \tag{3}$$

We assume CSs covers all $l_n$ of EVs, while some CSs do not cover EV's $l_n$. This scenario is depicted in Fig. 1. Thus, the acceptance probability of EV is proportional to the $l_k$ of CS. However, from Fig. 1, the CS enclosed in green circle gets the highest acceptance by EVs since it covers all locations. The CS's assignment probability is calculated in Eq. (3); where $R = 3$ is the number of regions. While the minimum distance of EV from CS is calculated in Eq. (4) [25].

$$A_{min}^p = 2r, \tag{4}$$

We consider the isolated CS, i.e., CS that covers only few EVs' location; hence, the average distance $AVG_{iso}^d$ is calculated by counting $R$ within EV's maximum travel distance to CS as given in Eq. (5) [25]; where $r = 2$ is a constant value.

$$AVG_{iso}^d = d_{n,k}^{\max} - r. \tag{5}$$

The CS's selection probability is solved as the hyperbolic function of the $Pr_b$ and $d_n^k$ and given in Eq. (6) [25].

$$CS_k^{sel} = \begin{cases} \frac{e^x - e^x}{e^x + e^{-x}},\ if\ d_n^k \leq d_{n,k}^{\max} \\ 0, \quad if\ otherwise, \end{cases} \tag{6}$$

where,

$$x = \alpha \frac{Pr_b}{d_n^k};\ 0 < CS_k^{sel} \leq 1, \tag{7}$$

where $\alpha$ is a constant value.

Assumptions: from Eq. (6), CS with lower distance and minimum offered price is selected with high probability; CS with higher distance and minimum offered price is selected with low probability, whereas, CS whose distance is more than the maximum distance of the concerned EV with higher offered price is not selected.

To further protect EV's location as well as the amount paid to CS, $\{\epsilon, \delta\}$-differential privacy is proposed in this paper. The communication between EVs and CSs formed a directed graph $G$, such that $G = \{V, E\}$, where $V$ is a set of nodes and $E$ is set of edges. $V = N \cup K$ and lets $\{j, i\} \in E$ if and only if node $i$ communicates with node $j$ [27]. Node $i$ is the out-bound of node $j$; however, self loop, i.e., $\{j, j\}$ is not considered in this paper [27]. We derive the in-bound and out-bound values from Fig. 2 as given in Table 2.

**Table 2.** Cardinality of in-bound and out-bound derived from Fig. 2.

| | A | B | C | D | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $N^-$ | 5 | 7 | 7 | 5 | 1 | 1 | 2 | 2 | 1 | 1 | 2 | 2 | 2 | 1 | 3 | 1 | 2 | 2 | 1 | 3 | 3 | 1 | 1 | 3 |
| $N^+$ | 5 | 7 | 7 | 5 | 1 | 2 | 4 | 2 | 2 | 4 | 3 | 4 | 1 | 1 | 3 | 1 | 3 | 1 | 2 | 2 | 1 | 1 | 2 | 2 |

In Table 2, stochastic row and column matrices are generated using Eqs. (8) and (9), respectively [27].

$$b_{i,j} = \begin{cases} \frac{1}{|N^+|+1}, \ if \ i \in N^+ \\ 1 - \sum_{i=1}^{|N^+|} b_{i,j}, \ if \ i = j \\ \frac{1}{|N^+|}, \quad if \ i \neq j, \end{cases} \tag{8}$$

$$z_{j,i} = \begin{cases} \frac{1}{|N^-|+1}, \ if \ i \in N^+ \\ 1 - \sum_{i=1}^{|N^-|} z_{j,i}, \ if \ i = j \\ \frac{1}{|N^-|}, \quad if \ i \neq j. \end{cases} \tag{9}$$

We generate the blockchain broadcast information about the $d_n^k$ and $Pr_b$ using Eqs. (10) and (11), respectively [27].

$$g_b = \begin{cases} d_{n,k}^{\min}, \ if \ i \in N^+ \\ d_{n,k}^{\max}, \ if \ i \in N^- \\ \sum_{i=1}^{|N^-|} b_{i,j} g_b + \eta pr_b, \quad if \ i \neq j, \end{cases} \tag{10}$$

$$pr_b = \begin{cases} Pr_b^{\min}, \ if \ i \in N^+ \\ Pr_b^{\max}, \ if \ i \in N^+, \end{cases} \tag{11}$$

where, $d_{n,k}^{\min}$ and $d_{n,k}^{\max}$ are minimum and maximum distances of EVs from CSs; whereas, $Pr_b^{\min}$ and $Pr_b^{\max}$ are minimum and maximum offered prices and $\eta = 0.8$ is scaling factor. The broadcast information is modified by adding a cumulative Laplace noise as given in Eqs. (12) and (13). Thus, Eq. (1) is updated with the new broadcast information as given in Eq. (16).

$$g_{b+1} = \begin{cases} g_{b+1} b_{i,j} + lap(y), \ if \ i \in N^+ \\ g_b b_{i,j} + lap(y), \quad if \ i \in N^-, \end{cases} \tag{12}$$

$$pr_{b+1} = \begin{cases} z_{j,i} pr_{b+1} + lap(y), \ if \ i \in N^+ \\ z_{j,i} pr_b + lap(y), \quad if \ i \in N^-, \end{cases} \tag{13}$$

where

$$lap(y) = \begin{cases} \frac{\sigma}{\sqrt{2}} e^{2y}, \ if \ y < 0.5 \\ \frac{-\sigma}{\sqrt{2}} e^{2(1-y)}, \ if \ y \geq 0.5, \end{cases} \tag{14}$$

where

$$\sigma = \frac{\max(y) - \min(y)}{\epsilon}, \tag{15}$$

$$BKB(b+1) = \{EV_n, CS_k, g_{b+1}, A_k^p, CS_k^{sel}, l_n, l_k, H_n\{l_n, P_n^{req}\}, H_k\{l_k, pr_{b+1}\}\}. \tag{16}$$

$BKB(b+1)$ is broadcast to the blockchain network. Even if an attacker has the broadcast information, it will be impossible to infer the ownership of information. Thus, we define the privacy risk of EVs $R_{i,n}^{val}$ over their private information $BKB(b+1)$ as [29]:

$$R_{i,n}^{val}(BKB(b+1)) = PC(BKB(b+1)).SL(BKB(b+1)), \tag{17}$$

where the privacy concern $PC(BKB(b+1)) \in \{0,1\}$ and sensitivity level $SL(BKB(b+1)) \in \{0,1\}$. Using $(\epsilon, \delta)$-differential privacy, the $SL(BKB(b+1))$ is obtained by finding their differences $(f(\overline{G_1}) - f(\overline{G_2}))$, i.e., the set $\overline{G_1}$ and $\overline{G_2}$ differing on at most one element [29]. However, $\epsilon$ and $\delta$ are privacy levels of price and location with given values of 1, 2, 3, 4, 5 and 6, respectively.

### 3.3 Blockchain Smart Contract

Figure 3 shows smart contract for the proposed scheme. Blockchain is unaware of when and where EV will go; hence, EV's exact location is preserved. Since CS status in public blockchain differs from that of a private blockchain. Thus, blockchain ensures CS is available in the urban context before assigning EV to prevent void contract [25]. Similarly, private blockchain must verify if CS is assigned to public blockchain or not before assigning EV to prevent void contract. For EV to make a charge request, its credit value (CR) is verified and authenticated with the $sk$ and $pk$ to ensure EV has been registered. If CR is not empty, EV can make a charge request by uploading its region and $P_n^{req}$ to the aggregator. The aggregator verifies region via region identity $Rid$. The $Rid$ is used to determine if EV is in a rural area (private blockchain) or urban area (public blockchain) for which the specified offered prices are determined. Also, the offered prices for types of EV are verified via EV identity $EVid$. Once CS supplied the required charging, payment is made to CS's wallet account by concerned EV. If the current time of CS is more than the agreed due time $CSdueTime$ to verify the payment, a token deduction is made against such CS.

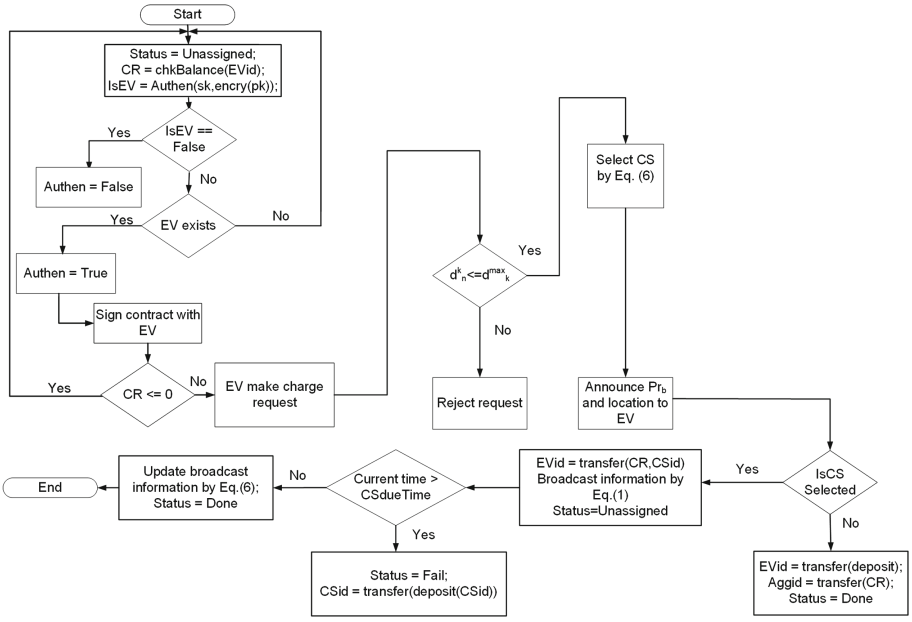


**Fig. 3.** Smart contract.

## 4 Simulation Results

Simulation results and discussions are presented in this section.

### 4.1 Experimental Setup

We develop our blockchain using the ethereum platform [30] with the following dependencies; Truffle v5.0.8 (core: 5.0.8), Solidity v0.5.0 (solc-js), Node v10.13.0 and Web3.js v1.0.0-beta.37. Also, we customize our codes using JavaScript. The hash operations are performed using the solidity keccak256 library and some of the data used are randomly generated, if not specified. Simulation results are generated using MATLAB2018. The hardware platform is a Dell i5, with 8 GB ram and CPU of 1.60 Hz and 1.80 GHz.

### 4.2 Simulation Dataset

In this section, simulation results describe the evaluation of the proposed blockchain based privacy preserving for EV's location. In this paper, 20 EVs and 4 CSs are used. The offered prices by the four CSs and the real distance between EVs from CSs are taken from [1]. The EV's battery capacity and CSs' specifications are also taken from [1] (Figs. 4 and 5).

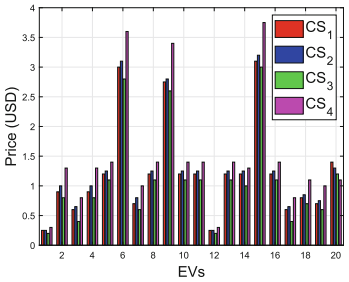


**Fig. 4.** Price offered by four CSs [1].

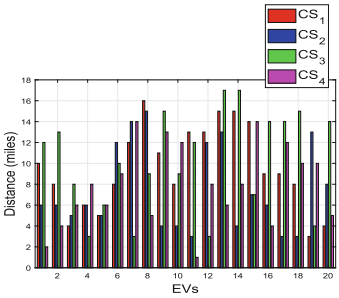


**Fig. 5.** Distance of EVs from CSs [1].

### 4.3 Evaluation of EV's Selection and CS's Assignment Probability

This section discusses the EV's acceptance and CS's assignment probability. EV accepts CS with the closest distance from its location. By assumption, if all CSs announce the same offered for charging of EV, then EV's selection probability will be reduced. Using Eqs. (6) and (7), the Fig. 6 shows the CS's selection probability is close to the maximum limit. The results further show that the EV's acceptance of CS can only be achieved if the number of counted regions fall within the EV's maximum distance to the CS. Thus, the probabilities of all CSs either as an edge or as isolated for being selected will be increased. However, the offered price by CS also determines its acceptance by EV. The CS with the closest distance and the lowest offered price has a high probability of being accepted. Also, the CS with the longest distance and lowest offered price is accepted with a low probability. Nevertheless, if the distance to CS is more than the maximum distance of EV, CS may be rejected even if it offers the lowest price. Using Eq. (2), the probability of CS being assigned to EV is based on distance and is proportional to regions where the distance is covered.

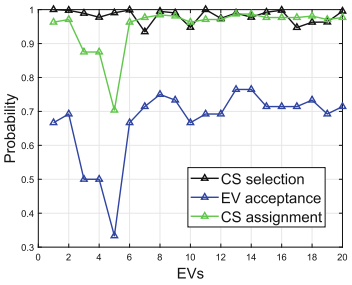


**Fig. 6.** Various probabilities of CSs and EVs.

### 4.4 Privacy Preserving Evaluations Using the Proposed Blockchain and Differential Privacy

This section discusses the $(\epsilon, \delta)$-differential privacy-preserving for the proposed blockchain scheme.

In Figs. 7 and 8, the individual EV privacy is protected against set theory attack [26]. The results further explained that as the privacy level increases, the risk revealing decreases as well. The proposed scheme also prevents linking based attack via $(\epsilon, \delta)$-differential privacy which hindered adversary activities [26]. The private blockchain approach of the scheme prevents data mining attack since transaction records of EVs are scattered across different private network which is strengthen by membership restriction.

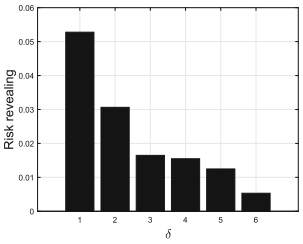


**Fig. 7.** Risk revealing versus privacy level for the offered price.

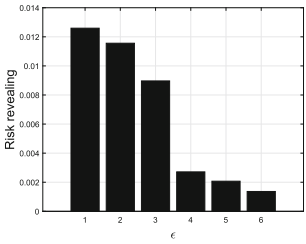


**Fig. 8.** Risk revealing versus privacy level for the distance.

### 4.5 Computational Blockchain Cost Analysis

Creating a new block in blockchain requires strict verification process from an authorized node. In this paper, PoA adopted from our previous work [28] where Pagerank rank mechanism is used to select the node as the authorized node on the basis of its reputation score. Hence, the latency of confirmation time is reduced since only authorized node is allowed to create a block and computes the assignment and selection probability off-chain, thereby reducing the number of computing resources needed on the chain. From Fig. 3, the time complexity of the smart contract is less than O(n) [25]. Hence, the computational burden has no influence on the blockchain.

## 5 Conclusion

This paper examines that transactional record on blockchain may raise privacy concern such as disclosing private information like location and price. Three ways locations of EV are disclosed such as current, previous and future are examined. To preserve the location privacy of EVs, a private blockchain is incorporated

which prevent re-identification attack due to membership restrictions. Thus, the transactional record histories of EVs cannot be inferred by the attacker since records are spread across the network. To further preserve the records, differential privacy is exploited to conceal the records against observational studies. The CS's assignment and EV's selection probability are derived based on the offered price and location of EVs. Simulation results demonstrate that privacy is achieved through risk revealing metric. Also, the proposed approach prevents semantic based attack since private blockchain is involved; data mining and linking based attack since differential privacy is used.

In the future, the neighboring energy trading where dynamic pricing is an issue for charging the EVs in a smart community will be explored. Furthermore, we intend to consider the initial state as the possible privacy breach, such that even if an attacker has the exact knowledge about the initial state of other EVs, it will be difficult to breach their privacy.

## References

1. Aujla, G.S., Kumar, N., Singh, M., Zomaya, A.Y.: Energy trading with dynamic pricing for electric vehicles in a smart city environment. J. Parallel Distrib. Comput. **127**, 169–183 (2019)
2. De Hoog, J., Alpcan, T., Brazil, M., Thomas, D.A., Mareels, I.: Optimal charging of electric vehicles taking distribution network constraints into account. IEEE Trans. Power Syst. **30**, 365–375 (2014)
3. Lin, C.-C., Deng, D.-J., Kuo, C.-C., Liang, Y.-L.: Optimal charging control of energy storage and electric vehicle of an individual in the internet of energy with energy trading. IEEE Trans. Industr. Inf. **14**, 2570–2578 (2017)
4. Aujla, G.S., Jindal, A., Kumar, N.: EVaaS: electric vehicle-as-a-service for energy trading in SDN-enabled smart transportation system. Comput. Netw. **143**, 247–262 (2018)
5. Liu, H., Zhang, Y., Yang, T.: Blockchain-enabled security in electric vehicles cloud and edge computing. IEEE Netw. **32**, 78–83 (2018)
6. Aitzhan, N.Z., Svetinovic, D.: Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans. Dependable Secure Comput. **15**, 840–852 (2016)
7. Kang, J., Rong, Y., Huang, X., Maharjan, S., Zhang, Y., Hossain, E.: Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. IEEE Trans. Ind. Inf. **13**, 3154–3164 (2017)
8. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system, vol. 1, pp. 1–9 (2008)
9. Zahid, M., Javaid, N., Rasheed, M.B.: Balancing electricity demand and supply in smart grids using blockchain. M.S. thesis, COMSATS University Islamabad (CUI), Islamabad 44000, Pakistan, July 2019
10. Rehman, M., Javaid, N., Awais, M., Imran, M., Naseer, N.: Cloud based secure service providing for IoTs using blockchain. In: 2019 IEEE Global Communications Conference: Communication & Information Systems Security, USA, pp. 1–7 (2019)
11. Javaid, A., Javaid, N., Imran, M.: Ensuring analyzing and monetization of data using data science and blockchain in loT devices. M.S. thesis, COMSATS University Islamabad (CUI), Islamabad 44000, Pakistan, July 2019

12. Mateen, A., Javaid, N., Iqbal, S.: Towards energy efficient routing in blockchain based underwater WSNs via recovering the void holes. M.S. thesis, COMSATS University Islamabad (CUI), Islamabad 44000, Pakistan, July 2019
13. Khan, R.J.U.H., Javaid, N., Iqbal, S.: Blockchain based node recovery scheme for wireless sensor networks. M.S. thesis, COMSATS University Islamabad (CUI), Islamabad 44000, Pakistan, July 2019
14. Kazmi, S.Z., Javaid, N., Imran, M.: Towards energy efficiency and trustfulness in complex networks using data science techniques and blockchain, M.S. thesis, COMSATS University Islamabad (CUI), Islamabad 44000, Pakistan, July 2019
15. Noshad, Z., Javaid, N., Imran, M.: Analyzing and securing data using data science and blockchain in smart networks. M.S. thesis, COMSATS University Islamabad (CUI), Islamabad 44000, Pakistan, July 2019
16. Guan, Z., Si, G., Zhang, X., Longfei, W., Guizani, N., Xiaojiang, D., Ma, Y.: Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities. IEEE Commun. Mag. **56**, 82–88 (2018)
17. Shen, M., Tang, X., Zhu, L., Xiaojiang, D., Guizani, M.: Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. IEEE Internet Things J. **1**, 1–11 (2019)
18. Li, L., Liu, J., Cheng, L., Qiu, S., Wang, W., Zhang, X., Zhang, Z.: CreditCoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. IEEE Trans. Intell. Transp. Syst. **19**(7), 2204–2220 (2018)
19. Wang, J., Li, M., He, Y., Li, H., Xiao, K., Wang, C.: A blockchain based privacy-preserving incentive mechanism in crowdsensing applications. IEEE Access **6**, 17545–17556 (2018)
20. Gao, F., Zhu, L., Shen, M., Sharif, K., Wan, Z., Ren, K.: A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. IEEE Netw. **99**, 1–9 (2018)
21. Feng, Q., Debiao, H., Zeadally, S., Khan, M.K., Kumar, N.: A survey on privacy protection in blockchain system. J. Netw. Comput. Appl. **1**, 1–14 (2018)
22. Naz, M., Javaid, N., Iqbal, S.: Research based data rights management using blockchain over Ethereum network. M.S. thesis, COMSATS University Islamabad (CUI), Islamabad 44000, Pakistan, July 2019
23. Ali, I., Javaid, N., Iqbal, S.: An incentive mechanism for secure service provisioning for lightweight clients based on blockchain. M.S. thesis, COMSATS University Islamabad (CUI), Islamabad 44000, Pakistan, July 2019
24. Craig, D.W.: Understanding the links between privacy and public data sharing. Nat. Methods **13**, 211 (2016)
25. Yang, M., Zhu, T., Liang, K., Zhou, W., Deng, R.H.: A blockchain-based location privacy-preserving crowdsensing system. Future Gener. Comput. Syst. **94**, 408–418 (2019)
26. Gai, K., Yulu, W., Zhu, L., Qiu, M., Shen, M.: Privacy-preserving energy trading using consortium blockchain in smart grid. IEEE Trans. Ind. Inf. **1**, 1–10 (2019)
27. Zhao, C., Chen, J., He, J., Cheng, P.: Privacy-preserving consensus-based energy management in smart grids. IEEE Trans. Sig. Process. **66**, 6162–6176 (2018)
28. Samuel, O., Javaid, N., Awais, M., Ahmed, Z., Imran, M., Guizani, M.: A blockchain model for fair data sharing in deregulated smart grids. In: 2019 IEEE Global Communications Conference: Communication & Information Systems Security, USA, pp. 1–7 (2019)

29. Yassine, A., Shirehjini, A.A.N., Shirmohammadi, S.: Smart meters big data: game theoretic model for fair data sharing in deregulated smart grids. IEEE Access **3**, 2743–2754 (2015)
30. Wood, G.: Ethereum: a secure decentralised generalised transaction ledger. Ethereum project yellow paper, vol. 151, pp. 1–32 (2014)