IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received October 29, 2020, accepted December 19, 2020, date of publication December 30, 2020,
date of current version January 13, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3048169

Blockchain Based Data and Energy Trading in Internet of Electric Vehicles

AYESHA SADIQ[1], MUHAMMAD UMAR JAVED[1], RABIYA KHALID[1], AHMAD ALMOGREN[2], (Senior Member, IEEE), MUHAMMAD SHAFIQ[3], AND NADEEM JAVAID[1], (Senior Member, IEEE)

[1]Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan
[2]Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia
[3]Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, South Korea

Corresponding authors: Ahmad Almogren (ahalmogren@ksu.edu.sa) and Muhammad Shafiq (shafiq.pu@gmail.com)

This work was supported by the King Saud University, Riyadh, Saudi Arabia, through the Researchers Supporting Project, under Grant RSP-2020/184.

ABSTRACT The drastic increase in real-time vehicle generated data of various types has imparted a great concept of data trading in vehicular networks. Whereas immense usage of Electric Vehicles (EVs) as mobile energy carriers have supported distributed energy trading due to their bidirectional charging and discharging capabilities. The trustless environment of Internet of Electric Vehicles (IoEV), including fuel vehicles and EVs, encounters trading disputes and conflicting interests among trading parties. To address these challenges, we exploit consortium blockchain to maintain transparency and trust in trading activities. Smart contracts are used to tackle trading disputes and illegal actions. Data duplication problem occurs when a dishonest user sell previously traded data multiple times for financial gain. Therefore, data duplication validation is done through previously stored hash-list at roadside units (RSUs) employed with bloom filters for efficient data lookup. Removing data duplication at an earlier stage reduces storage cost. Moreover, an elliptic curve bilinear pairing based digital signature scheme is used to ensure the reliability and integrity of traded data. To ensure persistent availability of traded data, InterPlanetary File System (IPFS) is used, which provides fault-tolerant and a reliable data storage without any single point of failure. On the other hand, the energy trading transactions among EVs face some security and privacy protection challenges. An adversary can infer the energy trading records of EVs, and launch the data linkage attacks. To address this issue, an account generation technique is used that hides the energy trading trends. The new account generation for an EV depends upon its traded volume of energy. The experimental results verify the efficiency of the proposed data and energy trading scheme in IoEV with the reliable and secure data storage.

INDEX TERMS Blockchain technology, smart contract, Internet of Electric Vehicles, data storage, data trading, IPFS, energy trading, privacy, data linkage attacks.

I. INTRODUCTION

The rapid growth in vehicular telematics and their advanced technological aspects has enabled vehicles to generate various types of data. Modern vehicles are retrofitted with the capabilities of communication and exchange of data with the surrounding environment. As a result of data sharing and communication among vehicles, Internet of Vehicles (IoV) is developing gradually, which supports an efficient and intelligent transportation system. However, the addition of Electric Vehicles (EVs) in IoV has given birth to the Internet of Electric Vehicles (IoEV). An On-Board Unit (OBU) is integrated in vehicles that allows Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication. For V2I communication, a Dedicated Short-Range Communication (DSRC) protocol is used [1]. The V2V and V2I communication enables vehicles to share and trade data in IoEV. The real-time data generated by vehicles can aid in business profit of organizations in the future.

However, IoEV is considered as a trustless environment, where the trading parties including data sellers, buyers and brokers are not loyal enough to be trusted. The trading parties may have disputes concerning payments and sharing of data. Thus, the opacity in trading information, payment disputes

The associate editor coordinating the review of this manuscript and approving it for publication was Alessandro Pozzebon.

and unauthorized data modifications are the major challenges of Data trading (D-trading) in IoEV.

IoEV nodes usually leverage third-party services and centralized storage systems because of their minimal storage space. The cloud servers are introduced to overcome data storage related problems. Although these cloud servers provide enough storage space and computing capabilities, the risk of data content exposure, and a single point of failure still prevail due to their centralized approach. Due to the growing number of vehicles, several IoEV nodes access the data simultaneously that imposes a burden on the centralized data storage system. There can be bottleneck and latency problems while accessing data. Therefore, a distributed storage system is needed that can assist in providing reliable data storage with the assurance of long-term data availability and tackling the inefficiency and storage cost problems in the centralized system. Moreover, traders with nefarious intentions can exchange the same or previously traded data for financial gain. This leads to the second-hand sharing of data and data duplication, which ultimately increases the storage cost.

Blockchain is considered an innovative approach for the trustless nature of the vehicular network because of its riveting features like decentralization, transparency, traceability and immutability. Bitcoin is the first invention of blockchain launched in 2008 by Satoshi Nakamoto as a digital cryptocurrency [2]. State of the art vehicles share their data with RSUs and store it on the blockchain, which may contain information about the whole data sharing process, recipients, owners and type of data. Thus, data can be securely traded among multiple entities in IoEV using blockchain. Secure data exchange mechanisms are introduced in the vehicular networks together with blockchain technology [3]. Blockchain, using the smart contract, provides decentralization of transactions and transparency. A smart contract is executed within the blockchain as an autonomous application [4]. It provides a self-contained system with predefined rules to establish interactions among interested trading parties without any central trusted entity. There are various other areas that accelerate the use of blockchain, such as the Internet of Things [5]–[7], healthcare [8], [9], agriculture [10], and many more. Besides the immense benefits of blockchain in a trustless environment and providing transparency in trading, privacy is still an issue in Peer-to-Peer (P2P) Energy trading (E-trading) among EVs.

In the past decade, EVs as a subclass of smart vehicles, have received an immense recognition due to their potential of providing viable and environmentally sound transportation system. Frequent charging is required by an EV to operate for certain miles. The rapid development in energy harvesting and communication technology in smart grids has enabled EVs to communicate with the surrounding environment. The energy generation cost is decreasing by integrating Renewable Energy Sources (RES) into smart grids [11], [12]. Apart from transportation service, EVs act as distributed moving energy carriers. They can play the role of consumers as well as energy suppliers. The bidirectional communications of EVs along with advanced energy supply systems alleviates the problem of energy demand-supply imbalance, and assists in meeting the current needs of energy in a sustainable and reliable manner [13]. EVs have ability to communicate with service providers for charging their batteries and acquire information about charging schedules. The EV Charging Stations (EVCSs) are responsible for energy supply and scheduling charging slots for EVs. There can be a scarcity in energy supply during peak hours [14]. To handle this energy demand and supply during peak hours, modern EVs can trade their surplus energy with other EVs that need to charge their battery. Due to this social communication among EVs, charging through another EV becomes possible [15].

However, during the E-trading and D-trading process, the privacy of vehicles is at risk. While communicating with EVCSs or other EVs, the private information of EVs can be revealed. Therefore, anonymous communications and secure payment mechanisms are required. In the previous centralized approaches, the central authorities have the data of all registered nodes, which raises some serious privacy issues. The trading transactions are stored publicly and validated by all participating nodes in the blockchain network. The transactions' data can be misused by linking it with other publicly available datasets to launch privacy-related linkage attacks. There are multiple data mining algorithms available that work with the raw data to launch attacks.

Thus, the major challenge in blockchain-based P2P E-trading and D-trading among vehicles is to design a secure privacy-preserving scheme. The first concern is to provide privacy while keeping EVs' personal information anonymous. Second issue is to hide data and energy trading trends of EVs using an appropriate method. Although noise-based schemes are used to achieve differential privacy of records, yet these schemes fail to provide accuracy in information. Therefore, the main objective is to hide the trading trends while restricting attackers to infer the information.

To address the aforementioned problems, a blockchain-based privacy-preserving technique is proposed to hide trading trends in vehicles. During the payment mechanism in P2P trading, new accounts are generated by using the account mapping technique to collect coins, which depends on a predefined criteria. Moreover, based on the previous work [16], the data storage issue is solved using InterPlanetary File system (IPFS) (briefly explained in Section II-D), and blockchain is integrated in IoEV for trading transparency. We aim to design a trustful, secure E-trading and D-trading with reliable data storage system. Removing of duplicate data at earliest helps to maintain the storage cost and bandwidth consumption. Besides, it prevents the second-hand sharing of data by vehicular users in IoEV. For making data duplication process more efficient, bloom Filters are employed as discussed in Section II-C. Contributions of the proposed work are as follows.

- A blockchain-based trading model is proposed in which blockchain is implemented on RSUs for performing secure and fair trading with transparent legal actions.

- Smart contracts are deployed to perform trading actions autonomously among trading parties to tackle trading disputes and facilitate in providing payments to the respective traders.
- Data duplication validation is carried out by computing trading data hash and its comparison with hash-list stored at RSUs. Moreover, bloom filters are employed to reduce the response time of existing data lookup mechanism.
- An external distributed storage, IPFS is introduced to ensure persistent availability of traded data with reliable storage and convenient access.
- A consortium blockchain-based privacy-preserving model is proposed for transparent E-trading among EVs.
- An account generation method is introduced that is based on time-series single exponential technique. In this method the previous E-trading records of EVs are used for hiding E-trading trends to prevent data linkage attacks.
- A security analysis of smart contracts is provided to examine the code, making it free of bugs, vulnerabilities and secure against all known attacks.
- The performance of the proposed model is evaluated by simulations. The results of these simulations validate the effectiveness of proposed system.

The rest of this article is organized as follows. The preliminaries for the proposed system model are discussed briefly in Section II. Section III provides related work. The problem statement is presented in Section IV. System model entities, design goals and attacker model are presented in Section V. In Section VI, the proposed blockchain-based D-trading and E-trading scheme is constructed in detail, followed by the algorithms used for the account mapping scheme in Section VII. The security analyses is presented in Section VIII. The results and discussion are demonstrated in Section IX. Finally, we conclude our work in Section X. All the notations and abbreviations used in this work are listed in Table 1.

II. PRELIMINARIES

In the following sections, preliminaries of the proposed model are discussed.

A. BILINEAR MAPPING

In cryptosystems, the concept of bilinear mapping [17] is originated from Weil and Tate pairing. It is known as pairing because the elements of the two groups are combined to yield an element of a third group. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be the two additive cyclic groups that generate a third group $\mathbb{G}_T$ of prime order q. Let ê be the bilinear map, it is denoted as:

ê: $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$

A bilinear map must satisfy the following three properties.

- Bilinearity: If two points X, Y $\in \mathbb{G}_1$ for all a, b $\in \mathbb{Z}_q^*$, we have:

$$\hat{e}\,(aX, bY\,) = \hat{e}(X, bY)^a = \hat{e}(aX, Y)^b = \hat{e}(X, Y)^{ab}$$
$$= \hat{e}(X, abY) = \hat{e}(abX, Y)$$

- Non-degeneracy: $X, Y \in \mathbb{G}_1$ exit such that $\hat{e}(aX, bY\,) \neq 1$, where 1 is identity element in group $\mathbb{G}_T$.
- Computability: For all X, Y such that X, Y $\in \mathbb{G}_1$, there is an efficient algorithm to compute $\hat{e}(X, Y)$.

B. BLOCKCHAIN

Blockchain technology is being praised as the ground breaking innovation due to its promising features and performance in trustless environments. It is a decentralized distributed ledger technology with time-stamped series of records stored on it. There is no central controlling authority and each node

TABLE 1. Nomenclature.

Notation	Description
DHT	Distributed Hash Table
DSRC	Dedicated Short Range Communication
EST	Exponential Smoothing Technique
EV	Electric Vehicle
EVCS	Electric Vehicle Charging Station
IoEV	Internet of Electric Vehicles
IoV	Internet of Vehicle
IPFS	Interplanetary File System
LMT	Lexicographic Merkle Tree
OBU	On-Board Unit
P2P	Peer to Peer
PoE	Proof of Event
PoS	Proof of Stake
PoW	Proof of Work
RES	Renewable Energy Sources
RSU	Roadside Unit
TA	Trusted Authority
TE	Trading Estimate
TWSL	Three Weight Subjective Logic
V2G	Vehicle to Grid
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
α	Digital signature
γ	Smoothing weight
λ	Pre-configured value
τ	Threshold value
$\mathcal{A}(.)$	Account generation function
$\mathcal{C}$	The amount of traded energy
$Cert_i$	Certificate
d_i	Data to be traded at t_i
ê	The bilinear map
$\mathcal{E}(.)$	Function of EST
E_i	Energy value at current iteration
E_{i-1}	Traded energy till last iteration
EV_s	Seller EV
$F(.)$	Threshold value setter function
$\mathbb{G}_1, \mathbb{G}_2; g_1, g_2$	Additive cyclic group; corresponding group generators
$\mathbb{G}_T$	Multiplicative group
k	No of hash functions for bloom filter
PId_i	The pseudo-id used by vehicle for communicating with RSU
q	Prime number
r_i	Random number selected by TA
R_i, U_i	Secret key pair provided to RSU
Req_si	Request generated by vehicle to RSU
S_i	Private key
$\mathcal{T}_c$	Time period
t_i	Timestamp
V_i	The ith real identity of a vehicle
W_{add_i}	Wallet address of a vehicle
Z_q	Prime field

has its own copy of digital ledger. All records stored on blockchain are publicly verifiable and available to each node in the network. A block is generated and added chronologically after successful transaction validation through a consensus mechanism. A unique cryptographic hash links each block with the previous one making it immutable in nature.

The public ledger is updated and synchronized among all nodes via consensus mechanism. The consensus mechanism ensures the mutual agreement of all participating nodes for transaction validation. There are number of consensus algorithms, including Proof of Work (PoW), Proof of Stake (PoS), Proof of Authority (PoA) and Delegated Proof of Stake (DPoS). The consensus mechanism is selected on the basis of network requirements, however, PoW is deemed to be more secure as compared to other consensus algorithms. There are two approaches used in blockchain, first one is the permissionless blockchain in which nodes can become part of blockchain network without any required permission, refereed to as public blockchain. The second approach is permissioned blockchain refereed to as private blockchain in which access control is implemented to restrict the number of participating nodes. In private blockchain only the allowed nodes can do read and write operations.

C. BLOOM FILTERS

It is a randomized data structure with less space usage. There are multiple bloom filter variants available that can facilitate membership queries in an efficient manner [18]. The bloom filter works with m bits of binary array with 0's and 1's. At first, each bits is set to 0. Data is mapped through k number of hash functions by setting k number of bits from 0 to 1 in a binary array, where $k < m$. In the first phase of data insertion, k array indices are returned after passing data through k hash functions in the filter. These resulting k number of array indices are set to 1 in bit array. Meanwhile, data lookup operation is carried out to check the particular array positions. It returns true, if any bit at the respective array index is set to 1 and vice versa. Although fast data insertion and data lookup have devised bloom filters so effective, still they encounter the problem of false positives. However, multiple variants of bloom filters are available to lessen the rate of false-positives upto an acceptable level [19].

D. IPFS

IPFS is a content addressable, open source, P2P distributed network to store and share data [20]. It utilizes computers swarm connected together without any central coordinating entity. The data stored in IPFS is assigned a unique cryptographic hash. It exploit the fundamental concept of Distributed Hash Tables (DHTs) to access files in the network based on their unique hash values. In summary, IPFS supports the sharing of data in a secure and reliable manner with high throughput and low latency. It provides concurrent access to the uploaded files without any delays. Moreover, data in IPFS can be stored permanently, which makes it an ideal data sharing platform [21].

E. D-TRADING

D-trading in vehicular networks is in its early stage. In future, it may embrace wider applications that can be studied and analyzed for further enhancement in the driving regulations and developing new system designs for traffic handling. The IoEV enabled D-trading can improve the quality of life by providing new opportunities in today's vehicular telematics. The real-time vehicle generated data can benefit several business entities and trading parties. Although the trading data in IoEV belong to several categories of vehicle generated data except for road safety messages. The trading data may contain road conditions, congestion statuses and environmental conditions. It may include data related to vehicles' usage, and their technical details like temperature oil, airbags and malfunction reports. Moreover, the proper use of this data can help in betterment of remote services booking, proactive safety measures, navigation services with virtual assistance, live road and environmental conditions, and reducing engineering costs. This D-taring occurs between RSUs and vehicles that are willing to participate in D-trading. Here, in case of D-trading, RSUs are considered as data brokers. They handle all D-trading requests from vehicles and process them. All D-trading validation checks are carried out by RSUs.

F. E-TRADING

EVs' collaboration with RES has facilitated in overcoming the various problems, including energy demand-supply, energy requirement in peak hours and RES over generation. EVs are provided incentives to take part in E-trading market. Since EVs are capable of consuming energy as well as supplying energy to other EVs. They can trade and communicate with the surrounding environment through V2V, V2I or Vehicle to Grid (V2G) communication modes. In the proposed system model, only V2V communication is considered for E-trading between EVs and RSUs. The RSUs involved in E-trading are considered as energy brokers. They handle E-trading requests and provide E-trading payment transfer decision for the corresponding EV to preserve their privacy.

III. RELATED WORK

In this section, the literature review is categorized as blockchain-based D-trading and storage, and blockchain-based E-trading.

A. BLOCKCHAIN-BASED D-TRADING AND STORAGE

With the advancement in IoEV and increasing traffic, several nodes are accessing the network at the same time. Data access authorization is a great challenge among vehicles that require an efficient response with minimum delay. The traditional networks with centralized storage confront bottleneck and latency issues due to increased traffic load. To support resource-intensive tasks and data storage, edge computing is introduced [22]. However, due to open mobile nature of vehicles, edge nodes are considered unreliable, which may cause security and privacy issues. Consequently, vehicles get unwilling to share or upload data to the edge nodes. To address the issues of high costs, inefficient and insecure data storage, a decentralized and distributed blockchain technology is integrated in IoV [3], [23], [24]. Authors in [3] have designed an edge computing based scheme accompanied by smart contracts for efficient data sharing. Data sharing rate increases with the increase in the number of vehicles, which inflicts a high demand for data storage. For selecting a valid data source, a reputation-based scheme is formulated using Three-Weight Subjective Logic (TWSL). The delay problem in [3] is handled by using edge computing, whereas in [23], efficiency in data sharing is achieved by using batch signature verification. However, data duplication and data credibility problem is not handled properly [3], [23].

Information dissemination among vehicles is of utmost importance, and so is the trustworthiness of information exchanged. Due to the high mobility and variability of vehicles [25], it is difficult to trust neighbouring vehicles. There are several types of communications in IoV, such as V2V, V2I and V2G. The unique features of vehicular networks, such as high mobility and open nature topology make them susceptible to various kinds of attacks. Thus, the security and reliability of messages are essential aspects to be addressed in vehicular communications. Moreover, important information does not reach to the nearby vehicles in real-time due to fake message dissemination. To prevent the distribution of fake messages, a blockchain-based trust models are proposed in [26], [27]. Authors in [26] have used a reputation evaluation algorithm based on reputation scores to calculate the trustworthiness of messages shared by vehicles. The reputation score is generated by the number of evidences collected from peers. Moreover, an efficient privacy-preserving authentication mechanism is developed by utilizing the features of the Lexicographic Merkle Tree (LMT). Whereas, authors in [27] have proposed a framework for traffic event validation using the Proof of Event (PoE) consensus mechanism. A threshold value is adjusted to reduce the dissemination of fake messages, and events are validated by the consensus mechanism strategy. However, the process of updating reputation values depends on the collected evidences from peers that causes transmission delay in case of increase vehicular traffic.

Trust among vehicles encourages them to communicate and share data [28]. Existing centralized trust models use cloud for storing data while restricting vehicles to rely only on the central server, which results in issues like single point of failure, latency and bottleneck. To solve these problem, authors in [29] have used a local blockchain to record trust values and message trustworthiness based on geographical location with PoW consensus mechanism. Whereas, authors in [30] have presented a blockchain-based decentralized trust model in which RSUs have information about vehicles. Trust is built upon the percentage of ratings collected from neighbouring vehicles. However, vehicles may behave selfishly and generate unfair ratings about other vehicles. Also, there is no authentication mechanism specified for vehicles before joining the network. Real identities of vehicles are not preserved, as ratings shared by vehicles contain sensitive data about their identity and location. While providing location proof of vehicles in a certain vicinity, location privacy of vehicles is not preserved [29]. Moreover, the PoW consensus mechanism used in [29] is difficult to perform in mobile nodes, whereas joint PoS and PoW algorithm is used in [30] that requires greater computational power.

Data exchange in vehicles is becoming popular with the growing vehicular traffic. Data exchange takes place simultaneously involving multiple parties that causes low information transparency and data modification problems. A truthful and secure data sharing model is required in the trustless environment in vehicular networks. Blockchain technology is used for data exchange due to its decentralized, immutable and traceable characteristics [31]–[33]. Authors in [34], [35] have proposed blockchain-based trust models with the consideration of preserving vehicle privacy and shared data credibility. A protocol is designed in [34] that allows vehicles to communicate anonymously using group signature. The reliability and effectiveness of protocol depend upon the length of the ring. Moreover, logistic regression is used to identify malicious vehicles based on their reputation values. However, this protocol is not efficient as the number of vehicles increases in the ring for generating a group signature.

The newly emerged paradigm, fog computing has been used previously to overcome latency problems [36]. However, the incessant surveillance can result in the leakage of location and identity privacy of vehicular users [37]. Authors in [38] have addressed communication overhead and inefficiency by using fog nodes in carpooling system. Blockchain-based fog nodes are implemented to ensure auditability of carpooling data. A proximity test is used along with the Public Key Infrastructure (PKI) approach for managing users' drop-off locations. Performance analysis is done on the blockchain construction, and time cost is compared for tracking users by RSUs that are considered as fog nodes. However, the semi-trusted fog nodes are not reliable, and they can be compromised by malicious users.

To preserve the privacy of users and to achieve social welfare maximization, authors in [39] have proposed a framework based on consortium blockchain in which pre-selected aggregators are responsible for auditing and verifying transactions. To improve D-trading efficiency, an iterative double auction mechanism is used to maximize social welfare by optimizing data pricing and protecting traders' privacy. Optimizing data pricing benefits both buyer and seller, which encourages users to participate in D-trading. However, a detailed incentive mechanism is required for the process of data transmission and a trusted intermediary is needed to tackle disputes among users.

Table 2 shows the summary of Section III-A. Most of the problems addressed include transparency in D-trading [39], secure and efficient sharing of data [3], [23], [26], data storage [3], [23] and trust management problems [27], [29], [30], [34]. Blockchain is exploited to solve several problems

TABLE 2. Blockchain-based D-trading and storage.

Technique(s)	Feature(s)	Objective(s)	Limitation(s)
TWSL [3]	Data sharing, storage and access authorization	Integration of edge nodes Reliable data storage Reputation evaluation	High storage cost Data duplication
Batch verification [23]	Efficient sharing and storage of data	Reliable and scalable data storage	Second-hand sharing of data
LMT [26]	Prevention of fake message distribution	Privacy-preserving authentication scheme Trust reputation evaluation	Transmission Delay
PoE [27]	Reducing fake message distribution Trust management	Identification of malicious vehicles Prevention of fake messages distribution	Transmission Delay Scalability
PoW [29]	Trust management Use of Edge nodes	Scalable scheme based on geographical locations Reducing latency by using edge nodes	Privacy leakage
PoW and PoS [30]	Trust management	Reduced latency using edge computing	Computational overhead
Logistic Regression, PoW and PBFT [34]	Trust management Anonymous Communication	Conditional privacy Auditable and scalable scheme	Latency issue
Double auction mechanism [39]	Transparency in data trading	Social welfare maximization of buyers and sellers Auditing and verification of transactions	Payment disputes

involving transparency, trust management and secure data sharing among vehicles.

B. BLOCKCHAIN-BASED E-TRADING IN EVs

The installation of RES is increasing gradually. To reduce the problem of RES over generation and divergence between the demand and supply, EV users need motivation to use RES. In [40], [41], the authors have proposed an incentive mechanism for the EV users to consume more and more RES. The proposed incentive scheme incorporates monetary and non-monetary incentives while minimizing energy costs and prioritizing the vehicles. The results show a significant increase in the solar consumption ratio due to the incentive scheme. However, the proposed scheme does not protect the privacy of the users.

The combination of RES and EVs has played an essential role in alleviating the problem of energy demand and supply. With the integration of RES [42], EVs are considered as the energy carriers for energy distribution to areas where energy demand is high. The energy delivery process by EVs has encountered a lot of problems, including EVs' selfishness and uncooperative behavior. EVs may not be willing to take part in the E-trading market. On the other hand, malicious EVs can launch various attacks to downgrade the energy delivery scale. To address these problems, authors in [43] have proposed a scheme for secure E-trading. A reputation-based consensus protocol is used for efficient transaction verification. Moreover, an incentive mechanism is used for proper scheduling of charging and discharging of EVs. Finally, a comparison is made with conventional schemes to demonstrate the efficiency of the proposed system. However, the PKI is used for puzzle solving in reputation-based consensus that is computationally expensive. The studies [44], [45] are based on the E-trading of hybrid EVs with surplus energy. The consortium blockchain is used for E-trading without dependence on any third party. A double auction mechanism is used to achieve the social welfare maximization of EVs and local aggregators. EVs place their electricity price bids without sharing any private information. Although the scheme provides anonymity, however, the privacy attacks are not considered that are possible by data mining methods. In [46], [47], the authors have used blockchain to enhance the security of E-trading transactions of EVs by using data coins. The delivery of data coins is performed using pseudonyms to avoid privacy disclosure. However, the detection of malicious attackers becomes complicated when a different pseudonym is used for every new transaction.

The solar energy generation has facilitated individuals to produce their own considerable amount of energy efficiently. However, due to varying usage of energy, the amount of solar energy produced by individuals may exceed their requirements [48]. This surplus energy can help in an individual's E-trading market growth. For neighbouring E-trading, a trustable environment is required as individuals may have their privacy concerns. In [49], [50], the E-trading model is proposed in the grid neighbouring system based on consortium blockchain. Authors in [49] have proposed a solution to preserve the privacy of users by screening their trading records to avoid privacy related attacks. Dummy accounts are used to add noise, which hides the data about active as well as inactive users. New accounts are created that depend on users' energy usage to provide privacy protection.

A considerable amount of payment records are generated during the energy transfer between EVs and smart grids. The payment records of energy usage can be shared for load and price forecasting, valuable services of energy and scheduling of energy consumption [51], [52]. The sharing of payment records comes with several privacy concerns. In [51], authors have proposed a privacy-preserving payment mechanism for V2G network. The proposed work supports anonymous payment and effective audit of energy transactions by leveraging a proper registration process. The proposed scheme surpasses Bitcoin and Ethereum in terms of transaction confirmation time and throughput. However, there is no motivation for EVs to participate in E-trading to meet the demand and supply

TABLE 3. Blockchain-based E-trading in EVs.

Technique(s)	Feature(s)	Objective(s)	Limitation(s)
Reputation-based scheme [43]	Reputation-based consensus protocol Incentive mechanism for charging and discharging of vehicles	Scheduling of EVs' charging and discharging Prevention of internal and external attacks by adversaries	Computationally expensive due to PKI approach
Iterative double auction [44]	Social welfare maximization using double auction mechanism Consortium blockchain to audit and verify transaction records Secure and trustful E-trading model	Balancing demand and response Improving transaction security without any trusted intermediary	Privacy attacks are not considered that are possible through data mining attacks
Proof of concept [51]	Privacy Preservation of shared data Auditing anonymous transactions A reliable payment mechanism	A secure payment mechanism Privacy preservation of payment records	No motivation for EVs to participate in E-trading No focus on Energy demand and supply
Credit-based scheme [53]	Reduction in transaction verification delay	Transaction delay	Requires integration in each client module that is expensive
Dynamic pricing scheme [58]	Preserving location privacy of vehicles	Optimal charging station selection Location privacy preservation	Not scalable

of energy. Authors in [53] have provided a credit-based solution for reducing transaction verification delay. This scheme involves central bank authority, which helps in managing payments and reducing the transaction confirmation delay time. However, the proposed blockchain-based scheme needs to be integrated into each client module for payment process that may cause privacy issues.

EVs' charging may require a longer time duration, which in turn demands for in-advance charging schedules on charging slots. In [54], [55], a blockchain-based charging scheme is proposed in the smart grid system. The main objective is to minimize the charging energy cost for EVs while minimizing the energy fluctuation levels in the smart grid [56]. The frequent charging of EVs and their charging schedules may leak their private information, including their locations, driving patterns and charging schedules. Authors in [57] have worked on charge supplier matching and charge scheduling. They have provided a homomorphic scheme-based solution to enable the location privacy of EVs. In [58]–[60], authors have proposed schemes for the selection of charging stations and dynamic pricing plans for EVs' charging. A protocol is designed in [58], for the selection of optimum charging stations by bidding dynamic tariffs, and users can select charging stations based on dynamic tariff decisions. The geographic location and the vehicles' identity are preserved at the charging stations, and their bids are publicly available in the blockchain.

Table 3 summarizes the literature presented in Section III-B. The problems addressed in E-trading mainly include EVs' charging and scheduling [43], energy supply and demand [44], [45], payment mechanisms [51] and optimal charging pricing [58]–[60].

IV. PROBLEM STATEMENT

Efficient and secure trading mechanisms are required to trade data and energy in IoEV. In [39], [44], double auction mechanisms are proposed for trading among buyers and sellers in IoV. However, a trusted mediator is required to tackle the possible trading disputes in the market. Moreover, the privacy of sellers is not preserved. In [51], a privacy preserving payment mechanism is proposed in V2G network. The proposed scheme provides privacy preservation and reliable payment mechanism with secure data sharing. However, tracking of vehicles' real identity and auditing their behavior involves a registration authority, which makes the proposed scheme partially decentralized. Moreover, some vehicles act maliciously to get benefits, e.g., sharing old or fake data. Therefore, a lookup mechanism is required to prevent repetition in data storage and trading. In [3], a reputation-based data sharing scheme with TWSL is developed to choose a more reliable data source. However, the data duplication and second-hand sharing is not prevented, which can cause high storage cost and unfair data trading. In [29], [30], PoW consensus is performed by vehicles, whereas joint PoS and PoW algorithm is used in [30] to build trust among vehicles. However, PoW is difficult to implement on mobile nodes because length of stable connection or meetup time is very short and PoW requires greater computational efforts. Moreover, transaction verification delay is another issue. Authors in [53] provided a credit-based solution for reducing transaction verification delay. This scheme involves central bank authority, which helps in managing payments and reducing the transaction confirmation delay time. However, the proposed blockchain-based scheme needs to be integrated into each client module for a payment transaction that may cause privacy issues, e.g., data linkage attacks. To address the privacy related issues of EVs, authors in [58] proposed a blockchain-based charging scheme for limited number of EVs. However, the proposed scheme is not scalable when the number of EVs is increased.

V. SYSTEM MODEL

For secure trading, a blockchain-based scheme is introduced for data and energy trading in IoEV that ensures a disputes free trading environment with reliable data

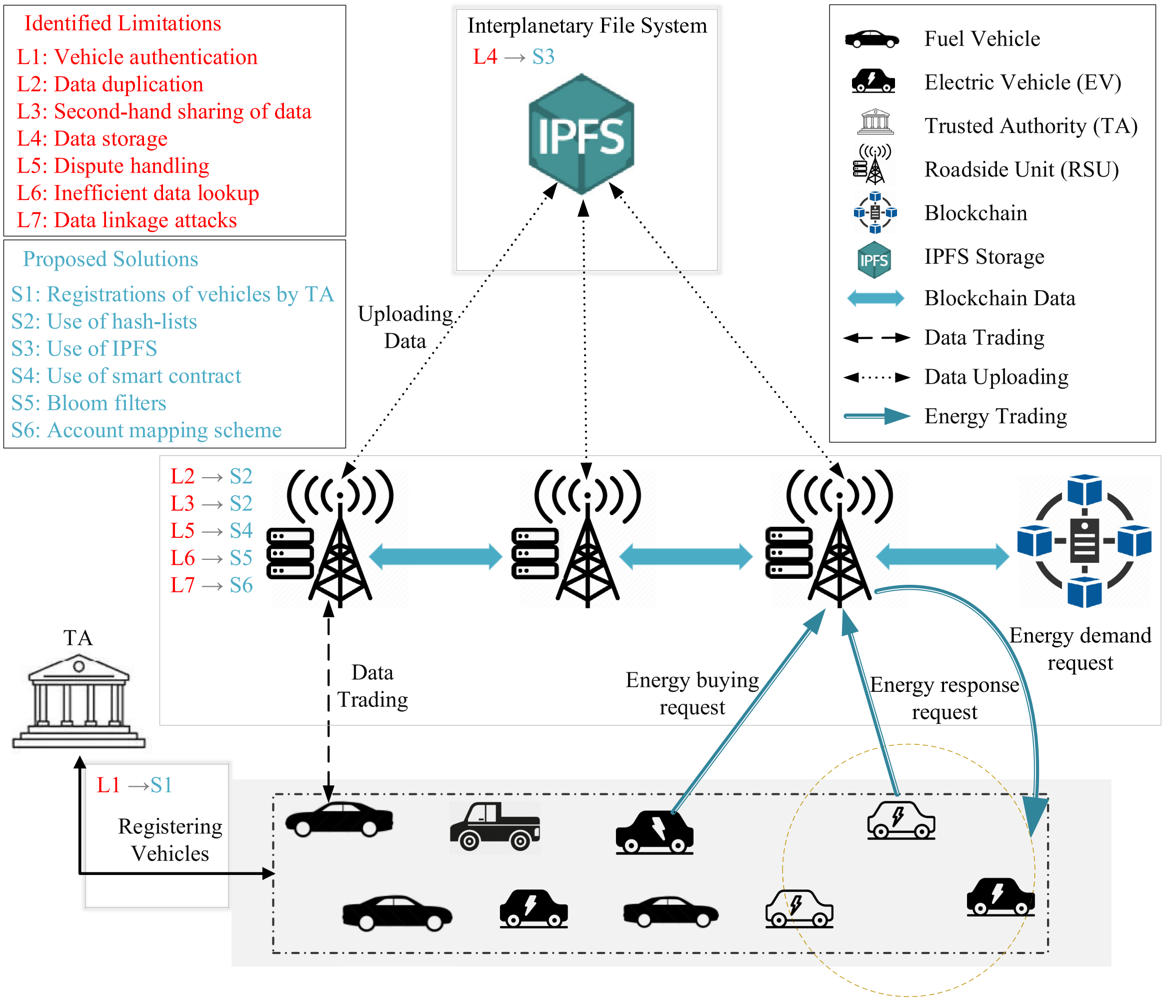


FIGURE 1. Proposed system model.

storage mechanism. The three layers in the proposed system model are: vehicular layer at the lowest level, the middle infrastructure layer and the top storage layer as shown in Fig. 1. The vehicular layer includes IoEV nodes or vehicles with V2I communication. RSUs form the infrastructure layer with the consortium blockchain as underlying technology, where RSUs are directly linked to one another through a wired connection. The third layer is the storage layer devised with IPFS for storing trading data.

In the proposed system model, we have addressed a number of limitations ranging from L1 to L7. Fig. 1 shows the mapping of identified limitations and their respective proposed solutions. The limitation L1 refers to the authentication of vehicles in IoEV network. It is mapped with proposed solution S1 to authenticate the vehicles. The limitations L2 and L3 refer to data duplication and second-hand sharing of data, respectively, which occur during D-trading. These limitations are addressed by solution S2 by performing data hash computation and its comparison with hash-list. Vehicles are not capable of storing data for a longer time that causes data storage problem, which is labeled as limitation L4. To solve this limitation, an IPFS is used as a solution S4 to handle data storage problem. The trading parties face payment disputes, indicated as limitation L5, which is handled by using smart contracts mapped as S4. The limitation L6 is about inefficient data lookup mechanism that is addressed by employing bloom filters for efficient data lookup referred to as solution S5. The limitation L7 is about data linkage attacks, which is addressed by using account mapping scheme referred to as solution S6.

A. ENTITIES

The entities for proposed system model are described briefly as follows:

- **Trusted Authority (TA)** The registration of IoEV nodes in the network is done by TA. RSUs are registered as data brokers and energy brokers, and vehicles as IoEV nodes. TA is responsible for maintaining the entire IoEV network and avoids adding malicious vehicles in the network to ensure the strength and security of the system. Before joining the IoEV network, all vehicles are required to register themselves by providing their details to TA. The registration process is done in an offline mode, i.e., vehicles submit the necessary details, including name, mobile number, address, etc. After that, each vehicle is provided by initial security parameters. Generally, TA is assumed to be infeasible to get compromised by any adversary because of its higher computational power, storage and communication capabilities. Geographically, each state has its own TA that is responsible for verifying the credentials of each vehicle from its corresponding registered state.

- **Vehicles**
  Vehicles in IoEV network include fuel vehicles and EVs. The simple fuel vehicle can perform D-trading whereas, EVs are capable of performing D-trading as well as E-trading. However, in our system model, EVs are restricted to perform only E-trading. In D-trading vehicles can play either role of data buyer or data seller. Whereas in E-trading, EVs act as either energy sellers or energy buyers based on their need for energy. The communication and computational capabilities of OBU enable vehicles to communicate with RSUs for D-trading or E-trading.
- **Smart Meters**
  The charging poles are integrated with smart meters that calculate and record the energy volume being traded by seller EVs. The recorded volume of energy helps buyer EVs to pay the price for traded energy.
- **RSUs**
  In the proposed system model, RSUs act as both data and energy brokers for handling the D-trading and E-trading requests, respectively. They work with the consortium blockchain; thus, the same digital ledger is shared among all RSUs. These are responsible for:
  - checking authenticity of vehicles,
  - handling D-trading and E-trading requests,
  - checking data duplication,
  - uploading traded data to IPFS,
  - account mapping of vehicles.
- **Blockchain**
  The consortium blockchain is applied on RSUs that facilitates in achieving trading transparency and traceability. Smart contracts are executed within the blockchain network and provide robustness in the system. Blockchain ensures security by providing immutability, tamper-proof records and transparency in trading. It consists of following three components.
  - Transaction Data: It is the information about trading transactions between vehicles and RSUs. It includes metadata, type of data, tags, timestamps, pseudo-id of vehicles.
  - Blockchain Network: The information about trading transactions is stored and uploaded on the blockchain. It is comprised of data blocks consisting of hash values and transactional data. Hash value refers to a link that provides connectivity of data blocks to one another.
  - Consensus Mechanism: In our scheme, PoW consensus is performed by RSUs, and transactional data is added to the data block. The transactional data is audited by all RSUs.
- **IPFS**
  An IPFS (as discussed in Section II-D) P2P network that is used to store traded data while ensuring its long-term availability.

B. DESIGN GOALS

The proposed system aims to guarantee the privacy of vehicles and secure trading in IoEV.

- **Privacy Preservation of Trading Trends**
  A considerable amount of work is done to preserve the privacy of vehicular users. Besides the privacy preservation,, the primary objective of this work is to prevent data linkage attacks on transactional data stored in the blockchain.
- **Data Duplication**
  Data duplication is removed through hash computation and comparison. The computed hash of traded data is compared with hash-list stored at RSUs to check if the computed data hash is already present in the list or not.
- **Reliable and Efficient Payments**
  An efficient and reliable payment mechanism is used in the proposed system model. All payment transactions are handled through smart contract. So, there are no chances of any disputes among vehicles.
- **Effective Audit of Anonymous Transaction**
  Vehicles in IoEV are assigned pseudo-ids that are used for communication and financial transactions in trading. The E-trading trends are hidden by using an account mapping scheme in which new accounts are created for seller EVs. Whenever a new account is created, the mapping between the original id, pseudo-id and real account are maintained for an effective audit of transactions in future.
- **Transparency**
  All trading processes are carried out by using a trading smart contract. The trading information is recorded on the blockchain. The seller and buyer information, related to either D-trading or E-trading, is publicly verifiable, which reduces the chances of disputes. Apart from avoiding trading disputes, transparency means that the vehicles must have knowledge about the shared information during trading.
- **Traceability**
  It refers to the information flow and traceable vehicles interactions. All vehicles, including malicious and non-malicious, are provided equal privileges in a network. Information shared among vehicles can be tampered by adversaries.

C. ATTACKER MODEL

In this section, possible attacks on the proposed system are discussed.

1) **Linkage Attacks**
In the threat model, it is considered that the adversary may have prior knowledge about datasets, including multiple resources, e.g., trading information from charging station, and publicly available trading records in the blockchain. The linkage attacks involve several methods that are launched by adversaries using various techniques like data mining algorithms. The common linkage attacks are semantic attacks [61], set theory-based attacks [62] and device id-based attacks [63].
2) **Privacy Disclosure**
Vehicles are connected to RSUs through wireless communication channels. The adversaries may eavesdrop payment-related information. This information is publicly available to all participating nodes in the network. A potential adversary may infer sensitive information of vehicles that may include vehicles' locations, charging patterns, buying and selling trends.
3) **Unreliable Payments**
An adversary may attempt to cheat vehicles or RSUs by making fake and unreliable payments. Double-spending attack can be caused by invalid use of energy coins, i.e., an adversary may use the same energy coin with two different transactions.
4) **Denial of Payment**
In trading, a seller vehicle may pretend about not receiving any payment. On the other hand, a buyer EV may also deny buying energy. This ultimately affects the transaction cost if any vehicle, either buyer or seller, causes the dispute and refuses to pay the cost [64].

VI. PROPOSED SCHEME

In this section, detailed trading scenarios in IoEV are presented using consortium blockchain. The first scenario is about D-trading and storage, and the second scenario is about screening of E-trading trends to preserve the privacy of EVs. Initially, all vehicles, either fuel vehicles or EVs, are registered by providing their personal details to TA. After registration process, vehicles in IoEV network can perform D-trading or E-trading.

1) SYSTEM INITIALIZATION

For system parameter initialization through pairing (as discussed in Section II-A), TA yields $\mathbb{G}_1$ and $\mathbb{G}_2$ along with two generators g_1 and g_2, respectively, that as a result generate a $\mathbb{G}_T$ of same prime order q. TA selects two random numbers a and b that belong to $\mathbb{Z}_q^*$ as its master private keys to computes its public key and a cryptographic hash function H such that $H : \{0, 1\} \rightarrow \mathbb{Z}_q^*$

Initially, a vehicle V_i submits its details to TA for generating pseudo-id PId_i and system parameters. There are k number of hash functions selected for bloom filter. The set of system parameters published by TA include $\{q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, H, k\}$.

Algorithm 1 D-Trading Algorithm

```
if (IsSourceValid == TRUE) AND
(IsDataValid == TRUE) then
    Generate $h_1 \leftarrow d_1$
    if ($H - list$ contains $h_1$) then
        return FALSE
    else
        add $h_1$ to $H - list$
        funds transfer to $W_{add_i}$
        sendDataToIPFS $d_i$
        Set dataSeller = $\{V_i - PId_i\}$
        Store tradeData $d_i$ against $h_i$
else
    Discard Request
```

2) REGISTRATION

When a vehicle V_i joins the IoEV network, TA selects a random number $r_i \in \mathbb{Z}_q^*$ with $r_i + a \neq 0 \bmod q$ and generates a secret key $S_i = g_1{}^{V_i + a}$. At the time of registration a pseudo-id PId_i is assigned to the vehicle against its the original identity $Id - V_i$ for anonymous communication in the network. The mapping between $Id - V_i$ and PId_i is maintained by TA. The pseudo-ids are required to be generated for each vehicle to ensure the validity of data source. Even if these pseudo-ids are inferred by adversary, the privacy of vehicles is not revealed because of zero knowledge about the vehicle.

A. D-TRADING AND STORAGE

In this section, detailed working steps for D-trading and storage are presented in six steps: (1) system initialization; (2) registration; (3) D-trading request; (4) RSU response and data duplication validation; (5) transaction validation and consensus; (6) uploading trading data to IPFS. Algorithm 1 presents the simplified D-trading steps and Fig. 2 shows the workflow of D-trading.

1) D-TRADING REQUEST

A vehicle using its PId_i requests a nearby RSU for D-trading. Thus, a data selling request Req_{s_i} generated by V_i with time stamp t_i is as follows: $Req_{s_i} = \{PID_i, t_i, d_i\}$.

Here, d_i represents the data to be traded. S_i yields digital signature α that is used by V_i to signs the d_i along with a certificate $Cert_i$. For data coins transfer, V_i sends its wallet address W_{add_i} to RSU. Finally, V_i forwards a data selling request as $\{Req_{s_i}, Cert_i, \alpha, W_{add_i}\}$ to RSU.

2) RSU RESPONSE AND DATA DUPLICATION VALIDATION

Upon receiving data selling request from V_i with PID_i, the digitally signed d_i is validated by RSU. The PID_i is used to authenticate the validity of data source. If the requesting

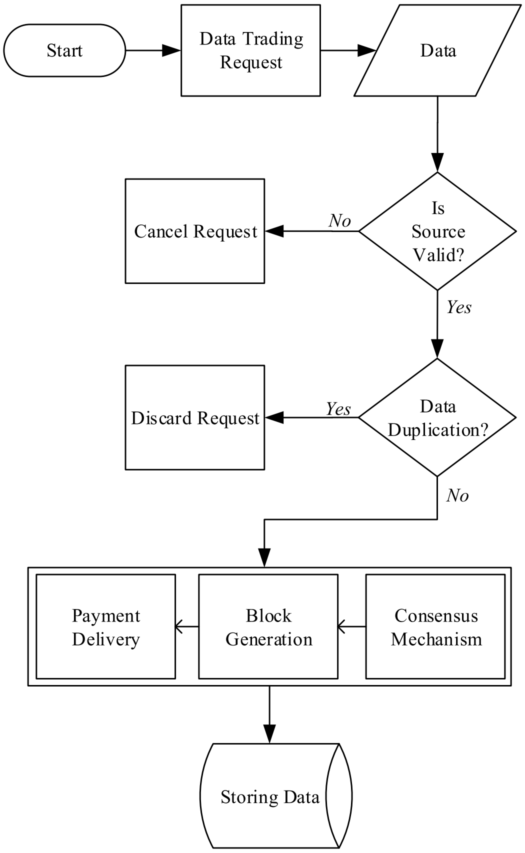


FIGURE 2. Work flow for D-trading operations.

vehicle is not registered with TA, then RSU rejects the trading request. Instead, if the D-trading request is from a legitimate vehicle then further actions are performed by RSU. All D-trading activities are performed using a smart contract. The contract is triggered upon meeting some pre-defined rules. For D-trading, there are certain conditions that must be satisfied in order to trade data.

- Authenticity of vehicles
- Credibility of data
- Data integrity verification
- Data duplication validation

The initial checks, including the authenticity of source, data credibility and data integrity, are verified by RSUs. For data duplication verification, if initial checks return true, then the hash of received data is computed as h_1. The h_1 is compared with the hash-list stored at RSUs. For efficient data lookup, we are using bloom filters (as discussed in Section II-C) to verify data duplication. The number of hash functions included in bloom filters is k; here, the k is 2, and the hash functions include murmur hash and fnv series hash. After d_i is passed through these hash functions, a quick response is generated for data duplication. It returns true if data is possibly present and returns false, if no previous mapping of traded data is present in the list.

3) TRANSACTION VERIFICATION AND CONSENSUS

By using smart contract, the payment is transferred from RSU to data seller vehicles. The payment mechanism that we followed is quite similar to proof of delivery scheme in [65]. This method enables trading actions to be transparent, and no trader can deny the payment transfer, which prevents payment disputes. Additionally, the D-trading information is also recorded in the blockchain and trading transactions are validated by RSUs using PoW consensus mechanism.

A consensus is carried out before updating the distributed ledger. At first, unconfirmed trading transactions are kept in a transaction pool. After the verification process, a block is generated with verified transactions. The consensus is reached through joint verification by all nodes in the network as a result of which block is added in the blockchain. The proposed model exploits consortium blockchain with the PoW consensus mechanism. All consensus nodes, i.e., RSUs are required to solve hash difficulty by competing each other. If a RSU solves the difficulty first, then it broadcasts the data block for block validation by other RSUs. The winner RSU receives reward from blockchain and is allowed to add the block into network.

4) UPLOADING DATA TO IPFS

The trading data is uploaded to IPFS, which is a distributed P2P network (as discussed in Section II-D). IPFS provides a reliable storage and ensures the persistent availability of traded data. It works without any central controlling entity and facilitates in easy and concurrent access of data. RSU sends payment to data seller vehicle and store transaction information in the blockchain. The distributed ledger is updated and shared among all RSUs and finally, the traded data is stored in the IPFS.

B. E-TRADING AND PRIVACY PRESERVATION

The steps involved in E-trading, including energy demand request, request matching and E-trading, are described as follows.

1) E-TRADING DEMAND REQUEST

Whenever an EV requires energy, it sends energy buying or energy demand request to RSU. This request includes the current location of EV, energy buying price, timestamp and amount of required energy. RSU after receiving the demand request from an EV, it authenticates the requesting EV. After authentication, EV is assigned a token against its pseudo-id.

2) E-TRADING RESPONSE REQUEST

Upon receiving an energy demand request from a legitimate EV, the RSU forwards this request to a pool of EVs in the proximity of requesting EV without revealing its location information to other EVs. The forwarding request includes energy demand and price. In response to the RSU's energy demand request, the EVs that are willing to sell energy send their energy selling request to the RSU. This response request includes energy volume and its price.

3) REQUEST MATCHING AND TOKEN ASSIGNMENT

Both demand and response requests are matched by RSUs. The response request that better matches the demand request in terms of energy price and volume as per demand is finalized by the RSU. After this request and response matching process, the seller and buyer EVs are assigned a token that validates the authentication of both seller and buyer EVs. The content of token assigned to both EVs includes time slot, charging pole location, energy volume to be traded and energy price.

C. ACCOUNT MAPPING

In the account mapping phase, the account mapping module (depicted in Fig. 3) is implemented with the objective to hide the private information of EVs about buying and selling of energy. The payment mechanism is handled through smart contract. It facilitates in providing payment in the form of coins to corresponding seller EV. Initially, buyer and seller EVs are assigned tokens that contain the information about traded energy volume and its price. After E-trading, coins are transferred to either the current account of seller EV or a new account is created. The account selection criteria depends on the energy volume and its price by seller EV. In the account mapping scheme, a threshold value is used to determine whether coins need to be transferred in a new or current account. A value setter function is used to determine the threshold value. We use τ to denote the threshold value. Each time the account selection criteria is determined using a dynamic threshold value instead of a fixed τ. The reason for using dynamic τ is to prevent data-mining attacks that are possible due to fixed threshold value. Let $F(.)$ be the τ-value setter function, now there are following two cases.

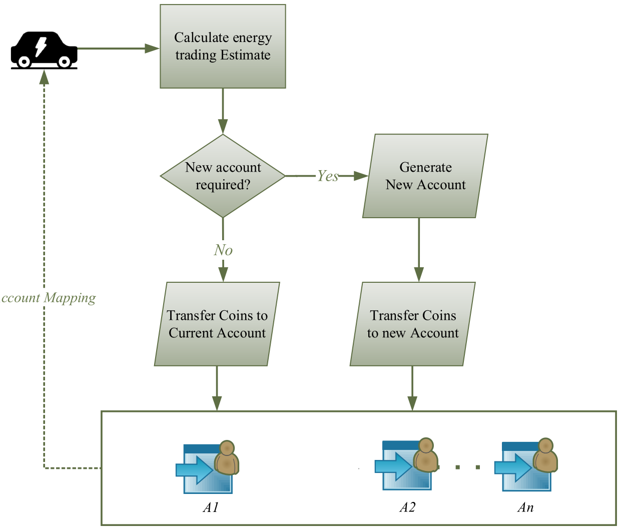

Calculate energy trading Estimate
New account required?
Yes
Generate New Account
No
Transfer Coins to Current Account
Transfer Coins to new Account
Account Mapping
A1
A2
An

FIGURE 3. **Account mapping of EVs.**

Case 1: If the coins transfer amount is lesser than the τ, then the transfer is made to the current account of seller EV.

Case 2: If the coin transfer amount is greater than the τ, then a new account is created for seller EV.

1) ACCOUNT GENERATION

For the account generation, assume a function $\mathcal{A}(.)$, which determines the condition for account generation. $\mathcal{A}(EV_s|\mathcal{C})$ refers to the function of seller EV_s with $\mathcal{C}$ be the amount of traded energy. It is important to figure out the proper configuration of the τ-value for the account generation process. There must be a proper method to discover its τ-value because simply relying on switching accounts is not enough to defend against attacks. Thus, a proper method for parallel trading with EV account is necessary instead of switching and blocking of the accounts. This value can be achieved through finding τ-value within a certain period of time $\mathcal{T}_c$. The maximum value for previously traded energy by a seller EV is calculated within $\mathcal{T}_c$. We have called this parameter a Trading Estimate (TE). While new accounts are created for an EV, a value λ is required to add trading records in the older account by setting up a percentage value of TE. λ is a pre-configured value. In the following Eq. 1, $\tau|EV_s$ shows the τ-value of seller EV and $\mathcal{E}(.)$ denotes the function of EST.

$$\mathcal{A}(EV_s|\mathcal{C}) = \tau|EV_s = TE \times \lambda = \mathcal{E}(.) \times \lambda. \tag{1}$$

Here, we are using the time-series method to predict the TE value from previous E-trading records. An Exponential Smoothing Technique (EST) is used, which is often used for the prediction of time-dependent data. The previous values are assigned an exponentially decreasing weight over time to predict future values using exponential function [66], [67]. Among single, double and triple EST, we have used single smoothing technique [68]. The function of EST, i.e., $\mathcal{E}(.)$ is shown in Eq 2.

$$\mathcal{E}(.) = E(i) = f(E(i-1)). \tag{2}$$
$$\mathbb{E} = \gamma E_i + (1-\gamma)E_{i-1}. \tag{3}$$

Here, in Equation 3, $\mathbb{E}$ refers to the forecasted value of energy whereas, E_i and E_{i-1} represent the values of energy at current iteration and traded energy till last iteration, respectively. The γ is a smoothing factor that shows the amount of weight added to previous values within the scope of (0, 1) [69]. For the month factor of time period T_c, the previous E-trading records are considered. Thus, Equation 3 can be written as follows:

$$\mathcal{E}(.) = (\gamma E_i + (1-\gamma)E_{i-1}) \times T_c. \tag{4}$$

Using Equation 4, the TE can be calculated to figure out the τ-value for seller EV.

VII. ALGORITHMS

In this section, the algorithms used in the proposed scheme are explained briefly. The Algorithm 2 is about account mapping, and the Algorithm 3 is about τ-value detection. The Algorithm 3 is executed within the Algorithm 2.

A. ACCOUNT MAPPING ALGORITHM

The Algorithm 2 is for EV account mapping, which is implemented in the payment transfer step. It depends on the

Algorithm 2 Account Mapping Algorithm

```
Input: $E_i$, $E_{i-1}$
Output: Coin Transfer Decision
Input Variables
Jump to Algorithm 3
Get $\tau$ value
if $\mathbb{E}_i \leq \tau \mid EV_i$ then
    $EV_{s_i} \mid \mathcal{C} \rightarrow$ Coin transfer
    Execute Case 1
    return Decision: Add Coins to Current Account
else
    Execute Case 2
    Construct Account Mapping
    return Decision: Add Coins to New Account
Add Records in Blockhain on returns
```

Algorithm 3 Threshold Value Detection Algorithm

```
Input: $E_i$, $E_{i-1}$, $\gamma$
Output: $\tau$-value, $\tau \mid EV_i$
Input Variables
/* Calculation for a single EV */
for ∀ trading records of an EV do
    Calculate average traded energy volume by an EV
/* Calculation for all EVs */
for ∀ trading records of sellers EVs do
    Calculate average traded volume by all EVs
Initialize Time factor $T_c$
for each Coin Transfer request do
    Read total accumulative traded $E_{i-1}$, $\tau$
    Calculate $\tau$ value using Equation 1
    return $\tau$-value
```

two sets of chores to be completed first. The first one is about decision making whether new account generation is required or not. If it returns a positive response, then a new account is created. On the other hand, if it returns a negative response, the execution of algorithm is terminated. The input of algorithm includes the E-trading history of seller EV, i.e., history about energy traded till last transaction and current trading energy volume of EV. The output generates a decision label, whether payment need to be transferred in the current or new account. The detailed description of Algorithm 2 is given below.

1) The first phase of algorithm involves τ-value detection of seller EV. After variables initialization, the execution is transferred to Algorithm 3 to get τ-value. This phase is the base for new account generation step. By using a smart contract, the automatic sum for the previously traded energy volume of seller EVs is calculated. As an energy broker, RSU is considered to be trustworthy, so there is no chance of privacy leakage.
2) After τ-value detection, the calculated sum of traded energy volume by EV is compared. If the traded volume of an EV is less than the τ-value, then the coins are transferred to its current account. Otherwise, coins are transferred to newly mapped account of EV.
3) The final phase outputs a decision label that determines the decision of coin transfer, which is recorded in the blockchain.

B. THRESHOLD DETECTION ALGORITHM

The Algorithm 3 is about τ-value detection that runs during phase 1 of Algorithm 2. This algorithm is formulated to achieve the upper limit of τ-value. The input parameters include the previous E-trading records of EVs. The previously traded energy volume of EV is required to calculate the time period. The detailed description of Algorithm 3 is given below.

1) In the first phase, the average traded energy of a single EV is calculated from its previous E-trading records within $\mathcal{T}_c$.
2) In the second phase, the average traded energy for all EVs is calculated using the time period parameter.
3) In the final phase, input values, including λ and γ are used to calculate $\mathcal{A}(.)$, i.e., $\mathcal{A}(EV_b|\mathcal{C})$.

The time complexity for the τ-value detection algorithm is $\mathcal{O}(n)$. For each seller EV, it is required to run this algorithm for calculating τ-value.

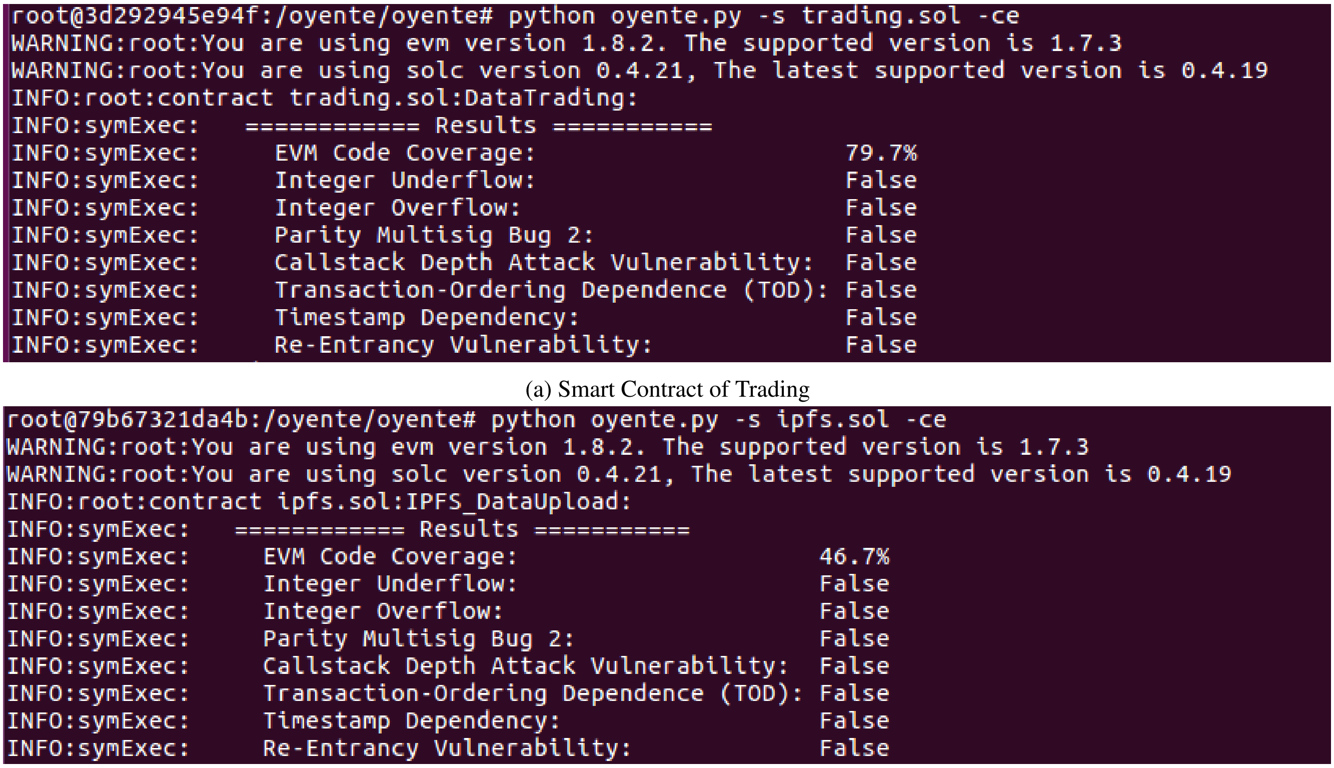
VIII. SECURITY ANALYSES

In this section, the vulnerability analyses of smart contracts is presented and security features are discussed as well that ensure the privacy of vehicles, integrity of traded data and transparency in trading actions.

A. SMART CONTRACT VULNERABILITY ANALYSIS

Smart contracts may be susceptible to attacks and vulnerabilities that arise due to weak programming practices. Since Ethereum is directly linked to monetary funds, so financial loss can occur if vulnerabilities are neglected. It is essential to make smart contracts code bug free. An open-source tool Oyente is used for analyzing smart contracts [70]. It analyzes smart contracts using symbolic execution techniques based on conditions, which are used as a formula to check input values in a smart contract for possible vulnerabilities. Several known attacks are reported in smart contracts, including Call Stack Depth, Integer Overflow and Underflow, Transaction Ordering Dependence, Re-Entrancy detection and Timestamp Dependency [71], [72]. These attacks are briefly summarized as follows.

- **Re-Entrancy Function**
  The repeated calls are made for the same function again and again for several times that the execution of any other function is not possible.
- **Timestamp Dependency**
  It involves manipulation of timestamp for blocks and transactions by participating nodes to generate their desired output.



```
root@3d292945e94f:/oyente/oyente# python oyente.py -s trading.sol -ce
WARNING:root:You are using evm version 1.8.2. The supported version is 1.7.3
WARNING:root:You are using solc version 0.4.21, The latest supported version is 0.4.19
INFO:root:contract trading.sol:DataTrading:
INFO:symExec:   ============ Results ===========
INFO:symExec:     EVM Code Coverage:                      79.7%
INFO:symExec:     Integer Underflow:                      False
INFO:symExec:     Integer Overflow:                       False
INFO:symExec:     Parity Multisig Bug 2:                  False
INFO:symExec:     Callstack Depth Attack Vulnerability:   False
INFO:symExec:     Transaction-Ordering Dependence (TOD):  False
INFO:symExec:     Timestamp Dependency:                   False
INFO:symExec:     Re-Entrancy Vulnerability:              False
```

(a) Smart Contract of Trading

```
root@79b67321da4b:/oyente/oyente# python oyente.py -s ipfs.sol -ce
WARNING:root:You are using evm version 1.8.2. The supported version is 1.7.3
WARNING:root:You are using solc version 0.4.21, The latest supported version is 0.4.19
INFO:root:contract ipfs.sol:IPFS_DataUpload:
INFO:symExec:   ============ Results ===========
INFO:symExec:     EVM Code Coverage:                      46.7%
INFO:symExec:     Integer Underflow:                      False
INFO:symExec:     Integer Overflow:                       False
INFO:symExec:     Parity Multisig Bug 2:                  False
INFO:symExec:     Callstack Depth Attack Vulnerability:   False
INFO:symExec:     Transaction-Ordering Dependence (TOD):  False
INFO:symExec:     Timestamp Dependency:                   False
INFO:symExec:     Re-Entrancy Vulnerability:              False
```

(b) Smart Contract of Data Storage in IPFS

FIGURE 4. Smart contracts vulnerability analyses.

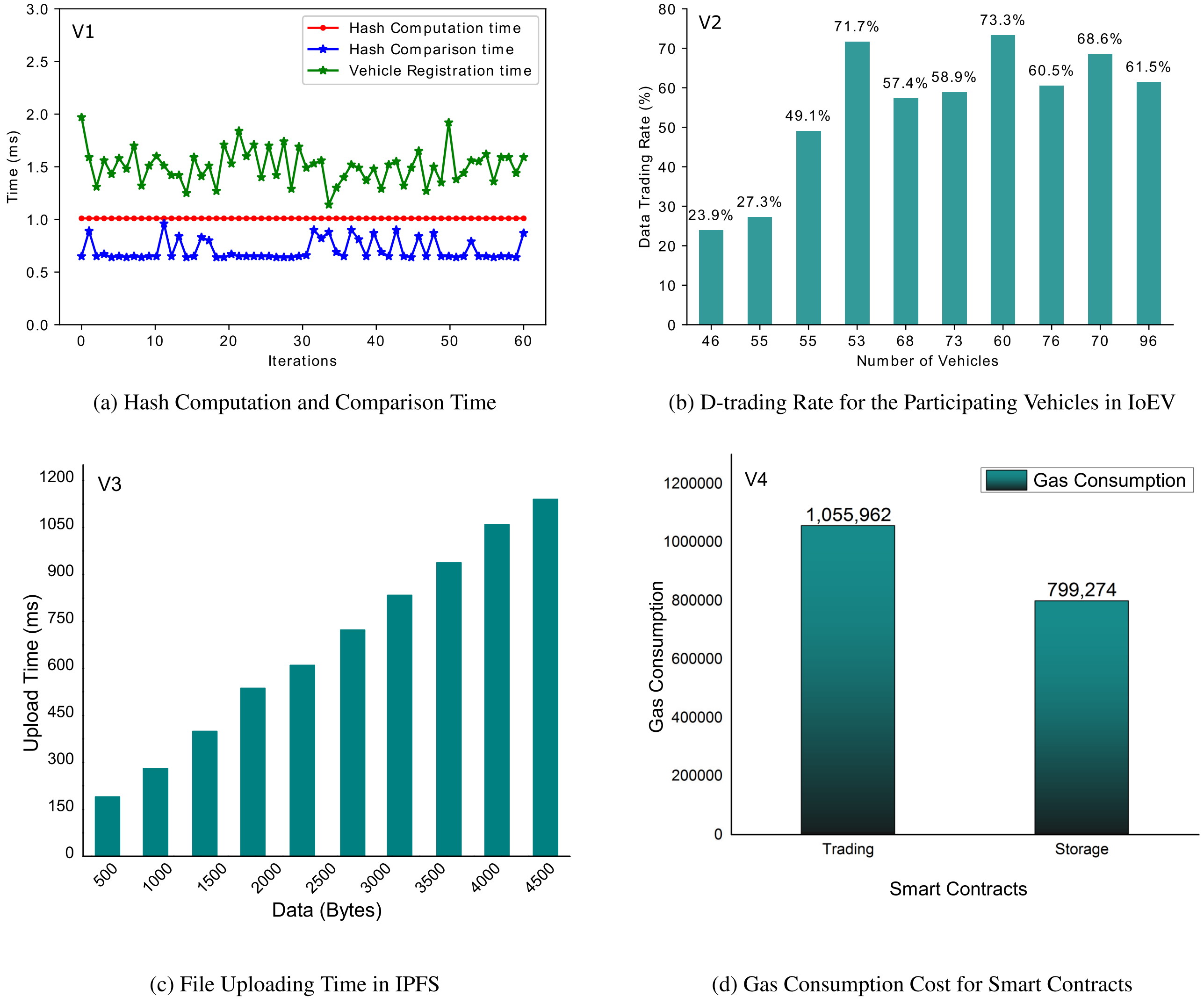
- **Call Stack Attack**
  Whenever the call stack exceeds the maximum of 1024 calls, an external function call may fail and result in throwing an exception. The attacker might be able to force call stack to the maximum value to launch this attack.
- **Parity Multisig Bug**
  In this attack an anonymous user executes a function named *initWallet* to gain knowledge about address of wallet owner and the required amount. It makes wallet inaccessible without affecting the wallet balance. The attacker makes himself the owner of contract and performs fund transfer transactions from wallet.
- **Transaction Ordering Dependence**
  It refers to the execution of transactions that are dependent on the amount of *gas* required. *Gas* price determines which transaction is required to be mined first. In this attack, *gas* price gets modified by an attacker (miner, owner, or another user) during the transaction processing before its completion.
- **Integer Overflow and Underflow Attack**
  The overflow occurs when a variable is incremented until it exceeds the allowed limit. Similarly, underflow works in the opposite direction, i.e., going beyond the minimum assigned value.

The smart contracts used in the proposed scheme are analyzed against the above-mentioned vulnerabilities, as shown in Fig. 4. The analyses results for vulnerabilities are reported *False*, which means that the smart contracts are secure and bug-free.

B. SECURITY FEATURES

In this section, we discuss how thes proposed schemes of D-trading and E-trading in IoEV ensure identity privacy of vehicles, integrity of traded data and transparency in trading actions. The objective is to achieve efficiency in trading along with the mentioned security features.

- **Identity Privacy**
  In the proposed model, the attacker cannot infer the actual identity of vehicles during D-trading because real identity of a vehicle is transformed into a pseudo-id, which is based on a digital signature scheme. The mapping between real identity and pseudo-id is only known to TA. Even if an attacker infers some identity-related information, it is impossible to determine the randomly selected value that is used by TA to generate pseudo-id.
- **Data Integrity and Non-Repudiation**
  After the vehicles are registered by TA, the identity of vehicles is verified by authorized RSUs. In D-trading, the traded data needs to be signed by legitimate vehicle. Only legalized and authenticated vehicles are allowed to trade data. The digitally signed data by authenticated vehicles ensures the integrity and non-repudiation of data.



(a) Hash Computation and Comparison Time

(b) D-trading Rate for the Participating Vehicles in IoEV

(c) File Uploading Time in IPFS

(d) Gas Consumption Cost for Smart Contracts

FIGURE 5. **Performance evaluation of proposed system.**

- **Decentralization**
  Instead of using centralized data storage mechanisms, our proposed model employs a distributed data storage system, i.e., IPFS. It eliminates the problems of central storage while reducing data storage cost. Moreover, it eliminates the malicious attacks related to centralized data storage systems.
- **Transparency**
  All trading transactions are performed using smart contracts. The trading information is recorded in the blockchain, which eliminates the chances of future disputes among trading parties. The trading transparency enables a vehicle to communicate and trade data in the trustless IoEV environment.

IX. SIMULATION RESULTS

The computations are performed using Ethereum, which is an open-source, well developed and a blockchain-based platform, launched in 2015 [73]. In Ethereum, transactions are of following three types.

1) Funds transfer
2) Smart contract deployment
3) Function execution within the deployed contract

A transaction is made whenever there is a change in the state of the network. All transactions are subject to a fee that is to be paid in terms of *gas*. The *gas* a fundamental unit for measuring the transaction and execution cost in Ethereum. In Ethereum, a parameter called *gas limit* indicates the overall quantity of *gas* for computing smart contract operations. The deployment cost of smart contract includes transaction and the execution cost. The price of adding transactions on the blockchain is termed as transaction cost. Whereas, the computational cost of each operation executed within the smart contract is termed as execution cost.

Experiments are performed on a PC with a hardware configuration of 1.70 GHz core i5-33177U CPU, 6 GB RAM

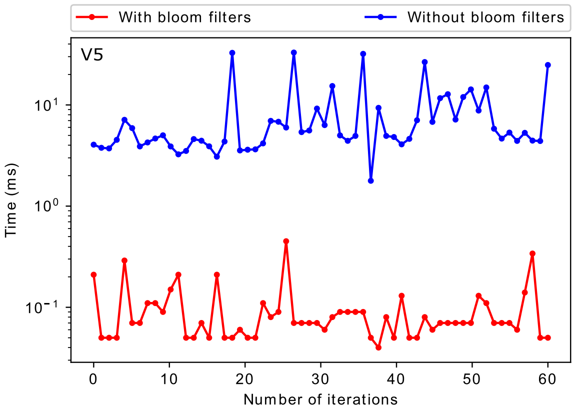


FIGURE 6. Time efficiency with and without bloom filter.

TABLE 4. V4: Transaction and execution cost.

Data (*Bytes*)	Transaction Cost (*gas*)	Execution Cost (*gas*)
647	994,648	712,916
1087	1,607,713	1,509,897
1579	2,285,181	2,153,893
1983	2,963,501	2,636,892
2450	3,632,083	3,075,338
2970	4,230,749	3,441,236
3345	4,820,073	4,027,692
3894	5,398,419	4,570,812
4390	6,016,662	4,969,228
4820	7,337,278	5,295,088

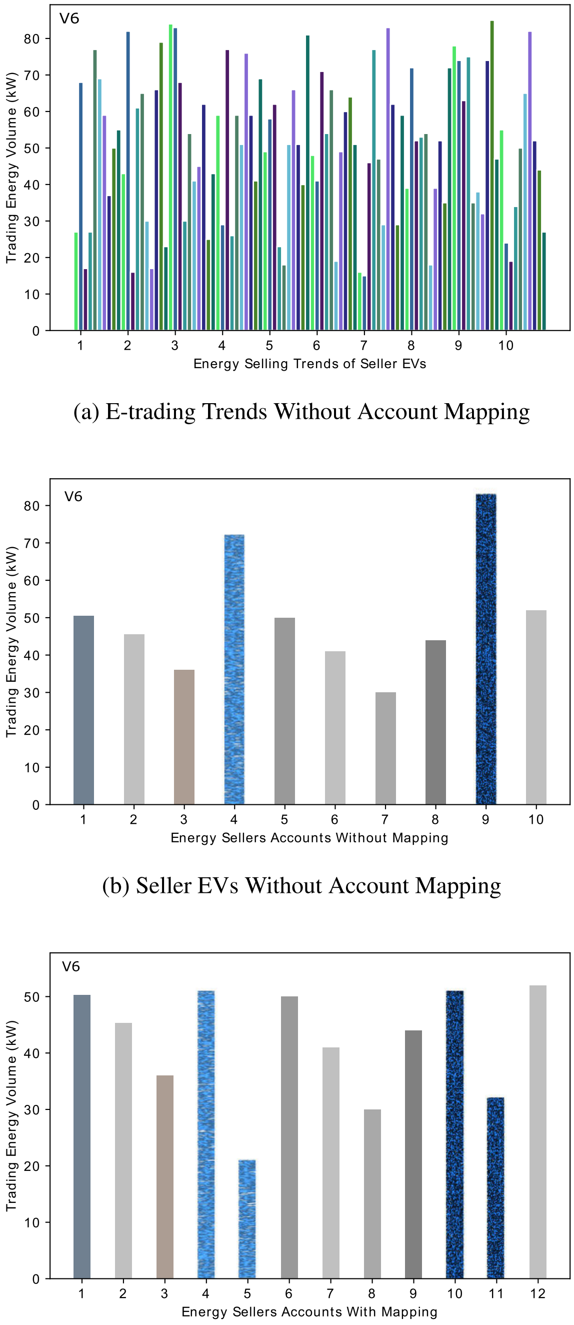
with Windows 10 operating system installed. Remix IDE is used along with Ganache and Metamask. Some simulations are performed using Python 3.6.

A. RESULTS FOR D-TRADING IN IoEV

All functions that are used in the smart contract for D-trading in IoEV require *gas* for their execution. These functions include smart contract deployment, hash computations, data duplication validation and uploading data to IPFS.

The tag V1 in Fig. 5a validates the proposed solutions S1 and S2 against the limitations L1, L2 and L3. Fig. 5a shows the time cost for registration of vehicles, hash computation and comparison functions. Registration of vehicles is performed by TA and its time cost is plotted against multiple iterations. Whereas, the hash computation and comparison functions are carried out by RSUs by using a hash-list that is already stored at RSUs. It takes constant time to compute the hash of traded data. Whereas, the time for hash comparison varies in each iteration. The time cost for both hash computation and hash comparison is minimum. It can be seen that the time required for registration is greater than the other two functions because vehicle registration is a one-time process, which takes an average time cost of 1 to 2 ms. It involves pseudo-id and certificate generation that are used for communication between vehicles and RSUs.

Fig. 5b is tagged as V2 that validates the solution S2 against the limitations L1 and L2. It illustrates the D-trading rate for the varying number of vehicles in IoEV network. The D-trading rate varies with the change in the number of vehicles at multiple instances. At a certain time period, only a few vehicles communicate with RSUs to trade data. D-trading rate ultimately increases with the increasing number of vehicles that are involved in D-trading. However, when more vehicles are involved in communication and D-trading, the D-trading rate may vary due to data duplication. As shown in Fig. 5b, the D-trading rate gets lower even in case of an increased number of participating vehicles. The lower D-trading rate occurs either due to data duplication or invalid



(a) E-trading Trends Without Account Mapping

(b) Seller EVs Without Account Mapping

(c) Seller EVs With Account Mapping

FIGURE 7. E-trading trends with and without account mapping scheme.

TABLE 5. Mapping of identified limitation with proposed solutions and validation results.

Limitations Identified	Proposed Solutions	Validation Results
L1: Vehicles in IoEV need to be registered for authentication and verification to avoid illegitimate vehicles in the network.	**S1:** TA is responsible for each vehicle registration and credentials verification by using Bilinear pairing. Before joining the network, vehicles provide their identity details to TA to get initial security parameters.	**V1:** No direct validation. However, the time cost for registration of vehicles is shown in Fig. 5a.
L2: Due to selfishness and for financial gain, EVs try to trade same data for multiple times, which results in data duplication.	**S2:** To prevent data duplication, the hash of data is computed by RSUs and its comparison is performed using previously stored data hash-list at RSU.	**V1, V2:** No direct validation. However, time cost for hash computation and comparison is shown in Fig. 5a. The minimal time is required to check the data duplication which does not causes any computation overhead. Moreover, the data duplication affects the trading rate that can be observed in Fig. 5b.
L3: The second-hand sharing of data involves re-selling of previously traded data, which may cause data duplication and unfair D-trading.	**S2:** The second-hand sharing of data is prevented by using data hash-list, which is managed by RSUs.	**V1, V2:** No direct validation. However, the time cost for hash computation and comparison can be seen in Fig. 5a. Moreover, the second-hand sharing may affect the trading rate that can be observed in Fig. 5b.
L4: Vehicles have limited storage capacity to store real-time vehicle generated data for longer period of time.	**S3:** A distributed storage, IPFS is used to ensure reliable storage of data and its availability for longer period of time.	**V3:** The time cost for uploading traded data in IPFS is shown in Fig. 5c for varying data size.
L5: The trading parties face payment disputes and unfair trading. A trusted intermediary is required for disputes handling.	**S4:** Smart contract is used for an efficient and reliable payment mechanism to avoid trading disputes and unfair payments.	**V4:** The costs of smart contracts are shown in Fig. 5d. Whereas the transaction and execution costs for variable data size are listed in Table 4.
L6: For checking data duplication in D-trading, an efficient data search mechanism is required.	**S5:** To make data lookup fast in data duplication, we used bloom filters probabilistic data structures that are space, and time-efficient.	**V5:** Fig. 6 validates the time efficiency of using bloom filters for fast data lookup. The time cost factor shows a clear difference in both cases, i.e., with and without bloom filters.
L7: E-trading records information is linked with publicly available datasets to launch linkage attacks.	**S6:** An account mapping scheme is used to hide E-trading trends. One-to-multiple accounts are assigned to EVs to ensure their privacy.	**V6:** Fig. 7a, Fig. 7b and Fig. 7c show the E-trading trends distribution with and without using account mapping scheme.

D-trading requests. Here, invalid D-trading requests refer to the requests that are sent by illegitimate vehicles or the requests that are proved invalid by RSU after performing the data duplication check.

The label V3 in Fig. 5c validates the solution S3 against the limitation L4. It demonstrates the time to upload data in IPFS. The limitation L4 is about data storage problem that is solved by using IPFS (solution S3). Time to upload traded data in IPFS differs according to the variable data size. The varying data size, ranging from 500 to 5000 bytes, is used for analyzing the upload time in IPFS. With the increasing data size in bytes, the upload time to store data in IPFS increases linearly.

The tag V4 in Fig. 5d, maps the proposed solution S4 against the limitations L5. In the proposed scheme, two smart contracts are used for D-trading, namely the trading contract and the storage contract. The deployment cost for both smart contracts is shown in Fig. 5d. The *gas* consumption cost for trading and storage contracts is 1,055,962 and is 799,274, respectively, which is acceptable. It presents the resources required during smart contract deployment in a real environment. Thus, resource utilization is low and manageable to trade data in real-time and storing data to IPFS.

Since the traded data is uploaded to IPFS that costs some amount of gas referred to as transaction and execution cost as shown in Table 4, which is tagged as V4. It shows the cost for different data sizes, ranging from 500 to 50000 bytes. With the increase in data size, more mount of gas is required that increases storage costs in a linear manner, which shows that the proposed system is scalable.

Fig. 6 is labeled as V5. It validates the solution S5 against the limitation L6. It shows the time cost for checking data duplication using bloom filters. Since bloom filters are known for their key feature of time efficiency, so during data duplication validation in D-trading by RSUs, bloom filters are employed for fast data lookup. The efficient response is very crucial in vehicular communications. As shown in Fig. 6, the time consumed in data lookup by bloom filters is significantly less than the time consumed by normal data search mechanism in hash-list. To show the time cost, a logarithm scale is used to make the time cost range visible without compressing down the smaller values at the bottom of graph. The time consumption for data lookup in both scenarios, i.e., with and without bloom filters, is clearly visible. This time consumption cost validates the efficiency of bloom filter in terms of efficient data lookup in hash-list during data duplication verification in IoEV enables D-trading.

B. RESULTS FOR PRIVACY-PRESERVING E-TRADING IN EVs

In this section, we present the simulation results for blockchain-based privacy-preserving E-trading for EVs using an account mapping scheme. The results for E-trading trends with and without mapping are shown in Fig. 7. Fig. 7a, Fig. 7b and Fig. 7c are labeled as V6 that validate the solution S6 against limitation L7, which is about data linkage attacks. Fig. 7a shows the E-trading trends of EVs in the absence of any account mapping scheme. It shows an irregular volume of energy traded from multiple EVs.

Fig. 7b and Fig. 7c show energy seller EVs' accounts with and without mapping, respectively. The textured illustrated bars in Fig. 7b illustrates the accounts of EVs with distinct E-trading volume. The corresponding textured bars in Fig. 7b are mapped in Fig. 7c using multiple accounts that result in uniform distribution of E-trading trends. Fig. 7c does not show any irregular or distinct traded volume trends within the current iteration. Because of the threshold value, the E-trading volume decides new account creation for EVs. The wave generated from the energy trends clearly shows that with a mapping scheme, the EVs energy trends are hidden. In Table 5, the identified limitations with their respective proposed solutions and validations are listed. There are no direct validation results for a few of the limitations; however, their effect can be seen in the referenced simulations results.

X. CONCLUSION

In this work, a consortium blockchain-based truthful D-trading and E-trading model is presented in IoEV. There are various issues that occur during trading, including illegal activities, denial of payment, conflicting interests of trading entities. We have addressed these problems by exploiting consortium blockchain for transparency in trading. Smart contracts are used to perform all trading actions. In D-trading, data duplication validation is performed by RSUs to minimize the storage cost. A hash-list is managed by RSUs to investigate for duplicate trading data. A hash of trading data is computed and then duplication verification is done using hash-list, which prevents the second-hand sharing of data. Bloom filters are implemented to make hash lookup mechanism fast and efficient. Furthermore, IPFS is introduced, which imparts a reliable storage and efficient retrieval of data and its availability for longer duration.

Furthermore, we present a blockcahin-based privacy-preserving model for EVs to solve the issues related to privacy leakage attacks in E-trading records. We have used a new account generation technique for hiding information about E-trading records. By using this technique, adversaries cannot infer the trading records of EVs even if the trading information is publicly available. The new account generation method depends on the amount of traded energy and (τ)-value. This value is calculated using an EV's current and previously traded energy volume. The τ-value helps in determining the decision about the payment transfer to EVs' current or new account. The security analyses of smart contracts is performed, which shows that the smart contracts used for trading are bug-free and secure against the known attacks. The simulation results demonstrate that the proposed blockchain-based D-trading scheme is efficient with minimum time cost, and it provides a reliable data storage mechanism. Additionally, the E-trading trends of EVs are hidden effectively.

In the next few years, the real-time vehicle generated data will be of great worth. Furthermore, the considerable rise in energy trading among EVs and their privacy concerns are likely to become an important issue to be addressed. As mentioned earlier that we are dealing with only two types of vehicles in IoEV. For now, we have restricted fuel vehicle to perform D-trading and EV is restricted to perform E-trading only. In the future work, we will work with hybrid vehicles as well that will b capable of performing both D-trading and E-trading.

Moreover, our future work will concentrate on reliable and efficient service provisioning mechanism by introducing a monitoring authority to keep check and balance on the services provided by RSUs. Further studies, which take a rating based reputation system into account, will need to be established.

REFERENCES

[1] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.

[2] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Nov. 20, 2019. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019.

[4] (2016). *White Paper—Ethereum/WiKi*. Accessed: Mar. 10, 2020. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[5] R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun, "Blockchain for large-scale Internet of Things data storage and protection," *IEEE Trans. Services Comput.*, vol. 12, no. 5, pp. 762–771, Sep. 2019.

[6] S. K. Singh, S. Rathore, and J. H. Park, "BlockIoTIntelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence," *Future Gener. Comput. Syst.*, vol. 110, pp. 721–743, Sep. 2020.

[7] T. Sultana, A. Almogren, M. Akbar, M. Zuair, I. Ullah, and N. Javaid, "Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices," *Appl. Sci.*, vol. 10, no. 2, p. 488, Jan. 2020.

[8] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102407.

[9] P. Dong, Z. Ning, M. S. Obaidat, X. Jiang, Y. Guo, X. Hu, B. Hu, and B. Sadoun, "Edge computing based healthcare systems: Enabling decentralized health monitoring in Internet of medical things," *IEEE Netw.*, vol. 34, no. 5, pp. 254–261, Sep. 2020.

[10] A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair, and M. Alam, "Blockchain-based agri-food supply chain: A complete solution," *IEEE Access*, vol. 8, pp. 69230–69243, 2020.

[11] M. A. Quddus, M. Kabli, and M. Marufuzzaman, "Modeling electric vehicle charging station expansion with an integration of renewable energy and vehicle-to-grid sources," *Transp. Res. E, Logistics Transp. Rev.*, vol. 128, pp. 251–279, Aug. 2019.

[12] M. B. Rasheed, N. Javaid, A. Ahmad, M. Awais, Z. A. Khan, U. Qasim, and N. Alrajeh, "Priority and delay constrained demand side management in real-time price environment with renewable energy source," *Int. J. Energy Res.*, vol. 40, no. 14, pp. 2002–2021, Nov. 2016.

[13] N. Javaid, S. Hussain, I. Ullah, M. Noor, W. Abdul, A. Almogren, and A. Alamri, "Demand side management in nearly zero energy buildings using heuristic optimizations," *Energies*, vol. 10, no. 8, p. 1131, Aug. 2017.

[14] S. Kazmi, N. Javaid, M. J. Mughal, M. Akbar, S. H. Ahmed, and N. Alrajeh, "Towards optimization of metaheuristic algorithms for IoT enabled smart homes targeting balanced demand and supply of energy," *IEEE Access*, vol. 7, pp. 24267–24281, 2019.

[15] E. Bulut, M. C. Kisacikoglu, and K. Akkaya, "Spatio-temporal non-intrusive direct V2V charge sharing coordination," *IEEE Trans. Veh. Technol.*, vol. 68, no. 10, pp. 9385–9398, Oct. 2019.

[16] A. Sadiq, N. Javaid, O. Samuel, A. Khalid, N. Haider, and M. Imran, "Efficient data trading and storage in Internet of vehicles using consortium blockchain," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2020, pp. 2143–2148.

[17] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, Jan. 2003.

[18] W. Xue, D. Vatsalan, W. Hu, and A. Seneviratne, "Sequence data matching and beyond: New privacy-preserving primitives based on Bloom filters," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2973–2987, 2020.

[19] L. Luo, D. Guo, R. T. B. Ma, O. Rottenstreich, and X. Luo, "Optimizing Bloom filter: Challenges, solutions, and comparisons," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1912–1949, 2nd Quart., 2019.

[20] J. Benet, "IPFS–content addressed, versioned, P2P file system," 2014, *arXiv:1407.3561*. [Online]. Available: http://arxiv.org/abs/1407.3561

[21] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38437–38450, 2018.

[22] S. Garg, A. Singh, K. Kaur, G. S. Aujla, S. Batra, N. Kumar, and M. S. Obaidat, "Edge computing-based security framework for big data analytics in VANETs," *IEEE Netw.*, vol. 33, no. 2, pp. 72–81, Mar. 2019.

[23] X. Zhang and X. Chen, "Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 58241–58254, 2019.

[24] T. Jiang, H. Fang, and H. Wang, "Blockchain-based Internet of vehicles: Distributed network architecture and performance analysis," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4640–4649, Jun. 2019.

[25] S. Kim, "Impacts of mobility on performance of blockchain in VANET," *IEEE Access*, vol. 7, pp. 68646–68655, 2019.

[26] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.

[27] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, and C.-C. Liu, "Blockchain-based traffic event validation and trust verification for VANETs," *IEEE Access*, vol. 7, pp. 30868–30877, 2019.

[28] M. Li, J. Weng, A. Yang, J.-N. Liu, and X. Lin, "Toward blockchain-based fair and anonymous ad dissemination in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 11248–11259, Nov. 2019.

[29] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new type of blockchain for secure message exchange in VANET," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 177–186, May 2020.

[30] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

[31] B.-K. Zheng, L.-H. Zhu, M. Shen, F. Gao, C. Zhang, Y.-D. Li, and J. Yang, "Scalable and privacy-preserving data sharing based on blockchain," *J. Comput. Sci. Technol.*, vol. 33, no. 3, pp. 557–567, May 2018.

[32] Q. Feng, D. He, S. Zeadally, and K. Liang, "BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4146–4155, Jun. 2020.

[33] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 3, pp. 516–526, Mar. 2017.

[34] X. Liu, H. Huang, F. Xiao, and Z. Ma, "A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4101–4112, May 2020.

[35] Y. Ming and H. Cheng, "Efficient certificateless conditional privacy-preserving authentication scheme in VANETs," *Mobile Inf. Syst.*, vol. 2019, pp. 1–19, Feb. 2019.

[36] A. Bonadio, F. Chiti, R. Fantacci, and V. Vespri, "An integrated framework for blockchain inspired fog communications and computing in Internet of vehicles," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 2, pp. 755–762, Feb. 2020.

[37] H. Li, L. Pei, D. Liao, G. Sun, and D. Xu, "Blockchain meets VANET: An architecture for identity and location privacy protection in VANET," *Peer-Peer Netw. Appl.*, vol. 12, no. 5, pp. 1178–1193, Sep. 2019.

[38] M. Li, L. Zhu, and X. Lin, "Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4573–4584, Jun. 2019.

[39] C. Chen, J. Wu, H. Lin, W. Chen, and Z. Zheng, "A secure and efficient blockchain-based data trading approach for Internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 9110–9121, Sep. 2019.

[40] T. Zhang, H. Pota, C.-C. Chu, and R. Gadh, "Real-time renewable energy incentive system for electric vehicles using prioritization and cryptocurrency," *Appl. Energy*, vol. 226, pp. 582–594, Sep. 2018.

[41] A. Khan, N. Javaid, and M. I. Khan, "Time and device based priority induced comfort management in smart home within the consumer budget limitation," *Sustain. Cities Soc.*, vol. 41, pp. 538–555, Aug. 2018.

[42] G. Hafeez, N. Javaid, S. Iqbal, and F. Khan, "Optimal residential load scheduling under utility and rooftop photovoltaic units," *Energies*, vol. 11, no. 3, p. 611, Mar. 2018.

[43] Y. Wang, Z. Su, and N. Zhang, "BSIS: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3620–3631, Jun. 2019.

[44] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized Peer-to-Peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[45] R. Khalid, N. Javaid, A. Almogren, M. U. Javed, S. Javaid, and M. Zuair, "A blockchain-based load balancing in decentralized hybrid P2P energy trading market in smart grid," *IEEE Access*, vol. 8, pp. 47047–47062, 2020.

[46] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Netw.*, vol. 32, no. 3, pp. 78–83, May 2018.

[47] S. Zahoor, S. Javaid, N. Javaid, M. Ashraf, F. Ishmanov, and M. Afzal, "Cloud–fog–based smart grid model for efficient resource management," *Sustainability*, vol. 10, no. 6, p. 2079, Jun. 2018.

[48] A. Mahmood, N. Javaid, M. A. Khan, and S. Razzaq, "An overview of load management techniques in smart grid," *Int. J. Energy Res.*, vol. 39, no. 11, pp. 1437–1450, Sep. 2015.

[49] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3548–3558, Jun. 2019.

[50] S. Aslam, N. Javaid, F. Khan, A. Alamri, A. Almogren, and W. Abdul, "Towards efficient energy management and power trading in a residential area via integrating a grid-connected microgrid," *Sustainability*, vol. 10, no. 4, p. 1245, Apr. 2018.

[51] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren, "A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," *IEEE Netw.*, vol. 32, no. 6, pp. 184–192, Nov. 2018.

[52] T. A. Alghamdi, I. Ali, N. Javaid, and M. Shafiq, "Secure service provisioning scheme for lightweight IoT devices with a fair payment system and an incentive mechanism based on blockchain," *IEEE Access*, vol. 8, pp. 1048–1061, 2020.

[53] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.

[54] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, "Adaptive blockchain-based electric vehicle participation scheme in smart grid platform," *IEEE Access*, vol. 6, pp. 25657–25665, 2018.

[55] N. Javaid, G. Hafeez, S. Iqbal, N. Alrajeh, M. S. Alabed, and M. Guizani, "Energy efficient integration of renewable energy sources in the smart grid for demand side management," *IEEE Access*, vol. 6, pp. 77077–77096, 2018.

[56] M. Zahid, F. Ahmed, N. Javaid, R. Abbasi, H. Zainab Kazmi, A. Javaid, M. Bilal, M. Akbar, and M. Ilahi, "Electricity price and load forecasting using enhanced convolutional neural network and enhanced support vector regression in smart grids," *Electronics*, vol. 8, no. 2, p. 122, Jan. 2019.

[57] F. Yucel, K. Akkaya, and E. Bulut, "Efficient and privacy preserving supplier matching for electric vehicle charging," *Ad Hoc Netw.*, vol. 90, Jul. 2019, Art. no. 101730.

[58] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," *Comput. Sci.-Res. Develop.*, vol. 33, nos. 1–2, pp. 71–79, Feb. 2018.

[59] M. Rasheed, N. Javaid, M. Awais, Z. Khan, U. Qasim, N. Alrajeh, Z. Iqbal, and Q. Javaid, "Real time information based energy management using customer preferences and dynamic pricing in smart homes," *Energies*, vol. 9, no. 7, p. 542, Jul. 2016.

[60] M. B. Rasheed, M. A. Qureshi, N. Javaid, and T. Alquthami, "Dynamic pricing mechanism with the integration of renewable energy source in smart grid," *IEEE Access*, vol. 8, pp. 16876–16892, 2020.

[61] A. Derhab, M. Guerroumi, A. Gumaei, L. Maglaras, M. A. Ferrag, M. Mukherjee, and F. A. Khan, "Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security," *Sensors*, vol. 19, no. 14, p. 3119, Jul. 2019.

[62] F. Xu, Y. Li, Z. Tu, S. Chang, and H. Huang, "No more than what I post: Preventing linkage attacks on check-in services," *IEEE Trans. Mobile Comput.*, early access, Oct. 15, 2019, doi: 10.1109/TMC.2019.2947416.

[63] C.-M. Chen, B. Xiang, Y. Liu, and K.-H. Wang, "A secure authentication protocol for Internet of vehicles," *IEEE Access*, vol. 7, pp. 12047–12057, 2019.

[64] Y. Zhao, Y. Li, Q. Mu, B. Yang, and Y. Yu, "Secure pub-sub: Blockchain-based fair payment with reputation for reliable cyber physical systems," *IEEE Access*, vol. 6, pp. 12295–12303, 2018.

[65] H. R. Hasan and K. Salah, "Proof of delivery of digital assets using blockchain and smart contracts," *IEEE Access*, vol. 6, pp. 65439–65448, 2018.

[66] R. J. Hyndman and G. Athanasopoulos, *Forecasting: Principles and Practice*. Melbourne, VIC, Australia: Monash Univ., 2018.

[67] A. Ahmad, N. Javaid, N. Alrajeh, Z. Khan, U. Qasim, and A. Khan, "A modified feature selection and artificial neural network-based day-ahead load forecasting model for a smart grid," *Appl. Sci.*, vol. 5, no. 4, pp. 1756–1772, Dec. 2015.

[68] D. Bissing, M. T. Klein, R. A. Chinnathambi, D. F. Selvaraj, and P. Ranganathan, "A hybrid regression model for day-ahead energy price forecasting," *IEEE Access*, vol. 7, pp. 36833–36842, 2019.

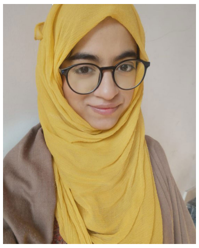
[69] T. Jonsson, P. Pinson, H. A. Nielsen, H. Madsen, and T. S. Nielsen, "Forecasting electricity spot prices accounting for wind power predictions," *IEEE Trans. Sustain. Energy*, vol. 4, no. 1, pp. 210–218, Jan. 2013.

[70] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 254–269.

[71] GitHub. (2018). *Ethereum Smart Contract Best Practices: Known Attacks*. Accessed: Mar. 27, 2020. [Online]. Available: https://consensys.github.io/smart-contract-best-practices/known_attacks

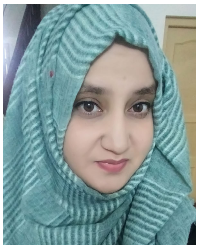
[72] Hackernoon.com. (2018). *Smart Contract Security: Part 1 Reentrancy Attack*. Accessed: Mar. 27, 2020. [Online]. Available: https://hackernoon.com/smart-contract-security-part-1-reentrancy-attacks-ddb3b2429302

[73] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Parity Technol., Berlin, Germany, Ethereum Project Yellow Paper 151, 2014, pp. 1–32. Accessed: Apr. 20, 2020. [Online]. Available: https://gavwood.com/paper.pdf



AYESHA SADIQ received the bachelor's degree in computer science from International Islamic University, Islamabad, Pakistan, in 2015, and the M.S. degree in information security from the Communications Over Sensors (ComSens) Research Laboratory, COMSATS University Islamabad, Islamabad Campus, in 2020, under the supervision of Dr. Nadeem Javaid. Her research interest includes blockchain in smart grids.

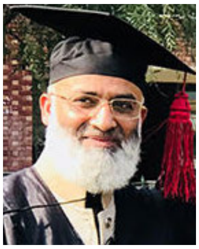
MUHAMMAD UMAR JAVED received the bachelor's and master's degrees in electrical engineering from Government College University Lahore, Lahore, Pakistan, in 2014 and 2018, respectively. He is currently pursuing the Ph.D. degree in computer science with the Communications Over Sensors (ComSens) Research Laboratory, COMSATS University Islamabad, Islamabad Campus, under the supervision of Dr. Nadeem Javaid. His research interests include smart grids, electric vehicles, and blockchain.



RABIYA KHALID received the M.C.S. degree from the Mirpur University of Science and Technology, Mirpur, Pakistan, in 2014, and the M.S. degree in computer science with a specialization in energy management in smart grid from the Communications Over Sensors (ComSens) Research Laboratory, COMSATS University Islamabad, Islamabad, Pakistan, in 2017, under the supervision of Dr. Nadeem Javaid, where she is currently pursuing the Ph.D. degree under the same supervision. She is currently working as a Research Associate with the ComSens Research Laboratory, COMSATS University Islamabad. She has authored more than 20 research publications in international journals and conferences. Her research interests include data science and blockchain in smart/micro grids.

AHMAD ALMOGREN (Senior Member, IEEE) is a Professor of Computer Science Department at the College of Computer and Information Sciences (CCIS), King Saud University (KSU), Riyadh, Saudi Arabia. Currently, he is the Director of Cyber Security Chair at CCIS, KSU. He received a Ph.D. degree in Computer Science from Southern Methodist University, Dallas, TX, USA, in 2002. Previously, he worked as the Vice Dean for the Development and Quality at CCIS. He also served as the Dean for the College of Computer and Information Sciences and the Head of Academic Accreditation Council at Al Yamamah University. He served as the General Chair for the IEEE Smart World Symposium and a Technical Program Committee member in numerous international conferences/workshops, such as IEEE CCNC, ACM BodyNets, and IEEE HPCC. His research areas of interests include mobile-pervasive computing and cyber security.

MUHAMMAD SHAFIQ received the master's degree in information technology (IT) from the University of the Punjab, Gujranwala, Pakistan, in 2006, the M.S. degree in computer science from the University Institute of Information Technology, Arid Agriculture University, Rawalpindi, Pakistan, in 2010, and the Ph.D. degree in information and communication engineering from Yeungnam University, South Korea, in February 2018. He has worked with the Faculty of Computing and IT, University of Gujrat, Gujrat, Pakistan, as a Faculty Member, from 2010 to 2014, and formerly held the same position with the Department of Computer Science and IT, Federal Urdu University, Islamabad, Pakistan. His research interests include the Internet of Things (IoT), the cognitive radio-based IoT networks-architecture and design, mobile-ad-hoc networks, wireless sensor networks, performance, management, and security, 5G cellular networks, admission control, and mobility management, device-to-device communications, medium access control protocols, the Internet routing protocols, spectrum trading and auctions, information systems, design, and access control, and human–computer interaction.



NADEEM JAVAID (Senior Member, IEEE) received the bachelor's degree in computer science from Gomal University, Dera Ismail Khan, Pakistan, in 1995, the master's degree in electronics from Quaid-i-Azam University, Islamabad, Pakistan, in 1999, and the Ph.D. degree from the University of Paris-Est, France, in 2010. He is currently an Associate Professor and the Founding Director of the Communications Over Sensors (ComSens) Research Laboratory, Department of Computer Science, COMSATS University Islamabad, Islamabad. He has supervised 126 master and 20 Ph.D. theses. He has authored more than 900 articles in technical journals and international conferences. His research interests include energy optimization in smart/micro grids, wireless sensor networks using data analytics, and blockchain. He was recipient of the Best University Teacher Award from the Higher Education Commission of Pakistan, in 2016, and the Research Productivity Award from the Pakistan Council for Science and Technology, in 2017. He is also an Associate Editor of IEEE Access, and an Editor of the *International Journal of Space-Based and Situated Computing* and *Sustainable Cities and Society*.