IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 6 July 2022, accepted 18 July 2022, date of publication 28 July 2022, date of current version 10 August 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3194513

RESEARCH ARTICLE

Secure Message Handling in Vehicular Energy Networks Using Blockchain and Artificially Intelligent IPFS

MUHAMMAD UMAR JAVED[1], ABID JAMAL[1], EMAN H. ALKHAMMASH[2], MYRIAM HADJOUNI[3], SAEED ALI BAHAJ[4], AND NADEEM JAVAID[1,5], (Senior Member, IEEE)

[1]Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan
[2]Department of Computer Science, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia
[3]Department of Computer Sciences, College of Computer and Information Science, Princess Nourah Bint Abdulrahman University, Riyadh 11671, Saudi Arabia
[4]MIS Department, College of Business Administration, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[5]School of Computer Science, University of Technology Sydney, Ultimo, NSW 2007, Australia

Corresponding author: Nadeem Javaid (nadeemjavaidqau@gmail.com)

This work is supported by Taif University Researchers Supporting Project number (TURSP-2020/292) Taif University, Taif, Saudi Arabia. This work is also supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R193), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

ABSTRACT In the underlying work, the problems faced during message dissemination in the conventional Vehicular Energy Networks (VENs) like lack of security, breach of personal identities, absence of trust between vehicle owners, etc., are tackled. In this study, a Blockchain (BC) based announcement system is proposed for VENs to ensure secure and reliable announcement dissemination in the proposed network. The proposed system is a three-layered system comprising message dissemination layer, storage layer and BC layer. In the first layer, all the vehicles are registered through a Certificate Authority (CA), which ensures only the legitimate vehicles become part of the proposed network and interact with each other. Later, in the second layer, the data sent by the vehicles is stored at the artificial intelligence based Interplanetary File System (IPFS), which is incorporated with the Road Side Units (RSUs). This ensures reduction in storage cost and data availability. Besides, vehicle owners' privacy is ensured by concealing the real identities of the vehicles. Moreover, the hashes of the data stored in the IPFS are stored in BC in the third layer. Also, lightweight trustworthiness verification of the vehicles, reputation based incentivization and concealing predictable trends in vehicles' reputation scores are performed in the same layer. Overall, the novelty of the proposed work lies in the fact that the proposed system efficiently tackles different problems encountered in the existing systems simultaneously. Through extensive simulations, it is inferred that the computational time is reduced by 15-18% and the storage overhead is reduced by 80-85%, respectively when storing hash of data on the BC network as compared to storing actual data on the network.

INDEX TERMS Blockchain, cuckoo filter, artificial intelligence based IPFS, message dissemination, privacy, vehicular energy network.

I. INTRODUCTION

Over the past few decades, migration of people from rural to urban areas is observed on a large scale in order to have access of the basic necessities of life. On one hand, the migration has provided the masses with multiple benefits. While on the other hand, it has caused some serious issues as well like scarcity of health facilities, decrease in employment opportunities, reduction in natural resources, etc. As a result of which, a huge shift from traditional means to latest and updated means is observed [1]. Moreover, the major reliance of the masses on electricity has led the world towards the development of smart grids and get rid of traditional grids, though gradually. The huge demand of electricity has also

The associate editor coordinating the review of this manuscript and approving it for publication was Adnan M. Abu-Mahfouz.

caused various issues like the imbalance between supply and demand, massive load shedding and blackouts, drastic increase in electricity prices, etc., [2]. To tackle the mentioned issues, the green and sustainable smart city proved to be a potential option. The smart city comprises smart homes, smart grids, smart hospitals, smart transportation, etc.

Vehicles in Vehicular Energy Networks (VENs), a major part of smart transportation, consist of On-Board Units (OBUs), which assist the vehicles in communicating with the nearby vehicles and other infrastructure via a Dedicated Short-Range Communication (DSRC) protocol. Moreover, in VENs, energy is transferred from one place to another through electric vehicles (EVs). Although, there are other communication protocols as well, which come under the umbrella of C-V2X. Despite, DSRC is used because of its less transmission time than C-V2X, a more mature and a fully designed communication protocol as compared to C-V2X, etc., [3]. Moving ahead, in VENs, vehicles share important information about road and traffic conditions to inform other network participants about the potential hazards like roadside accidents, drastic weather conditions, etc., through messages, termed as announcement messages [1]. Announcement messages are the messages delivered by the vehicles that contain important information like information about road accidents, road blockage, natural calamities, etc. These messages are important because they guide the incoming vehicles to make proper decisions in time and change their route accordingly, which will save both their time and energy.

VENs provide numerous advantages to vehicle users [4], [5]. However, they are also subjected to many threats like disseminating fraudulent information, Single Point of Failure (SPoF), absence of privacy preservation, etc. Various solutions are proposed on the basis of Blockchain (BC) to address these concerns in VENs [6], [7]. The major issues faced in the centralized VENs like lack of trust and security are tackled using BC [1]. Both academia and industry have embraced BC as a Distributed Ledger Technology (DLT) to a remarkable extent over the past few years owing its various fascinating features like transparency, tamperproof and data immutability. In BC, the blocks are linked together cryptographically to store the transactional data. Satoshi Nakamoto was the first one who came up with the idea of BC in 2008 [8]. The authors in [9] proposed a BC based model for supply chain management comprising Internet of Things (IoT), which ensures trust between the entities. The proposed model ensures simple data sharing, and reduction in requirements of computational power, storage and latency. However, many potential drawbacks are also found in BC based VENs that limit their efficiency and question their feasibility despite of their numerous benefits [10]. Moreover, an OBU is a resource-constrained device that cannot perform a computationally intensive consensus process like Proof-of-Work (PoW). Additionally, due to the limited storage, the vehicles cannot store a complete copy of the ever-growing distributed ledger.

Besides, the internal attackers can purposefully share false information to mislead the network participants. Hence, it is necessary to efficiently identify and remove the internal attackers from the network. To overcome this issue, some of the researchers propose reputation mechanisms to identify the malicious users based on the users' ratings [11]. In the underlying work, the major issues related to data dissemination like breach of security, authentication of vehicles, expensive and non-tamper proof data storage, lack of trust between network entities, etc., are tackled.

A. CONTRIBUTIONS

The major contributions of the proposed work are as follows. The novelty of the work lies solely in the proposed system model, which is both unique and efficient.

- A vehicular announcement scheme based on BC technology is proposed where lightweight announcement sharing is ensured.
- Data is distributively stored in Artificial Intelligence (AI) powered Interplanetary File System (IPFS), which ensures storage cost reduction and data availability.
- The vehicles' reputation information and the hashes provided by the IPFS upon data storage are uploaded on Ethereum BC.
- The pseudonyms are generated using Elliptic Curve Cryptography (ECC), which ensures anonymity.
- A reputation based incentive scheme is used for encouraging honest behavior of users and provisioning of true announcement ratings.
- A Cuckoo Filter (CF) is employed for validating vehicles' trustworthiness while hiding vehicles' actual reputation scores.

B. MOTIVATION AND PROBLEM STATEMENT

The traditional and centralized systems are getting obsolete with every new day because of a large number of issues related to them like lack of trust, single point of failure, etc. People are shifting towards the use of latest and decentralized systems. The huge shift of people from traditional means to latest and state-of-the-art means not only provides numerous benefits but also poses serious threats. Moreover, the shortcomings of the traditional energy trading schemes like lack of trust, loss of privacy and security, unauthorized and harmful requests, etc., need to be addressed. In lieu of this, the authors of [5] provide BC based solutions to tackle issues of latency, network overhead, security, and privacy. These systems ensure efficient energy trading in VENs. However, the proposed systems also come with issues like generation of a large number of requests by EVs, which further increases the networks' computational overhead. Apart from that, the sudden increase in the number of vehicles leads to traffic jams and roadside accidents [6]. Additionally, the simultaneous creation and transmission of messages by vehicles causes the gradual loss of crucial information, which also becomes the reason of road congestion and mishaps.

Keeping the issues in view and being motivated from [1], [12], [26], in the proposed work, a BC based model is proposed, which ensures efficient message dissemination along with efficient data storage, users' privacy preservation and reputation based incentivization.

II. RELATED WORK

The authors in [14] make use of microtransactions for minimizing the communication and storage overhead in VENs. The authors also ensure the integrity of data collected from different vehicles along with the integrity of traffic records and traceability. The authors in [15] propose a BC based framework for smart parking of vehicles in a sustainable city environment. The vehicles are first authenticated and verified, and then are allowed to become a part of the vehicular network. Moving ahead, a frequently occurring issue in BC based VENs is privacy leakage, which occurs due to the transparency feature of the BC. Another issue that commonly occurs in VENs is data repudiation. In the existing schemes, researchers use pseudonyms to hide the Real Identities *RIDs* of the users [16]. However, in these schemes, a static pseudonym is provided to the vehicles. As a result, the adversaries can perform background knowledge attack using static pseudonyms to find the *RIDs* of the users. Some authors propose pseudonym update mechanisms to overcome this issue [17]. On the other hand, internal attackers can distribute misleading information in the networks without being detected because the networks lack tracking methods. One of the major issues that occur in centralized public key infrastructure is the privacy leakage issue.

The authors in [18] propose that the users should go for pseudonyms' generation using a distributed pseudonym management system to safeguard against privacy leakage issue. However, the system falls short of tracing the malicious vehicles present in the network. In [19], the authors exploit Certificate Authority (CA) based distributed authentication. However, the users' authentication information is stored in a centralized fashion, which makes it vulnerable to SPoF. The authors use BC and edge computing collectively to ensure that vehicles' registration and trust information are stored efficiently [10]. However, the proposed method lacks in protecting the users against the privacy leakage issue. In [20], [21], the authors address the issue of inefficient key management in VENs. The authors in [20] develop a lightweight key agreement protocol based on bivariate polynomial. Moreover, an asymmetric group key agreement protocol based on BC technology is proposed in [21]. However, due to the lack of an efficient storage mechanism, both of these schemes suffer from scalability issue. In order to handle the Certificate Revocation List (CRL) efficiently, the authors in [22], [23] recommend the usage of certificate revocation methods in VENs. Using the CRL, it is checked if a specific user's certificates have been revoked or not. The authors in [24] proposed a BC based network that increases network security by revoking malicious vehicles from the network. In the proposed model, revocation is done on the basis of clustering. Moreover, in [25], multiple semi-trusted authorities are being utilized along with BC technology in the proposed network. The vehicles in the network are authenticated via certificateless signature through a key distribution method. Moving ahead, the authors in [26] put forward federated learning based BC assisted message dissemination technique. The proof of federated learning mechanism is used in the paper. Moreover, theoretical and practical analyses of the proposed technique are presented. In the proposed work, the focus is on the broadcast of the important messages in the vehicular network. Besides, Table 1 presents the comparison of the proposed work with the existing literature. The comparison is made on the basis of five parameters, denoted as P1-P5 where P1, P2, P3, P4 and P5 represent authentication, encryption, trustworthiness, data storage and message dissemination, respectively.

TABLE 1. Comparison with existing literature.

Paper	P1	P2	P3	P4	P5
[14]	Yes	Yes	No	No	No
[15]	Yes	Yes	No	Yes	No
[16]	Yes	Yes	No	No	No
[17]	Yes	No	No	No	No
[18]	Yes	Yes	No	No	Yes
[19]	Yes	Yes	No	Yes	Yes
[20]	Yes	Yes	No	No	Yes
[21]	Yes	Yes	No	No	Yes
[22]	Yes	Yes	No	Yes	Yes
[23]	Yes	Yes	No	No	Yes
[24]	No	No	Yes	No	No
[25]	Yes	No	No	Yes	Yes
Proposed	Yes	Yes	Yes	Yes	Yes

III. SYSTEM MODEL

In order to facilitate safe and efficient information sharing in VENs while protecting users' privacy, a hybrid BC based announcement dissemination architecture is presented in the underlying work. The proposed system model shown in Figure 1 comprises three layers: announcement message dissemination layer, storage layer and BC layer. In the first layer, the vehicles are registered by CA. Afterwards, the vehicles interact with each other and share messages. Moving ahead, in the second layer, Road Side Units (RSUs) are connected to one another and oversee the entire network's activities. The data generated by the vehicles is provided to the RSUs. Moreover, IPFS is incorporated with RSUs to ensure efficient data storage. The data delivered to the RSUs is sent to IPFS for storage purpose. This saves storage cost and assures data availability. IPFS splits the data into chunks and generates a hash for the data, which is stored on the Ethereum BC, implemented in the third layer. In the third layer, CF is also employed to store vehicles' reputation scores. Moving ahead, in Figure 1, the Public TX Data refers to the reputation scores of the vehicles, which are publicly available. This data is stored in the CF. While the Private TX Data refers to the hash of the data provided by the IPFS that is stored in Ethereum BC. The figure also includes the lists

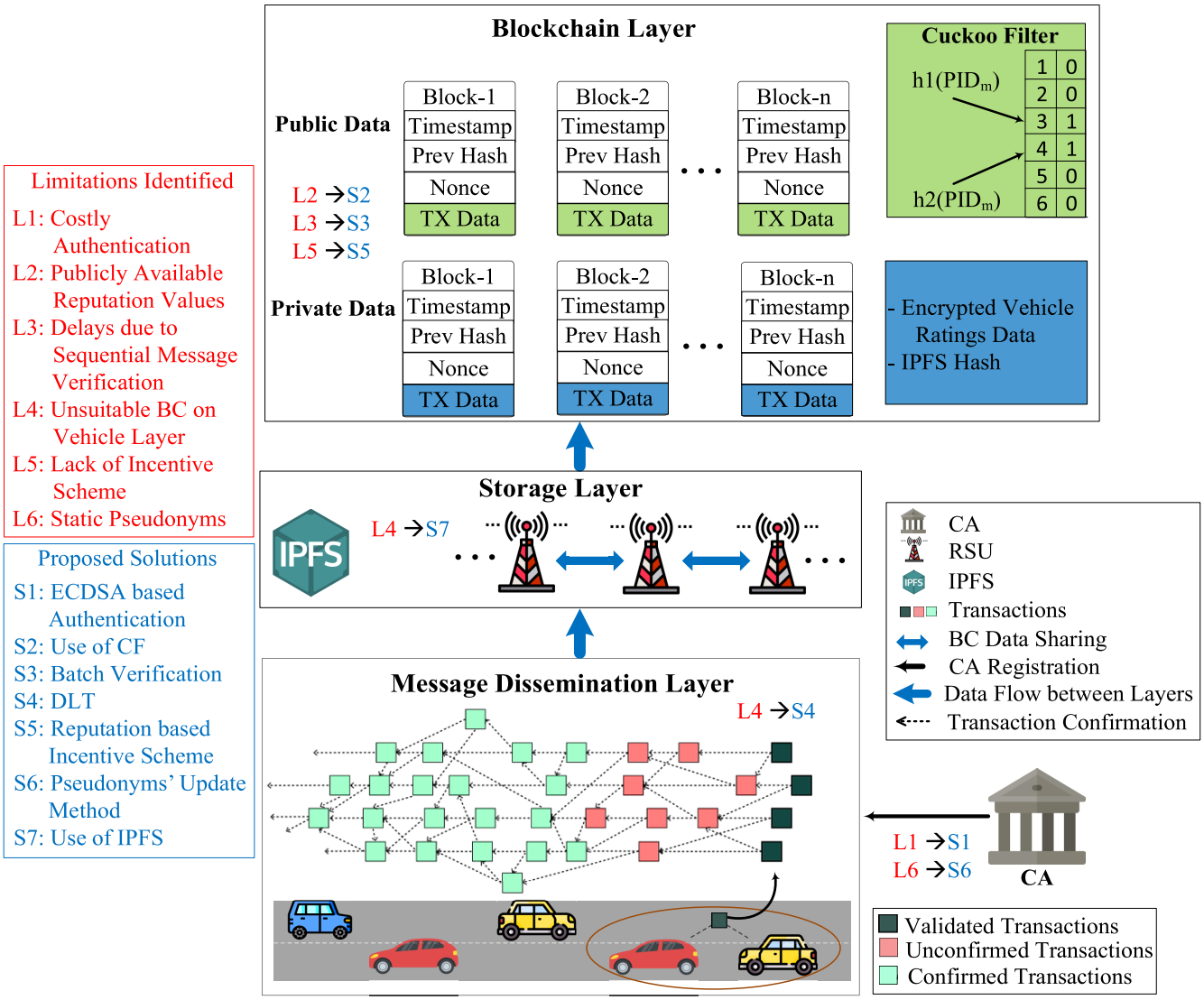


FIGURE 1. 3-Layered proposed system model comprising announcement message dissemination layer, Storage layer and BC layer.

of the limitations that have been identified from the existing literature and their recommended solutions. The proposed solutions are designated from $S1$ to $S7$ while the limitations are labeled from $L1$ to $L6$. Figure 2 shows the flowchart of the proposed system model.

A brief description of the entities involved in the proposed model is provided below, in the order of their occurrence in the model. It is to be noted that the proposed work is an extended form of the existing work [13].

A. VEHICLES

DSRC protocol provides Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication in VENs. Vehicle keys are stored in OBUs, which are considered to be tamper-proof devices. V2V communication comprises exchanging of traffic conditions, road incidents, advertisements and other information between vehicles. The vehicles provide ratings on the basis of received announcements to minimize the spread of misleading information. The vehicles are rewarded for providing honest ratings and are penalized for providing dishonest ratings.

B. CERTIFICATE AUTHORITY

When it comes to VENs, CA is the central organization that ensures only the approved users become part of the network. It is assumed that CA is fully trustworthy and shows high robustness against all assaults and threats. When registering a vehicle in the proposed approach, the vehicle's *RID* information is sent to CA. The vehicles are provided with Pseudonym Certificates (PCs) by CA. Moreover, *RIDs* and the vehicle's Pseudo Identities *PIDs* are encrypted, allowing for conditional anonymity. Besides, malevolent vehicles' digital certificates are revoked and their *RIDs* are exposed in case of a malicious activity, preventing them from rejoining the network.

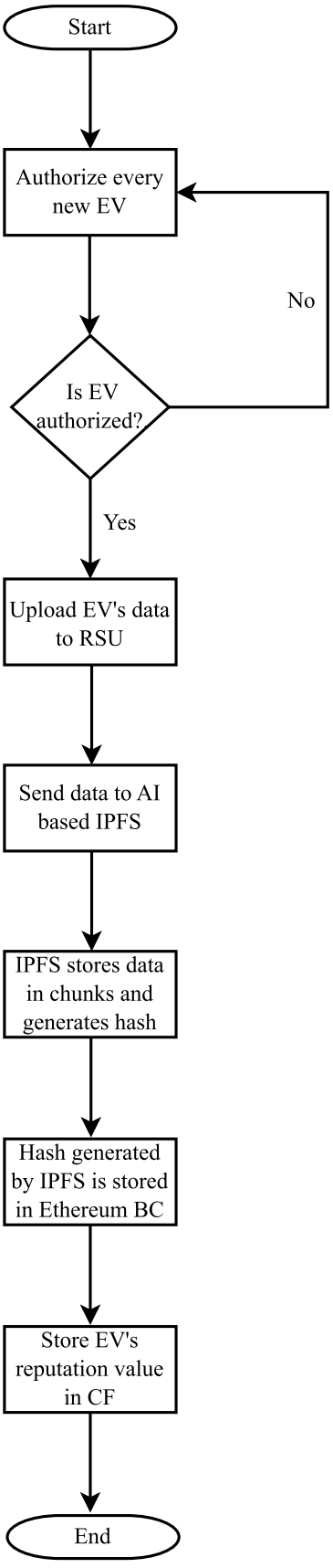


FIGURE 2. Flowchart of proposed system model.

C. ROAD SIDE UNITS

RSUs control the entire network in VENs and deliver different services to the vehicles. In addition to being networked, RSUs possess significant computing capabilities. RSUs are part of the data storage layer where IPFS is integrated on them. Vehicles' announcement records are stored in RSUs, which ensures data accessibility. Moreover, RSUs are the approved nodes in the BC layer, which are responsible for accomplishing the following tasks: (i) calculate a vehicle's reputation score using the feedback provided by other vehicles, (ii) add *PIDs* of malicious users to a CF and (iii) store the vehicular announcement data on IPFS, discussed in the next subsection.

D. INTERPLANETARY FILE SYSTEM

For distributive data storage, IPFS is used. Each file saved on IPFS has a unique hash value, which is subsequently used to retrieve the file [27]. The system is made scalable and efficient by uploading the historical records on the IPFS. The storage of hash values provided by IPFS in BC minimizes the cost incurred while storing data on BC, discussed in the next subsection.

E. BLOCKCHAIN

Ethereum BC [28] is implemented on the RSUs in the proposed scheme. Transparency, integrity and immutability of data are ensured using BC. To prevent data loss due to data pruning, the message records are uploaded to IPFS while their hash values are saved on BC. Smart contracts are used to save and access the data in and from BC. In the proposed model, a block in BC contains a header and a body. The header is used for identifying a distinct block in the BC. It contains the current block hash and the metadata. The metadata includes the version of the current block, hash of the previous block, Merkle root hash, nonce and timestamp. Hash is defined as the output generated when an input data of arbitrary length is converted to a unique, fixed size output comprising string of characters [29]. Merkle root hash is defined as the combined hash value of all the transactions present in a particular block [30]. While nonce is defined as a 4-byte field that starts from 0 and increases for every hash calculation [30]. Besides, the data related to BC transactions is stored in the block body. In the proposed network, IPFS hashes of message records, encrypted vehicles' rating data and information related to CF (discussed in the next subsection) are saved in the block body.

F. CUCKOO FILTER

For checking the affiliation of an element with a specific set, a new data structure is used. The authors in [31] propose to replace the Bloom Filter (BF) with CF. BF is used to check whether an element is a part of a set or not. It is a space-efficient probabilistic data structure. It offers many advantages like space efficiency, fast query time as compared to conventional hash table, etc. However, it has some

disadvantages as well. The major disadvantage is that the elements once stored in the BF cannot be deleted. This is where CF comes into play. CF provides dynamic adding and removing of elements, higher lookup performance than BF, more space efficiency than BF, etc., [31]. Moreover, cuckoo hashing is used in the CF. The reduction in the false positive rate and storage consumption is ensured using CFs.

IV. DESIGN GOALS

In this section, the goals of the proposed work are discussed.

A. PRIVACY

In BC based VENs, privacy is considered as one of the fundamental requirements. The use of static pseudonyms leads to vehicles' privacy leakage issue. The identification of a user by an adversary is also possible using static pseudonyms. Moreover, the publicly available vehicles' reputation scores are used as quasi-identifiers to perform background knowledge attack. Therefore, to prevent the adversaries from identifying the vehicles, dynamic pseudonyms are used.

B. NON-REPUDIATION

It is an important attribute of VENs, which prevents the vehicles from denying that they have sent an announcement message in the network. Previously, the authors used BC to enable non-repudiation on vehicle layer. However, the overwhelming computational cost and storage overhead incurred while doing so is not suitable for the resource-constrained vehicles.

C. DATA AVAILABILITY AND STORAGE

Data availability is necessary for the distributed systems. However, in order to reduce the storage cost, the historical transactions must be deleted, which causes data loss. To overcome the data loss issue, the historical transaction records are stored on a distributed storage system, i.e., IPFS. Only the hash values of the transaction records are saved on BC. It is done to minimize the data storage cost of BC.

D. TRACEABILITY

The CA possesses the information of mapping between *RIDs* and *PIDs* of the vehicles. The digital certificates of the malicious vehicles are revoked by CA using the mapping between *RIDs* and *PIDs* upon their involvement in the fraudulent activities.

E. VEHICLES' ENTHUSIASM

Our proposed scheme encourages the users to provide feedback about the announcements they receive using a reputation based incentive mechanism. The Feedback Messages *FBs* sent by the vehicles are used for calculating the reputation values of the announcement sharing vehicles. The reputation values of the vehicles are also linked with the system performance. More the reputation of a vehicle, better the performance would be. Moreover, the reputation values of vehicles also help in deciding what data to be stored on the IPFS. The data coming from the high-reputed vehicle is given more importance as compared to the data coming from low-reputed vehicle. This in turn further increases the system performance.

V. THREAT MODEL

In this section, the possible security threats to the proposed model are discussed.

A. PRIVACY LEAKAGE DUE TO STATIC PSEUDONYMS

In [32], the authors use static pseudonyms to hide the *RIDs* of the vehicles. However, it enables the adversaries to perform background knowledge attack, which leads to privacy leakage. Hence, it is necessary to periodically change and update the pseudonym of each vehicle.

B. PRIVACY LEAKAGE DUE TO QUASI-IDENTIFIERS

To ensure trust in BC based VEN schemes, many reputation mechanisms are developed [33]. In these schemes, the vehicles' rating values are stored publicly on BC so that vehicles can verify the trustworthiness of their peers. However, these values are used by adversaries to perform cyber attacks and cause privacy leakage. The leakage occurs due to the foreseeable patterns' identification of the rating values. In most of the reputation schemes, the rating values either increase or decrease by a certain number depending on the vehicles' reputation. This fluctuating pattern along with the location information help the adversary to launch a background knowledge attack against the vehicles.

C. INTERNAL ATTACKERS' SCENARIO

The authenticated users may attempt to share false information about road incidents for malicious purposes. Hence, it is necessary to enable conditional privacy so that the internal attackers are easily identified and the responsible vehicles are revoked from the network.

VI. PROPOSED METHODOLOGY

The proposed methodology of the underlying work is discussed in this section.

A. SYSTEM INITIALIZATION

In the proposed system, Advanced Encryption Standard (AES) is used for symmetric encryption of the vehicles' reputation scores through AES_{key}. In AES, two keys are used: public and private. The former is used for encryption while the latter is used for decryption [34]. CA sends the AES_{key} to all RSUs through a secure channel for sharing the encrypted data. CA also generates a pair of public and private keys, given as SK_{CA} and PK_{CA}. These keys are used by the CA itself to encrypt the mapping between *RID* and *PID*. Moreover, the *RIDs* of the EVs are concealed using ECC asymmetric encryption technique having PK_{ECC} and SK_{ECC} keys after they are registered in the network. ECC is an elliptic curve based public key encryption technique. It is used to create small and efficient cryptographic keys [35].

The conditional anonymity is also ensured using ECC. Furthermore, ECDSA is employed for performing authentication using digital signatures, given as Sig_{PR}. ECDSA is a complex public key encryption algorithm that uses ECC to generate keys that are smaller in size as compared to keys generated by other digital signing algorithms. It creates certificates that are used for user authentication [36]. Also, a CF is used for storing the *PIDs* of the malicious EVs, denoted as CF_{mal}. In the proposed work, hashing is done using Secure Hashing Algorithm 256 (SHA256), given as $H : \{0, 1\}^* \rightarrow Z^*$. SHA256 is a hashing algorithm that is used in digital certificate and data integrity. It takes an input of 2^{64} bits and generates an output of 256-bits [37].

B. REGISTRATION

For registration, the vehicle V_i generates its public and private keys (PK_{V_i}, SK_{V_i}). Afterwards, the V_i sends its RID_{V_i} information and PK_{V_i} to CA in order to receive the PC. CA checks RID_{V_i} of the vehicle in existing certificates' list. If it exists, CA rejects the request. Otherwise, CA generates an initial PC, denoted as $PC^0_{V_i}$ for V_i (the 0 in $PC^0_{V_i}$ shows the index of the PC). The CA also creates an encrypted mapping $Enc(RID_{V_i}||PC^n_{V_i})$ to identify the vehicle in case of malicious activities. Hence, in case of disputes, the *RIDs* of the vehicles are revealed.

C. PSEUDONYM UPDATE

The use of static pseudonyms can cause privacy leakage. Hence, the pseudonyms should be periodically updated to prevent tracing attacks. The vehicles get their PCs updated in case of privacy leakage, certificate expiration, etc. The periodic generation of static pseudonyms is performed by CA. This generation is performed in the following manner. The V_i sends the pseudonym update request to CA, given as $PseudonymUpdateRequest = (Sig_{PR_{V_i}}, PUReq, PC^n_{V_i})$, where $PC^n_{V_i}$ is the current PC. Upon receiving the request, CA verifies it. If the request is found to be valid, CA generates a new PC for the vehicle, given as $PC^{n+1}_{V_i}$. After the generation of the PC, it is matched with the existing PCs. If no existing Pc is found, the new PC is added to the list of PCs of the vehicles in an encrypted form as $Enc(RID_{V_i}||PC^n_{V_i}||PC^{n+1}_{V_i})$. It is to be noted that periodic generation of the PCs incurs high computation cost. However, our main focus is on the safety of the vehicle users so increase in computational cost is not considered important. Furthermore, as in the proposed system, only legitimate and registered vehicles take part. Therefore, there are less chances of users' privacy leakage. As a result, less chances of increase in computational cost.

D. ANNOUNCEMENT SHARING

In the proposed scheme, a lightweight BC based scheme is used for announcement message sharing. When an announcement initiator vehicle V_i initiates an announcement $Tx_{V_i1} = (Event, Loc, ts, Sig_{SK_{V_i}})$, it needs to approve two randomly selected transactions. Here, *Loc* is the location of the event, *ts* is the timestamp and $Sig_{SK_{V_i}}$ is the digital signature. Each transaction is represented by a unique ID, denoted as *TxID*. The steps taken during announcement sharing in the proposed system are: (i) when V_{i1} observes an accident and wants to create an announcement, it generates a transaction $Tx_1 = (Event, Loc, ts, PID_{V_{i1}}, Sig_{SK_{V_i}})$, (ii) V_{i1} randomly selects two transactions Tx_2 and Tx_3 initiated by V_{i2} and V_{i3}, respectively, (iii) V_{i1} checks the trustworthiness of V_{i2} and V_{i3} by requesting for the latest CF having malicious vehicles' data CF_{mal} from the RSU via smart contract, (iv) V_{i1} checks the *PIDs* of V_{i2} and V_{i3} in CF_{mal}. If the *PIDs* of these vehicles are found in CF_{mal}, their transactions are rejected. Otherwise, V_{i2} and V_{i3} are approved and their records are added and (v) after approving Tx_2 and Tx_3, Tx_1 becomes valid. It is approved by other vehicles in the similar manner. However, as the vehicles often share announcements in the network, a high transaction confirmation rate is expected to be achieved.

E. INCENTIVE MECHANISM

To prevent internal attackers from sharing false information in the network, an incentive mechanism is proposed. It is proposed to encourage the vehicles to provide honest feedback about the transactions. The steps followed in the proposed incentive mechanism are: (i) when a false announcement transaction Tx_i is identified in the network, multiple V_fs send the *FBs*, denoted as $FB_{V_f}(Tx_1)$ to the RSU. The *FB* is given as follows. $FB_{Vf} = (Tx_1, FALSE, Loc_{V_f}, ts, Sign_{SK_{V_f}})$. Here, Tx_1 is the announcement about which the *FB* is generated. *FALSE* or *TRUE* is the feedback about the Tx_1, Loc_{V_f} is the location of the V_f and $Sign_{SK_{V_f}}$ is the digital signature, (ii) the RSU verifies the signature of n number of FB^n messages sent by multiple $V_f s$ using the batch verification mechanism, (iii) the respective RSU checks the correctness of all FB^n received from the $V_f s$ present in its vicinity and (iv) the vehicles that provide correct *FB* are rewarded with the incentives. The vehicles gain incentive for sharing *FB* about *Tx*. The amount of incentive increases as the number of *FB* increases. However, verifying a large number of *FBs* individually impedes the performance of RSUs.

F. REPUTATION CALCULATION

For reputation calculation, an RSU uses a V2V communication record from time t_1 to t_2, denoted as $(TRecord_{t1-t2})$. It also assembles the *FB* list as FB^{List}_{t1-t2}. The steps involved in reputation calculation are: (i) RSU gets $TRecord_{t1-t2}$ and assembles the list of *FB* as FB^{List}_{t1-t2} (ii) RSU stores the *PIDs* of a malicious vehicle as PID_m in CF_{mal}, (iii) RSU uses the FB^{List}_{t1-t2} to find the negative *FB* against a specific transaction Tx_{V_1}, (iv) *FB* is only considered valid if the location of V_f is near the location of Tx_{V_1} and there are at least 5 other *FBs* for the same Tx_{V_1}, (v) if at least 5 negative *FBs* are received against Tx_{V_1}, the reputation value of V_1 is decreased and the *ReputationList* is updated accordingly, (vi) the process is repeated for all *FBs* and eventually, the $ReputationList_{t1-t2}$

is updated, (vii) the *PIDs* of vehicles whose reputation values are below the threshold are added to CF_{mal}, (viii) the $ReputationList_{t1-t2}$ is encrypted using the shared AES_{key} as $RL_{enc} = Enc(ReputationList_{t1-t2})_{AES}$, (ix) the $TRecord_{t1-t2}$, FB^{List}_{t1-t2} and RL_{enc} are uploaded to IPFS to retrieve the hash $IPFSHash_{t1-t2}$ and (x) finally, the $IPFSHash_{t1-t2}$ and CF_{mal} are made public once they are added to the BC.

G. DATA STORAGE

After calculating the reputation values by utilizing message records and FB^{List}, the data is uploaded to IPFS, which minimizes storage space requirements and makes the system scalable. The IPFS returns a hash value for the data, given as $IPFSHash(data) = IPFSHash(TRecord_{t1-t2}||FB^{List}_{t1-t2}||RL_{enc})$. BC is used to store the hash value and share it with all other RSUs. It is to be noted here that in the proposed model, only that data is stored in IPFS, which is selected from the data coming from different vehicles using Artificial Intelligence (AI). This thing reduces the load both on the BC and the IPFS. If AI is not employed, then all incoming data will be forwarded to the IPFS, which will in turn overburden the IPFS and increase both the data storage and the data retrieval time.

Algorithm 1 Insert an Element in Cuckoo Filter

Begin
Inputs: Two hash functions $h1$ and $h2$, a bit-array with n bits, the ith bucket, denoted as $B[i]$, a list of *PIDs* to be inserted to the CF, denoted as L
Output: CF_{mal}
while L is not empty
Extract features by FCN-8 as I'
Let x_{PID} be the first *PID* in the L
if B[h1(x)] is empty **then**
Remove x_{PID} from the L
  elseif B[h2(x) is empty] **then**
  Place x_{PID} in $B[h2(x)]$
    else
    Let y_{PID} be the element in $B[h2(x)]$
    Prepend y_{PID} to L
    Place x_{PID} in $B[h2(x)]$
endif
endwhile
Return CF
End

VII. DISCUSSION OF SIMULATION RESULTS

To test the efficiency of the proposed model, we performed simulations on an Intel(R) Core(TM) m3-7Y30 machine having 1.00 GHz processor and 8.00 GB RAM. For implementing the proposed system, Python 3 is used while Solidity language is used to develop the smart contracts. In the simulation section, the implementation of different processes involved in the proposed system model, i.e., authentication, encryption and decryption, data storage and retrieval, Ethereum BC, and execution time and false positive rate of CF is provided.

Algorithm 2 Reputation Calculation

Begin
Inputs: $TRecord_{t1-t2}$, FB^{List}_{t1-t2},
Outputs: $Enc(ReputationList)_{AES}$, CF_{mal}, $IPFSHash_{t1-t2}$
while FB^{List}_{t1-t2} is not empty
Let $FB^n(Tx_{V_1})$ be the n number of FB in the FB^{List}_{t1-t2} generated against Tx_{V_1} and saved in $TRecord$, where Tx_{V_1} is the transaction performed by V_1
if Count of $FB^n(Tx_{V_1}) >= 10$ **then**
  for Each$FB(Tx_{V_1})$ **do**
    if $FB(Tx_{V_1}).location! = Tx_{V_1}.location$ **then**
    Reject the $FB(Tx_{V_1})$
    elseif $FB(Tx_{V_1}).location == Tx_{V_1}.location$ **then**
    $Mcount = +1$
    endif
  endfor
endif
if $Mcount >= 5$ **then**
Reduce the reputation of V_1 by 0.2
Update the *ReputationList*
Provide incentives to V_f
endif
for Each*PID* in *ReputationList* **do**
  if $Reputation < 5$ **then**
  Add the *PID* in CF_{mal}
  endif
endfor
endwhile
Encrypt *ReputationList* with AES_{key}
$RL_{enc} = Enc(ReputationList)_{AES}$
Upload ($TRecord_{t1-t2}$, FB_{t1-t2}, RL_{enc}) to IPFS and get $IPFSHash_{t1-t2}$
Add (CF_{mal}, $IPFSHash_{t1-t2}$) to BC
End

A. RESULTS FOR CUCKOO FILTER

A comparison of false positive rate between CF and BF is presented in Figure 3. It is observed that for less number of elements, the BF yields a lower false positive rate. However, when the number of elements is increased, the false positive rate of BF increases. From the figure, it is obvious that the false positive rate of CF remains close to 0.02 or 2%. While the false positive rate of BF is close to 0.10 or 10%. Therefore, we deduce that CF performs more efficiently when dealing with a large number of elements. Since the proposed scheme deals with a large number of elements, so CF is used as it is found more suitable than BF. Moreover, Figure 4 shows the time comparison between CF and BF when storing different number of events. From the figure, it is obvious that the time remains almost the same for 30000 events. As the number of events increases, a vivid difference in time is observed.

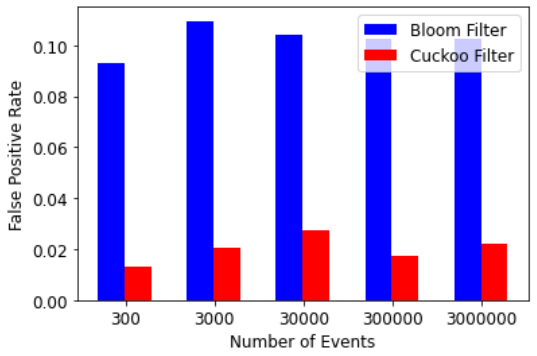


FIGURE 3. Comparison of CF and BF in terms of false positive rate.

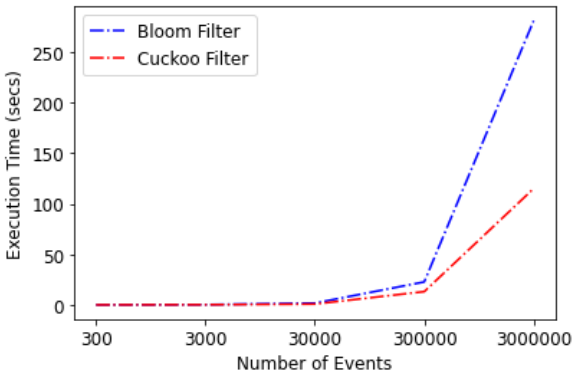


FIGURE 4. Comparison of CF and BF in terms of execution time.

The execution time of BF increases exponentially beyond 30000 events while the execution time of CF increases gradually.

B. AUTHENTICATION SCHEME RESULTS

In the proposed system, ECDSA is used for authentication to reduce the overall computational overhead of the cryptographic operations including certificate generation, encryption and decryption. The time incurred by ECDSA for key generation, signature and verification is depicted in Figure 5. The simulations are performed for 10 times and the average execution time is calculated. It is evident from the figure that ECDSA scheme takes significantly large time for key verification, i.e., almost 0.008 secs. While time taken for key generation and key signing is less, i.e., almost 0.004 secs.

C. ENCRYPTION AND DECRYPTION RESULTS

In this subsection, the time consumed for encryption and decryption of data using AES is discussed. From Figure 6, it is obvious that time taken for encryption is larger than time taken for decryption. For encryption, almost 10 ms time is taken while for decryption, almost 1 ms time is taken.

D. ETHEREUM BC RESULTS

The gas consumption for smart contract's functions is shown in Figure 7. Gas consumption means the digital currency charged when performing transactions. It is also charged whenever deploying the BC smart contract. It is calculated

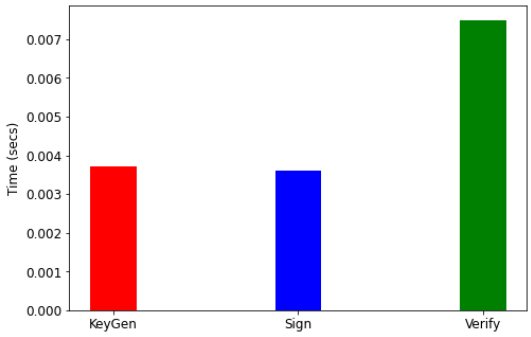


FIGURE 5. Time consumed by three different functions when using ECDSA.

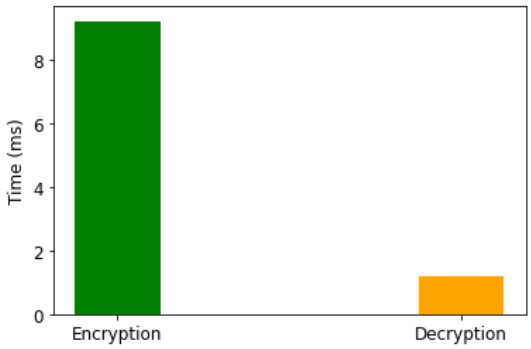


FIGURE 6. Comparison of encryption time and decryption time when using AES.

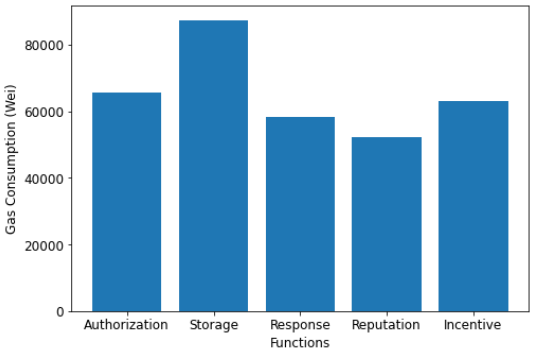


FIGURE 7. Gas consumption for different functions used in smart contract.

whenever a transaction is performed or a smart contact is deployed. In our case, the gas consumption is given in Wei when deploying the smart contract on Remix-IDE. Moreover, another unit of gas consumption is Ethers [38], where 1 Gwei = 0.000000001 Ethers. The vehicles' rating data is encrypted in the proposed system using an AES encryption algorithm before uploading it to the ledger. The "Storage" function uploads the encrypted vehicles' rating data in the ledger while "Response" function retrieves the encrypted data from the BC. The rating data is used for classifying the vehicles as malicious or benign. Furthermore, "Authentication" function authenticates the vehicles, "Reputation" function provides reputation to the vehicles and "Incentive" function provides incentives to the benign users.

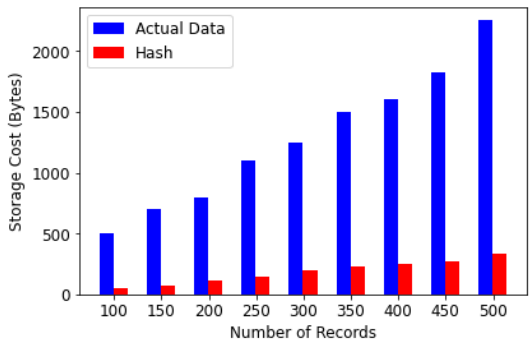


FIGURE 8. Storage cost comparison of actual data and hash when using IPFS.

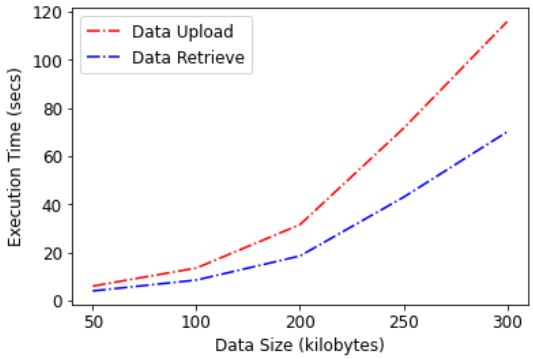


FIGURE 9. Execution time comparison of data upload and data Retrieve when using IPFS.

E. IPFS RESULTS

In the proposed system, the rating data received from vehicles is sent to RSUs. After verification, this data is encrypted and stored on IPFS to save storage space. The IPFS generates the hash value for that data, which is then stored on the BC for data integrity. Figure 8 shows the size comparison of the rating data and its corresponding hash values, given in terms of storage cost, measured in bytes. It should be noted that the size of hash is independent of the increase in data size and it remains almost the same. The increase in size shown in the figure is due to the accumulation of the hash values. On the other hand, the size of actual data increases with the increase in the number of records. Figure 9 shows the comparison between data upload and data retrieve time for data of different size. It is obvious that for small data, increase is not much and vice versa. It is noted that as the data size increases, the increase in data upload time is more than increase in data retrieve time. It is because when data is uploaded, it is to be divided into chunks before storage, which becomes more time consuming as the data size increases.

VIII. SECURITY FEATURES

In this section, we discuss how our proposed scheme tackles the existing security issues. Since our proposed scheme involves BC, it inherits various security features including data integrity, decentralization, prevention of SPoF, non-repudiation, data availability and trust. Some of the security features of the proposed scheme are discussed below.

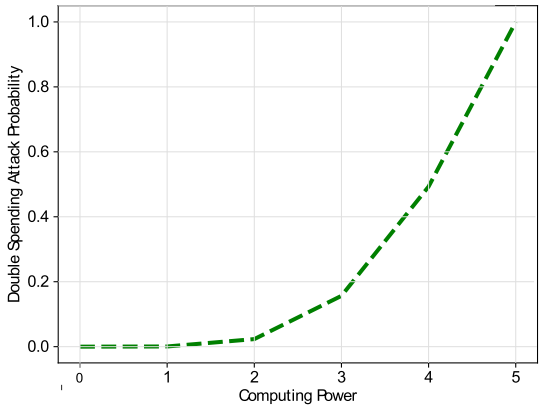


FIGURE 10. Probability of double spending attack against attacker's computing power.

A. DATA INTEGRITY AND AVAILABILITY

In BC based systems, the data is stored in DLT. The copies of the ledger are shared with all the nodes of the network. Any change in the ledger is reflected across all the nodes. Hence, the attackers cannot modify the data without notifying others. Since the data is stored in a peer-to-peer manner, data availability is ensured.

B. CONFIDENTIALITY

BC does not inherent confidentiality because the data is verified by all network participants for achieving consensus. However, in the proposed scheme, data is encrypted before storing it on the BC to ensure confidentiality.

C. NON-REPUDIATION

In BC, once the data is stored, it cannot be changed. It can only be updated in the new block, which is visible to all the network participants. Hence, once a transaction is performed, it cannot be repudiated by the users.

D. SINGLE POINT OF FAILURE

The BC prevents the SPoF issue as it is a decentralized technology and involves consensus between all nodes. BC is maintained by a group of network participants. Every new block that is added to the BC is accepted by most of the network participants unlike the traditional centralized systems, where a single entity makes all decisions.

IX. SECURITY ANALYSIS

The proposed model is analyzed from security perspective and the analysis results are discussed in this section. The analysis is performed on the bases of double spending attack, quasi-identifiers and smart contract vulnerabilities.

A. DOUBLE SPENDING ATTACK

In double spending attack, the attacker spends the same cryptocurrency token twice or sends it to multiple users, simultaneously. This attack occurs when the attacker possesses more computational power than the honest miners. The attackers can mine fraudulent blocks and add them to the BC before the honest miners. In BC, the longest chain is considered authentic. When the attacker with high computa-

```
root@ff15f0134916:/oyente/oyente# python oyente.py -s contractJ1.sol
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 contractJ1.sol:contract1:
INFO:symExec:   ============ Results ===========
INFO:symExec:     EVM Code Coverage:                    99.6%
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
INFO:symExec:   ====== Analysis Completed ======
root@ff15f0134916:/oyente/oyente#
```

FIGURE 11. Oyente analysis of smart contract.

tional power mines more blocks than the honest miners, the blocks mined by the honest miners are discarded. This causes resource wastage for the honest miners.

Figure 10 shows the probability of the double spending attack with respect to the computational power of the attackers. To simulate this attack, q, K and τ are used. q is the probability that attacker will mine the block before the honest miner, K is the number of confirmations required to validate the blocks and τ is the average time required by the honest and attacker nodes for mining [40].

The mathematical formulation of double spending attack is taken from [41]. A double spending attack's probability is expressed as the possibility of the attacker proceeding from block 1 to block n and ending up at the difference of blocks $K - n$. It is given in Equation 1.

$$DS_N(q, K) = 1 - \sum_{n=0}^{K} P_N(q, K, n)(1 - C_N(q, K - n - 1)), \tag{1}$$

where P_N is the attacker's potential progress function P for the model of S. Nakamoto in terms of Poison distribution. The probability that an attacker node mines the block faster than a honest node is given in Equation 2.

$$\begin{aligned} P(T_q < T_p) &= \int_0^\infty P(T_q = x)P(T_p > x)dx, \\ &= \int_0^\infty \frac{q}{\tau} e^{(\frac{-q}{\tau}x)} e^{(\frac{-p}{\tau}x)} dx, \\ &= q \int_0^\infty \frac{1}{\tau} e^{(\frac{-1}{\tau}x)} dx, \\ &= q. \end{aligned} \tag{2}$$

where T_q and T_p represent the time needed by the attacker nodes and the honest nodes to mine a block, respectively. P is defined in terms of the time advantage t for fake block generation and $p = 1 - q$.

B. ANALYSIS OF SMART CONTRACTS

Vulnerabilities in the smart contracts cause a potential financial loss. Hence, it is necessary to analyze the smart contracts before deploying them on the main Ethereum network. Oyente is an open-source auto-auditing tool for smart contracts, which analyzes smart contracts against different vulnerabilities. It uses a symbolic execution technique to analyze the smart contracts by validating the input values of the functions for identifying possible security flaws. Some of the well-known vulnerabilities identified by Oyente include Integer Overflow/Underflow, Parity Multisig Bug 2, Re-Entrancy Vulnerability, Timestamp Dependency, Transaction-Ordering Dependence and Callstack Depth Attack Vulnerability [43]. Figure 11 illustrates that the designed smart contract is resistant against the mentioned vulnerabilities.

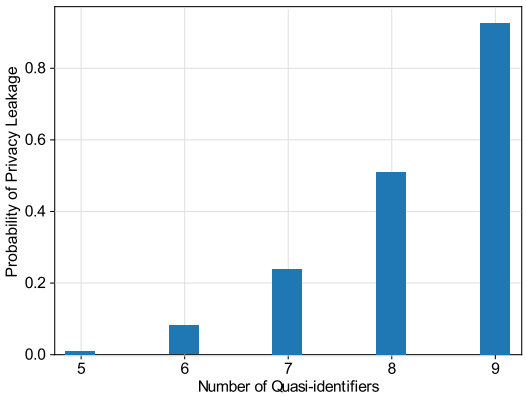


FIGURE 12. Probability of privacy leakage against number of quasi-identifiers.

C. PRIVACY LEAKAGE DUE TO QUASI-IDENTIFIERS

The reputation data is generally kept public, which ensures that data sharing and trading are performed in a secure manner. However, the publicly available reputation information of users can act as a quasi-identifier and the malicious users can use it along with some background knowledge to expose the user IDs. The authors in [42] use the following formula for identifying the relationship between the probability of privacy leakage $P_{leakage}$ and the number of quasi-identifiers x.

$$P_{leakage} = b_3x^3 + b_2x^2 + b_1x + b_0, \tag{3}$$

where b_3, b_2, b_1, b_0 are parameters in the third-order Taylor formula and their values are 0.0049, -0.0454, 0.1248, and -0.0921, respectively. The effect of quasi-identifiers on $P_{leakage}$ is depicted in Figure 12. It is observed that by increasing the number of quasi-identifiers, the value of $P_{leakage}$ substantially increases. For that reason, we hide the exact reputation scores of vehicles in the proposed scheme.

X. CONCLUSION

In the proposed work, a BC based message announcement system is put forward for efficient information dissemination in VENs. The proposed system is a three-layered system comprising message dissemination layer, storage layer and BC layer. The registration of vehicles is performed in the first layer. In the second layer, the data is uploaded and saved in AI based IPFS incorporated with the RSUs. Upon data storage, IPFS generates the hash values for the data, which are forwarded and saved in the Ethereum BC, deployed in the third layer. In addition, CFs are used to store the foreseeable trends in vehicles' reputations values. Furthermore, incentives are provided to users in the proposed model to ensure sharing of honest reviews. Moreover, through extensive simulations, it is inferred that the computational time of the proposed system is reduced by 15-18% and the storage overhead is reduced by 80-85%, respectively when storing hash of data on the BC network as compared to storing actual data on the network. The security analyses results prove that the system is robust both against the smart contract vulnerabilities and the cyber attacks like double spending attack.

ACKNOWLEDGMENT

The authors would like to acknowledge Taif University Researchers Supporting Project number (TURSP-2020/292) Taif University, Taif, Saudi Arabia. The authors would like also to acknowledge Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R193), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

REFERENCES

[1] M. U. Javed, N. Javaid, M. W. Malik, M. Akbar, O. Samuel, A. S. Yahaya, and J. B. Othman, "Blockchain based secure, efficient and coordinated energy trading and data sharing between electric vehicles," *Cluster Comput.*, vol. 25, no. 3, pp. 1839–1867, Jun. 2022, doi: 10.1007/s10586-021-03435-9.

[2] S. Dorahaki, R. Dashti, and H. R. Shaker, "Optimal energy management in the smart microgrid considering the electrical energy storage system and the demand-side energy efficiency program," *J. Energy Storage*, vol. 28, Apr. 2020, Art. no. 101229, doi: 10.1016/j.est.2020.101229.

[3] GTT Wireless. (2022). *DSRC vs C-V2X: Comparing the Connected Vehicles Technologies—GTT Wireless*. Accessed: Jul. 23, 2022. [Online]. Available: https://gttwireless.com/dsrc-vs-c-v2x-comparing-the-connected-vehiclestechnologies/

[4] Y. Wang, H. T. Luan, Z. Su, N. Zhang, and A. Benslimane, "A secure and efficient wireless charging scheme for electric vehicles in vehicular energy networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 1491–1508, Feb. 2022, doi: 10.1109/TVT.2021.3131776.

[5] 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, doi: 10.1109/TII.2019.2908497.

[6] O. Samuel, N. Javaid, A. Almogren, M. U. Javed, U. Qasim, and A. Radwan, "A secure energy trading system for electric vehicles in smart communities using blockchain," *Sustain. Cities Soc.*, vol. 79, Apr. 2022, Art. no. 103678, doi: 10.1016/j.scs.2022.103678.

[7] Q. Luo, Y. Zhou, W. Hou, and L. Peng, "A hierarchical blockchain architecture based V2G market trading system," *Appl. Energy*, vol. 307, Feb. 2022, Art. no. 118167, doi: 10.1016/j.apenergy.2021.118167.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Bus. Rev.*, 2008, Art. no. 21260. Accessed: Jul. 23, 2022. [Online]. Available: http://bitcoin.org/bitcoin.pdf

[9] M. S. Al-Rakhami and M. Al-Mashari, "A blockchain-based trust model for the Internet of Things supply chain management," *Sensors*, vol. 21, no. 5, p. 1759, Mar. 2021, doi: 10.3390/s21051759.

[10] 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, doi: 10.1016/j.dcan.2019.04.003.

[11] A. M. Almuhaideb and S. S. Algothami, "Efficient privacy-preserving and secure authentication for electric-vehicle-to-electric-vehicle-charging system based on ECQV," *J. Sens. Actuator Netw.*, vol. 11, no. 2, p. 28, Jun. 2022, doi: 10.3390/jsan11020028.

[12] M. Baza, A. Sherif, M. M. E. A. Mahmoud, S. Bakiras, W. Alasmary, M. Abdallah, and X. Lin, "Privacy-preserving blockchain-based energy trading schemes for electric vehicles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 9369–9384, Sep. 2021, doi: 10.1109/tvt.2021.3098188.

[13] A. Jamal, S. Amjad, U. Aziz, M. U. Gurmani, S. Awan, and N. Javaid, "A privacy preserving hybrid blockchain based announcement scheme for vehicular energy network," in *Complex, Intelligent and Software Intensive Systems*. Cham, Switzerland: Springer, 2021, pp. 142–151, doi: 10.1007/978-3-030-79725-6_14.

[14] E.-H. Diallo, O. Dib, and K. A. Agha, "A scalable blockchain-based scheme for traffic-related data sharing in VANETs," *Blockchain, Res. Appl.*, vol. 3, no. 3, Sep. 2022, Art. no. 100087, doi: 10.1016/j.bcra.2022.100087.

[15] S. Singh, Y. Pan, and J. H. Park, "Blockchain-enabled secure framework for energy-efficient smart parking in sustainable city environment," *Sustain. Cities Soc.*, vol. 76, Jan. 2022, Art. no. 103364, doi: 10.1016/j.scs.2021.103364.

[16] A. Lei, Y. Cao, S. Bao, D. Li, P. Asuquo, H. Cruickshank, and Z. Sun, "A blockchain based certificate revocation scheme for vehicular communication systems," *Future Gener. Comput. Syst.*, vol. 110, pp. 892–903, Sep. 2020, doi: 10.1016/j.future.2019.03.039.

[17] I. Ullah, M. A. Shah, A. Khan, C. Maple, and A. Waheed, "Virtual pseudonym-changing and dynamic grouping policy for privacy preservation in VANETs," *Sensors*, vol. 21, no. 9, p. 3077, Apr. 2021, doi: 10.3390/s21093077.

[18] L. Benarous, B. Kadri, and A. Bouridane, "Blockchain-based privacy-aware pseudonym management framework for vehicular networks," *Arabian J. Sci. Eng.*, vol. 45, no. 8, pp. 6033–6049, Aug. 2020, doi: 10.1007/s13369-020-04448-z.

[19] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, 2019, doi: 10.1109/access.2019.2936575.

[20] Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu, and W. He, "An efficient decentralized key management mechanism for VANET with blockchain," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5836–5849, Jun. 2020, doi: 10.1109/tvt.2020.2972923.

[21] Q. Zhang, Y. Li, R. Wang, J. Li, Y. Gan, Y. Zhang, and X. Yu, "Blockchain-based asymmetric group key agreement protocol for internet of vehicles," *Comput. Electr. Eng.*, vol. 86, Sep. 2020, Art. no. 106713, doi: 10.1016/j.compeleceng.2020.106713.

[22] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for VANETs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 12, pp. 2792–2801, Dec. 2019, doi: 10.1109/tvlsi.2019.2929420.

[23] K. Prateek, F. Altaf, R. Amin, and S. Maity, "A privacy preserving authentication protocol using quantum computing for V2I authentication in vehicular ad hoc networks," *Secur. Commun. Netw.*, vol. 2022, pp. 1–17, Mar. 2022, doi: 10.1155/2022/4280617.

[24] A. Didouh, H. Labiod, Y. E. Hillali, and A. Rivenq, "Blockchain-based collaborative certificate revocation systems using clustering," *IEEE Access*, vol. 10, pp. 51487–51500, 2022, doi: 10.1109/access.2022.3160171.

[25] A. Tomar and S. Tripathi, "BCAV: Blockchain-based certificateless authentication system for vehicular network," *Peer-to-Peer Netw. Appl.*, vol. 15, no. 3, pp. 1733–1756, May 2022, doi: 10.1007/s12083-022-01319-2.

[26] F. Ayaz, Z. Sheng, D. Tian, and Y. L. Guan, "A blockchain based federated learning for message dissemination in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 1927–1940, Feb. 2022, doi: 10.1109/tvt.2021.3132226.

[27] M. U. Javed, N. Javaid, A. Aldegheishem, N. Alrajeh, M. Tahir, and M. Ramzan, "Scheduling charging of electric vehicles in a secured manner by emphasizing cost minimization using blockchain technology and IPFS," *Sustainability*, vol. 12, no. 12, p. 5151, Jun. 2020, doi: 10.3390/su12125151.

[28] D. Vujicic, D. Jagodic, and S. Randic, "Blockchain technology, Bitcoin, and Ethereum: A brief overview," in *Proc. 17th Int. Symp. INFOTEH-JAHORINA (INFOTEH)*, Mar. 2018, doi: 10.1109/INFOTEH.2018.8345547.
[29] Investopedia. (2022). *Understanding Hash*. Accessed: Jul. 23, 2022. [Online]. Available: https://www.investopedia.com/terms/h/hash.asp
[30] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, p. 352, 2018, doi: 10.1504/ijwgs.2018.095647.
[31] B. Fan, D. G. Andersen, M. Kaminsky, and M. D. Mitzenmacher, "Cuckoo filter: Practically better than Bloom," in *Proc. 10th ACM Int. Conf. Emerg. Netw. Experiments Technol.*, Dec. 2014, pp. 75–88, doi: 10.1145/2674005.2674994.
[32] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs," *IEEE Access*, vol. 7, pp. 56656–56666, 2019, doi: 10.1109/ACCESS.2019.2913682.
[33] A. Khalid, M. S. Iftikhar, A. Almogren, R. Khalid, M. K. Afzal, and N. Javaid, "A blockchain based incentive provisioning scheme for traffic event validation and information storage in VANETs," *Inf. Process. Manage.*, vol. 58, no. 2, Mar. 2021, Art. no. 102464, doi: 10.1016/j.ipm.2020.102464.
[34] P. Singh and S. Kumar, "Study & analysis of cryptography algorithms: RSA, AES, DES, T-DES, blowfish," *Int. J. Eng. Technol.*, vol. 7, no. 1, p. 221, Dec. 2017, doi: 10.14419/ijet.v7i1.5.9150.
[35] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, "Elliptic curve cryptography in practice," in *Financial Cryptography and Data Security*. Berlin, Germany: Springer, 2014, pp. 157–175, doi: 10.1007/978-3-662-45472-5_11.
[36] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, Aug. 2001, doi: 10.1007/s102070100002.
[37] D. Rachmawati, J. T. Tarigan, and A. B. C. Ginting, "A comparative study of message digest 5(MD5) and SHA256 algorithm," *J. Phys., Conf. Ser.*, vol. 978, Mar. 2018, Art. no. 012116, doi: 10.1088/1742-6596/978/1/012116.
[38] M. M. A. Khan, H. M. A. Sarwar, and M. Awais, "Gas consumption analysis of Ethereum blockchain transactions," *Concurrency Comput., Pract. Exp.*, vol. 34, no. 4, Feb. 2022, Art. no. e6679, doi: 10.1002/cpe.6679.
[39] Y. Li and B. Hu, "An iterative two-layer optimization charging and discharging trading scheme for electric vehicle using consortium blockchain," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2627–2637, May 2020, doi: 10.1109/tsg.2019.2958971.
[40] R. Khalid, M. W. Malik, T. A. Alghamdi, and N. Javaid, "A consortium blockchain based energy trading scheme for electric vehicles in smart cities," *J. Inf. Secur. Appl.*, vol. 63, Dec. 2021, Art. no. 102998, doi: 10.1016/j.jisa.2021.102998.
[41] C. Pinzón and C. Rocha, "Double-spend attack models with time advantange for bitcoin," *Electron. Notes Theor. Comput. Sci.*, vol. 329, pp. 79–103, Dec. 2016, doi: 10.1016/j.entcs.2016.12.006.
[42] L. Kuang, Y. Zhu, S. Li, X. Yan, H. Yan, and S. Deng, "A privacy protection model of data publication based on game theory," *Secur. Commun. Netw.*, vol. 2018, pp. 1–13, Oct. 2018, doi: 10.1155/2018/3486529.
[43] S. Amjad, S. Abbas, Z. Abubaker, M. H. Alsharif, A. Jahid, and N. Javaid, "Blockchain based authentication and cluster head selection using DDR-LEACH in internet of sensor things," *Sensors*, vol. 22, no. 5, p. 1972, Mar. 2022, doi: 10.3390/s22051972.

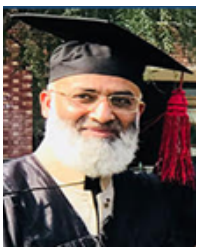
MUHAMMAD UMAR JAVED received the bachelor's and master's degrees in electrical engineering from the Government College University Lahore, Lahore, Pakistan, in 2014 and 2018, respectively. He is currently pursuing the Ph.D. degree with the Communications Over Sensors (ComSens) Research Laboratory, Department of Computer Science, COMSATS University Islamabad, Islamabad, under the supervision of Prof. Nadeem Javaid. He has authored more than 20 research publications in international journals and conferences. His research interests include smart grid, electric vehicles, and blockchain.

ABID JAMAL received the M.S. degree in information security from the Communication Over Sensors (ComSens) Research Laboratory, Department of Computer Science, COMSATS University Islamabad (CUI), Islamabad, Pakistan, under the supervision of Prof. Nadeem Javaid. He has authored five research publications in international conferences. His research interests include blockchain, information security, and vehicular networks.

EMAN H. ALKHAMMASH received the M.Sc. and Ph.D. degrees in computer science from the University of Southampton, U.K. She is currently working as an Associate Professor in computer science at Taif University, Saudi Arabia. Her research interests include formal methods, AI, and data science. She was awarded a Senior Fellow of the Higher Education Academy (FHEA), in March 2020.

MYRIAM HADJOUNI received the M.Sc. degree (Hons.) from the Higher Institute of Management of Tunis, University of Tunis, Tunisia, in 2005, and the joint Ph.D. degree (Hons.) in computer science from Paris XI (actual new name Paris Saclay) University, France, and Manouba University, Tunisia, in 2012. She is currently working as an Assistant Professor with the Computer Sciences Department, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia. Her research interests include but not restricted to information retrieval, artificial intelligence, data science, data analytic, big data, and image retrieval.

SAEED ALI BAHAJ received the Ph.D. degree from Pune University, India, in 2006. He is currently an Assistant Professor at the MIS Department, COBA, Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia. He is also an Associate Professor at Hadhramout University, Yemen. His main research interests include artificial intelligence, information management, forecasting, information engineering, big data, and information security.



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 a Professor and the Founding Director of the Communications Over Sensors (ComSens) Research Laboratory, Department of Computer Science, COMSATS University Islamabad, Islamabad Campus. He is also working as a Visiting Professor with the School of Computer Science, University of Technology Sydney, Australia. He has supervised 158 master's and 27 Ph.D. theses. He has authored over 900 articles in technical journals and international conferences. His research interests include energy optimization in smart/microgrids and in wireless sensor networks using data analytics and blockchain. He was a recipient of the Best University Teacher Award (BUTA'16) from the Higher Education Commission (HEC) of Pakistan, in 2016, and the Research Productivity Award (RPA'17) from the Pakistan Council for Science and Technology (PCST), in 2017. He is an Associate Editor of IEEE Access and an Editor of *Sustainable Cities and Society*.