applied sciences

MDPI

Article

Blockchain-Based Secure Data Storage for Distributed Vehicular Networks

Muhammad Umar Javed [1], Mubariz Rehman [1], Nadeem Javaid [1,*], Abdulaziz Aldegheishem [2], Nabil Alrajeh [3] and Muhammad Tahir [4]

[1] Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan; umarkhokhar1091@gmail.com (M.U.J.); mubarizrahman@gmail.com (M.R.)

[2] Traffic Safety Technologies Chair, Urban Planning Department, College of Architecture and Planning, King Saud University, Riyadh 11574, Saudi Arabia; aldeghei@ksu.edu.sa

[3] Biomedical Technology Department, College of Applied Medical Sciences, King Saud University, Riyadh 11633, Saudi Arabia; nabil@ksu.edu.sa

[4] College of Computer Science and Engineering (CCSE), University of Jeddah, Jeddah 21959, Saudi Arabia; mtyousaf@uj.edu.sa

* Correspondence: nadeemjavaidqau@gmail.com

Received: 15 February 2020; Accepted: 9 March 2020; Published: 16 March 2020

Abstract: In this paper, a blockchain-based secure data sharing mechanism is proposed for Vehicular Networks (VNs). Edge service providers are introduced along with ordinary nodes to efficiently manage service provisioning. The edge service providers are placed in the neighborhood of the ordinary nodes to ensure smooth communication between them. The huge amount of data generated by smart vehicles is stored in a distributed file storage system, known as Interplanetary File System (IPFS). It is used to tackle the issues related to data storage in centralized architectures, such as data tampering, lack of privacy, vulnerability to hackers, etc. Monetary incentives are given to edge vehicle nodes to motivate them for accurate and timely service provisioning to ordinary nodes. In response, ordinary nodes give reviews to the edge nodes against the services provided by them, which are further stored in a blockchain to ensure integrity, security and transparency. Smart contracts are used to automate the system processes without the inclusion of an intermediate party and to check the reviews given to the edge nodes. To optimize gas consumption and to enhance the system performance, a Proof of Authority (PoA) consensus mechanism is used to validate the transactions. Moreover, a caching system is introduced at the edge nodes to store frequently used services. Furthermore, both security and privacy are enhanced in the proposed system by incorporating a symmetric key cryptographic mechanism. A trust management mechanism is also proposed in this work to calculate the nodes' reputation values based upon their trust values. These values determine the authenticity of the nodes involved in the network. Eventually, it is concluded from the simulation results that the proposed system is efficient for VNs.

Keywords: Vehicular Networks; Interplanetary File System; Edge Vehicular Nodes; Proof of Authority; Blockchain; Road Side Unit

1. Introduction

With the drastic advancements made during the last few years, the number of smart vehicles has increased manifold. These smart vehicles come together and establish a Vehicular Network (VN), which serves various purposes, such as traffic regulation, prevention of accidents and critical message sharing between vehicles [1]. Nowadays, electric car manufacturers are developing autonomous vehicles equipped with a number of different functionalities like cruise control, intelligent decision making, auto pilot driving modes, etc. According to some studies, the market size of autonomous vehicles will increase tenfold and the market value will grow from $54.23 billion to $556.67 billion in near future [2]. Smart vehicles are equipped with different sensors and wireless communication modules that allow vehicles to sense various information, such as road conditions, traffic rates, accident reports, etc. This sensory information is shared with other smart vehicles and Road Side Units (RSUs) and is known as Vehicle-to-Vehicle (V2V) communication and Vehicle-to-Road-Side-Unit (V2R) communication, respectively. During the last few years, smart vehicles have gained much popularity due to their excellent features and capabilities. The huge increase in the number of smart vehicles leads to the generation of huge amount of real-time sensory data, which become quite difficult to handle as the time progresses. To store this huge data in a secured manner, a secure communication channel is required. The traditional centralized systems lack in providing required functionalities. Therefore, to overcome the above mentioned limitations, there is a need for a decentralized architecture that fulfills the VN's requirements. However, decentralized systems still face some issues like lack of security and privacy, lack of trust, etc.

To provide security, ensure privacy and establish trust between entities, blockchain technology was introduced by Satoshi Nakamoto in 2008 [3]. It is an increasing list of records, stored in the form of blocks, which are joined together in a chronological order to form a chain using cryptographic hashes. Each block contains multiple components, such as a cryptographic hash of the previous block, timestamp at which block is generated, transaction data in the form of Merkle root tree and nonce, which is an arbitrary number used for mining process. The basic structure of the block is shown in Figure 1. With the invention of blockchain, limitations of centralized architecture are eliminated. Blockchain ensures security, privacy preservation, decentralized architecture and data integrity. Due to the excellent features of blockchain, it is being used in various fields of life like Internet-of-Things (IoT) [4], smart grids [5], VNs, etc. Secure data sharing among smart vehicles is also made possible because of blockchain technology. Existing blockchain systems are designed for resource-efficient devices.

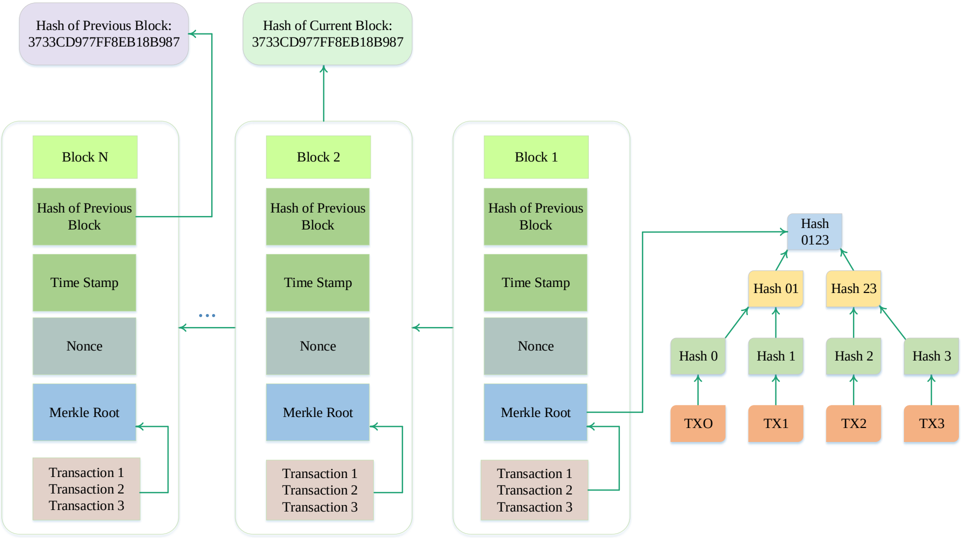


Figure 1. Basic Structure of Block.

This research work is an extension of [6]. In this paper, a secure blockchain-based data sharing architecture is proposed for VNs. Each ordinary vehicle communicates with edge node vehicle for the required service. There are predefined service charges against each service. Whenever an ordinary node requests for a service, a predefined amount is deducted from its account. For the storage of data generated by vehicles, a distributed data storage mechanism is used. For each vehicle, the trust value is calculated to determine the reputation of each vehicle. Crypto ID is assigned to each vehicle for the reduction of malicious activities in the network. The reputation values of vehicles are stored in blockchain against their respective IDs.

1.1. Motivation

In recent years, VN has gained much popularity and has grown remarkably. The use of the Interplanetary File System (IPFS) and edge vehicle nodes support data sharing mechanisms and secure communication on a reliable channel. Lack of security and privacy-related problems of VN are solved using the blockchain technology, which provides features of openness, decentralization, distributed ledger and tamper-proof system. However, blockchain is a high resource-consuming technology having a high storage requirement. By keeping these issues in mind and being motivated from [7], we proposed a blockchain-based secure data sharing mechanism for VN.

1.2. Problem Statement

The development of a secure service provisioning mechanism for IoT became a reality with the advent of blockchain technology. In IoT, many electronic devices are connected together to form a network. Due to the rapid increase in IoT devices, huge amounts of data are being generated. To handle this huge volume of data efficiently and securely, a decentralized data control mechanism is required [8]. Authors in [9] proposed a blockchain-based secure service provisioning mechanism for IoT using blockchain. The service codes are protected from untrustworthy edge servers involved in edge transparent computing network, using blockchain technology. The effectiveness of the system is evaluated for resource constraint devices through simulation results. However, neither a service charging mechanism nor a cryptographic mechanism for secure communication is considered. In [10], authors proposed an edge transparent computing network for smart transportation, in which both centralized and distributed architectures are used for efficient and cost-effective communication. Edge servers are placed in a distributed manner to provide essential services and to achieve localization. However, efficient deployment of edge servers, enabling caching techniques and data monetization among IoT are not considered. With the increase in population, smart vehicles are increasing with every passing day. In [7], the authors proposed a blockchain-based VN, which allows the development of a distributed network for large scale vehicles in an efficient and effective manner. However, for reliable communication among vehicles and for efficient data storage, there is a need of a trust management and distributed file system. In V2V communication, vehicle's ID number is used normally for communication purpose. However, it leads to the privacy leakage issue. To tackle the biasness issue and to encourage users, an incentive mechanism is required. However, no incentive mechanism for vehicles is introduced in [7].

1.3. Contributions

The key contributions of our proposed system are:

- we proposed a blockchain-based VN for reliable data sharing between resource constrained ordinary nodes,
- to store the huge data generated by smart vehicles, a distributed file system, i.e., IPFS is used,
- all the transactions are automated and the reviews are checked using smart contracts,
- Proof of Work (PoW) is replaced with Proof of Authority (PoA) to reduce latency and increase throughput of the system,
- cryptocurrency based incentive mechanism is proposed for edge vehicle nodes. If a valid service is provided by an edge vehicle node, then it is awarded with some incentive,
- caching technique is introduced in edge vehicle nodes to optimize the cost of the proposed system,
- Intelligent Vehicle Trust Point (IVTP) is introduced to calculate the trust values of ordinary vehicle nodes and
- to share data in a secure manner, a cryptographic mechanism: symmetric key encryption/decryption, is used.

The rest of the work is structured as follows. The related work is categorized in three main categories, i.e., blockchain in IoT, healthcare and Wireless Sensor Network (WSN) and is given in

Section 2. In Section 3, proposed system model is presented and its detailed description is given. In Section 4, simulation results are provided with their discussion. Whereas, Section 5 concludes the paper and discusses about the future work.

2. Literature Review

In this section, the literature review of blockchain technology is given. This literature review is divided into three broad categories: blockchain in IoT, blockchain in healthcare and blockchain in WSN, given in Sections 2.1, 2.2 and 2.3, respectively. The related work is summarized in Table 1.

2.1. Blockchain in IoT

In [7], the authors proposed a blockchain-based adhoc VN, which allows VN to be scalable for large scale vehicles. Using the blockchain technology, a secure environment is proposed for both end-users and the machine side. In this model, vehicles are also able to share their resources for revenue generation.

Authors in [9] proposed a blockchain-based secure service provisioning mechanism for IoT. Edge servers are placed in a network to provide efficient services for resource constraint devices. To minimize the computational cost, PoA consensus mechanism is used. From the simulation results, the effectiveness of the proposed system is evaluated. However, service charging is not considered. With the advancements made in IoT technologies, security, privacy and credibility issues arise, which need to be tackled. Authors in [10] presented a blockchain-based hybrid architecture for smart cities. Taking benefits from both centralized and distributed architectures, the authors proposed a hybrid network architecture. Software Defined Networking (SDN) and blockchain are used together in the proposed work. The authors divided the network into two main parts: the core network and the edge network. Argon2 based PoW consensus mechanism is used to ensure security and privacy. However, efficient deployment of edge nodes and caching techniques are not considered. In [11], the authors proposed a blockchain-based credibility verification method for IoT. The authors proposed a self-organizing blockchain structure. The effectiveness of the proposed system is evaluated using response time and storage efficiency. However, the proposed work lacked in achieving complete decentralization. Authors in [12] proposed a framework for data sharing in a distributed system with a fine-grained access control mechanism. To overcome the limitations of centralized architecture, the authors proposed a distributed system, which uses Ethereum blockchain and Attribute Based Encryption (ABE) scheme. The feasibility of the system is analyzed through experimental analysis. However, access policy updates and user attribute revocation are not considered.

In [13], the authors proposed a novel attribute based access control mechanism for IoT, which ensured scalability and robustness of the system. PoW consensus mechanism is not used for IoT devices, which significantly decreased the communication overhead. However, the real-time scenario is not considered. Authors in [14] proposed a blockchain-based data sharing mechanism, while using fine-grained access control and Artificial Intelligence (AI). Two blockchains are proposed for the data-sharing mechanism, named as: Data chain and Behaviour chain. The proposed system is based on hyper ledger Fabric. However, the scope of the proposed work is limited. Hence, the economic impact of the proposed work is not considered. In [15], authors proposed an E-business model for IoT using blockchain technology. The authors proposed a Peer to Peer (P2P) model for using blockchain technology. Distributed Autonomous Corporation (DAC) is used for P2P trading, which is based on machine learning algorithms to make it intelligent. In the proposed work, DAC performed trading through Person-to-Machine (P2M) mechanism.

In [16], the authors proposed a framework for Intelligent Vehicle (IV) using blockchain technology and solved the problems of authentication and trust. The dynamic traffic rate is considered for simulations. The concept of IVTP is introduced for accessing the trustworthiness of other vehicles. With the help of blockchain, a large number of vehicles are handled in a real-time scenario. The proposed system performed well in case of heavy traffic.

Table 1. Summarized Literature Review.

Domain	Problem Identified	Proposed Solution	Technique	Results	Limitations
VN [7]	Insecure communication in large scale VN	Vehicular ad-hoc network for scalable VN	Not explicit	Scalability of the system is achieved	Limited resource sharing scenario
IoT [9]	Insecure service provisioning for IoT	Secure service provisioning mechanism	Blockchain with PoA consensus algorithm	Secure service provisioning achieved	Service charging is not considered
IoT [10]	Optimization of the system performance	Blockchain-based hybrid network architecture	Hybrid architecture with Argon2 based PoW	Reduction in computational time	Efficient deployment of edge node is not considered
IoT [11]	Credibility verification in IoT	Blockchain-based credibility verification method	Self organization blockchain structure	Response time and storage capacity are optimized	Complete decentralization is not achieved
IoT [12]	Authentication of IoT	Attribute based access control mechanism	Blockchain-based access control mechanism	Secure access control policies achieved	Users attribute revocation is not considered
IoT [13]	Security and authentication	Decentralized access control mechanism	Blockchain and Attribute based access control	Scalability and robustness achieved	No real-time scenario is considered
IoT [14]	Secure data sharing scenario	Efficient access control and permission levels	Data chain and behaviour chain is used for data sharing	Security and privacy preserving data sharing systems	Proposed system is designed only for a single system
IoT [15]	Third party involvement	DAC	Blockchain with e-trading system	Secure trading environment	Designed only for two commodities
IV [16]	Authentication and trust of vehicles	Dynamic traffic rates	IVTP	Large number of vehicles are handled	Temporal complexity faced
IoV [17]	Real-time response in V2V communication	Blockchain-based VN	Blockchain with PoW	Storage capacity is optimized	No real-time traffic conditions are considered
VN [18]	Trust management system for VN	Bayesian inference model	Blockchain with PoW	Trust value is calculated	Privacy preservation is not considered
IoT [19]	Computational power of lightweight clients	Fair payment scheme with secure service provisioning	Blockchain with PoA	Service provisioning cost is reduced	No security check on lightweight clients and service providers
Healthcare [20]	Security of the medical data	E-health management system	Blockchain with PoW	Scalability is achieved	Proposed system is designed for a limited scenario
WSN [21]	Optimizing data storage in wireless nodes	Incentive mechanism for data storage	Blockchain with PDP	Data storage capacity is optimized	Two blockchains are used
WSN [22]	Data storage and computational complexity	Rolling blockchain concept	PoW is not used	Secure data storage achieved	No security analysis done
Cellular network [23]	Authentication of CSI	Blockchain-based data intensive system	Blockchain for cellular network	Spectra efficiency is improved	Only handles non-cooperative mobile users

In [17], the authors proposed a blockchain-based distributed network architecture for the Internet of Vehicles (IoV). To overcome challenges of real-time response in VN, a distributed architecture is proposed. The secure storage of big data is the main concern of blockchain-based VNs. However, the real-time traffic rate is not considered by IoV. In [18], the authors presented a blockchain-based decentralized trust management system for VN. The proposed work is aimed at maintaining trust between the vehicles. Vehicles are able to query the trust value of neighbours using Bayesian inference model. RSUs participated in the network to calculate the trust value of each vehicle. From the experimental results, it is concluded that proposed system is more efficient in terms of calculating and storing trust value. However, privacy preservation is not considered in this paper. Authors in [19] proposed a consortium blockchain-based service provisioning scheme for lightweight clients. The issue of less computational capabilities of these devices is tackled. In the proposed work, an incentive mechanism is proposed to encourage the participants. To reduce resource consumption, PoA consensus mechanism is used instead of PoW in the proposed work. The comparison between hashing algorithms is also performed to check which algorithm performed better in the proposed model. Furthermore, the service provisioning is performed at reduced cost.

2.2. Blockchain in Healthcare

In [20], the authors proposed an Electronic health (E-health) record sharing system, in which privacy and security issues are tackled using blockchain technology. Privacy of Personal Health Information (PHI) is preserved by blockchain. All the data are in encrypted form and is equipped with the keyword search algorithm. From the simulation results, the authors deduced that the proposed scheme performs better in terms of data security and control over data access. Medical research is increasing with every coming day and generated data are stored in form of records [24]. E-health record is facing huge challenges, such as record tampering, unauthorized data access and identity tracking. With the help of blockchain, authors conclude that data are made reliable and more secure. The medical information audit function is used to fulfill the security requirements.

The health data are stored electronically, termed as Electronic Medical Records (EMR) [25]. However, it is a tiresome task to share medical data among different medical entities due to privacy issues. For providing security, trust and tamper-resistant maintenance of health records, blockchain technology is proposed. Data sharing with blockchain also provides privacy. Blockchain is used to store the transaction data. A huge amount of data are stored in IPFS, which ensures scalability and data confidentiality. The proposed solution also ensures data privacy with the data-sharing mechanism. Medical records play a vital role in the lives of human beings and cause an increase in medical data [26]. Remote patient monitoring is used in IoT to sense medical data and provide healthcare to patients. There are many issues which arise when sharing the patients' health data between medical entities publicly. To tackle the aforementioned issues, a system to tackle privacy leakage problems and to anonymize the data generated by wearable healthcare devices is proposed.

2.3. Blockchain in Wireless Sensor Network (WSN)

In WSN, different issues exist like data storage, computational complexity and node failure. In [21], an incentive mechanism for WSN is proposed. The WSN nodes that store the data are awarded with incentives upon reliable storage of data. More the data are stored, more the incentive amount is given. Two blockchains are used in the proposed scenario: data storage and access control. Instead of using PoW consensus mechanism, the authors used Provable Data Possession (PDP). PoW has the major limitation of high resource consumption, which is tackled using PDP. With blockchain technology, storage complexity is also optimized. In WSNs, nodes are resource constraint entities, which have less computational power. By keeping this issue in mind, the authors proposed a novel rolling blockchain mechanism in [22] that overcomes data storage and computational complexity problems. Due to the resource constraint nature of WSN nodes, PoW is not advisable to be used in WSN. From simulation results, authors concluded that if the network is denser, then there is less chance of node failure and vice versa. The excessive node failure leads to network breakdown.

In [23], the authors presented a framework for Device-to-Device (D2D) cellular network. The main objective of the proposed framework is to authenticate Channel State Information (CSI). In a data intensive system, D2D communication is not suitable for large number of mobile users. The proposed algorithm improved the spectra efficiency without using any consensus mechanism. However, this system is only designed for non-cooperative mobile users.

3. Proposed System Model

In this section, we discuss about the proposed system model, which is a blockchain-based VN. The proposed model is intended to ensure trusted service sharing between vehicles. The proposed system enables V2V communication in a secure environment and tackles various challenges of the VN.

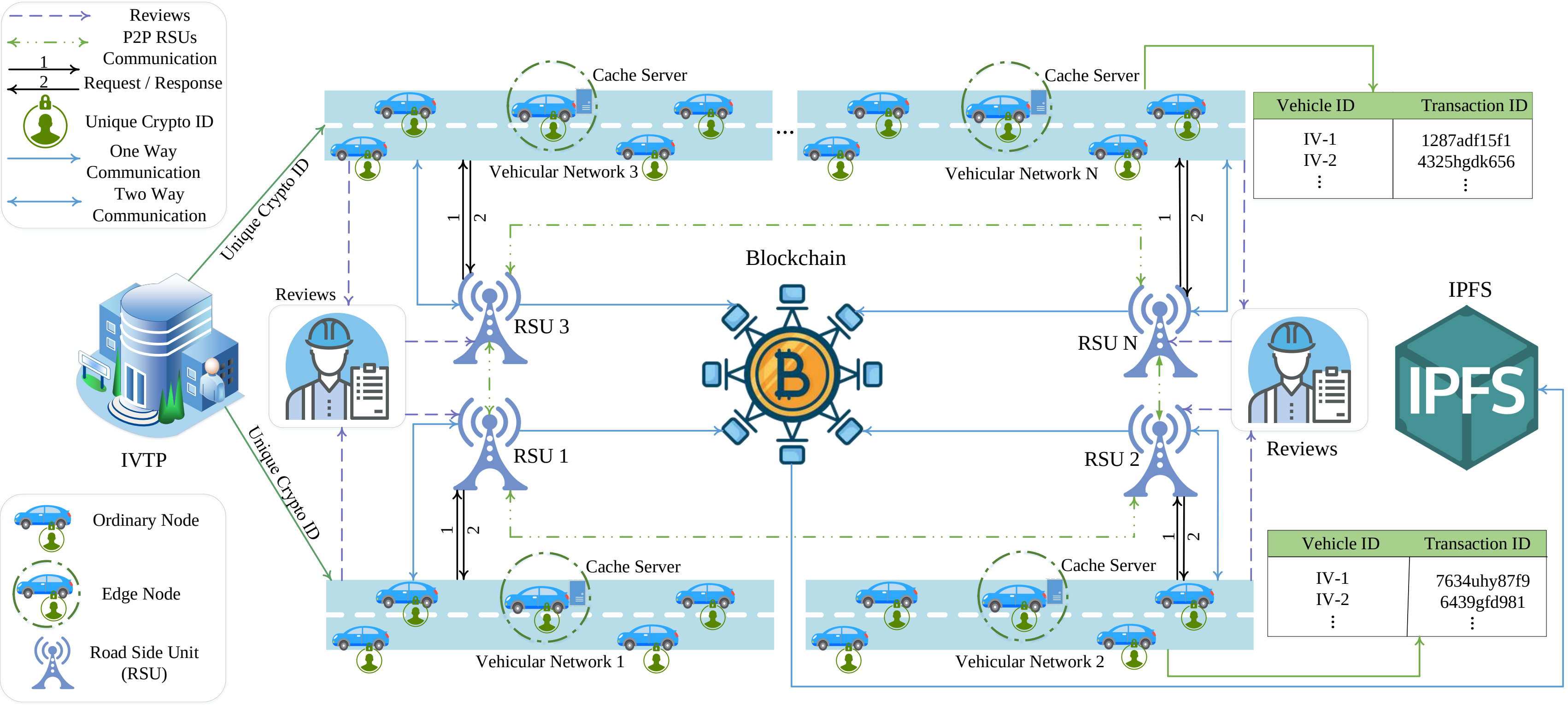
3.1. Architecture Overview

Being motivated from the system model proposed in [7], we proposed our system model for VN. Our proposed system model allows the development of the distributed VN in an efficient manner. Figure 2 illustrates the proposed system model designed to meet the requirements and challenges of VN. In the model, RSUs are static nodes, which are placed in a distributed manner to ensure efficient service provisioning. In the figure, three different types of nodes exist, which are: ordinary nodes, edge nodes and RSUs. Smart vehicles are considered as ordinary nodes that perform V2V communication. Ordinary nodes are resource constraint nodes having low storage capability, less computational power and low battery life. Edge nodes have more computational power than ordinary nodes and are shown in a green circle. Whereas, RSUs act as static nodes. Edge nodes handle service requests/responses. An ordinary node requests a service from edge nodes in a distributed manner. Due to the distributed placement of the edge nodes and RSUs, scalability and availability of the system are achieved. In the proposed model, two types of communication take place, which are: V2V and V2R. For efficient performance, all nodes need to be in active states at all times. For more reliable communication, the cryptographic mechanism is proposed, which ensures security and privacy.

Whenever a new unrecognized vehicle joins the network, a distinct crypto ID is issued to the vehicle by an IVTP organization. Each vehicle in a VN has its unique crypto ID, which is used to establish trust between vehicles in a communication network. IVTP calculates the trust value that ensures the reputation of a vehicle. Greater the IVTP value, higher will be its reputation and honor. All the RSUs primarily contain sensory information, which is required by the ordinary nodes. All RSUs are connected in a P2P manner.

3.2. Edge Node Model Overview

Each edge node comprises three types of computational assets, which are: computing, sensing and data storing. Depending on these assets, edge nodes are distinguished from controller nodes. These edge servers get the vehicle information from ordinary nodes and transfer it to the controller nodes, which use IPFS to store this information. Various types of services are supplied by the edge nodes, such as road accidents, traffic blockage, sensory data of smart vehicles and service sharing. Depending on the service given by edge nodes, ordinary nodes give a rating. Depending upon which, the behavior of edge nodes is determined. If the service required by an ordinary node is available with the edge node, then it is transferred by the edge node itself. The edge node communicates with RSU to response against the service request. Edge nodes store frequently used services in cache memory, which improves the overall system's efficiency by reducing the delay in response to the service requests.



Vehicle ID	Transaction ID
IV-1 IV-2 ⋮	1287adf15f1 4325hgdk656 ⋮

Vehicle ID	Transaction ID
IV-1 IV-2 ⋮	7634uhy87f9 6439gfd981 ⋮

Figure 2. Proposed System Model.

3.3. Incentive Mechanism in VN

In a VN, sensory information is collected from smart vehicles and stored in IPFS. Whenever a smart vehicle requests a service, edge nodes communicate with the RSU. The RSU then checks the blockchain and gives response against the service request. Some smart vehicles are not involved in service sharing process due to their selfishness or lack of trust. Hence, the system's performance is compromised. To overcome this limitation, the incentive mechanism is proposed. Whenever some sensory information is provided by an ordinary node, it is awarded with incentives. This incentive amount is given in the form of cryptocurrency, which is further converted to local currency for getting different benefits from it. In our proposed system, the incentive is given as a reward after valid service sharing. By the involvement of incentive mechanism, problems of selfishness and low user participation are tackled. Algorithm 1 gives the basic flow of service provisioning to ordinary nodes and incentive provisioning to edge nodes.

Algorithm 1: Algorithm of Service and Incentive Provisioning in VN.

```
1  Initialization
2  Inputs: Ordinary node ($o_n$), Set of ordinary nodes ($O_n$), Edge node ($e_n$), Set of edge nodes ($E_n$),
     Service required ($Ser_{req}$), Set of services ($S_n$), RSU
3  Outputs: Incentive given ($Inc_{giv}$), Incentive denied ($Inc_{den}$)
4  for $Ser_{req}$ by $o_n$ from $e_n$, where $o_n \in O_n$ and $e_n \in E_n$ do
5      if ($Ser_{req} \in S_n$) then
6          if ($Ser_{req}$ $\exists$ at $e_n$) then
7              Grant service to the ordinary node, $o_n$
8              else
9                  Forward the service request to RSU and goto step 12
10             end
11         end
12         if ($Ser_{req}$ $\exists$ at RSU) then
13             Grant service to the ordinary node, $o_n$
14             else
15                 Give response to $o_n$: "Invalid request"
16             end
17         end
18         else
19             Give response to $o_n$: "Invalid request"
20         end
21     end
22 end
23 if Service is provided to $o_n$ then
24     Incentives given ($Inc_{given}$) to $e_n$
25     else
26         Incentives not given ($Inc_{den}$) to $e_n$
27     end
28 end
29 End
```

3.4. RSU Overview

RSUs are the static nodes, which are used to gather and store all the information provided by the vehicles. In the proposed model, distributed connections are established between RSUs and edge nodes to provide services like road information, traffic rate, road accident details and nearly located charging stations. In real-time vehicular environments, data generated by smart vehicles is large in quantity. Therefore, most of the data are stored in RSUs because storing such huge amount of data at edge nodes is a time consuming task. To ensure uninterruptible information provisioning to all vehicles and edge nodes, RSUs remain in active state at all times.

3.5. Authentication of VN

For authentication of the vehicles involved in the proposed blockchain network and for the prevention of malicious activities, IVTP is used. In IVTP, a unique crypto ID is assigned to each vehicle in the network, which is used for its identification. The records of assigning crypto IDs to different vehicles are also stored in IVTP. Whenever, a new malicious node wants to participate in a network, it is easily detected as malicious due to the absence of its crypto ID. Furthermore, the trust value for each vehicle (based on service sharing) is also calculated through IVTP.

3.6. Caching and IPFS

In the proposed VN, smart vehicles communicate with the edge nodes and request for a service. The edge nodes either fulfill the service request by themselves or communicate with RSUs for the fulfillment of user requests. This whole process requires a large execution time, involving various delays like propagation delay, transmission delay, etc. However, the real-time VN is a time-sensitive system. To optimize the gas consumption and reduce the execution time, cache memory is used at the edge nodes, where frequently used sensory information is stored. Instead of fetching the required information from RSU, cache memory provides the vehicles with the requested information, which leads to reduction in the execution time. IPFS is used for distributed data storage while considering the issues of centralized systems, such as single point of failure, data leakage, etc. [27]. In IPFS, data integrity is also achieved using the unique hashes assigned to data blocks. In case of data tampering, the complete hash of data block changes. Algorithm 2 gives the flow of IPFS.

3.7. Workflow of Proposed System

In the proposed blockchain-based VN, smart vehicles are registered using crypto IDs provided by IVTP. A list of all the registered vehicles is stored in the proposed blockchain network. Ordinary vehicles communicate with edge node vehicles for required services. The edge node vehicles then communicate with RSUs to entertain the request of ordinary vehicles and respond accordingly. All communications in the blockchain network are done in an encrypted form to ensure privacy. In the proposed model, encryption is done using AES128 technique. The trust values of vehicles are calculated via IVTP, which further determine the behavior of the smart vehicles. The information provided by the vehicles to RSUs is saved using IPFS, which stores the provided information in a distributed hash table and generates corresponding hashes. These hashes are then stored in the blockchain network. For making the system efficient in terms of resource utilization, PoA consensus mechanism is used instead of PoW. Cache server is used at the edge node layer, which stores the frequently used services. Whenever an ordinary vehicle sends request for a service, the edge node vehicle checks its cache server. If the required service is present at the cache server, then the required service is transferred by edge node vehicle itself. Else, the service request is forwarded to RSU, which then provides the required service. If the required service is not present at RSU, then the vehicle is replied with a message *"invalid service"*. With the use of the cache server, the overall communication time of a system is optimized. Incentives are awarded to edge nodes for efficient sharing of validated services. However, there are pre-defined service charges against each service, which are to be paid by the ordinary nodes. All the financial transactions are stored in blockchain.

Algorithm 2: Algorithm of Data Storage in IPFS.

```
Initialization
Inputs: Ordinary node $O_n$, Sensory information
Outputs: Provisioning of sensory information file
for All ordinary nodes, $O_n$ do
    Retrieve the information
    Sends the information to IPFS
    IPFS stores the information in distributed hash table
    IPFS assigns hash to the information file stored
    Sends the hash information to blockchain
end
for Information retrieval request from $O_n$ do
    Checks for the authentication of the $O_n$
    if $O_n$ is authenticated then
        Checks for the hash provided by $O_n$
        if Hashes match then
            Provides information file to $O_n$
            else
                Denies provisioning of information file
            end
        end
        else
            Blacklists the $O_n$ and denies provisioning of information file
        end
    end
end
End
```

4. Simulations and Results

In this section, the simulation results of the proposed model are discussed in detail. Moreover, the security analysis and attacker model are presented in this section. The security features of the proposed model are also presented.

4.1. Simulation Environment

For proposed work, Ethereum is used for performing simulations. Ethereum provides user friendly environment as compared to bitcoin. Ethereum supports Decentralized Applications (DApps) for the blockchain-based environment. Ethereum is efficient than bitcoin network in terms of number of transactions validated in one second. Turing complete scripting language, known as Solidity, is used for implementing smart contracts.

4.1.1. Remix Integrated Development Environment (Remix IDE)

Remix IDE is used for simulation of smart contracts based on Solidity language. It is a web browser based development environment, through which deployment and execution of smart contracts is made possible.

4.1.2. Ganache

Ganache is a blockchain-based software, which provides virtual accounts for executing smart contracts. For each account, a unique address is stored in Ganache. It also performs mining process through which transaction is validated and added to the blockchain. In each account, predefined amounts of virtual ethers are stored. These ethers are used as a cryptocurrency in a blockchain environment.

4.1.3. MetaMask

Metamask is the browser extension used for Ganache and Remix connectivity. Metamask also provides facility of connectivity with local host and other blockchain networks, such as Rinkeby and Ropsten.

4.1.4. System Specification

The specifications of system used for network simulations are: HP 450G ProBook, having 1 TB Hard Drive and 8 GB RAM.

4.2. Results and Discussions

In this subsection, the overall performance of our proposed system is given. The execution cost and transaction cost are measured in terms of *gas*. Any action performed in an Ethereum environment is considered a transaction. For each transaction, pre-defined amount of gas consumption is charged. The pre-defined gas consumption amount is mentioned in Ethereum yellow paper [28].

$$1 \text{ gas unit} = 4 \text{ gwei } (1 \text{ Ether} = 1000{,}000{,}000 \text{ gwei})$$

In Figure 3, we calculate the total gas consumption based on two different consensus mechanisms. Two smart contracts are designed for the proposed system. One contract is of IPFS and the other is of VN. From the experimental analysis, we conclude that the PoA consensus mechanism is more efficient than PoW, in terms of gas consumption. In PoW, all miners participate in the complex mathematical puzzle-solving process, which requires a large execution time as well as excess resource consumption. From the simulation results, it is shown that PoA is efficient for resource constraint devices.

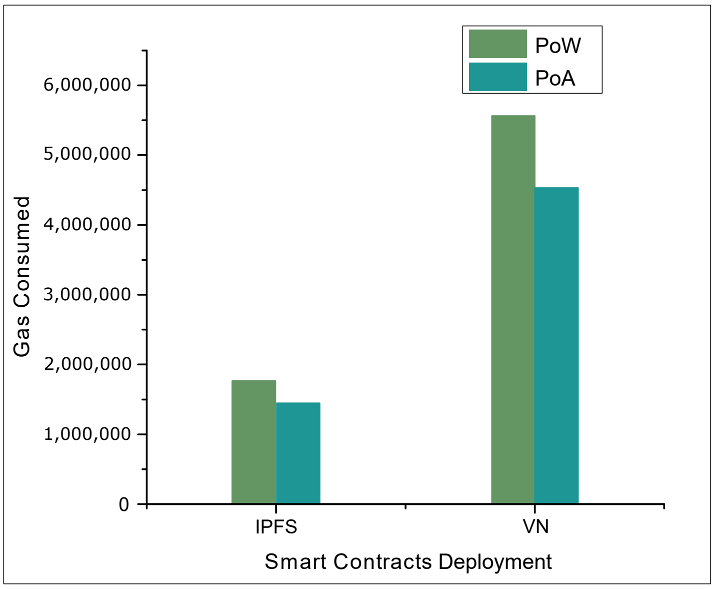


Figure 3. Smart Contracts Deployment Cost.

In Figure 4, gas consumption of main functions of IPFS is presented. It is observed that function *Add Data* consumes more gas than other functions and it depends on the size of the file to be uploaded and the network conditions. Once the data are uploaded, the gas consumption is not too much high, which shows the effectiveness of the system. IPFS is used as a secure data storing and sharing mechanism, which supports data integrity. We proposed modular contract based system in which impact of attacks is minimum.

In Figure 5, gas consumption of different phases of IPFS, which are: *Return Hash*, *Set Access Rights*, *Set Recipient* and *Set Blacklist* is presented. From the simulation results, we conclude that gas consumption of these functions is not very high. Our proposed system is efficient and flexible for resource limited devices. In Figure 6, the transaction cost and execution cost of main functions of VN smart contract are given in terms of *gas*. Four functions are performed in VN, which are: *deployment cost, register vehicle, service request* and *service response*. The difference between both cost is observed because execution cost is always less than the transaction cost. The reason is execution cost is the cost of executing only a certain function. Whereas, transaction cost involves both the contract deployment cost and the function execution cost.

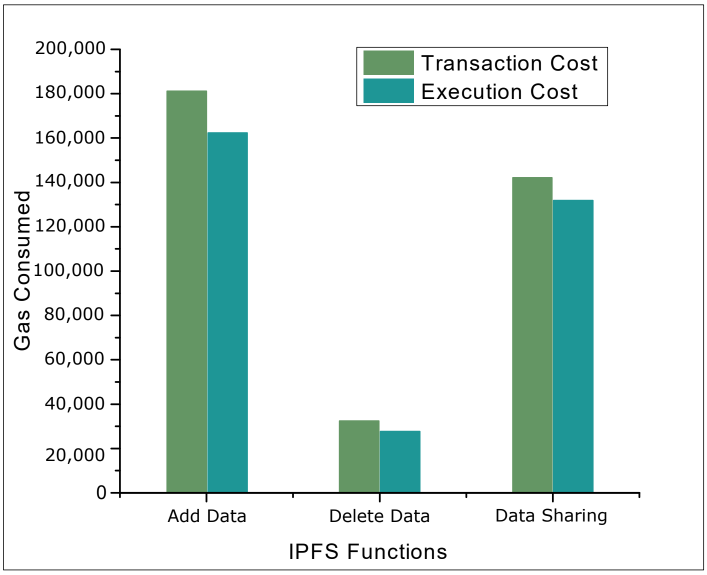


Figure 4. Gas Consumption for IPFS Functions.

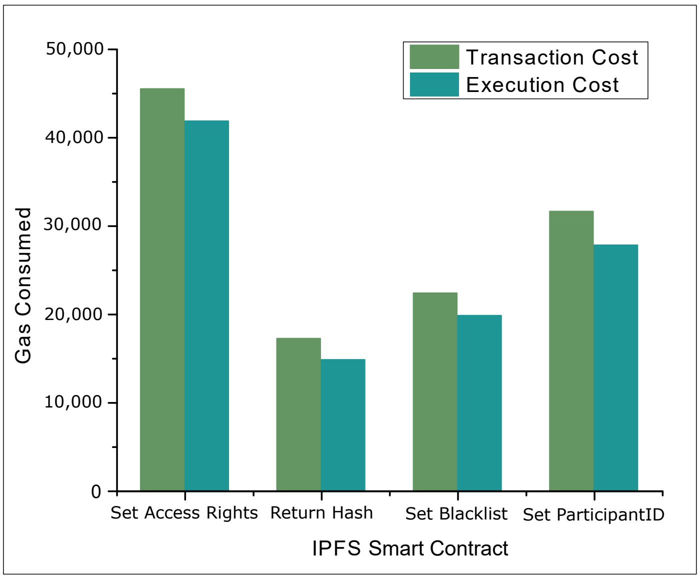


Figure 5. Gas Consumption for IPFS Smart Contract.

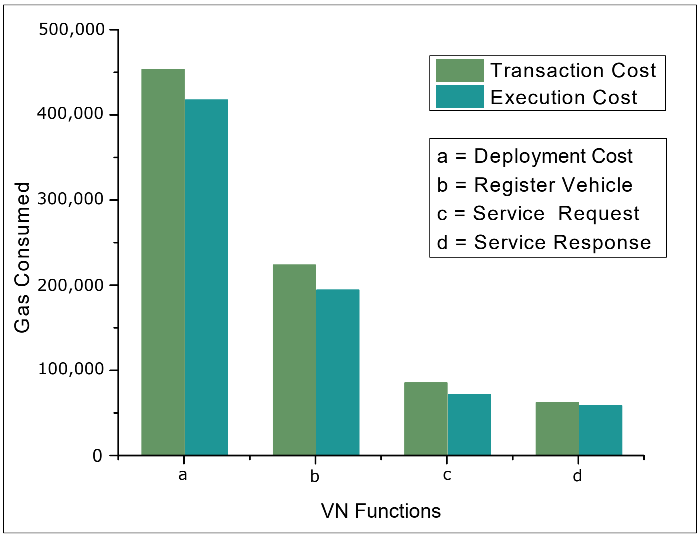


Figure 6. Gas Consumption for VN Functions.

In Figure 7, the execution cost and the transaction cost of different phases of VN smart contract are presented, in terms of gas. These phases are: *assigning unique crypto ID, incorporation of cache memory in edge vehicles* and *trust management among edge vehicles and ordinary vehicles*. From the results, we conclude that the trust management function consumes more gas as compared to other phases. Moreover, incorporation of cache memory optimizes the gas consumption. From gas consumption, we conclude that there is a smooth difference between gas consumptions of different phases.

In Figure 8, comparison between different hashing algorithms is presented. With respect to our proposed system, keccak256 is efficient in terms of resource consumption. By using keccak256, resource consumption of proposed system is optimized and integrity of the system is achieved.

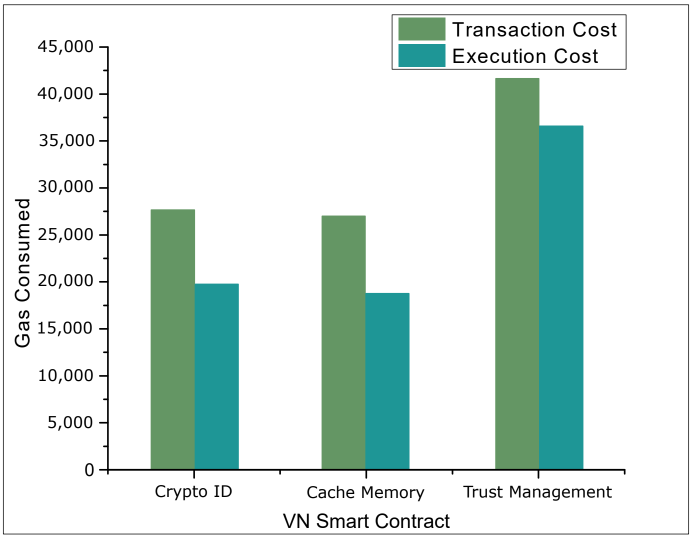


Figure 7. Gas Consumption for VN Smart Contract.

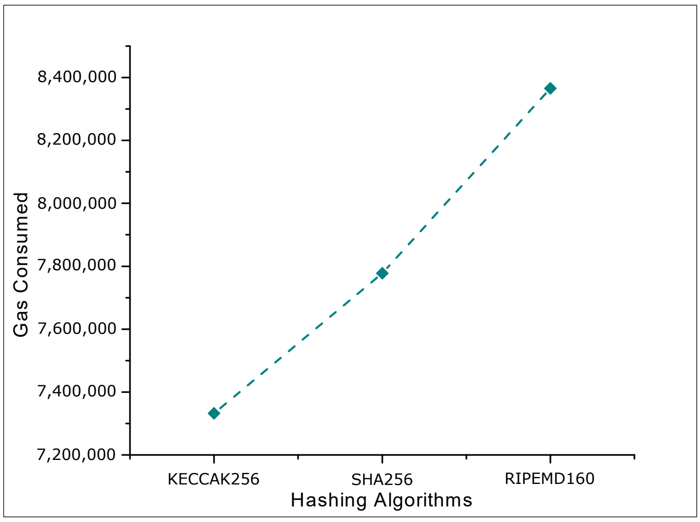


Figure 8. Comparison of Hashing Algorithms.

In Figure 9, system performance is evaluated using cache server and without using cache server. Cache servers are placed in edge vehicle nodes. When ordinary vehicles request for sensory information from edge vehicles, they check their cache memory for required service and give response. From the simulation results, we conclude that with the involvement of cache server, both the gas consumption and the execution time of the system are optimized and vice versa. With cache memory, both the communication time and the service charges are also minimized. In Figure 10, comparison between different cryptographic mechanisms is performed. The main aim of this comparison is to evaluate the performance of algorithms and to identify which encryption algorithm is suitable for our proposed system. The encryption mechanism is performed out of the blockchain. Average execution time is considered as a performance parameter through which the performance of an algorithm is evaluated. Encryption time is the total time taken for converting plain text into cipher text and depends on two main factors: size of data (to be converted) and size of key (to be generated). In our proposed system, each vehicle communicates with other vehicle in an encrypted form. From comparison of different hashing algorithms, we conclude that AES128 is better in terms of average execution time. Though, AES256 is based on the same mechanism on which AES128 works; still, the key size of AES256 is greater than AES128, that is why its execution time is high. With the utilization of encryption algorithms, system security is achieved; while, user comfort is compromised. DES algorithm converts message into block of 64 bits and divides key into three different parts. Due to this, the performance of algorithm becomes worst. Affine cipher algorithm performs worst than all other algorithms because its key is composed of two parts. During encryption process, first part of key is multiplied with data in plain text and then second part is added. We conclude that both AES128 and AES256 perform better than other algorithms. However, their execution time varies with the key size.

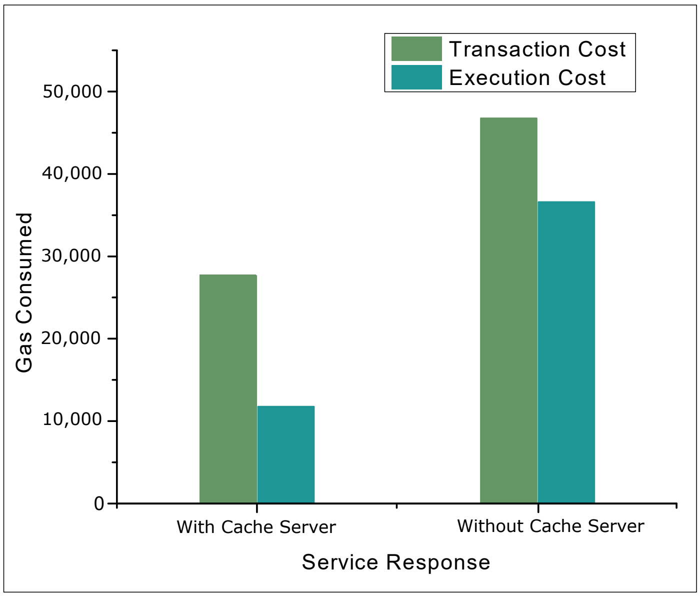


Figure 9. Performance of System with and without Cache Server.

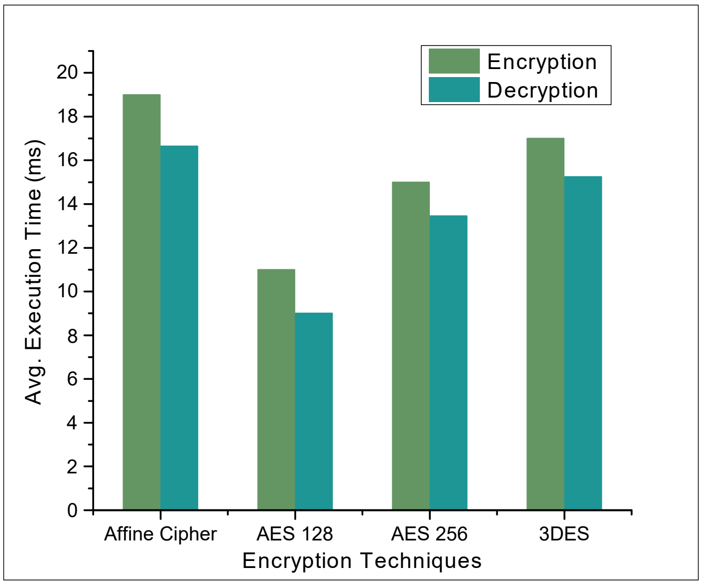


Figure 10. Comparison of Encryption/Decryption Algorithms.

In Figure 11, a trust value is calculated by first dividing the number of successful transactions by the total number of transactions and then multiplying the result by 100 (Equation (1)). The total number of successful transactions is calculated by subtracting invalid/unsuccessful transactions from the total transactions which occurred. In our proposed system, trust management is considered between ordinary vehicles and edge node vehicles. From the simulation results, we conclude that as the total number of successful transactions increases, trust rate also increases. The higher the trust rate, the higher the reliability of the system. Due to this, network communication also increases with minimum chances of malicious activities. The number of malicious activities are also reduced.

$$Avg.\ Trust\ Rate = \frac{No.\ of\ Successful\ Transactions}{Total\ no.\ of\ Transactions} * 100 \tag{1}$$

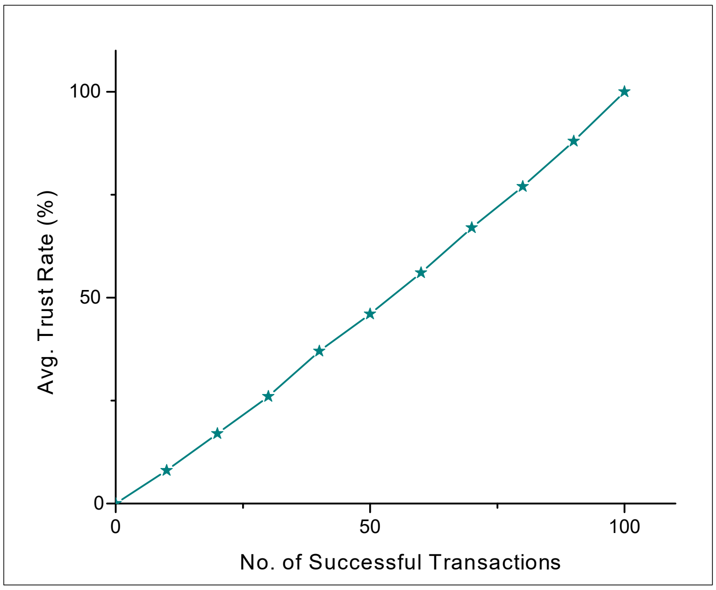


Figure 11. Trust Management between Ordinary and Edge Node Vehicles.

4.3. Security Analysis of the Proposed System

In this subsection, the security analysis of the proposed system is presented. For analysis, we used Oyente software, which is compatible with Ethereum-based blockchain systems. Oyente provides flexible environment which supports Solidity, Serpent and low-level Lisp-like languages. Oyente generates a report as output, in which mostly reported vulnerabilities are shown. From critical security analysis, it is shown that our proposed system is efficient and secure against many vulnerabilities, such as Parity Multisig Bug 2, Callstack Depth Attack Vulnerability and Re-Entrancy Vulnerability. However, the proposed system still faces one vulnerability, known as Integer Overflow. The impact of this vulnerability is limited because integer overflow occurs when an input value is greater than the integer capacity. Our proposed system is designed for smart vehicles and all parameters are set accordingly, that is why it is secure against many vulnerabilities. An analysis report is shown in Figure 12, which proves that our system is secure and efficient against different vulnerabilities.

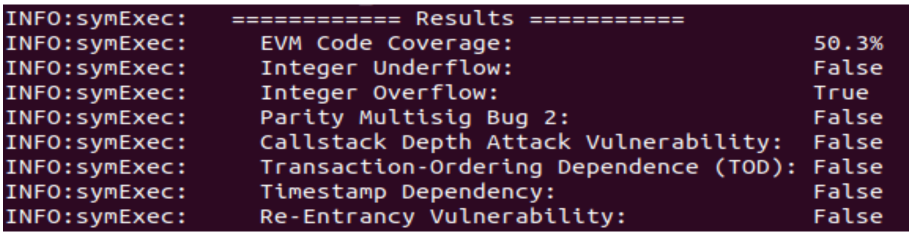

```
INFO:symExec:   ============ Results ===========
INFO:symExec:     EVM Code Coverage:                       50.3%
INFO:symExec:     Integer Underflow:                       False
INFO:symExec:     Integer Overflow:                        True
INFO:symExec:     Parity Multisig Bug 2:                   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
```

Figure 12. Security Analysis of Proposed System.

4.4. Attacker Model

In our proposed system, security and privacy are the main concerns for data sharing among vehicles. Vehicles communicate with each other for sharing sensory information. The main concern is to prevent privacy leakage and to ensure security against potential threats. We consider an attacker model tested against following attacks, for our proposed system.

4.4.1. Forgery Attack

The malicious node uses the fake signature of an authorized vehicle and transfers it to the network participants.

4.4.2. Man-in-the-Middle Attack

The malicious node intercepts the shared data between vehicles and performs data tampering. While, the sender and receiver are unaware of the facts.

4.4.3. Identity Revealing Attack

The malicious nodes target an authorized vehicle and reveal its real identity. Further, malicious nodes try to get personal data of users, which leads to users' privacy leakage.

4.5. Propositions

This subsection provides four different propositions along with their proofs.

Proposition 1. *A malicious node can intercept communication between vehicles. However, it cannot get significant information about the plain text from the ciphertext.*

Proof. In the proposed system, communication between vehicles is secured using encryption algorithms. Even if the malicious node can get the ciphertext, it is almost impossible for it to retrieve the plain text from the ciphertext. A private key is required for decrypting the data, which is unique and quite difficult to guess. Another way to get the plain text is to generate a new key at every iteration. However, in this case, different plain text is obtained at each iteration. Therefore, it is still quite impossible to get original plain text. □

Proposition 2. *A malicious node can send transactions to other vehicles in a network. However, it is impossible to get the signature of the authorized vehicle.*

Proof. In the proposed system, each vehicle has a unique crypto ID, which acts as a unique identification of the vehicle. IVTP is responsible for providing secure crypto IDs to vehicles. In V2V communication, vehicles communicate with each other using the crypto IDs. The complete information of the vehicle is stored in IPFS, using the unique crypto ID. The identity of the vehicle is not used by a malicious node because it does not know the original crypto ID of the vehicle. □

Proposition 3. *Suppose that a malicious node can access the data stored in IPFS. Still, it cannot tamper the data or cause the issue of single point of failure.*

Proof. In our proposed system, we used a distributed file system (IPFS) for data storage; so, it is quite impossible for a malicious node to cause the issue of single point of failure. Even if the malicious node can access IPFS, it still cannot tamper the data. All the data stored in IPFS is encrypted using symmetric key encryption. To retrieve or read the stored data, a private key is required, which is unique and cannot be guessed easily by a malicious node. Therefore, it is very difficult for a malicious node to tamper the data or to perform any malicious activity. □

Proposition 4. *PoA consensus mechanism causes privacy leakage problem. However, our system ensures privacy of the system.*

Proof. In our proposed system, we used PoA consensus mechanism; in which, a miner is selected for validation of the transactions. A group of nodes having large number of computational resources are considered as miners. Winner among this group is selected by considering its reputation value. So, there is no privacy leakage problem in our proposed system. □

4.6. Security Features of Proposed System

In this subsection, security features of our proposed model are presented.

4.6.1. Data Integrity

In our proposed system, data generated by vehicles is encrypted using symmetric key encryption. Data is stored in a distributed file system, i.e., IPFS, which returns the hash of the data stored in it. This hash is stored in blockchain, which ensures data integrity because it is not possible to tamper the data in blockchain.

4.6.2. Privacy Preservation

In our proposed system, crypto ID is used for communication between the vehicles. The real identification number of the vehicle is not used as its identity, because it leads to a privacy leakage problem. Hence, the privacy of the proposed system is preserved using the crypto IDs. All the transactions in VN are in encrypted form, which ensures data privacy. Therefore, our proposed system preserves the privacy of both data and user's identity.

4.6.3. Data Confidentiality

All the communications between vehicles are encrypted using symmetric key encryption, which makes it difficult for the malicious node to tamper the communication data. Only an authorized user has access to the encrypted data. By using an encryption mechanism, malicious activities are prevented.

4.6.4. Single Point of Failure

In our proposed system, a distributed file storage system, i.e., IPFS, is used. The file is divided into different chunks, which are stored at each node of the network. IPFS acts as a P2P network, which overcomes the problem of single point of failure. Hence, our proposed system is robust and achieves high throughput.

4.6.5. Availability

In our proposed system, data are stored in IPFS in a distributed manner. A distributed hash table is maintained against the data stored in IPFS. Whenever data are required, a request of data are sent to a specific node at which data are placed. Due to the distributed storage, the availability of data is achieved while ensuring high throughput of the system.

5. Conclusions and Future Work

In this research work, a blockchain-based resource efficient and secure data sharing mechanism for VN is proposed. A distributed file storage system (known as IPFS) is considered to tackle the issues related to a centralized storage system. To maintain the trust value of vehicles and to ensure fair payment against given services, IVTP is introduced. For each service, pre-defined amount of charges are to be paid by the ordinary nodes. We introduced blockchain technology to optimize resource utilization of the proposed network and to ensure establishment of a secure data sharing environment. Reviews given by the ordinary nodes are considered as feedback against services delivered by the edge vehicle nodes. Depending on these reviews, the reputation of each edge vehicle node is determined. The edge vehicle nodes are awarded with incentives depending upon the reviews they get from the ordinary nodes. The simulation results show that the gas consumption of the proposed system model is decreased by almost 15%–20% when using PoA instead of PoW. Moreover, it is analyzed that our proposed system provides an efficient and secure data sharing mechanism for VN. However, the tradeoff lies between the system's cost and the data size. The cost of authenticating the vehicles and storing the data increases with the increase in the size of data.

In future, a fake review detection system will be considered for ordinary vehicles, which will lead to verification of the reputation of ordinary vehicles. To find an equilibrium between a system's cost and data size, different algorithms will be designed.

Author Contributions: M.U.J. and N.J. proposed and implemented the main idea; M.U.J. and M.R. performed simulations and wrote the simulations section; N.J., A.A. and M.T. organized and refined the manuscript; M.U.J., N.J. and N.A. worked together and responded to the distinguished reviewers' comments. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Deanship of Scientific Research, King Saud University through the Vice Deanship of Scientific Research.

Acknowledgments: The authors are grateful to the Deanship of Scientific Research, King Saud University, KSA for funding through the Vice Deanship of Scientific Research Chairs.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this paper:

ABE	Attribute Based Encryption
AI	Artificial Intelligence
CSI	Channel State Information
DAC	Distributed Autonomous Corporation
D2D	Device to Device
DApps	Decentralized Applications
E-health	Electronic health
EMR	Electronic Medical Record
IDE	Integrated Development Environment
IPFS	Interplanetary File System
IoT	Internet of Things
IoV	Internet of Vehicles
IVTP	Intelligent Vehicle Trust Point
IV	Intelligent Vehicle
IDE	Integrated Development Environment
PDP	Provable Data Possession
PoA	Proof of Authority
PoW	Proof of Work
P2P	Peer to Peer
P2M	Person to Machine
PHI	Personal Health Information
SDN	Software Defined Networking
WSN	Wireless Sensor Network
V2R	Vehicle to Road Side Unit
V2V	Vehicle to Vehicle
VN	Vehicular Network

References

1. Hartenstein, H.; Laberteaux, K. *VANET: Vehicular Applications and Inter-Networking Technologies*; Wiley: Chichester, UK, 2010; Volume 1.
2. Allied Market Research. Autonomous Vehicle Market by Level of Automation. 2018. Available online: Https://www.alliedmarketresearch.com/autonomous-vehicle-market (accessed on 18 November 2019).
3. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2018. Available online: Https://bitcoin.org/bitcoin.pdf (accessed on 18 November 2019).
4. Rehman, M.; Javaid, N.; Awais, M.; Imran, M.; Naseer, N. Cloud based Secure Service Providing for IoTs using Blockchain. In Proceedings of the IEEE Global Communications Conference (GLOBCOM 2019), Waikoloa, HI, USA, 9–13 December 2019.

5. Samuel, O.; Javaid, N.; Awais, M.; Ahmed, Z.; Imran, M.; Guizani, M. A Blockchain Model for Fair Data Sharing in Deregulated Smart Grids. In Proceedings of the IEEE Global Communications Conference, Waikoloa, HI, USA, 9–13 December 2019.
6. Rehman, M.; Khan, Z.A.; Javed, M.U.; Zohaib, M.; Iftikhar, U.M.; Bux, I.; Javaid, N. A blockchain-based distributed vehicular network architecture for smart cities. In Proceedings of the International Conference on Advanced Information Networking and Applications, Caserta, CE, Italy, 15–17 April 2020.
7. Sharma, P.K.; Moon, S.Y.; Park, J.H. Block-VN: A distributed blockchain-based vehicular network architecture in smart City. *J. Inf. Process. Syst.* **2017**, *13*, 184–195.
8. Sultana, T.; Almogren, A.; Akbar, M.; Zuair, M.; Ullah, I.; Javaid, N. Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices. *Appl. Sci.* **2020**, *10*, 488. [CrossRef]
9. Xu, Y.; Wang, G.; Yang, J.; Ren, J.; Zhang, Y.; Zhang, C. Towards secure network computing services for lightweight clients using blockchain. *Wirel. Commun. Mob. Comput.* **2018**, *2018*. [CrossRef]
10. Sharma, P.K.; Park, J.H. Blockchain-based hybrid network architecture for the smart city. *Future Gener. Comput. Syst.* **2018**, *86*, 650–655. [CrossRef]
11. Qu, C.; Tao, M.; Zhang, J.; Hong, X.; Yuan, R. Blockchain-based credibility verification method for IoT entities. *Secur. Commun. Netw.* **2018**, *2018*. [CrossRef]
12. Wang, S.; Zhang, Y.; Zhang, Y. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *IEEE Access* **2018**, *6*, 38437–38450. [CrossRef]
13. Ding, S.; Cao, J.; Li, C.; Fan, K.; Li, H. A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT. *IEEE Access* **2019**, *7*, 38431–38441. [CrossRef]
14. Zhang, G.; Li, T.; Li, Y.; Hui, P.; Jin, D. Blockchain-based data sharing system for ai-powered network operations. *J. Commun. Inf. Netw.* **2018**, *3*, 1–8. [CrossRef]
15. Zhang, Y.; Wen, J. The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Netw. Appl.* **2017**, *10*, 983–994. [CrossRef]
16. Singh, M.; Kim, S. Branch based blockchain technology in intelligent vehicle. *Comput. Netw.* **2018**, *145*, 219–231. [CrossRef]
17. Jiang, T.; Fang, H.; Wang, H. Blockchain-based internet of vehicles: Distributed network architecture and performance analysis. *IEEE Internet Things J.* **2019**, *6*, 4640–4649. [CrossRef]
18. Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V.C. Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet Things J.* **2018**, *6*, 1495–1505. [CrossRef]
19. Alghamdi, T.A.; Ali, I.; Javaid, N.; Shafiq, M. Secure Service Provisioning Scheme for Lightweight IoT Devices with a Fair Payment System and an Incentive Mechanism based on Blockchain. *IEEE Access* **2019**, *8*, 1048–1061. [CrossRef]
20. Zhang, A.; Lin, X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *J. Med. Syst.* **2018**, *42*, 140. [CrossRef]
21. Ren, Y.; Liu, Y.; Ji, S.; Sangaiah, A.K.; Wang, J. Incentive mechanism of data storage based on blockchain for wireless sensor networks. *Mob. Inf. Syst.* **2018**, *2018*. [CrossRef]
22. Kushch, S.; Prieto-Castrillo, F. A rolling blockchain for a dynamic WSNs in a smart city. *arXiv* **2018**, arXiv:1806.11399.
23. Di, L.; Tang, Y. Blockchain consensus based user access strategies in D2D networks for data-intensive applications. *IEEE Access* **2018**, *6*, 72683–72690.
24. Han, S.H.; Kim, J.H.; Song, W.S.; Gim, G.Y. An empirical analysis on medical information sharing model based on blockchain. *Int. J. Adv. Comput. Res.* **2019**, *9*, 20–27. [CrossRef]
25. Wu, S.; Du, J. Electronic medical record security sharing model based on blockchain. In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, Kuala Lampur, Malaysia, 19–21 January 2019.
26. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy-preserving healthcare blockchain for iot. *Sensors* **2019**, *19*, 326. [CrossRef]

27. Naz, M.; Al-zahrani, F.A.; Khalid, R.; Javaid, N.; Qamar, A.M.; Afzal, M.K.; Shafiq, M. A secure data sharing platform using blockchain and interplanetary file system. *Sustainability* **2019**, *11*, 7054. [CrossRef]
28. Gavin, W. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.