# Blockchain-Based Adaptive Trust Management in Internet of Vehicles Using Smart Contract

Pranav Kumar Singh, *Member, IEEE*, Roshan Singh, Sunit Kumar Nandi, *Student Member, IEEE*, Kayhan Zrar Ghafoor, *Senior Member, IEEE*, Danda B. Rawat, *Senior Member, IEEE*, and Sukumar Nandi, *Senior Member, IEEE*

***Abstract*— In the Internet of Vehicles (IoV), vehicles communicate wirelessly with other vehicles, sensors, pedestrians, and roadside units. IoV is aimed at improving road safety, driving comfort, and traffic efficiency. However, IoV is exposed to a range of threats to security and privacy. The presence of dishonest and misbehaving peers in the system is of a major concern, which may put lives in danger. Thus, establishing trust among these probable untrusted vehicles is one of the most significant challenges of such a network. The critical pitfalls of existing and traditional mechanisms are scalability, a single point of failure, maintaining the quality of service, verification, and revocation and dealing with sparsity, consistency, availability, efficiency, robustness, privacy concerns are some of the biggest challenges to be addressed. Blockchain technology, with its great success in applications like cryptocurrencies and smart contracts, is considered as one of the potential candidates to build trust in IoV. In this paper, we propose a blockchain-based decentralized trust management scheme using smart contracts. Specifically, we introduce the concept of blockchain sharding for reducing the load on the main blockchain and increasing the transaction throughput. Our proposal has two key contributions: blockchain to maintain and update reliable and consistent trust values across the network and incentive scheme to encourage peers to perform well. We also conduct extensive experiments, which demonstrate the implementation feasibility of proposed mechanisms in the real world.**

***Index Terms*— IoV, trust management, smart contract, ethereum, blockchain.**

Manuscript received January 31, 2020; revised April 30, 2020; accepted June 15, 2020. This work was supported by the Information Security and Education Awareness Project-Phase II (ISEA-II at IIT Guwahati), an initiative of the Ministry of Electronics and Information Technology, Government of India. The Associate Editor for this article was Z. Lv. *(Corresponding author: Danda B. Rawat.)*

Pranav Kumar Singh is with the Department of Computer Science and Engineering, IIT Guwahati, Guwahati 781039, India, and also with the Central Institute of Technology Kokrajhar, Kokrajhar 783370, India (e-mail: snghpranav@gmail.com).

Roshan Singh is with the Open Source Intelligence Laboratory, Department of Computer Science and Engineering, IIT Guwahati, Guwahati 781039, India (e-mail: roshansingh3000@gmail.com).

Sunit Kumar Nandi is with the Department of Computer Science and Engineering, National Institute of Technology Arunachal Pradesh, Yupia 791112, India, and also with IIT Guwahati, Guwahati 781039, India (e-mail: sunitnandi834@gmail.com).

Kayhan Zrar Ghafoor is with the Department of Software Engineering, Salahaddin University-Erbil, Erbil 44002, Iraq, and also with the School of Mathematics and Computer Science, University of Wolverhampton, Wolverhampton WV1 1LY, U.K. (e-mail: kayhan@ieee.org).

Danda B. Rawat is with the Department of Electrical Engineering and Computer Science, Howard University, Washington, DC 20059 USA (e-mail: db.rawat@ieee.org).

Sukumar Nandi is with the Department of Computer Science and Engineering, IIT Guwahati, Guwahati 781039, India (e-mail: sukumar@iitg.ac.in).

Digital Object Identifier 10.1109/TITS.2020.3004041

## I. Introduction

THE Internet-of-Vehicles (IoV) is now on the verge of deployment in the real world because of various advancements in radio access, core network, and automotive technologies [1], [2]. Vehicles nowadays are equipped with powerful sensors, communication, storage, and computational capabilities. The three main radio access technologies, which are being integrated with the vehicles are Dedicated Short Range Communication (DSRC), cellular and Wi-Fi [3], [4]. DSRC is the key radio technology used for vehicular communication in the USA and Europe [5]. Cooperative Intelligent Transportation Systems (C-ITS) [6] in Europe and Wireless Access in Vehicle Environments (WAVE) [7] in the USA are two well-known protocol stacks developed for vehicular communications and use DSRC at the physical layer [8]. IoV allows communication not only between Vehicle-to-Vehicle (V2V) but also between Vehicle-to-Infrastructure (V2I) and facilitates a variety of safety and non-safety applications. The safety applications can be of type collision warning, spot warning, intersection movement assistant, work-zone warning, etc. It also allows vehicles to share information about traffic and road conditions with their neighbors. The non-safety applications are mainly related to mobility (route guidance, traffic updates, navigation, etc.), and infotainment (streaming, VoIP, media download, etc.) [9].

All the messages related to safety applications are broadcasted over the control channel (CCH) of the DSRC via V2V communication, which can be of type periodic beacons or event-based alarms. Cooperative Awareness Message (CAM) in Europe and Basic Safety Message (BSM) in the USA are the two popular safety messages which are broadcasted periodically for safety and awareness [10]. The decentralized environmental notification message (DENM) [11] is an event-driven message which is transmitted to notify some hazards or warning such as road accidents. In IoV, when a vehicle receives a DENM for some incident, it uses the information to avoid an unwanted situation such as accident, congestion, or some dangerous situation by effectively reacting to it. Consequently, the reliability and trustworthiness of the received messages are of paramount significance as the

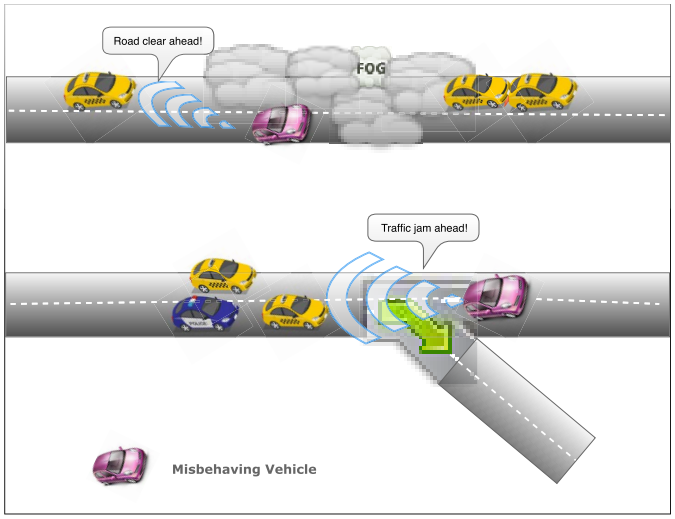



Fig. 1. Example scenarios of misbehavior in IoV.

system's acceptance and efficacy depend on them because they can affect driving decisions, and any wrong decision can have disastrous consequences.

Fig. 1 demonstrates misbehavior scenario in IoV. A malicious or misbehaving vehicle in low visibility conditions can send a fake message (using the protocol semantics) to other vehicles and conveys that the road ahead is clear while there is a road accident. Similarly, it can also generate a fake message claiming that there is traffic congestion ahead. Such misbehaviors can lead to catastrophic situations, reduce traffic efficiency, and as a whole lower the trust level on IoV.

Trust management in IoV implements the reputation of vehicles based on both the trust value scored from its past behavior (reputation) and neighbors opinion about the received message broadcasted by the alarmer vehicle for an event. Trust management can also facilitate incentives mechanism for the peers who behave well in the system and have earned a better trust score. There can be punishments for the dishonest or misbehaving peers in terms of trust score reduction and revocation after a certain limit of misbehavior is crossed or defined threshold has been reached [12].

Different trust management systems proposed for IoV fall into the following two classifications: centralized and decentralized. There are a fair amount of works available in both categories, which are discussed in Section II. However, the key pitfalls of existing works in these categories are as follows. In the centralized approach, trust management is done on the central server; therefore, scalability, single point of failure, maintaining the quality of service, verification, and revocation are some of the most significant challenges. In the decentralized approach, trust management is performed either at the vehicular plane or the roadside unit (RSU) plane. However, dealing with sparsity, consistency, availability, efficiency, robustness, privacy concerns [13], and faults at the RSU plane remain open issues in the decentralized approach.

The blockchain is one of the disruptive technology in the financial industry, first proposed as the underlying technology for Bitcoin by Satoshi Nakamoto in 2008 [14]. Blockchain has become one of the driving forces of industrial IoT or Industry 4.0 [15], [16]. It is attracting a lot of attention from industries, academia, and research organizations. Its remarkable features such as high security (Merkel tree, hash function), decentralization, consensus (Proof of Work (PoW)), consistency, and reliability make it one of the potential candidates for establishing and managing the trust model in IoV [17].

In the literature (Section II), there are blockchain-based works proposed for solving trust management and privacy-related issues in IoV. However, addressing the scalability issue of the blockchain used remains a significant concern while implementing it in IoV. Our work is an extension of existing work, where we introduce the concept of sharing to solve the scalability problem while managing trust in the IoV. Our framework is adaptive because it can be integrated with various existing misbehavior detection strategies (discussed in the literature) for trust management and also establish the process of revocation of misbehaving vehicles in IoV.

In this paper, we propose a blockchain-based decentralized trust management system for IoV. The primary goal of the proposed mechanism is effective trust establishment and management in a distributed fashion. The main contributions of this paper are as follows:

- We propose a scheme for trust management at the edge, i.e., at the roadside units (RSU) plane of IoV, which is decentralized in nature and based on the blockchain technology. RSUs at the edge collaboratively maintain vehicle trust values that are updated, reliable, and consistent, helping to accomplish our objective in a decentralized manner.
- We incorporate the idea of shards for reducing the workloads from the main maintained blockchain.
- We use an open-source platform, Ethereum blockchain [18], that facilitates smart contracts to demonstrate the feasibility of implementation and strength of our proposed decentralized trust management strategy.

The outline of the rest of the paper is as follows. Section II present the survey on various techniques of trust management used in a vehicular network. Section III presents the detail of the system framework consisting of the architecture and system model. In Section IV, we discuss the details of our basics of the blockchain platform of trust management in IoV. Experiment details, case study algorithms are present in Section V. The obtained results and discussion about it are present in Section VI. Finally, Section VII presents the final conclusion.

## II. Related Work

As illustrated in Fig. 2, research studies on trust models that include misbehavior detection in vehicular networks can be classified into three types [12], [19]: data-centric, entity-centric, and hybrid or combined. Similarly, deployment strategies for trust management can be broadly categorized into centralized and decentralized types.

### A. Trust Models

Data-centric trust models concentrate on data trust calculation, while entity-centered trust models focus on a vehicle's

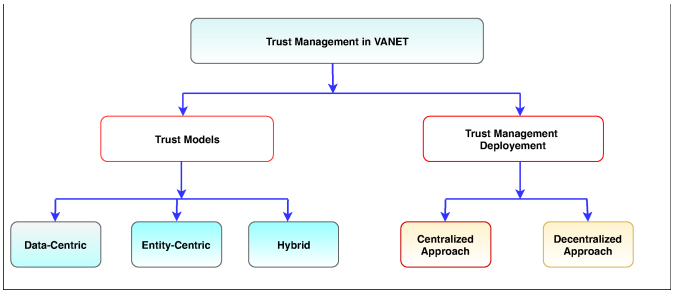



Fig. 2. Trust management in vehicular networks.

trustworthiness computations. The characteristics of both data-centric and entity-centric are combined in hybrid trust models to assess the trust of a vehicle (entity) and the information (data) it transmits [20].

*1) Data-Centric:* In this approach, the trustworthiness of data in terms of correctness, authenticity, and accuracy is computed. Since data plays a crucial role in such networks, it is assessed for trustworthiness before propagating it to others. Trust models using the data-centric approach are often based on the context of the event and considers location and time proximity, reports of the same event, and event types. Raya *et al.* have identified five popular techniques for data-centric trust models [21]: Most Trusted Report (MTR), Weighted Voting (WV), Majority Voting (MV), Bayesian Inference (BI), and the Dempster-Shafer Theory (DST).

Various research studies [21]–[26] exist in the literature that uses data-centric trust models in a vehicular network, each having their strength and weaknesses. However, the common deficiency is that making a trust decision takes a longer time. Two other major concerns are flooding of duplicate data in dense traffic conditions, and performance issues in sparse traffic conditions.

*2) Entity-Centric:* In this approach, the trustworthiness of entities (vehicles) plays a major role rather than the data. In vehicular networks, the trustworthiness of the entities has been considered as the basis for secure routing and reliable data delivery. There exist various entity-centric trust models in the literature that evaluate trustworthiness using the following methods: multifaceted approach (experience, role, priority and majority opinion) [27], infrastructure-based trust and reputation approach (recommendation given by vehicles and RSUs) [28], cluster-oriented approach [29], dynamic entity-centric trust based on weight (application data and node) [30], etc.

Three critical issues associated with entity-centric trust models are: First, this model does not consider the data for assessing the trust, which is an essential object. Thus, even if the transmitter is trustworthy, the correctness of received data in the presence of attackers remains uncertain. Secondly, it can perform well in low mobility and high vehicle density scenarios. Still, in high mobility and sparse traffic conditions, it may fail to obtain adequate data necessary for trust assessment. Third, this model depends heavily on the central authority to verify trust, which is the bottleneck. For example, in the case of role-based trust models [27].

*3) Hybrid:* Hybrid trust models utilize vehicles' trust to assess data trustworthiness. In other words, both the data and entity are considered as the main objects in vehicular networks. Trust assessment is performed on the basis of the trustworthiness of the vehicles and the data they exchange. In the literature, very few hybrid trust models based proposals are available, which are as follows.

A beacon-based trust management system (BTM) was proposed in [31] to prevent sending false messages by internal attackers. With their proposed trust models, authors have also tried to preserve location privacy in VANET. The authors proposed a trust model in [32] that evaluates message trustworthiness in the presence of Sybil and packet duplication attacks. In [33], the authors proposed a hybrid trust model, where data trust is achieved through multiple vehicle data collection and entity trust via recommendation and functional approach.

Since this model covers both the data and entity trust, it also inherits most of the challenges associated with those two models. The complexity of implementing existing hybrid trust models is very high because a significant amount of messages need to be exchanged for data and entity trust assessment.

To summarize this section, we see that there are various data-centric and node-centric mechanisms present in the literature; however, there are multiple challenges associated with them, such as detection delay, overhead in communication, oversampling, and cascading, etc.

### *B. Trust Management Architecture*

In vehicular networks, trust management architecture can either be centralized or decentralized. This relies on how trust models were implemented to establish trust, manage reputation, store, update, evaluate, verify, propagate it, etc.

*1) Centralized Trust Management:* In a centralized architecture, a central trusted entity or server deployed in a secure zone is responsible for trust management, for example, a trusted third party deployed in a PKI-based security framework of the vehicular network. Trust management schemes based on a centralized approach have been proposed in [34]–[38].

In [34], the authors proposed TRIP, a novel mechanism to counter the attacks of dropping rational and irrational packets. TRIP is stimulation and punishment-based strategies for mobile nodes. Most of the processes of the proposed mechanism, such as receipts session processing, credit account update, state update, and eviction of a malicious node, are executed at a centralized trusted third party end. In [35], the authors proposed a centralized evaluation entity that processes locally created misbehavior reports of the vehicular and RSU plane. The central entity uses the reputation and trust information present in received reports to ensure the long-term functionality of the system.

Li *et al.* [36] proposed a reputation system-based announcement scheme. The sensed data for traffic-related events are announced to neighbors by the vehicles. These messages are evaluated for their credibility and generated feedback reports uploaded to the centralized entity for reputation updates. In [37], authors proposed a reputation-based global trust establishment (RGTE) scheme for VANETs. This scheme

allows for sharing the trust information safely by applying statistical laws. There is a centralized reputation management center (RMC) which gathers trust from all authorized nodes. It calculates the reputation of a vehicle but first filters out any suspicious trust messages.

In general, the schemes mentioned above need to have a centralized reputation management server to evaluate trust, establish a global reputation, and implement incentive strategies. However, such centralized trust management systems are impractical for a highly dynamic network like VANETs. For such systems, it is challenging to deal with scalability, fault-tolerance, robustness, performance, and security-related issues.

*2) Decentralized Trust Management:* Various research studies have introduced a decentralized system for trust management to address the challenges associated with the above-mentioned centralized mechanisms.

The data-centric trust model introduced by Gurung *et al.* [24] relied on a decentralized approach: the trustworthiness of the message is evaluated in the vehicular plane without the need for any additional centralized architecture. The proposed model takes into account factors such as similarity of content, the similarity of the route, and conflict of content. Huang *et al.* [25], in its data-centric approach, used the voting-based system in a vehicular plane.

In 2016, the authors [39] proposed a conditional probability-based approach to detect malevolent vehicles at the vehicular plane. In this approach, the generated rating for a particular event is uploaded to the nearby RSU to maintain the trust information at the RSU plane. In the same line of thought, the authors [40] proposed the Distributed Reputation Management System (DREAMS) and introduced Vehicular Edge Computing (VEC) to execute vehicle reputation management functions (maintenance, manifestation, update, and usage) locally.

*3) Blockchain Related Work:* There are works [41], [42] published in 2018: In [41], the authors proposed a trust model from data-centric category and decentralized trust management using blockchain for vehicular networks. They used the Bayesian Inference model to assess the trustworthiness of the messages received from neighboring peers. Vehicles periodically upload the generated rating for each origin vehicle to the nearby RSU. The trust value offset is calculated at the RSU, and then block formation is done and finally added to the blockchain maintained in the RSU plane. Using this strategy, RSUs work together to maintain a blockchain that is reliable and consistent. The authors demonstrated the efficacy and feasibility of the proposed approach with the help of simulation. In [42], the authors proposed an anonymous reputation system based on blockchain (BARS) to establish trust and preserve privacy in VANETs simultaneously. In [43], authors propose an intelligent vehicle trust point system for vehicle communication using vehicular cloud computing and blockchain technologies. Authors demonstrate a use-case of the approach implementation along-with reward allocation in a road intersection scenario. Proof-of-Driving (PoD) was used as a consensus mechanism at the vehicular plane to reach the consensus among the vehicles. The algorithm requires validation from 50% of the vehicles within the network for a message to be accepted. However, the work does not emphasize much on the internal aspects of the maintained blockchain at the RSU plane, such as the node characteristics, transaction types, and the blockchain consensus mechanism to be used. In [44], the authors proposed a blockchain-based data sharing and trust management system in VANETs. The approach uses two smart contracts, one for interactions between RSUs and intelligent vehicles, while the other one is used for storing and retrieving data from the blockchain. A PUF (Physically Unclonable Function) was used for generating and assigning a unique ID to the vehicles.

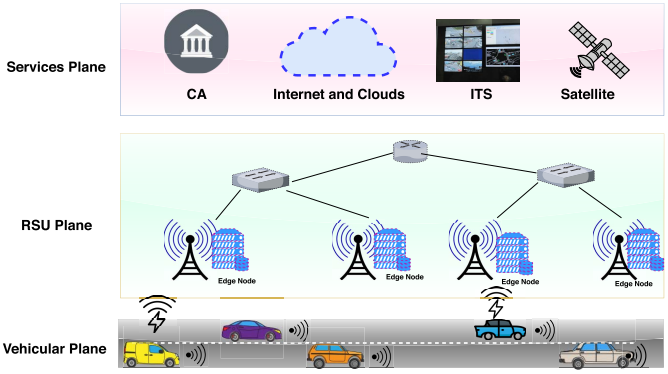



Fig. 3. IoV system architecture.

To summarize this section, we saw a variety of centralized and decentralized trust management systems intended to ensure trust management for IoV. To this end, our work is such a contribution, and not only we propose a unique solution, but we also test it on a testbed to demonstrate its effectiveness and feasibility in the real world. With the introduction of a public blockchain, we aim to make the system decentralized, thus increasing the availability and enhancing the security of the system. Moreover, we introduce the novel idea of sharding that increases the transaction throughput of the blockchain network.

## III. System Model

We formalize the IoV architecture in this section and discuss the key entities of the system.

### A. Architecture

Fig. 3 shows the IoV architecture having three vital planes [45]: vehicular plane, set of RSUs as Edge Computing plane (to facilitate blockchain), and central services plane. The central services plane includes certificate authority (CA), ITS services, Internet services, cloud-based services [46], etc.

### B. Key Entities

- **Roadside Units (RSUs):**
  In our proposed scheme, we considered the flourished stage of IoV, where RSUs are equipped with powerful computing and storage capacity, reliable and secured backhaul links to service plane, sensors, and secure wireless communication technologies for V2I/I2V connectivity. We can refer to it as the edge node, which can

facilitate required caching, storage, communication, and computation to our proposed blockchain-based mechanism. It is also responsible for updating vehicle categories based on their sensing capacity, profile, and past behavior.

- **Vehicles:** Vehicles in the IoV are equipped with an on-board unit (OBU) that runs WAVE protocol stacks for vehicular communication. OBUs of the vehicles have communication, computation, storage, and navigation capabilities. We call them intelligent vehicles.
- **Traffic Authority (TA):** TA is the supreme authority and plays a crucial role in IoV as doing the registration of the vehicles and deployment of the Regional Authorities. TA collects the information from the vehicles and issues them certificates via the Certificate Authority. It also assigns initial trust value to the registered vehicles. In any system, there is always a hierarchy of trust levels. Vehicles can earn trust value by performing well. Vehicles who behave badly in the network are put into the Misbehaving Vehicle (MV) category.
- **Certificate Authority (CA):** CA uses the collected credentials and information of the vehicles by the TA registration and issues them certificates (certified keys) for communications security and privacy. The role of CA is defined in detail in [47].
- **Regional Authority:** The entire vehicular environment is divided into a number of regions based upon the geo-locations. RA works in accordance with the TA and is responsible for deploying and maintaining the infrastructure in its territory. RA is also responsible for providing vehicles entering its territory with a set of short term keys for communications within the territory.
  Note: The trust value is dynamic and may increase or decrease based on their behavior in the network.

## IV. Framework for Trust Management

Vehicles at the vehicular plane participate in a number of events at the vehicular plane. For each event, a vehicle exchanges a number of messages with its peers. A vehicle checks for the integrity and authenticity of each message received for an event. If any inconsistencies in the messages are detected, it is reported to the RSU for action. The RSUs are edge nodes in our IoV framework and are capable of running a distributed consensus of blockchain for trust management. Based on the smart contract logic that we deployed, RSUs execute the operation and update the trust score of vehicles depending on their behavior. More details about the mechanism, platform, implementation are given in subsequent sections.

### *A. Blockchain Platform for Trust Management*

A blockchain is a decentralized, distributed, unalterable, and append-only ledger that guarantees transparency in the chain's transactions. Blockchain can be used as a platform to build trust among untrusted parties. It facilitates storing the state in a distributed fashion among nodes of the network and continues to exist as long as a network of nodes exists [48]. We propose a decentralized system for trust management in IoV, taking into account the core concepts of the blockchain. The core contribution of our work is designing, implementing, and evaluating an application using smart contracts for trust management in IoV. Before providing details of implementation, we provide an abstract overview of the smart contract, and ethereum platform and discuss some key features of the blockchain.

### *B. Sharding in Blockchain*

The current blockchain-based system with Proof-of-Work as the consensus mechanism faces the problem of scalability. The two most popular public blockchain platform Bitcoin and Ethereum has an average transaction throughput of 8 txps(transactions per second) and 15 txps, respectively. In contrast, its counterpart VISA offers transaction throughput of around 1700 txps. Blockchain sharding is an upcoming blockchain research domain that aims at improving the blockchain scalability in terms of transaction throughput by dividing the transaction loads on the full blockchain into several sub blockchains where each sub blockchain maintains a localized set of transactions. In blockchain sharding, the entire blockchain network is divided into some shards. A shard is a sub blockchain maintained by a subset of nodes, also known as the committees from the global blockchain network. Each shard collects and processes a disjoint set of transactions. A shard is maintained by a committee of $k$ members. Generally, $k$ is significantly small in number as compared to the participants in the global blockchain network. Having a smaller $k$ facilitates to execute BFT based consensus algorithms; however, challenge-response based consensus algorithms can also be used here. Smaller $k$ also facilitates better use of network bandwidth for propagating the blocks as the committee members are mostly localized.

### *C. Smart Contract*

A smart contract is a component of blockchain 2.0 that extends the capability of the earlier use-case specific blockchain, by allowing code snippets defining business logic to be deployed on top of the blockchain. The smart contract ensures fraud-free contract execution without any trusted third party. It is a programmed logic having a predefined set of rules [49]. It enables users to execute a script in a verifiable manner on a blockchain network and enables several issues to be solved in a way that minimizes the need for trust. In essence, smart contract functions as an autonomous entity on the blockchain and can execute logic deterministically as a function of the data provided to the blockchain.

### *D. Ethereum Platform*

Ethereum is an open-source blockchain platform that supports smart contracts. The platform facilitates the use of various programming languages to write the smart contract [18]. These smarts contracts can be converted into bytecode and are executed on Ethereum Virtual Machine (EVM). Ethereum facilitates the execution of its private and permissioned blockchain instance. In such an instance, only peers that are

allowed to enter the network can view transaction data. Among those, only nodes that are granted special rights can participate in the mining.

*1) Ethereum Blockchain Accounts:* An entity holding an internal state is associated with an account in Ethereum. Ethereum distinguishes between two kinds of accounts, accounts owned externally and contract accounts. An externally owned account contains a private key making it a personal account. The key owner can send transactions to other externally held accounts or contract accounts from his/her account.

### E. Features

*1) Decentralization:* Decentralization is one of the primary objectives of blockchain technology. Blockchain inherently keeps its data stored in multiple copies over multiple geographical locations making it highly available and lowering any successful attempts to the modification of on chained data. It will require a malicious entity to have a hold on at least 51% of computing power in the blockchain network to execute a data alteration attempt successfully [50].

*2) Irreversibility and Immutability:* Transactions once recorded in the blockchain cannot be reversed. The immutability property of the transactions recorded on the chain increases with each successive block being added in the chain. Once committed, the transactions can not be altered.

*3) Digital Signature:* Digital Signature is a facility provided by Public Key Infrastructure(PKI) that allows a party to prove the authenticity of data. Data is digitally signed by the sender party with their private key and is verified by the receiving party by the globally available public key of the sender. Each transaction in the blockchain network is digitally signed by the executor's private key and is verified by the miners with the available executor's public key ensuring non-repudiation against the execution of the transaction. The elliptic curve digital signature algorithm (ECDSA) is the standard algorithm used in blockchain [51].

## V. Experiment and Case Study

This section provides the experimental details of our blockchain-based approach to trust management.

### A. Trust Management Using Blockchain

In this section, we include details of the blockchain-based trust management module proposed at the edge nodes (RSU plane) of the IoV framework. Our proposed blockchain-based framework for trust management is shown in Fig. 4.

### B. Initialization

The initialization processes of our system are as follows:

*1) Responsibility Assignment and Infrastructure Setup:* The Traffic Authority initializes the system by deploying a Certificate Authority and assigning a number of Regional Authorities in IoV. Once the regional authorities are assigned by the TA, each regional authority deploys the necessary infrastructures such as the RSUs for the functioning of the IoV. The maintenance and control of a territory's infrastructure is the exclusive responsibility of the Regional Authority concerned.

*2) Vehicle Registration:* A vehicle($V$) generates its temporary public

$$PU_t^v$$

and private

$$PR_t^v$$

key and send it to the Traffic Authority (TA).

$$SEND[E(PU_t^{TA}, details|PU_t^v)]$$

. The TA after verifying the details generate a pseudonym for the vehicle

$$V_{pseudo}$$

and SEND it to the Certificate Authority CA,

$$SEND[V_{pseudo}]$$

if the details are found to be valid and authentic. CA generates a certificate

$$Certificate^V$$

for the received

$$V_{pseudo},$$

signs and writes the public key onto the ***globalBC*** (global blockchain) denoting it to be a valid public key and sends

$$Certificate^V$$

to the TA. The TA passes the certificate to the $\boldsymbol{V}$ further by-

$$SEND[E(PU_t^v, Certificate^V)]$$

The mapping of the

$$V_{pseudo}$$

to the actual identity of the vehicle $V$ lies with the TA only. The sequence diagram for obtaining a certificate by $\boldsymbol{V}$ is shown in Fig. 5.

*3) Short Term Key Distribution by Regional Authorities:* Whenever a vehicle passes through different regions, the vehicle is provided with a set of short term key pairs valid for that region only based upon the information available from the public blockchain. The Regional Authority gets the Trust Value of the vehicle and Wallet Score and stores these values against the temporary allocated address of the vehicle onto the local blockchain within the region. All the communications within that region take place with those sets of local key pairs only. When the vehicle is set to leave the region, it executes a transaction when the transaction gets minted onto the sharded blockchain. The Regional Authority executes a global transaction against the permanent public address of the vehicle that updates the score value of the vehicle on the ***globalBC*** (global blockchain).

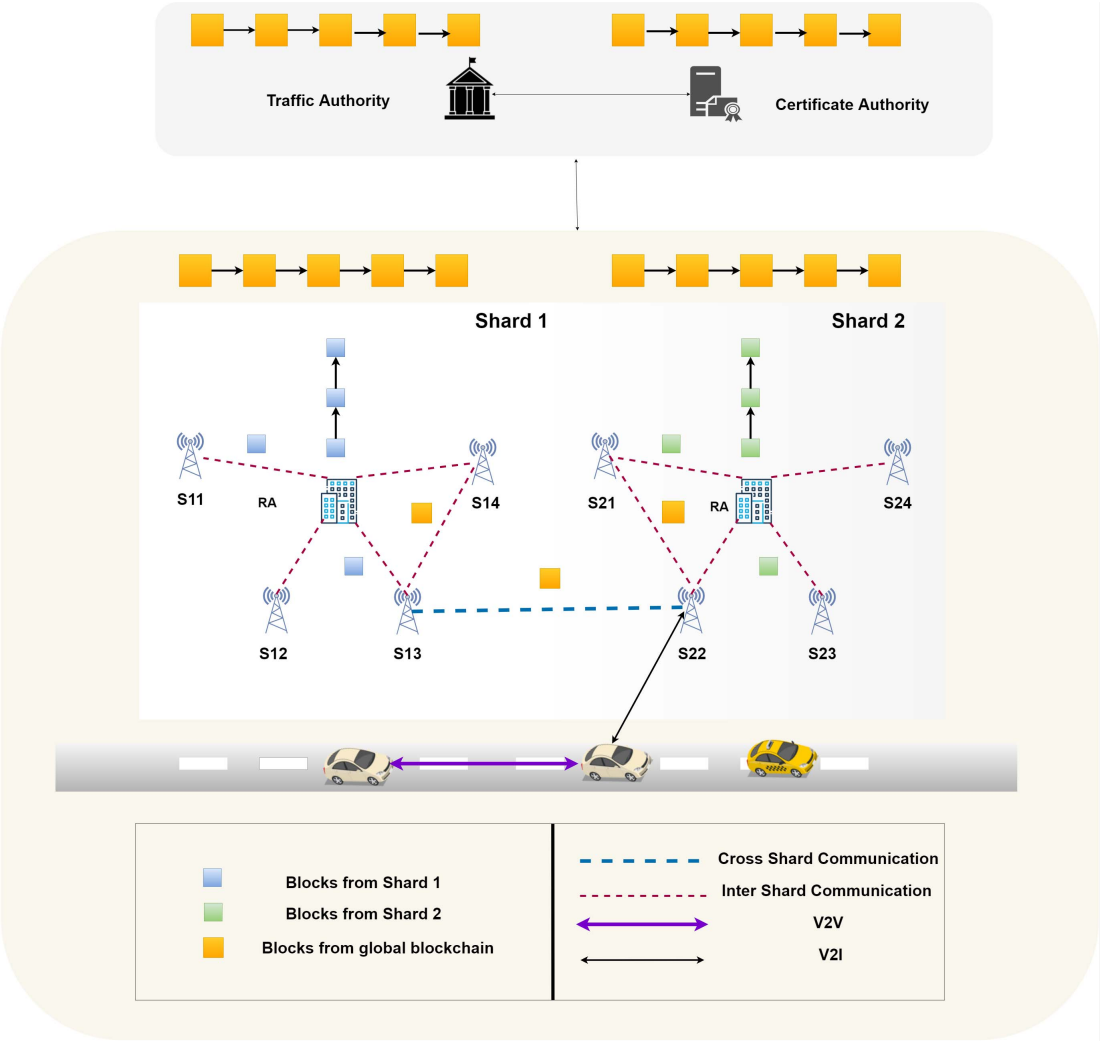



Fig. 4. Proposed blockchain based framework for trust management.

*4) Blockchain Setup:* In our system of IoV, we propose to set up a global blockchain along with that we propose to set up the localized blockchain, also known as shards at various places, for improving the transaction throughput. The global blockchain is maintained by the TA, CA, and the RA in the IoV and is open and decentralized. Because of the open and permissionless nature of participants of the blockchain network, the blockchain use PoW(Proof-of-Work) as the consensus mechanism. The true sense of decentralization of the global blockchain comes with the notion of allowing the participation of the RAs along-with the TA and the CA. As an RA is free to deploy its infrastructure or the RSUs, it gives the RAs the freedom to deploy as many infrastructures as per its need and capacity, hence increasing the difficulty of competition. An RA can decide the amount of computational allowable for the mining as per its flexibility. Whereas, each RA maintains a blockchain shard for processing the localized transactions generated in its territory. The responsibility of maintaining the localized blockchain lies with the RA and the infrastructure deployed in its territory. Due to the nature of being permissioned and closed, it is possible to execute an authoritative consensus mechanism within the localized blockchain network or the shard.

We propose to implement the following authoritative module in our work:

A shard exists in each territory. The maintenance of the shard lies with the RA and its deployed infrastructure; the RSUs. We choose to use an authoritative consensus mechanism in the shard. Our authoritative consensus mechanism lies with a set of validators in our case, the RA and its RSUs. The RA is the initial validator and is authorized to allocate and deallocate the validation right to its RSUs. The consensus is achieved in rounds, where in each round, a validator proposes a block with the localized transactions coming from the shard. Other validators in the shard check for the authenticity and validity of the block and accept and add the block to the blockchain if it is found valid. In the event that a block is found invalid, validators in the shard call to vote against the faulty validator, and if a majority votes against the validator, the validator is removed from the list.

*5) Prototype: Testbed:* Fig. 6 illustrates the prototype (6a) and our testbed setup (6b) corresponding to it that contains

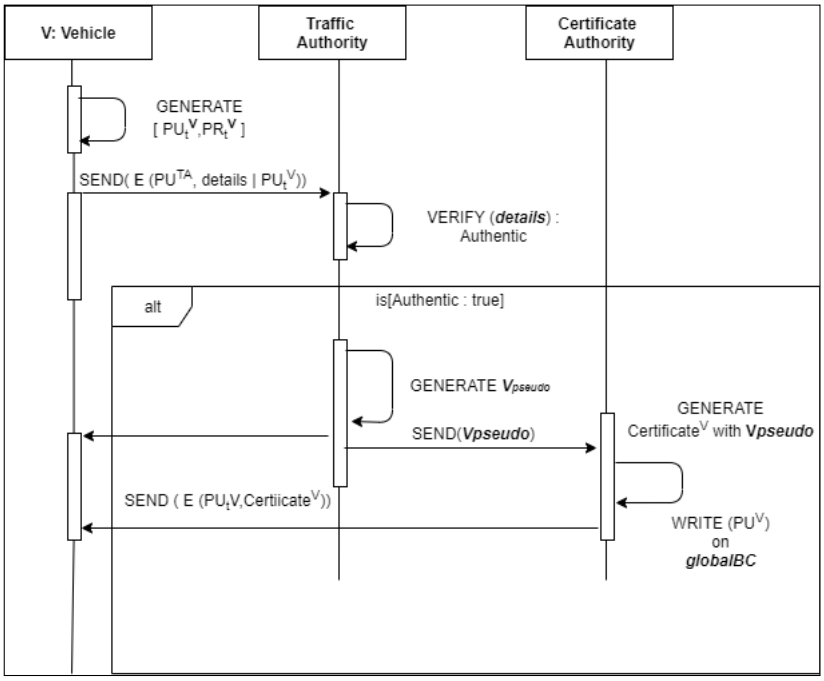
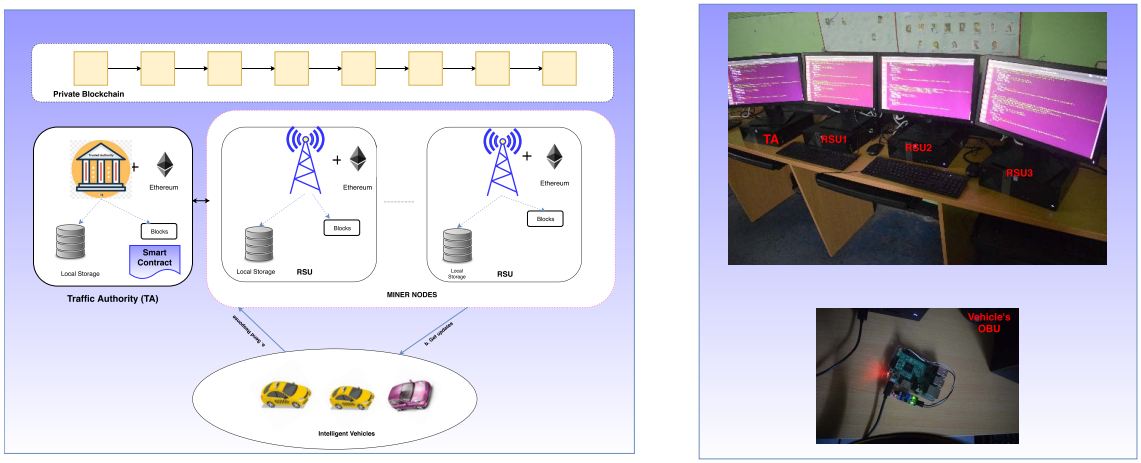



Fig. 5. Sequence diagram for obtaining certificate.




(a) Blockchain Prototype of IoV

(b) Testbed Setup

Fig. 6. Prototype and testbed setup of private blockchain for trust management in IoV.

various entities of the proposed blockchain framework for trust management in IoV. The experiment demonstrates the maintainance of the ***globalBC***.

To implement our decentralized approach using a smart contract, we use a private permissioned Ethereum blockchain [52]. Private blockchain handles the flow of data based on the TA's specified and deployed smart contract or authorized policies. We use the cryptocurrency ether, which is provided in the core of the ethereum client as a medium of exchange. Credit scores earned by the *intelligentVehicles* can be redeemed as the ether, which can be utilized by them for accessing various ITS related services.

The network proposed consists of three node types: full nodes, light nodes, and miner nodes.

**i) Full Node:** A full node is a node that has the complete blockchain downloaded and available on the network. A full node fully enforces all of the rules of the blockchain.

**ii) Light Node:** A light node does not maintain an entire ledger of records on the blockchain; however, it gets the information of its interest from its peer trusted full nodes. This facilitates low capacity end devices to participate in the blockchain network without downloading an entire copy of the chain locally. The trusted peer nodes act as an endpoint for the light nodes.

**iii) Miners:** Miners are the maintainers of a blockchain network that hold a full copy of the blockchain and are responsible for verifying the validity and authenticity of each incoming transaction in the network. They execute

computationally expensive mathematical operations, also known as mining, prior to adding a block onto the chain.

In our private blockchain, the TA is a full node which may act as a miner or may not. The RSUs acts as a miner, whereas the vehicles are considered to be light nodes. Miners and full are preferred to be always active.

The testbed details are as follows: All PCs are of hardware configuration CPU: Intel $Core^{TM}$ i7-7700 3.60GHz, 8 GB RAM, the hard drive of 1 TB and running OS Ubuntu 18.04.1 LTS. Each full node, including the TA run Ethereum's geth 1.8.17-stable client. We used 4 PCs with the above configurations, out of which one takes the role of TA, and the other three are RSUs. We use Raspberry Pi 3.3 PC as an OBUs of vehicles. They report about the misbehavior detection to one of the RSU. Raspberry Pi 3 also runs Ethereum's geth 1.8.18 ARMv7 stable release and can work as a light node for executing the transactions. Raspberry Pi 3 node interacts with the RSU in wireless infrastructure mode. The backbone connectivity of TA and RSUs are wired network. For writing and compiling the contract, we used the Remix integrated development environment(IDE) and for Solidity, a browser-based IDE.

We conducted testbed experiments where the Raspberry Pi 3 node (vehicle) sends a set of the transaction of type *reportSuspicion* to our private blockchain platform in an asynchronous manner, i.e., all transactions are transmitted without waiting for a blockchain response. We implemented it to create the scenario of multiple vehicles reporting about the misbehavior to RSU after local detection. The no. of requests was set to 1, 100, 500, 750, and 1000. The obtained experimental results averaged over three independent runs. The transactions are placed in a javascript file and executed from the Raspberry Pi 3 light node. The interaction between the nodes in the private blockchain is accomplished with HTTP connections and web3.js and node.js API.

*6) Main Procedure:* We considered the use case of earning reputation by a vehicle through their contribution to misbehavior detection. An intelligent vehicle participates in various events at the vehicular plane. For an event, a set of messages are exchanged between an event generating intelligent vehicle and other intelligent vehicles in its range.

**Step 1 Transaction collection and Validation:** Vehicles participating in the event checks the validity (authenticity and integrity) of the received message. We assume that the intelligent vehicles are running sophisticated models that help them to detect the truthfulness of the received messages in the vehicular plane.

**Step 2 Report Suspicion:** An intelligent vehicle reports suspicious behavior from its peer vehicles by analyzing their responses to an event. An intelligent vehicle reports the suspicion by calling *reportSuspicion*, which in turn results in a transaction.

**Step 3 Block Sealing:** RSUs in the region upon receiving the transactions checks the validity of the transaction and seal the transaction in a block, which is eventually committed onto the sharded blockchain.

**Step 4 Report Analysis by the RSU:** RSUs at some random interval of time execute the *analyseReports* function. By executing the function, RSU checks for the correctness of the claim by an intelligent vehicle against another, suspecting it of a misbehaving one. Since the RSUs execute these functions at certain random duration, the duration should be such that by the time an RSU calls the function, all the transactions from that event have got mined into some blocks and are added to the blockchain. After the execution of the function, the suspecting vehicle gets punished if the claim turns out to be true, and the reporting vehicles get rewarded for their contribution.

**Step 5 Mining:** The RSUs at the RSU Plane receives the transactions corresponding to the ***globalBC*** and checks for its validity. RSUs acting as miner nodes bundle these received transactions together to form a block and perform a rigorous Proof-of-Work to get the block on the blockchain. Upon finding a block, a miner broadcasts the block to his peers. Since all the nodes in the network agree on this block, a consensus is reached, and that block is added to the blockchain.

**Step 6 Claim of Reward by the vehicles:** Once the RSU analyses the responses for an event and the reporting turns out to be true. Then the participating vehicles who honestly reported for the event can claim the rewards by calling *claimReward*. A vehicle needs to claim its reward from any previous event before participating in the next event.

**Step 7 Vehicle leave from a region:** In case a vehicle leaves a region and tries to enter another region, it executes a `LEAVE-REGION` transaction.

Once the transaction is successfully minted onto the local blockchain maintained in the region, the RA executes a transaction that updates the score values on the global blockchain taking the current values of the Trust Value and Wallet Score from the Smart Contract. The RA maps the temporary credentials of the leaving vehicle to its actual permanent address thus updating the score values of the leaving vehicle *V*.

*7) Preliminaries:* In our blockchain framework of trust management, the Trusted Authority governs the deployment of the smart contracts. Each Regional Authority(RA) deploys the same version of the smart contract, as mentioned by the TA. The RA puts the hash of each of the deployed smart contracts onto the public blockchain. Thus, a vehicle before interacting with the smart contract in a RA can verify the credibility of the contract. Road Side Units (RSUs) are configured and added to the blockchain by the TA calling *configureRSU*. The RSUs are the entity responsible for analyzing the reports. TA is also responsible for adding new vehicles into the system by calling *configureVEH*. At the time of registration, the TA provides the vehicle with a set of private/public key pairs before it enters the road. This can be done within an authoritative domain.

The vehicles registered to the system are termed as *intelligentVehicle* in our smart contract analogy. An *intelligentVehicle* senses from its environment and participates in various events at the vehicular plane. In each event, a set of messages are exchanged among the vehicles many of these messages are incorrect and are generated from the misbehaving vehicles. Each event has a unique id, which we term as the session in our smart contract analogy. An *intelligentVehicle* reports about any suspicious activity on the road by calling *reportSuspicion.*

Before calling *reportSuspicion* an *intelligentVehicle* checks for any unclaimed rewards that it has earned for participating in some earlier reporting. If yes, then it calls *claimReward* and claims the reward. The RSUs call *analyseReports* with an arbitrary interval of time to analyze the reports given by a set of vehicles for a particular session.

The smart contract maintains a set of registers with the help of mappings provided in solidity, a mapping is a hash table, which consists of key types and value type pairs.

- **Personal Transaction Register (PTR):** It keeps track of the information of the vehicle participating in a reporting session, the reporting that they make, and the status of the rewards to be received by them.
- **Score and Status Register (SSR):** It maintains the score of the reported vehicle from a session and also the verification status of those reports by the RSU.
- **Vehicle Register (VR):** VR maintains the information specific to a vehicle, such as an account no., credit score, trust value (TV), revocation status, claimed rewards and rewards yet to claimed.
- **Session Register (sessionRegister):** sessionRegister stores all the necessary information corresponding to a session such as total no. of vehicles participated, addresses of participating vehicles, address of alarmer vehicle (i.e., the first vehicle reporting a particular session), vehicle enrollment status (i.e., whether or not a vehicle is already enrolled in the session).
- **Vehicle in Session Register (VISR) and Claimable Reward Register (CR):** VISR is used by the report analyzing entities at the time of analyzing the reports. CR keeps track of all the vehicles which are eligible for getting a reward for their participation in the certain session.

*8) Access Rights and Other Logics:* We provide appropriate access modifiers in the smart contract restricting a set of entities to execute certain functionalities of the contract. Like only an *intelligentVehicle* can call *reportSuspicion*. Similarly, only the TA can call *configureRSU* and only the RSUs can call *analyseReports*. The snippet of modifiers that we implemented in the smart contract for various access rights are shown in Fig. 7.

```
modifier intelligentVehicle(address _acno){
    bool is_VEH_intelligent = false;
        if(VR[_acno].acno == _acno){
            is_VEH_intelligent = true;
        }
        require(is_VEH_intelligent == true,"Not an Intelligent Vehicle");
        _;
}

modifier OnlyTA{
    bool auth = false;
    if(msg.sender == TAaddress){
        auth = true;
    }
        require(auth == true,"You are not the Traffic Authority");
        _;
}

modifier OnlyRSU{
    bool flag = false;
    for(uint i=0;i<RoadSideUnits.length;i++){
       if(msg.sender == RoadSideUnits[i]){
           flag = true;
       }
    }
    require(flag == true,"You are not a RSU");
    _;
}
```

Fig. 7. Smart contract logics for access rights.

```
modifier notBlocked(address suspected_vehicle){
    bool flag = false;
    if(VR[suspected_vehicle].time > now){
        flag = true;
    }
    require(flag == false,"You are blocked for 1 minute");
    _;
}

modifier notRevoked(address _acno){
    bool statusRevocation = false;
    for(uint i=0;i<RevocationList.length;i++){
           if(RevocationList[i] == _acno){
               statusRevocation = true;
           }
       }
       require(statusRevocation == false,"Your vehicle is Revoked");
       _;
}
```

Fig. 8. Revocation status of an vehicle.

The smart contract, besides managing the trust and detecting the false reporting of the vehicle, also takes care of the revocation of the vehicles relaying falsified messages. We consider two types of revocation here:

*a) Soft Revocation:* Each time a vehicle detected as misbehaving, it gets its TV deducted by 1. It gets itself blocked for a fixed interval of time during which it cannot execute any transactions on the blockchain.

*b) Hard Revocation:* Vehicles whose TV (trust value) falls below a threshold automatically gets revoked from the system. This revocation is permanent, and only the TA has the authority to bring the revoked vehicles back in the system, which it can do within an authoritative domain. The snippet of these logics of the smart contract is shown in Fig. 8.

We wrote various other important logics to deal with situations that may arise in real life IoV framework when dealing with trust management. For example, an appropriate logic in the smart contract to take care of duplicate submission of response by vehicles, etc. Due to space constraint, we only provide the snippet of a very few logics.

*9) Algorithms:* The three algorithms that we implemented in the smart contract to deal with reporting, analyzing, updating the trust score (increasing, decreasing putting in a revocation list), and providing incentives are given as follows.

In Algorithm 1, an *intelligentVehicle* calls *reportSuspicion* for reporting suspicious activities around itself. The reporting vehicle includes the session ID and suspected vehicle address in the transaction and sends it to the network to get it mined. The mining RSUs include these transactions to form a block and attempt to add the blocks in the blockchain.

In Algorithm 2, the RSUs call *analyseReports* at random interval of time different for each RSU. On being called, the module analyses the responses received within a particular

**Algorithm 1** Handle Reporting of an Event

**Require:** $x$ (session ID), *suspectedVehicle* (Suspected Vehicle Address)
**Ensure:** Suspicion Reported
***Require:*** msg.sender (*Reporting Vehicle*) is an intelligentVehicle, msg.sender is notRevoked, suspected Vehicle is an intelligent Vehicle, msg.sender is not Blocked
$s \leftarrow sessionRegister[x]$
**if** $x$ is a new session **then**
  Add $x$ to *RegisteredSession* list
  $s.alarmer \leftarrow msg.sender$
  $s.count \leftarrow 1$
**end if**
$V \leftarrow VISR[x][s.count]$
$P \leftarrow PTR[msg.sender][x][suspectedVehicle]$
$S \leftarrow SSR[x][suspectedVehicle]$
$v \leftarrow VR[msg.sender]$
$C \leftarrow CR[v.reportNumber]$
**if** The session is in *RegisteredSession* and the report is not duplicate **then**
  $V.registeredAddress \leftarrow msg.sender$
  $V.doubtyVehicle \leftarrow suspectedVehicle$
  $S.score \leftarrow S.score + 1$
  $P.isrewardReceived \leftarrow false$
  $P.submitted \leftarrow true$
  $C.session \leftarrow x$
  $C.suspectedVehicle \leftarrow suspectedVehicle$
  $v.reportNumber \leftarrow v.reportNumber + 1$
  $s.count \leftarrow s.count + 1$
**end if**

**Algorithm 2** Analyzing Report and Trust Update

**Require:**
**Ensure:** Analysed reports
***Require:*** There must exist some session in *RegisteredSession* list which reports are not yet analyzed, msg.sender is RSU
Select an unprocessed session $x$ from *RegisteredSession* list
$s \leftarrow sessionRegister[x]$
**for** Each participating vehicle $i$ in the session $x$ **do**
  $V \leftarrow VISR[x][i]$
  $suspectedVehicle \leftarrow V.doubtyVehicle$
  $S \leftarrow SSR[x][suspectedVehicle]$
  $v \leftarrow VR[suspectedVehicle]$
  **if** s.count $>= 4$ **and** S.score $>$ s.count/2 **then**
    $v.TV \leftarrow v.TV - 1$
    $v.time \leftarrow v.time + 1\ minutes$
    **if** v.TV $< 0$ **and** v.Revoked $!=$ true **then**
      Put *suspectedVehicle* into *RevocationList*
      $v.Revoked \leftarrow true$
    **end if**
    $S.verificationResult \leftarrow true$
  **end if**
**end for**

**Algorithm 3** Reward Claim by an Intelligent Vehicle

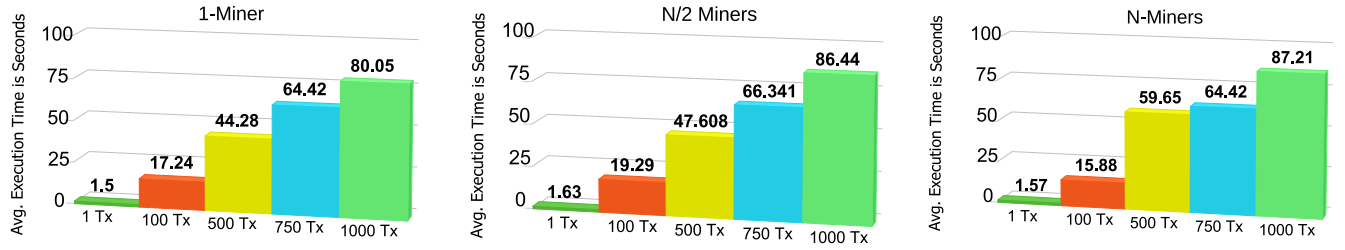
**Require:**
**Ensure:** Reward claimed credited to msg.sender account
***Require***: msg.sender (*Claiming Vehicle*) is *intelligentVehicle*, msg.sender is notRevoked
$v \leftarrow VR[msg.sender]$
$C \leftarrow CR[v.claimNumber]$
$x \leftarrow C.session$
$suspectedVehicle \leftarrow C.suspectedVehicle$
$S \leftarrow SSR[x][suspectedVehicle]$
$P \leftarrow PTR[msg.sender][x][suspectedVehicle]$
$s \leftarrow sessionRegister[x]$
**if** *msg.sender* has not claimed rewards for session $x$ **then**
  **if** The reports of the session $x$ is analysed by the RSU **then**
    **if** *P.submitted* == *S.verificationResult* **then**
      $v.creditScore \leftarrow v.creditScore + 5$
      $v.TV \leftarrow v.TV + 1$
      $v.claimNumber \leftarrow v.claimNumber + 1$
      **if** s.alarmer == msg.sender **then**
        $v.creditScore \leftarrow v.creditScore + 2$
      **end if**
      $P.isrewardReceived \leftarrow true$
    **end if**
  **end if**
**end if**

session. The module gets the session to be analyzed from the RegisteredSession list. The module checks the score of each vehicle reported as suspicious in a session. The minimum number of vehicles needed to participate in an event is considered to be 4. The consideration is made to handle a scenario where an attacker vehicle creates a session and reports against a benign vehicle. Since no other vehicle will be reporting for the same session and thus by the 51% rule used in our analyzing module, the report will be considered as true, resulting in an undesired punishment to the benign vehicle. Otherwise, if the majority of the participating vehicles identifies a vehicle to be suspicious, the reporting is considered to be true, and the TV of the suspected vehicle is decremented by 1 and is blocked for a minute. If the suspicious activity of the vehicle continues, the vehicle is revoked from the system.

In Algorithm 3, *claimReward* is called by an *intelligentVehicle* for claiming the rewards to be received for participating in true reporting in some earlier season. For true reporting, the TV of the reporting vehicle is incremented by 1, and the credit score of the vehicle is incremented by 5. If the reporting vehicle was the first one to report the suspicious activity, then the vehicle is considered as an alarmer vehicle, and the account of the vehicle is credited with 2 more credit points. Once *inteliigentVehicle* executes it, a transaction will be generated, which gets mined by the RSU/miner.

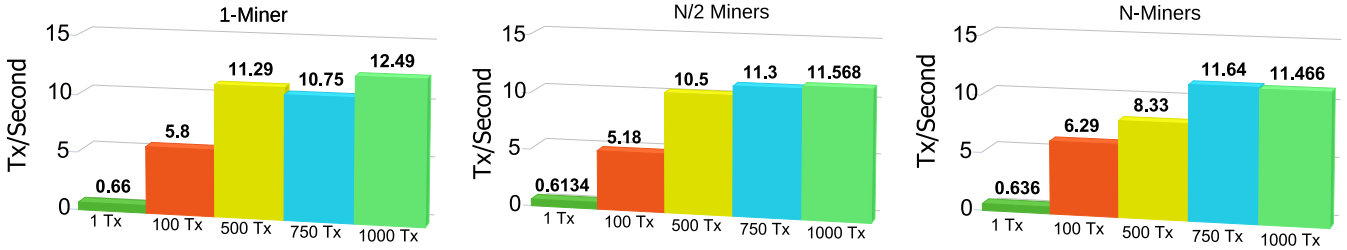
## VI. Results and Discussion

The performance of the blockchain testbed is presented in this section. We show the average throughput and execution time of our decentralized approach that uses a smart contract




(a) Avg. Execution Time with 1-Miner (b) Avg. Execution Time with N/2 Miners (c) Avg. Execution Time with N Miners

Fig. 9. Avg. execution time performance.




(a) Avg. Throughput with 1-Miner (b) Avg. Throughput with N/2 Miners (c) Avg. Throughput with N Miners

Fig. 10. Average throughput performance.

on Ethereum Blockchain for trust management at RSU plane of IoV.

### *A. Performance Evaluation of Blockchain Framework*

Values collected for each transaction in order to assess the performance of our configured private blockchain are as follows. Transaction (Tx) Deployment Time (t1): Unix time when transactions were deployed. Transaction (Tx) Completion Time (t2): Unix time when the blockchain confirmed transactions. The transaction completion time was collected through web3.js APIs that returns transaction details.

We choose transaction execution time and throughput as parameters for evaluating our set up the private blockchain.

*1) Execution Time:* The execution time is the total amount of time (seconds) during which all transactions in the dataset were executed and confirmed by the blockchain. It is the duration of time elapsed when the first transaction was deployed to the time when the last transaction is mined.

*2) Throughput:* It is defined as the number of successful transactions per second from the first deployment time of the transaction. Average throughput is the average over execution time.

*3) Comparing Average Execution Time:* The performance is compared to the differences in execution time of varying transactions with three distinct sets of miners: 1, N/2, and N (in our case, N=4), as shown in Fig. 9a, Fig. 9b, and Fig. 9c, respectively. The execution time grows as the number of transactions in the dataset increases. For a batch of 1000 transactions, the blockchain takes 80.05, 86.44, and 87.21 seconds with 1, N/2 and N miners.

*4) Comparing Average Throughput:* Fig. 10a, Fig. 10b, and Fig. 10c shows the average throughput plot for varying sets of transactions with 1, N/2, and N miners, respectively. For a batch of 1000 transactions, the average throughput is found to be 12.49, 11.568, 11.466. Besides, one can see that as the number of transactions in a set increases, the rate of throughput increase decreases. Thus, for a huge set of transactions, the average throughput will become some constant value.

*5) Discussion:* As we can see from the average execution time plot and the average throughput plot, increasing the number of miner nodes does not have a significant impact on improving system performance. However, an increased number of miner nodes will definitely help in making the system decentralized in a true manner, which comes at the cost of higher power consumption.

*6) What We Achieved?:* Through our proposed mechanism for trust management using blockchain, we achieved the following goals.

- **Encourage to behave well:** We introduced an incentive mechanism for vehicles behaving well and helping in detection of misbehavior and reporting of true information to RSU. The incentives scored can be redeemed for various services such as insurance premiums, maintenance, etc.
- **Revocation:** Authorized peers who misbehave continuously will lose their reputation in terms of trust score and will eventually be removed from the system. However, the TA can do the root cause analysis for misbehavior, and if it finds that it was intentional, then appropriate action must be taken.
- **Decentralized Approach:** In the proposed mechanism, most of the tasks such as verification, computation, result calculation, proof of work, mining, etc. are done at the edge level of IoV in a decentralized manner, i.e., in

a distributed fashion at the RSU plane. This approach will minimize the delay incurred in communication between vehicle and CA or TA, maximize scalability, reliability, and can deal with fault tolerance.

- **Consistency:** The distributed RSUs executing blockchain technology maintains a consistent trust database. Any changes made in the database at any RSU propagated across all other RSUs via the blockchain in the network.
- **Availability:** The consistent information about the trust and its reward is always available at the edge of the IoV. Vehicles requesting that information can easily access them.

## VII. Conclusion

In this paper, we proposed mechanisms that manage trust using blockchain in IoV. We have provided a survey of existing works available in this increasingly important area. We proposed a blockchain-based decentralized approach in which CA/TA deployed the smart contract, and all RSUs work in a distributed manner to maintain consistent vehicular trust database and enhance reliability, availability, and consistency. We introduced the idea of maintaining sharded blockchains, that will not only reduce the propagation delay of transactions but will also increase the throughput and efficiency of the entire system. We also introduced incentive strategy for the vehicles participating in event detection, i.e., their contribution in the detection of a true event and its accurate reporting helps them to get rewards, which they can redeem for various services and payments. The proposed incentive mechanism encourages participating peers to perform well and get wallet points. However, if they do not perform well, they can be revoked from the system. We demonstrated the performance of our framework in terms of average throughput and execution time by deploying the private blockchain on the testbed, thus demonstrating its feasibility.

In this work, we have not considered the misbehavior detection and local detection checks using plausibility factors, filters, consistency (position, speed, heading), beacon frequency, etc. at the vehicular plane of IoV. As future work, we will try to integrate the misbehavior detection process and the privacy part. We will look for the role of AI in the misbehavior detection and efficient consensus algorithms in the RSU plane of IoV for decentralized trust management.

## Acknowledgment

The authors would also like to thank the editorial team and all the anonymous reviewers for their valuable suggestions and comments, which helped to improve the quality of the work.

## References

[1] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of DSRC and cellular network technologies for V2X communications: A survey," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9457–9470, Dec. 2016.

[2] F. Chiti, R. Fantacci, Y. Gu, and Z. Han, "Content sharing in Internet of vehicles: Two matching-based user-association approaches," *Veh. Commun.*, vol. 8, pp. 35–44, Apr. 2017.

[3] H. D. Abdulkarim and H. Sarhang, "Normalizing RSS values of Wi-Fi access points to improve an integrated indoors smartphone positioning solutions," in *Proc. Int. Eng. Conf. (IEC)*, Jun. 2019, pp. 171–176.

[4] H. S. Maghdid, A. Al-Sherbaz, N. Aljawad, and I. A. Lami, "UNILS: Unconstrained indoors localization scheme based on cooperative smartphones networking with onboard inertial, Bluetooth and GNSS devices," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Apr. 2016, pp. 129–136.

[5] Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: Applications and related technical issues," *IEEE Commun. Surveys & Tuts.*, vol. 10, no. 3, pp. 74–88, 3rd Quart., 2008.

[6] C. Campolo, A. Molinaro, and R. Scopigno, "From today's VANETs to tomorrow's planning and the bets for the day after," *Veh. Commun.*, vol. 2, no. 3, pp. 158–171, Jul. 2015.

[7] R. A. Uzcategui, A. J. De Sucre, and G. Acosta-Marum, "Wave: A tutorial," *IEEE Commun. Mag.*, vol. 47, no. 5, pp. 126–133, May 2009.

[8] K. Z. Ghafoor, M. Guizani, L. Kong, H. S. Maghdid, and K. F. Jasim, "Enabling efficient coexistence of DSRC and C-V2X in vehicular networks," *IEEE Wireless Commun.*, vol. 27, no. 2, pp. 134–140, Apr. 2020.

[9] G. Karagiannis *et al.*, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 584–616, 4th Quart., 2011.

[10] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 770–790, 1st Quart., 2018.

[11] *Intelligent Transport Systems (ITS); Vehicular communications; GeoNetworking; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service*, Standard TS 102 637-3, ETSI, Tech. Spec., Sep. 2010.

[12] J. Zhang, "Trust management for VANETs: Challenges, desired properties and future directions," *Int. J. Distrib. Syst. Technol.*, vol. 3, no. 1, pp. 48–62, Jan. 2012.

[13] P. K. Singh, S. N. Gowtham, T. S, and S. Nandi, "CPESP: Cooperative pseudonym exchange and scheme permutation to preserve location privacy in VANETs," *Veh. Commun.*, vol. 20, Dec. 2019, Art. no. 100183.

[14] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Tech. Rep., 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[15] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3680–3689, Jun. 2019.

[16] J. Huang *et al.*, "Blockchain based mobile crowd sensing in industrial systems," *IEEE Trans. Ind. Informat.*, to be published, Jan. 3, 2020, doi: 10.1109/TII.2019.2963728.

[17] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.

[18] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Apr. 2014.

[19] S. A. Soleymani *et al.*, "Trust management in vehicular ad hoc network: A systematic review," *EURASIP J. Wireless Commun. Netw.*, vol. 2015, no. 1, p. 146, Dec. 2015.

[20] F. Ahmad, J. Hall, A. Adnane, and V. N. L. Franqueira, "Faith in vehicles: A set of evaluation criteria for trust management in vehicular ad-hoc network," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jun. 2017, pp. 44–52.

[21] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proc. IEEE INFOCOM 27th Conf. Comput. Commun.*, Apr. 2008, pp. 1238–1246.

[22] N.-W. Lo and H.-C. Tsai, "A reputation system for traffic safety event on vehicular ad hoc networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, p. 9, Dec. 2009.

[23] A. Wu, J. Ma, and S. Zhang, "RATE: A RSU-aided scheme for data-centric trust establishment in VANETs," in *Proc. 7th Int. Conf. Wireless Commun., Netw. Mobile Comput.*, Sep. 2011, pp. 1–6.

[24] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks," in *Network and System Security. NSS* (Lecture Notes in Computer Science), vol. 7873, J. Lopez, X. Huang, and R. Sandhu, Eds. Berlin, Germany: Springer, 2013.

[25] Z. Huang, S. Ruj, M. A. Cavenaghi, M. Stojmenovic, and A. Nayak, "A social network approach to trust management in VANETs," *Peer-to-Peer Netw. Appl.*, vol. 7, no. 3, pp. 229–242, Sep. 2014.

[26] J. Kamel, F. Haidar, I. B. Jemaa, A. Kaiser, B. Lonc, and P. Urien, "A misbehavior authority system for Sybil attack detection in C-ITS," in *Proc. IEEE 10th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, New York, NY, USA, 2019, pp. 1117–1123, doi: 10.1109/UEMCON47517.2019.8993045.
[27] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 41, no. 3, pp. 407–420, May 2011.
[28] F. Gómez Mármol and G. Martínez Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 934–941, May 2012.
[29] U. Khan, S. Agrawal, and S. Silakari, "Detection of malicious nodes (DMN) in vehicular ad-hoc networks," *Proc. Comput. Sci.*, vol. 46, pp. 965–972, Jan. 2015.
[30] X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in VANETs," *Ad Hoc Netw.*, vol. 55, pp. 107–118, Feb. 2017.
[31] Y.-M. Chen and Y.-C. Wei, "A beacon-based trust management system for enhancing user centric location privacy in VANETs," *J. Commun. Netw.*, vol. 15, no. 2, pp. 153–163, Apr. 2013.
[32] H. Sedjelmaci and S. M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks," *Comput. Electr. Eng.*, vol. 43, pp. 33–47, Apr. 2015.
[33] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, Apr. 2016.
[34] M. E. Mahmoud and X. Shen, "An integrated stimulation and punishment mechanism for thwarting packet dropping attack in multihop wireless networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 8, pp. 3947–3962, Oct. 2011.
[35] N. Bißmeyer, J. Njeukam, J. Petit, and K. M. Bayarou, "Central misbehavior evaluation for VANETs based on mobility data plausibility," in *Proc. 9th ACM Int. Workshop Veh. Inter-Netw., Syst., Appl. VANET*, 2012, pp. 73–82.
[36] Q. Li, A. Malip, K. M. Martin, S.-L. Ng, and J. Zhang, "A reputation-based announcement scheme for VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 9, pp. 4095–4108, Nov. 2012.
[37] X. Li, J. Liu, X. Li, and W. Sun, "RGTE: A reputation-based global trust establishment in VANETs," in *Proc. 5th Int. Conf. Intell. Netw. Collaborative Syst.*, Sep. 2013, pp. 210–214.
[38] C. Lai, K. Zhang, N. Cheng, H. Li, and X. Shen, "SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 6, pp. 1559–1574, Jun. 2017.
[39] J. Oluoch, "A distributed reputation scheme for situation awareness in vehicular ad hoc networks (VANETs)," in *Proc. IEEE Int. Multi-Disciplinary Conf. Cognit. Methods Situation Awareness Decis. Support (CogSIMA)*, Mar. 2016, pp. 63–67.
[40] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 5, pp. 25408–25420, 2017.
[41] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.
[42] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.
[43] M. Singh and S. Kim, "Intelligent vehicle-trust point: Reward based intelligent vehicle communication using blockchain," 2017, *arXiv:1707.07442*. [Online]. Available: http://arxiv.org/abs/1707.07442
[44] U. Javaid, M. N. Aman, and B. Sikdar, "DrivMan: Driving trust management and data sharing in VANETs with blockchain and smart contracts," in *Proc. IEEE 89th Veh. Technol. Conf. (VTC-Spring)*, Apr. 2019, pp. 1–5.
[45] P. K. Singh, S. K. Nandi, and S. Nandi, "A tutorial survey on vehicular communication state of the art, and future research directions," *Veh. Commun.*, vol. 18, Aug. 2019, Art. no. 100164.
[46] T. Mekki, I. Jabri, A. Rachedi, and M. ben Jemaa, "Vehicular cloud networks: Challenges, architectures, and future directions," *Veh. Commun.*, vol. 9, pp. 268–280, Jul. 2017.
[47] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017.
[48] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat, and S. Nandi, "An efficient blockchain-based approach for cooperative decision making in swarm robotics," *Internet Technol. Lett.*, vol. 3, no. 1, Jan. 2020, Art. no. e140.
[49] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, pp. 1–21, Sep. 1997.
[50] C. Dannen, *Introducing Ethereum and Solidity*, vol. 1. Berkeley, CA, USA: Apress, 2017.
[51] 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.
[52] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2017, pp. 1–6.

**Pranav Kumar Singh** (Member, IEEE) received the B.Tech. and M.Tech. degrees in computer science and engineering from Dr. A.P.J. Abdul Kalam Technical University (formerly UPTU) and NERIST, India, respectively. He is currently pursuing the Ph.D. degree with the Department of Computer Science and Engineering, IIT Guwahati, India. He is working as an Assistant Professor with the Department of Computer Science and Engineering, Central Institute of Technology at Kokrajhar, India. He has more than 12 years of teaching experience. He has also served as a Nodal Officer NKN and IPv6 Road Map of CITK, an initiative by the Government of India. His research interests include vehicular communications, security and privacy, software-defined vehicular networking, QoS and QoE in wireless communication, intelligent transportation systems, blockchain, and the IoT.

**Roshan Singh** received the Diploma and B.Tech. degrees in computer science engineering from the Central Institute of Technology at Kokrajhar, Kokrajhar, India, in 2016 and 2019, respectively. He is an Assistant Project Engineer with the Open Source Intelligence Laboratory, IIT Guwahati, Guwahati, India. His research interests include blockchain technology, the IoT, and social network analytics.

**Sunit Kumar Nandi** (Student Member, IEEE) is currently pursuing the Ph.D. degree in computer science and engineering with the IIT Guwahati. He is a Trainee Teacher with the Department of Computer Science and Engineering, National Institute of Technology Arunachal Pradesh. He is the Leading Officer with Techno FAQ Digital Media, an e-magazine focusing on science, engineering, business, and education. He has spent two years in the telecom industry, and seven years in developing open source software as a volunteer with the team at the SuperX Operating System Project. He also mentors startups in developer operations, IT infrastructure, and financial services. He published 20 articles in international journals and conferences. His research interests include operating systems, computer networking, and cognitive data mining.

**Kayhan Zrar Ghafoor** (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from Salahaddin University-Erbil in 2003, the M.Sc. degree in remote weather monitoring from Koya University in 2006, and the Ph.D. degree in wireless networks from University Technology Malaysia in 2011. He is currently working as an Associate Professor with Salahaddin University-Erbil and a Visiting Scholar with the University of Wolverhampton. Prior to that, he was a Post-Doctoral Research Fellow with Shanghai Jiao Tong University, where he contributed to two research projects funded by the National Natural Science Foundation of China and the National Key Research and Development Program. He also served as a Visiting Researcher with University Technology Malaysia. He is the author of two technical books, seven book chapters, and 65 technical articles indexed in ISI/Scopus. He was a recipient of the UTM Chancellor Award at the 48th UTM Convocation in 2012.

**Danda B. Rawat** (Senior Member, IEEE) received the Ph.D. degree from Old Dominion University, Norfolk, VA, USA. He is a Professor with the Department of Electrical Engineering and Computer Science, the Founding Director of the Data Science and Cybersecurity Center, the Director of the Cybersecurity and Wireless Networking Innovations (CWiNs) Laboratory, and the Graduate Program Director of the Howard-CS Graduate Programs at Howard University, Washington, DC, USA. His professional career comprises more than 15 years in academia, government, and industry. He has secured over $5 million in research funding from the U.S. National Science Foundation, the U.S. Department of Homeland Security, the Department of Energy, the National Nuclear Security Administration (NNSA), DoD Research Laboratories, Industry (Microsoft, Intel, etc.), and private foundations. He has published over 200 scientific/technical articles and nine books. He is engaged in research and teaching in the areas of cybersecurity, machine learning, and wireless networking for emerging networked systems, including cyber-physical systems, the Internet-of-Things, smart cities, software-defined systems, and vehicular networks. He is a Senior Member of ACM, a member of ASEE and AAAS, and an IET Fellow. He served as a Technical Program Committee (TPC) member for several international conferences. He was a recipient of the NSF CAREER Award in 2016, the U.S. Air Force Research Laboratory (AFRL) Summer Faculty Visiting Fellowship in 2017, the Outstanding Research Faculty Award (Award for Excellence in Scholarly Activity) at GSU in 2015, the Best Paper Awards, and the Outstanding Ph.D. Researcher Award in 2009. He has delivered over 15 keynotes and invited speeches at international conferences and workshops. He has been serving as an Editor/Guest Editor for over 30 international journals. He has been in Organizing Committees for several IEEE flagship conferences, such as the IEEE INFOCOM, the IEEE CNS, the IEEE ICC, and the IEEE GLOBECOM.

**Sukumar Nandi** (Senior Member, IEEE) was a Visiting Senior Fellow with Nanyang Technological University, Singapore, from 2002 to 2003. He is a Senior Professor with the Department of Computer Science and Engineering, IIT Guwahati, India. He has coauthored a book *Theory and Application of Cellular Automata* (IEEE Computer Society) and four book chapters on sensor/vehicular networks. He has published around 400 journals articles/conference papers. His research interests include traffic engineering, wireless networks, network security, distributed computing, VLSI design, and data mining. He is a Senior Member of the Association for Computing Machinery and a fellow of The Institution of Engineers (India), The Institution of Electronics and Telecommunication Engineers (India), and the Indian National Academy of Engineering (INAE).