International Journal of Data and Network Science 7 (2023) 745–756

Contents lists available at GrowingScience

International Journal of Data and Network Science

homepage: www.GrowingScience.com/ijds

A trust management model in internet of vehicles

Fayez Alazemi[a], Ahmed Al-Mulla[b], Mousa Al-Akhras[c], Mohammed Alawairdhi[b], Marwah Al-Masri[b], Hani Omar[d*] and Hazza Alshareef[b]

[a]*Department of Computer Science and Information Systems, College of Business Studies, PAAET, Kuwait*
[b]*Department of Computer Science, College of Computing & Informatics, Saudi Electronic University, Riyadh, Saudi Arabia*
[c]*Computer Information Systems Department, King Abdullah II School for Information Technology, The University of Jordan, Amman 11942, Jordan*
[d]*Faculty of Information Technology, Applied Science Private University, Amman, Jordan*

C H R O N I C L E

Article history:
Received: December 2, 2022
Received in revised format: December 29, 2022
Accepted: February 5, 2023
Available online: February 5, 2023

Keywords:
Internet of Things (IoT)
IoT
Internet of Vehicles
IoV
Trust Management
Traffic
Accident
Vehicle
Model
Authentication

A B S T R A C T

The Internet of Things (IoT) is one of the most evolving technologies, which has a major impact on our daily life. Almost all new devices will have a feature to be connected and controlled over the Internet. Several applications are utilizing IoT to enhance routine processes and actions efficiently. The Internet of Vehicles (IoV) evolved from IoT, where vehicles communicate with each other or with other objects to have a better transportation environment to reduce the number of accidents and save people's lives. IoV is considered new fields that need security requirements including confidentiality, integrity, availability, authentication, and trust. Trust management technique is used to validate entities behaviors automatically against well-defined policies. The major categories of trust model in IoV are based on entity, data, or a combination of both. This paper proposes a trust model which is based on a combination of entity and data to define the trust of vehicles and utilize the public key infrastructure to distribute certificates to vehicles. Based on certificate validation, messages will be trusted and accepted. This model has been tested across different simulation scenarios which showed that the proposed model detected malicious vehicles and trusted vehicles did not accept their messages.

1. Introduction

The Internet of Things (IoT) is growing rapidly and has a direct impact on our daily life from different aspects such as healthcare, smart grid, smart cities, automated transportation, and home automation. The increasing rate of IoT devices is extremely high as it is expected to reach 100 billion devices by the year 2025 (Rose et al., 2015). The IoT industry is expected to have a major expansion on the economic market as its estimated revenue is about $1.3 trillion (Gubbi et al., 2013). There are several object types which are interconnected in IoT including sensors, actuators, Radio Frequency Identification (RFID), and mobile devices. IoT mainly relies on the Internet to communicate between the smart devices which enable them to be controlled and reached from anywhere. However, the Internet has many security threats which will be transferred to IoT as well. Many IoT devices are manufactured with insecure design which enable attackers to utilize them to perform their attacks. One of the most famous attacks was the Mirai attack which infected about 2.5 million IoT devices and launched Distributed Denial of Service (DDoS) attacks (Hernandez, 2020). According to Kaspersky Lab collection, the number of malware samples has increased quickly from 3129 to 121588 samples within a few years which shows that there are a lot of vulnerabilities in

* Corresponding author.
E-mail address: hani_omar@hotmail.com (H. Omar)

ISSN 2561-8156 (Online) - ISSN 2561-8148 (Print)

doi: 10.5267/j.ijdns.2023.2.003

IoT (Kuzin et al., 2018). In addition, IoT devices have many limitations from computing, power, and resources perspective which make addressing security issues a challenge (Hassija et al., 2019).

Internet of Vehicles (IoV) has been developed from the IoT family with focus on communication between vehicles and infrastructure devices (Nanda et al., 2019). The number of vehicles is increasing dramatically which influences driving conditions. As a result, the number of accidents is continuously increasing which results in physical injuries and losing people's lives. In addition, drivers may have some difficulties reaching out to the destination especially during extreme congestion which can happen due to either accidents or bad weather conditions (Gazdar et al., 2017). Consequently, IoV technology received huge interest from commercial companies and academic researchers since it can assist in resolving issues related to transportation (Yang et al., 2014). One of the key advantages of IoV is cooperating with other vehicles to avoid collisions or direct vehicles to a route with less traffic (Garcia-Magarino et al., 2018). On the other hand, there are many security challenges facing IoV including data integrity and authenticity. For instance, malicious messages or warnings about fake accidents being sent by malicious vehicles which could result in traffic jams on specific routes (Gazdar et al., 2017).

IoV evolved from traditional Vehicular AD-HOC Network (VANET) (Sharma et al., 2018). According to the World Health Organization (WHO), traffic accidents are considered one of the top ten causes which lead to death (World Health Organization, 2015). This transportation issue received high attention by many governments and authorities to find a solution to minimize the number of accidents. VANET was proposed as a transportation technology to manage the traffic efficiently by using direct communication between the vehicles or through fixed infrastructure like Road-Sides Unit (RSUs) (Ahmad et al., 2020). VANET has limitations due to the lack of computation ability and no cloud connectivity since it is based on ad-hoc architecture. IoV as a more complex network covers more services than the one provided by VANET. IoV consists of several elements such as users, vehicles and other smart devices connected to the network. IoV has an advantage over VANET since it is capable of computation and cloud connectivity functions (Sharma et al., 2018). Moreover, the advent of the emerging technologies like blockchain, cloud, SDN as well as artificial intelligence bring new opportunities to propose more relevant approaches within the trust management mechanisms within the IoV context (Hbaieb et al., 2022).

VANETs have been developed to improve traffic management efficiency and reduce the risks introduced by vehicles such as vehicle collisions and pedestrian accidents. However, VANETs lack compatibility with personal devices or cloud computing. Additionally, it does not have reliable Internet connection and it has very limited computing power. These limitations motivated researchers to have more intelligent vehicles which have better communications mechanisms that lead to a new concept called IoV. Since IoV is a new paradigm and a new research area, there is a need to explore and discuss the issues in this paradigm from different aspects such as possible applications areas, communication requirements and security challenges (Sharma, & Kaushik, 2019). One of the security challenges in IoV is the assessment of vehicles or messages trustworthiness that could spread and break the core functionality of IoV systems. A great risk to people's safety and lives could happen as a consequence of false messages sent by malicious nodes. Therefore, designing an effective trust management system for IoV is very crucial (Gai et al., 2017).

This paper represents a management model based on certificate validation, messages will be trusted and accepted. This model has been tested across different simulation scenarios for entities which can be used in IoV environments in order to detect malicious vehicles and eliminate the malicious messages from propagating through the IoV network. This paper is organized as follows: section 2 summarizes the IoV background, section 3 represents related work, section 4 discusses the proposed methodology, section 5 demonstrates the experimental setup, section 6 analyses the research results, and section 7 concludes the paper.

2. Internet of Vehicles

This section introduces IoV characteristics, architecture and security requirements.

2.1. Internet of Vehicles Special Characteristics

There are some special attributes of IoV which make it different from other IoT environments. The first characteristic is the mobility of the vehicles as they must move around, and they may get some temporary wireless disconnection during specific times. Another characteristic is the user's safety since this system interacts with the user directly. User safety is considered one of the top priorities for this system which requires real time messages communication and to avoid messages delay. In addition, from a security perspective mobility and wireless connectivity should be implemented securely to be protected from attackers (Sharma et al., 2018).

2.2. Internet of Vehicles Architecture

There are three main components in IoV: user, communication, and cloud. User component targets the client users who are involved in IoV including vehicles drivers, passengers inside the vehicles connected to the IoV through a smartphone or a laptop, and pedestrians outside vehicles but connected to IoV and looking for Taxi availability. Communication is the core component in IoV as it is the platform where all vehicles are connected and exchange their information directly or through

some provided service from the cloud functions (Sharma et al., 2018). There are different communication styles which may occur in IoV. Most common ones are:

Vehicle to Vehicle (V2V): This communication occurs between the vehicles to share information or work-cooperatively to complete an intensive task related to a traffic scenario as shown in Fig. 1 (Liang et al., 2017). This communication is usually meant for short term connectivity because of the high mobility of vehicles (Chai et al., 2019).

Vehicle to Infrastructure (V2I): Vehicle to Infrastructure communication deals with the communication between the vehicle and the static infrastructure components such as RSU or base station which is usually located at a fixed location alongside the road as shown in Fig. 1 (Ahmad et al., 2020). This approach enhances the capabilities of the nodes (vehicles, RSUs, etc.) to communicate with each other on a local network and with other networks globally through the Internet using dedicated short-range communication (DSRC) (Iqbal et al., 2019).

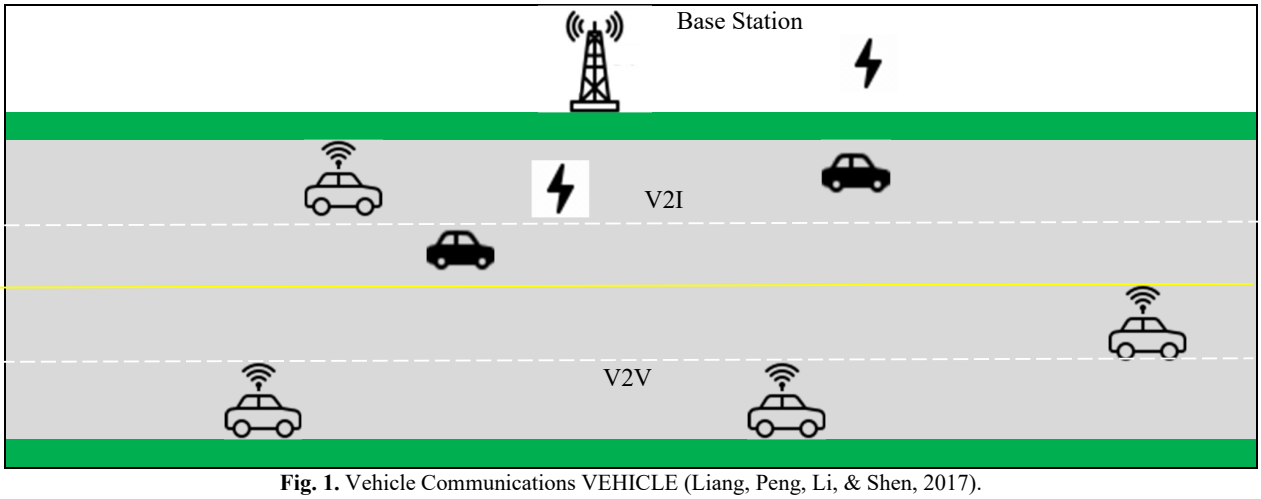

Fig. 1. Vehicle Communications VEHICLE (Liang, Peng, Li, & Shen, 2017).

Infrastructure to Infrastructure (I2I): Infrastructure to Infrastructure communication appears between the different infrastructure's components such as between RSUs or a RSU and a base station.

Vehicle to Pedestrian (V2P): Vehicle to Pedestrian communication involves the transmission of data between the pedestrian walking around the vehicles and the services that might be provided by vehicles such as Cab services. This communication can prevent collisions between vehicles and the people.

Cloud components are used to perform the calculations needed on the data gathered from the vehicles. There are multiple services that can be provided to vehicles such as storage as a service, network as a service or data as a service **(**Sharma et al., 2018).

2.3. Internet of Vehicles Security Requirements

IoT and IoV require some prerequisites to be realized in the real world. One of the requirements is high-speed infrastructure which supports scalability, mobility, and connectivity to the devices in the environment. From a security perspective, the following security requirements need to be addressed (Airehrour et al., 2016).

- Authentication: This process is necessary to identify objects uniquely in IoT and IoV to have strong authentication method and prevent object impersonation (Djedjig et al., 2018).
- Authorization: It ensures that only authorized users can connect and perform allowed actions in IoT and IoV environments (Djedjig et al., 2018).
- Availability: One of the basic requirements of IoT and IoV is to be available all the time for service and working as expected (Djedjig et al., 2018). Confidentiality: Data during communication or at rest in IoT and IoV should be encrypted and accessed only by authorized users (Djedjig et al., 2018).
- Integrity: The integrity of data is very crucial as using tampered data by malicious activities can have a severe damage to IoT and IoV. Therefore, any unauthorized modifications of data should be detected (Djedjig et al., 2018).
- Privacy: Private data must be protected from third parties during different data states including data at rest, in transit and at processing (Djedjig et al., 2018).
- Non-repudiation: The connected entities in IoT and IoV should not be able to deny the received data or commands from the control (Kouicem et al., 2018).

- Trust: Due to the complexity of IoV and IoT architectures and special characteristics of these environments, there is a need for a system which can automatically protect trustworthy entities in the environment and detect the untrusted nodes in order to isolate them from the network and enable the functions to only run on trusted zone (Djedjig et al., 2018).

3. Literature review

Trust management in IoV is still immature and a new research area. Trust management in IoV mainly focuses on two components namely entities and data. Therefore, trust management models are categorized into three categories including data-oriented, entity oriented, and hybrid trust models. Trust models in IoV have two major elements. The first one is the mobile vehicles. The other one is RSU, which is static with fixed infrastructure. Trust models based on RSU are usually centralized trust models, while the other type is a distributed trust model where vehicles compute the trust in a distributed manner **(**Ahmad et al., 2020).

3.1. Entity-Oriented Trust Models

Entity-oriented trust models have different mechanisms to detect and eliminate malicious nodes from the network by assessing the trustworthiness of nodes based on entity (vehicle). These trust models heavily rely on messages generated by the nodes and its neighbors. Neighbors can evaluate the node that generated the message to the node evaluator which needs to know the reputation of the message sender **(**Ahmad et al., 2020). Many studies focused on entities' trust models. A cluster-based mechanism was proposed by Khan et al. where the cluster head is responsible to compute the trust in the network (Khan et al., 2015). The cluster head uses a watchdog method in nationhood where honest vehicles report their recommendation about misbehaving nodes in the nationhood to the cluster head. Once those vehicles are identified, trusted authority remove them from the network **(**Ahmad et al., 2020).

Another type of trust model which uses centralized methodology is presented by Mármol and Pérez (2012 (2012). It utilizes the fixed infrastructure for the assessment of neighbors' reputation. The goal of this technique is to recognize legitimate and malicious vehicles quickly. A trust score is calculated depending on recommendation from the fixed infrastructure, recommendation provided by neighbors, and previous direct observations. Once trust score is calculated, the message will be accepted if it is trustworthy or rejected if it is not. (Mármol, & Pérez, 2012). Another approach which utilizes data mining to calculate trust score was proposed by Yang. The author uses data mining to see the similarity between the messages in the network and then evaluate the received message based on Euclidean distance and the reputation weight of other vehicles (Yang, 2013).

3.2. Data-Oriented Trust Models

Data-oriented trust model focuses on the data exchanged among the vehicles and the trust is computed based on opinions gathered from other vehicles **(**Ahmad et al., 2020). One of the approaches which adapted this model is called intrusion-aware trust model, which can discover malicious messages such as fake location (Shaikh, & Alzahrani, 2014). The vehicles which require to know the trust score for a message perform trust calculation through different stages. First, the confidence value is calculated which is based on location and time nearness for every message. Then, a fuzzy logic method is used to check the trustworthiness of the message. A message is accepted only if it exceeds specific trust threshold **(**Ahmad et al., 2020).

Another proposed model by Wu et al. which utilizes a centralized approach to evaluate the trustworthiness of data (Wu et al., 2011). In this model, trust is calculated at the RSU based on feedback and observation. Whenever a vehicle identifies an event, it will observe it and share observation with the RSU. The RSU updates the list of events with the observation factors and calculates the trust on them. Then, the RSU spreads the new trust value to vehicles for this event (Wu et al., 2011). More recent research which focuses on data-oriented models was proposed by Gazdar et al. (2017). Each vehicle assesses the received data continuously to see if they are trustworthy based on direct experience in the network. The main idea of this approach is classifying the vehicles into two groups, trusted vehicles and malicious vehicles. Each vehicle has a trust table that is updated frequently based on received messages from nearby vehicles. The trust value gets incremented for messages received from trusted vehicles while it gets decremented for malicious vehicles (Gazdar et al., 2017).

3.3. Hybrid Trust Models

Hybrid trust model evaluates the credibility of entity (vehicle) and the exchange data. This model relies on vehicle reputation to calculate the trust as it assumes that legitimate data would impact the sender's reputation. These trust models are complex as they require lot of messages processing in a very short time **(**Ahmad et al., 2020). One of the research projects that adapted this model was proposed by Dhurandher et al. who used reputation and different plausibility checks to distribute a message in the network (Shrestha, & Nam, 2017). This model divided the evaluation of trust to eliminate malicious vehicles from the network into four steps. First, discovery will be done by neighbors. Second, data will be spread once neighbors are discovered. Third, a trust decision is received and last the neighborhood needs to be monitored continuously **(**Ahmad et al., 2020).

A different approach was proposed by Shrestha et al. to compute the trust nodes close to each other by two mechanisms (Shrestha, & Nam, 2017). The first one is to calculate the trust in the node itself then it calculates the trust of the received data. The first step is accomplished by a clustering algorithm where trusted and malicious vehicles are classified into two

pools to identify trusted neighbors. After node trust is done, the data gets validated based on a specific threshold created by random walk algorithm (Ahmad et al., 2020). The significance of these contributing parameters of entities and data is typically represented by associating a weighting factor to each contributing attribute. The values assigned to these weighting factors are often set manually, i.e., these values are predefined and do not take into consideration any affecting parameters (Siddiqui et al., 2021).

3.4. Other Trust Models in IoV

Tang et al. proposed a trust management model using cloud computing (Tang et al., 2016). The authors suggested having two boards in each vehicle. Private board to keep record of the direction interaction and public board to fetch data from the cloud shared by other vehicles. The trust will be determined based on the comparison between the two boards (Ahmad et al., 2020). Yang et al. (2018) proposed a decentralized trust model by using a Blockchain to store the rating data which is generated by every vehicle and share it with the nearby RSU. The RSU does the calculations for the rating and then added as a block in the block chain (Ahmad et al., 2020). Singh et al. proposed a blockchain-based decentralized trust management scheme using smart contracts. Specifically, we introduce the concept of blockchain sharing for reducing the load on the main blockchain and increasing the transaction throughput (Singh et al., 2020).

Javid et al. (2020) proposed a blockchain-based protocol for IoV using smart contracts, physical unclonable functions (PUFs), certificates, and a dynamic Proof-of-Work (dPoW) consensus algorithm. While Talal et al. (2019) designed a decentralized secure collaboration scheme that protects the vehicles in the IoV environment against the attacks on data integrity. First, the trustworthiness of the vehicles is computed based on their experience acquired from direct interactions using a Bayesian inference model. Then, based on the established trust relationships between the vehicles (Halabi, & Zulkernine, 2019). In order to avoid collusion attacks, Chen et al. proposed Trust Management Based on Evidence Combination (TMEC) scheme, which adopts the trust recommendation of collaborative filtering and selects the trustworthy neighbors by using Cosine-based similarity, ultimately to get a more accurate global trust value (Chen et al., 2018).

4. The Proposed Methodology

In the proposed trust model for IoV, we assume that public key infrastructure is implemented. There will be a central authority to distribute the certificates called National Center of Digital Certification (NCDC) of Saudi Arabia. NCDC is a government agency in Saudi Arabia responsible for the management of Public Key Infrastructure (PKI), and it's under authority of the Ministry of Communication and Information Technology and aims at providing trust services for the secure information exchange and transmission between participants including government sectors, citizens and the business sector. Each vehicle will need to have a certificate from the Digital Certification Center of Saudi Arabia after verifying the vehicle identity through the Department of Traffic (DoT) in Saudi Arabia as shown in Fig. 2.

The first phase in the proposed trust model is the registration process and it involves the following four steps:

Step 1: Vehicle (A) requests a certificate from DoT.
Step 2: DoT validates vehicle (A) owner request and information.
Step 3: If vehicle A's request is verified, DoT will send a request for a certificate which includes the owner information and public key from NCDC.
Step 4: NCDC of Saudi Arabia will issue a certificate to Vehicle (A).

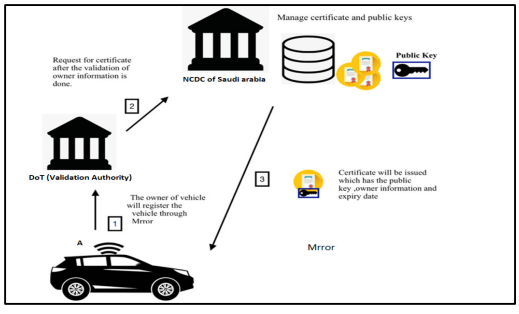

Fig. 2. Proposed Trust Model Registration Phase

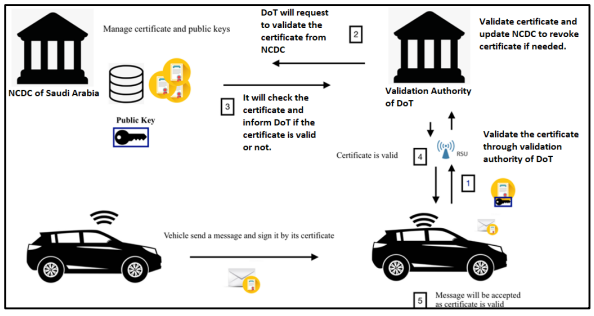

Fig. 3. Certificate Validation Process

The next phase is the validation process where messages will be transmitted across vehicles and each vehicle will validate the vehicle certificate first to accept or reject the message as shown in Fig. 3. The pseudo code for the validation process is shown in Algorithm 1, which can be used to validate messages between the vehicles.

Algorithm 1. Validation Process Algorithm.

Input:
Received broadcasted Vehicle Massage(VM) by vehicle Vi(i = 1, 2...n); received Public key Vehicle (PV)

Output:

Accepted(VM)/ Dropped(VM)
Fetching Certificate Repository (CR) of valid certificate;
Fetching Certificate Revocation List (CRL) repository.
Checking the content of VM (position, time, messages)
While *receiving PV (for each received message)* **do**
If (*PV not exist in CR)* **then**
return (dropped MV);
If (*PV exist in CR and in CRL*)
return (dropped MV);
else if (*PV exist in CR and Checking is OK and not in CRL*) **then**
return (accepted VM with trusted content);
else if (*PV exist in CR AND CHECKING IS NO and not in CRL*) **then**
return (accepted VM with less trusted content);
Other Checking to verify the Authentication
end
end

Any vehicle can receive broadcasted Vehicle Message (VM) with the Public Key Vehicle (PV). The recipient can validate the (VM) by checking the authentication of the sender and the content of the message by requesting the status of validity of certificate and the content of the message from DoT. There is Certificate Repository (CR) for the valid certificate, and Certificate Revocation List (CRL) for invalid certificates. The DoT has access to check the validation of the vehicle's certificate by fetching the information from both CR and CRL. On the other hand, DoT will check the content of VM by comparing the position of sender, time, and the content by comparing it with other messages from other vehicles in the same circumstances. If PV does not exist in CR or exist in CRL, the VM will be dropped. Otherwise, the DoT will return a validated VM to the recipient with a level of warning related to the content. In case there is mismatching between the position of VM and the content, the DoT will send to the recipient to be careful with less serious content, in this case DoT will confirm another verification process for the sender to detect malicious content. Depending on the other verification, DoT will take appropriate action to revoke the certificate or detect any internal problem related to penetration to the Road-Side Unit (RSU) or internal system. If a vehicle was reported or DoT discovered a malicious vehicle, then DoT can request the NCDC of Saudi Arabia to revoke a certificate by moving it to the Certificate Revocation List as shown in Figure 4. The VM should be under checking frequently even though it is approved. So, the recipient can be updated for any changes for the certificate of the VM.

The certification revocation process involved the following three steps:

Step 1: DoT validation authority observed a malicious vehicle (A) due to a report to re- verify, owner changed, or leaked private key.

Step 2: DoT validation authority will send a request to NCDC of Saudi Arabia to revoke/move a certificate and its public key to certificate revocation list.

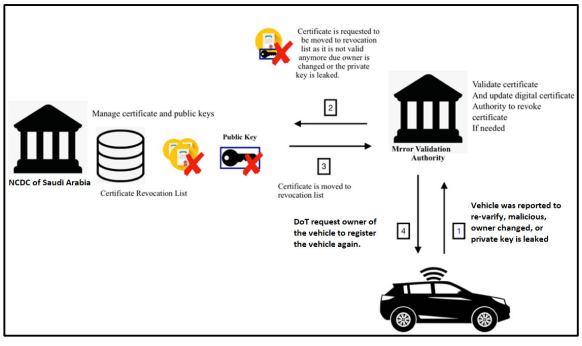

Fig. 4. Certificate Revocation Process

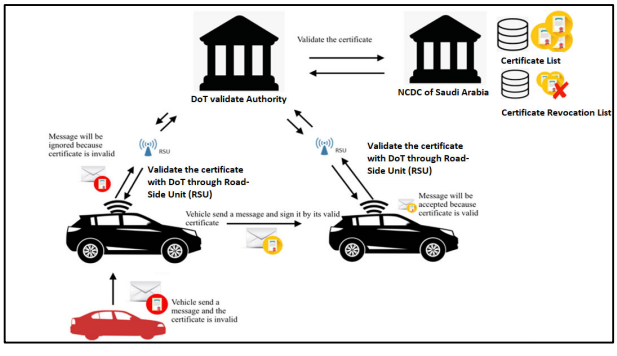

Fig. 5. Proposed Trust Model Design.

Step 3: NCDC of Saudi Arabia will revoke/move vehicle certificate and its public key to revocation certificate list.

Step 4: DoT will send to the new owner to register in the system.

By applying this design, only messages from validated vehicles will be accepted. Each vehicle must sign the message with its certificate in order to communicate with other vehicles. The vehicle, which received the message, will communicate with DoT validation authority through RSU to validate the message. Once the certificate is validated, the message will be accepted; otherwise, the message will be ignored as illustrated in Fig. 5.

5. Experimental Setup

Vehicular Network Open Simulator (VENTOS) is an open-source framework which was built for simulation of vehicular networks (Amoozadeh et al., 2015). It was developed on top of two simulators. The first one is OMNeT++ which is an event-driven network simulation (Wehrle et al., 2010). The other one is SUMO (Lopez et al., 2018), a simulator which can be used for vehicle mobility and road traffic simulation. VENTOS has a lot of features and can be used in various scenarios. It supports different wireless communication including Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications. The VENTOS framework requires some prerequisites to be installed to be able to use the framework. The Ubuntu version used is 16.04.6 LTS. It also requires some packages and repositories which need to be cloned to the VM. The perquisite packages and software are summarized in Table 1.

Table 1
List of Packages, Repositories and Software.

Package/ Repository / Software	Usage
Git	**Clone repo from GitHub.**
GCC, GCC++	**Required by OMNeT ++**
Open JDK 1.7/1.8	**Required by OMNeT ++**
SUMO	**An open source software simulation used for vehicle mobility.**
OMNeT++	**An open source software used for network simulation.**
VENTOS	**VENTO framework used to integrate SUMO and OMNeT++**

There are many components included in the VENTOS Framework such as messages, network description files, nodes, Traffic Control Interface (TraCI) and many others. The messages by default get accepted during the communication between vehicles to RSU or other vehicles. Consequently, the workflow illustrated in Fig. 6 is applied to the message coming from vehicle to vehicle or RSU to validate the identity of the vehicle before accepting the message. Storing all data from different parts of this model in the cloud. Vehicles, DoT, RSU, and NCDC generate data and need to be stored. Therefore, timeliness of Cloud databases is a main concern. Unfortunately, neither real-time is easily ensured on large distributed systems nor accurate and effective methodologies have been established to evaluate time-related performance. The way the Cloud database stores and retrieves records has a large impact on the overall time performance; and, since different optimization techniques are probably applied depending on the estimated activity, this delay may hugely vary when the number of nodes changes (Ferrari et al., 2020).

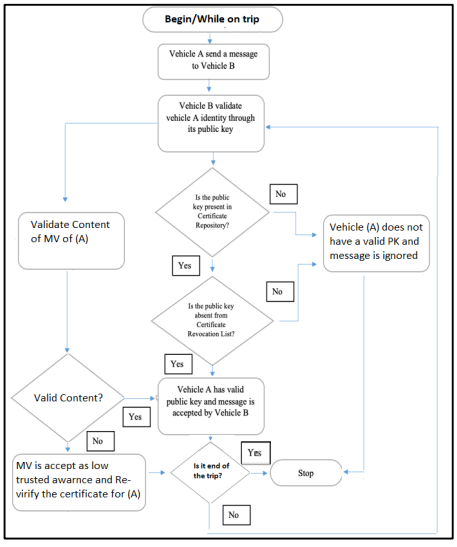

Fig. 6. Validating Vehicles Before Accepting Message Workflow

6. Research Results and Discussions

We have implemented the proposed approach over VENTOS Framework and developed different scenarios to validate the proposed approach. We started with a very simple scenario then we made more complicated ones. This section discusses and shows the results of different scenarios that show the communication between different vehicles and illustrates that messages from trusted vehicles are accepted while messages from malicious vehicles are ignored.

6.1. First Scenario

The first scenario has three trusted vehicles and an accident which is an obstacle occurred in lane 2 as shown in Fig. 7. The first trusted vehicle, colored in green, is going into the same lane where the accident happens and then notifies the RSU about the accident as shown in Fig. 8.

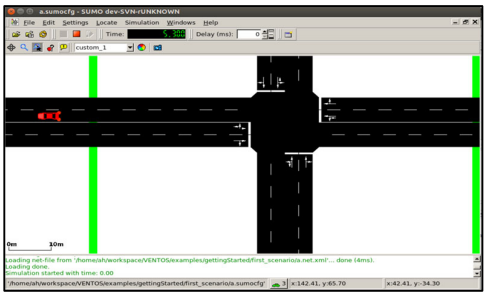

Fig. 7. Scenario1: Vehicle Accident (Obstacle) Occur in Lane 2

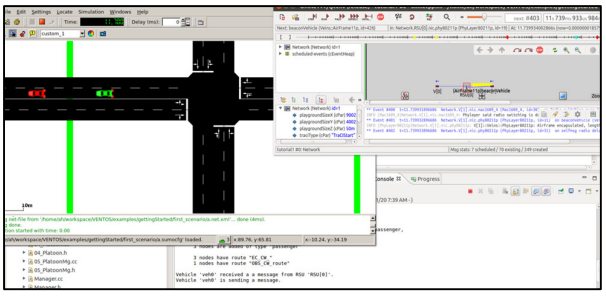

Fig. 1. Scenario 1: A Trusted Vehicle Communicates with the RSU to Inform about Accident

The RSU will communicate with incoming vehicles, colored in yellow, and request them to change their lanes to the first lane as shown in Fig. 9. The RSU range is represented by the green color lines in the simulation diagram. As per the RSU communication and since the message was generated from a trusted vehicle, the message is accepted by the incoming vehicles, and they will change their lanes to lane 1 as shown in Fig. 10.

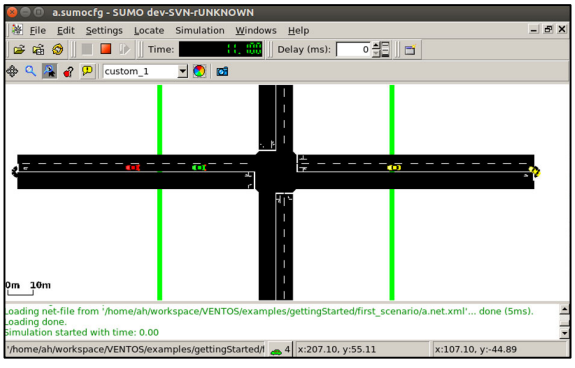

Fig. 9. Scenario 1: The RSU Communicates with the Incoming Vehicles

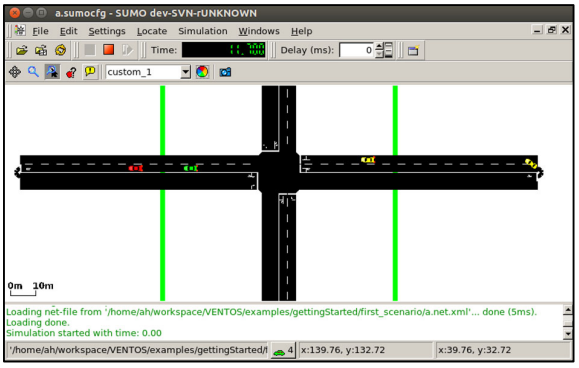

Fig. 2. Scenario 1: Message is Accepted, and Vehicle Change its Lane to Avoid the Accident

6.2. Second Scenario

The second scenario has one malicious vehicle which attempts to send a message to other vehicles and the RSU to change their lanes to the lane where the accident occurs; but the other vehicles will not accept the message since the vehicle is not trusted. The malicious vehicle is colored in red as shown in Fig. 11. Fig. 12 shows that the vehicles did not accept the message and did not change their lane.

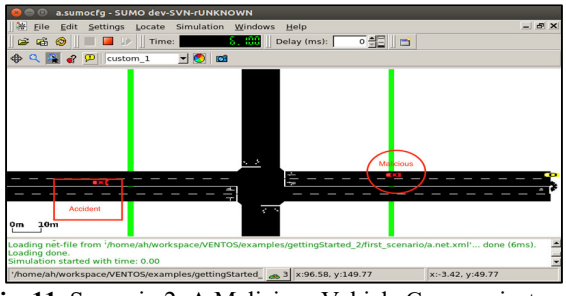

Fig. 11. Scenario 2: A Malicious Vehicle Communicates with the RSU and other Vehicles to Change Them

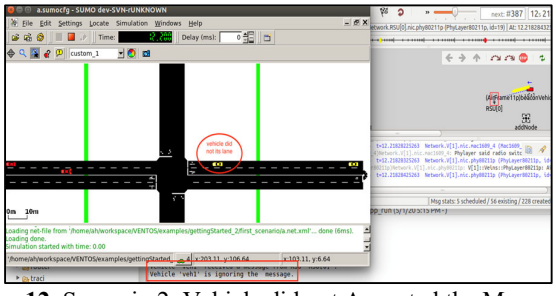

Fig. 12. Scenario 2: Vehicle did not Accepted the Message

6.3. Third Scenario

In this scenario, the first two scenarios are combined, where a trusted vehicle reports an accident (obstacle) in the road and a malicious vehicle sends a message to other vehicles for them to be on the same road that has the accident. Fig. 13 shows three vehicles. Two of them are moving (colored in greed and red). The last one represents an accident. The green colored car is the trusted vehicle where it will communicate with the RSU and incoming vehicles to change their lanes, while the red is the malicious vehicle that will communicate with a false message in order keep incoming vehicles on the same lane that has the accident. The yellow car in Fig. 14 is the vehicle which is coming after the two vehicles. The yellow vehicle will accept the message from the green vehicle as it is a trusted vehicle and will ignore the message from the red vehicle as it is not trusted as shown in Fig. 15.

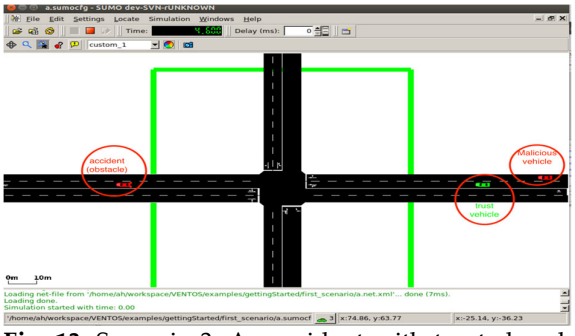

Fig. 13. Scenario 3: An accident with trusted and untrusted vehicles scenario

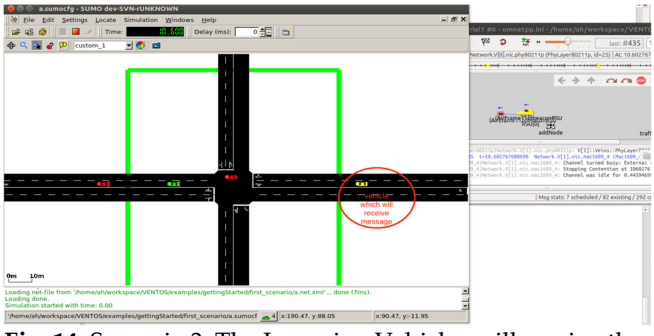

Fig. 14. Scenario 3: The Incoming Vehicles will receive the Message and Accept or Ignore the Message Based on Trust

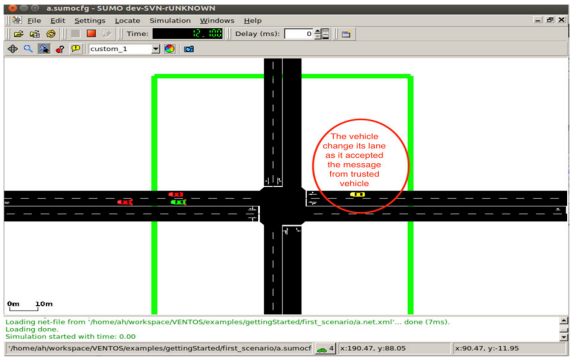

Fig. 15. Scenario 3: Yellow Vehicle Accepts the Message and Change the Lane

6.4. Fourth Scenario

In this scenario, there are four vehicles that move in a highway, then a trusted vehicle, colored in green, communicates with these four vehicles to set their speeds to 10 as advised by the road sign as shown in Fig. 16. All four vehicles, colored in yellow, will accept the message since it is coming from a trusted vehicle, and they gradually change their speeds as shown in the output log shown in Fig. 17. Then, a malicious vehicle, colored in red, will communicate with the four vehicles and give them a false message to reduce their speeds to 0 in order to make them crash but the malicious message is dropped as shown in the log in Fig. 18.

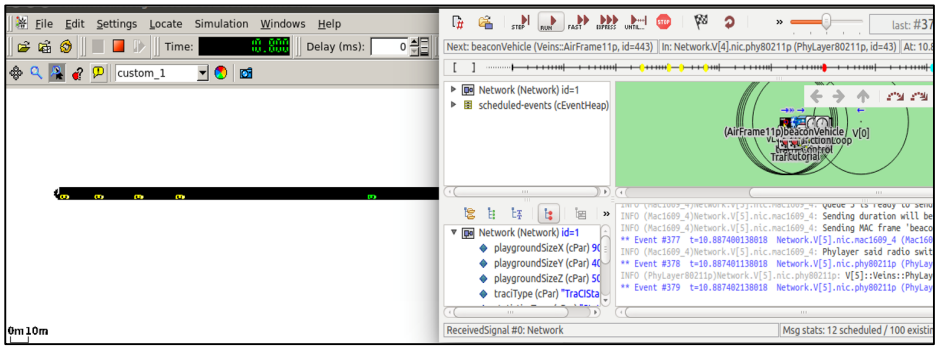

Fig. 3. Scenario 4: Trusted Vehicle Communicates with other Vehicles

index	timeStamp	vehid	lanepos	speed
353	35.20	veh1	313.83	10.00
353	35.20	veh2	290.43	10.00
353	35.20	veh3	267.03	10.00
353	35.20	veh4	243.64	10.00

Fig. 4. Scenario 4: Part of the Output Log Shows that Vehicle Speed is 10

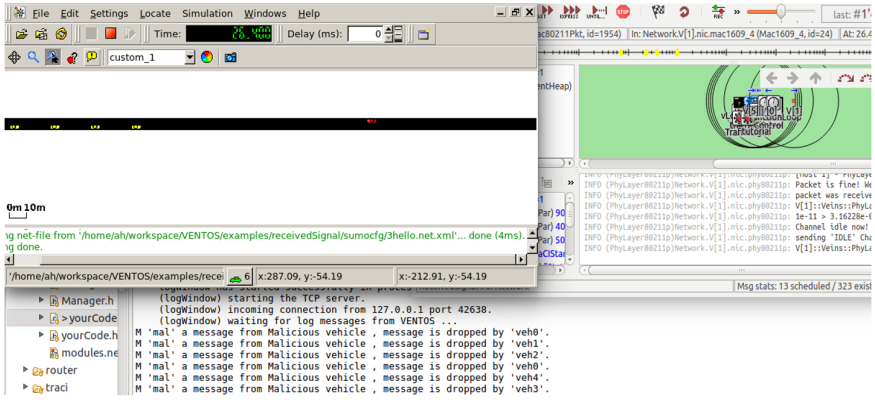

Fig. 5. Scenario 4: Vehicles Dropping Messages from Malicious Vehicle

6.5. Fifth Scenario

In this scenario, we have applied a similar approach as scenario four where trusted vehicles will communicate with each other to recommend the speed to be 10, and malicious vehicles communicate with other vehicles to set their speeds to be 0. However, we have made it to be on a large scale as we have added a small part of Stockholm city and included 6 RSUs as shown in Fig. 19. The number of trusted vehicles is 10 and the number of malicious vehicles is 2. The trusted vehicles ignore messages from malicious vehicles as shown in Fig. 20.

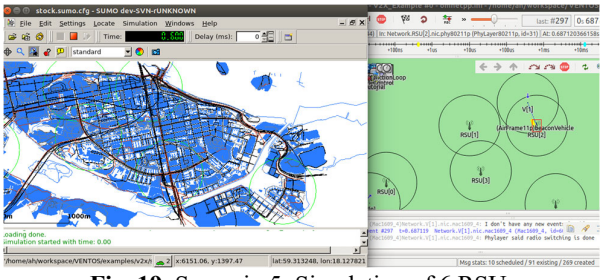

Fig. 19. Scenario 5: Simulation of 6 RSUs

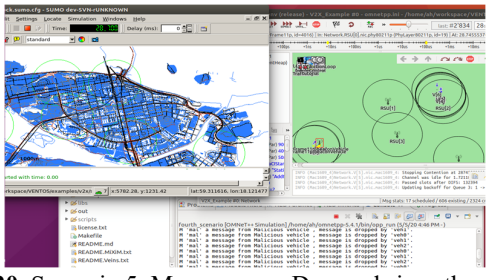

Fig. 20. Scenario 5: Messages are Dropped since they are coming from Untrusted Vehicles

7. Conclusions and Future Work

In this paper, we have reviewed previous studies in trust management of the IoV field. Trust management models in IoV can be divided into three categories. First, trust models are based on an entity where trust is evaluated based on the entity, if the entity is trusted then the data coming from this entity is trusted. The second approach is based on data where trust value is calculated based on trust value of data which can be evaluated from different entities or based on predefined rules such as accuracy of data. The third method is a combination of the previous two approaches which is considered as the most complex way of building a trust model.

In this paper, a new trust model is proposed based on entities with the utilization of the public key infrastructure to distribute valid certificates to the vehicles from trusted certificate authority called Digital Certificate Center of Saudi Arabia in our model. Owners of the vehicle will register their vehicles with Mirror validation authority which cross checks the identity and raises a request to the Digital Certificate Center of Saudi Arabia to issue a certificate to the vehicle which will contain the public key. The vehicles will validate the certificate and public key in order to accept or reject a message. Different scenarios were discussed, and messages are accepted from trusted vehicles and dropped from untrusted ones. This approach can protect from man-in-the-middle attack as public key infrastructure ensures the integrity as any alteration of the message will be detected and can be prevented.

For future work, we recommend improving this trust model by combining it with a reputation trust model in order to evaluate messages before accepting them even if they come from a trusted vehicle. This will protect vehicles from hijacking scenarios.

In addition, this trust model can be evaluated in more complex scenarios or compared with other trust models to realize its performance analysis.

References

Ahmad, F., Adnane, A., Kerrache, C. A., Franqueira, V. N., & Kurugollu, F. (2020). Trust management in vehicular ad-hoc networks and Internet-of-Vehicles: Current trends and future research directions. In *Global Advancements in Connected and Intelligent Mobility: Emerging Research and Opportunities* (pp. 135-165). IGI Global.

Airehrour, D., Gutierrez, J., & Ray, S. K. (2016). Secure routing for internet of things: A survey. *Journal of Network and Computer Applications*, *66*, 198-213.

Amoozadeh, M., Deng, H., Chuah, C. N., Zhang, H. M., & Ghosal, D. (2015). Platoon management with cooperative adaptive cruise control enabled by VANET. *Vehicular communications*, *2*(2), 110-123.

Chai, H., Leng, S., Zhang, K., & Mao, S. (2019). Proof-of-reputation based-consortium blockchain for trust resource sharing in internet of vehicles. *IEEE Access*, *7*, 175744-175757.

Chen, J. M., Li, T. T., & Panneerselvam, J. (2018). TMEC: a trust management based on evidence combination on attack-resistant and collaborative internet of vehicles. *IEEE Access*, *7*, 148913-148922.

Djedjig, N., Tandjaoui, D., Romdhani, I., & Medjek, F. (2018). Trust management in the internet of things. In *Security and Privacy in Smart Sensor Networks* (pp. 122-146). IGI Global.

Ferrari, P., Sisinni, E., Depari, A., Flammini, A., Rinaldi, S., Bellagente, P., & Pasetti, M. (2020). On the performance of cloud services and databases for industrial IoT scalable applications. *Electronics*, *9*(9), 1435.

Gai, F., Zhang, J., Zhu, P., & Jiang, X. (2017). Ratee-based trust management system for internet of vehicles. In *Wireless Algorithms, Systems, and Applications: 12th International Conference, WASA 2017, Guilin, China, June 19-21, 2017, Proceedings 12* (pp. 344-355). Springer International Publishing.

Garcia-Magarino, I., Sendra, S., Lacuesta, R., & Lloret, J. (2018). Security in vehicles with IoT by prioritization rules, vehicle certificates, and trust management. *IEEE Internet of Things Journal*, *6*(4), 5927-5934.

Gazdar, T., Belghith, A., & Abutair, H. (2017). An enhanced distributed trust computing protocol for VANETs. *IEEE Access*, *6*, 380-392.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), 1645-1660.

Halabi, T., & Zulkernine, M. (2019, May). Trust-based cooperative game model for secure collaboration in the internet of vehicles. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access*, *7*, 82721-82743.

Hbaieb, A., Ayed, S., & Chaari, L. (2022). A survey of trust management in the Internet of Vehicles. *Computer Networks*, *203*, 108558.

Hernandez, P. (2020, February 21). McAfee reports: About 2.5 million IoT devices were infected by Mirai botnet in Q4 of 2016.

Iqbal, R., Butt, T. A., Afzaal, M., & Salah, K. (2019). Trust management in social internet of vehicles: factors, challenges, blockchain, and fog solutions. *International Journal of Distributed Sensor Networks*, *15*(1), 1550147719825820.

Javaid, U., Aman, M. N., & Sikdar, B. (2020). A scalable protocol for driving trust management in internet of vehicles with blockchain. *IEEE Internet of Things Journal*, *7*(12), 11815-11829.

Khan, U., Agrawal, S., & Silakari, S. (2015). Detection of malicious nodes (DMN) in vehicular ad-hoc networks. *Procedia computer science*, *46*, 965-972.

Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, *141*, 199-221.

Kuzin, M., Shmelev, Y., & Kuskov, V. (2018). New trends in the world of IoT threats. *Kaspersky Lab*.

Liang, L., Peng, H., Li, G. Y., & Shen, X. (2017). Vehicular communications: A physical layer perspective. *IEEE Transactions on Vehicular Technology*, *66*(12), 10647-10659.

Lopez, P. A., Behrisch, M., Bieker-Walz, L., Erdmann, J., Flötteröd, Y. P., Hilbrich, R., & Wießner, E. (2018, November). Microscopic traffic simulation using sumo. In *2018 21st international conference on intelligent transportation systems (ITSC)* (pp. 2575-2582). IEEE.

Mármol, F. G., & Pérez, G. M. (2012). TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of network and computer applications*, *35*(3), 934-941.

Nanda, A., Puthal, D., Rodrigues, J. J., & Kozlov, S. A. (2019). Internet of autonomous vehicles communications security: overview, issues, and directions. *IEEE Wireless Communications*, *26*(4), 60-65.

Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The internet society (ISOC)*, *80*, 1-50.

Shaikh, R. A., & Alzahrani, A. S. (2014). Intrusion-aware trust model for vehicular ad hoc networks. *Security and communication networks*, *7*(11), 1652-1669.

Sharma, N., Chauhan, N., & Chand, N. (2018, December). Security challenges in Internet of Vehicles (IoV) environment. In *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)* (pp. 203-207). IEEE.

Sharma, S., & Kaushik, B. (2019). A survey on internet of vehicles: Applications, security issues & solutions. *Vehicular Communications*, *20*, 100182.

Shrestha, R., & Nam, S. Y. (2017). Trustworthy event-information dissemination in vehicular ad hoc networks. *Mobile Information Systems*, *2017*.

Siddiqui, S. A., Mahmood, A., Sheng, Q. Z., Suzuki, H., & Ni, W. (2021). A survey of trust management in the internet of vehicles. *Electronics*, *10*(18), 2223.

Singh, P. K., Singh, R., Nandi, S. K., Ghafoor, K. Z., Rawat, D. B., & Nandi, S. (2020). Blockchain-based adaptive trust management in internet of vehicles using smart contract. *IEEE Transactions on Intelligent Transportation Systems*, *22*(6), 3616-3630.

Talal, M., Zaidan, A. A., Zaidan, B. B., Albahri, A. S., Alamoodi, A. H., Albahri, O. S., ... & Mohammed, K. I. (2019). Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review. *Journal of medical systems*, *43*, 1-34.

Tang, Z., Liu, A., Li, Z., Choi, Y. J., Sekiya, H., & Li, J. (2016). A trust-based model for security cooperating in vehicular cloud computing. *Mobile information systems*, *2016*.

Wehrle, K., Günes, M., & Gross, J. (Eds.). (2010). *Modeling and tools for network simulation*. Springer Science & Business Media.

World Health Organization. (2015). *Global status report on road safety 2015*. World Health Organization.

Wu, A., Ma, J., & Zhang, S. (2011, September). RATE: a RSU-aided scheme for data-centric trust establishment in VANETs. In *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing* (pp. 1-6). IEEE.

Yang, F., Wang, S., Li, J., Liu, Z., & Sun, Q. (2014). An overview of internet of vehicles. *China communications*, *11*(10), 1-15.

Yang, N. (2013). A similarity based trust and reputation management framework for vanets. *International Journal of Future Generation Communication and Networking*, *6*(2), 25-34.

Yang, Z., Yang, K., Lei, L., Zheng, K., & Leung, V. C. (2018). Blockchain-based decentralized trust management in vehicular networks. *IEEE internet of things journal*, *6*(2), 1495-1505.