Computers, Materials & Continua
DOI:10.32604/CMC.2021.017620
Article

Tech Science Press

Context and Machine Learning Based Trust Management Framework for Internet of Vehicles

Abdul Rehman[1,*], Mohd Fadzil Hassan[1], Yew Kwang Hooi[1], Muhammad Aasim Qureshi[2], Tran Duc Chung[3], Rehan Akbar[4] and Sohail Safdar[5]

[1]Computer and Information Science Department, Centre for Research and Data Science (CeRDaS), Universiti Teknologi PETRONAS, 32610, Seri Iskandar, Perak Darul Ridzuan, Malaysia
[2]Department of Computer Science, Bahria University, Pakistan
[3]Computing Fundamental Department, FPT University, Hoa Lac Hi-Tech Park, Hanoi, Vietnam
[4]Department of Information Systems, Universiti Tunku Abdul Rahman, Malaysia
[5]Information Technology Department College of IT, AHLIA University, Bahrain
[*]Corresponding Author: Abdul Rehman. Email: abdul_18000023@utp.edu.my
Received: 05 February 2021; Accepted: 22 March 2021

Abstract: Trust is one of the core components of any ad hoc network security system. Trust management (TM) has always been a challenging issue in a vehicular network. One such developing network is the Internet of vehicles (IoV), which is expected to be an essential part of smart cities. IoV originated from the merger of Vehicular ad hoc networks (VANET) and the Internet of things (IoT). Security is one of the main barriers in the on-road IoV implementation. Existing security standards are insufficient to meet the extremely dynamic and rapidly changing IoV requirements. Trust plays a vital role in ensuring security, especially during vehicle to vehicle communication. Vehicular networks, having a unique nature among other wireless ad hoc networks, require dedicated efforts to develop trust protocols. Current TM schemes are inflexible and static. Predefined scenarios and limited parameters are the basis for existing TM models that are not suitable for vehicle networks. The vehicular network requires agile and adaptive solutions to ensure security, especially when it comes to critical messages. The vehicle network's wireless nature increases its attack surface and exposes the network to numerous security threats. Moreover, internet involvement makes it more vulnerable to cyber-attacks. The proposed TM framework is based on context-based cognition and machine learning to be best suited to IoV dynamics. Machine learning is the best solution to utilize the big data produced by vehicle sensors. To handle the uncertainty Bayesian machine learning statistical model is used. The proposed framework can adapt scenarios dynamically and infer using the maximum possible parameter available. The results indicated better performance than

existing TM methods. Furthermore, for future work, a high-level machine learning model is proposed.

Keywords: Internet of vehicles (IoV); trust management (TM); vehicular ad hoc network (VANET); machine learning; context awareness; bayesian learning

1 Introduction

The coming era is of high-speed communications and the Internet of things (IoT). By 2025, IoT will be connecting up to 21 billion devices [1]. The Vehicular ad hoc network (VANET) is one of the research areas shifting towards IoT, such as the Internet of vehicles IoV [2–6]. Since the IoV is not yet standardized, a few studies have been carried out in this field. Security in wireless networks has always been a core challenge, especially ad hoc networks where each time distinct nodes are likely to involve in network formation [7,8]. Similarly, the biggest threat for IoV is a security breach [9,10], which can cause a catastrophic sequence of chain accidents, traffic congestions, and diverting traffic to a specific path. The vehicular network has unique properties, unlike other wireless networks. The vehicle network's dynamic topology increases the attack-surface [11,12], allowing malicious nodes to launch an attack through a security breach. Moreover, the vehicle networks have no geographical limits that make vehicle to vehicle communication very critical. Trust plays an essential role in ensuring security in wireless networks.

Several models have been proposed for trust evaluation in VANET/Intelligent transport system (ITS) over the years, and each model has adopted different techniques and methods. Due to the heterogeneous nature, many factors need to be considered while evaluating the trust, which is missing in existing static models. Every model has one thing in common; they have selected set parameters or scenarios that are not ideal for changing vehicle networks. In a small experimental setting, most models have attempted to solve such issues that work only if significant changes are not made. In conclusion, the vehicle network is a complex system for which the available models are unable to provide an adaptive solution. The proposed TM framework uses the context-aware cognitive approach to solve the problem. Our work is motivated to fill that gap where TM is flexible and static. The framework constructs a scenario-based context for every other critical message received. The framework is subsequently structured to adopt the appropriate trust module for each scenario.

The vehicular network TM schemes must be adaptive to the environment. Artificial intelligence (AI) is the core approach to developing context-awareness. AI techniques are the most effective for building context [13]. Cognitive inferencing is used for context-awareness in the presented TM framework. Besides context-awareness, machine learning is another suitable technology to be implemented on IoV gathered data. Taking full use of IoV big data is one of this study's goals, which requires machine learning solutions. Machine learning is the best approach to single out the malicious nodes from VANET [14,15]. Machine learning algorithms proved dynamic properties to assure security in VANETS [15,16]. The vehicular network has not taken full use of machine learning yet. Trust is one of the areas that can be managed using machine learning. Within the trust, uncertainty is the critical issue faced by the vehicular network during trust evaluation. The framework uses a statistical machine learning technique; Bayesian machine learning (BML) evaluates trust under uncertainty. BML provides multilevel adaptive features to match the dynamic nature of IoV [17,18].

An overview of the IoV architecture is presented in Fig. 1. The centralized data repository is managed through cloud services. Vehicle nodes are equipped with an On board unit (OBU) that simultaneously function as fog nodes with a local data repository called OBUfog. The local data repository is synchronized parodically with a centralized repository. The trust value of all nodes is stored and updated in a centralized database. The framework uses a local data repository for immediate data access, and it is useful in case of the unavailability of internet access or disconnection from the centralized system. The unavailability of a centralized system is a frequent issue with vehicular networks. The use of a decentralized approach is equally helpful to deal with critical issues in communication security.

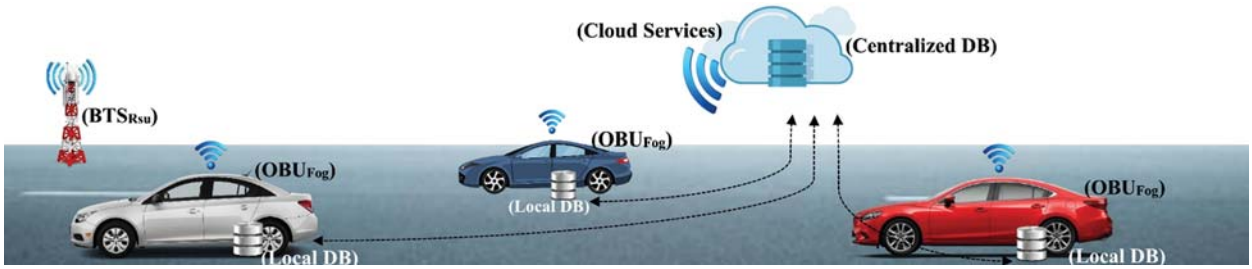

Figure 1: An overview of the IoV architecture, with all nodes equipped with OBUfog and local data repository, connected to a centralized cloud database using BTSRsu

The rest of the paper is organized as Section 2 is the literature review, Section 3 explains the proposed framework. Section 4 discusses the trust evaluation process Section 5 is performance analysis. The last section concludes the research study.

2 Literature Review

The security of any information system has always been a critical concern. In a study [4] on the upcoming challenges of IoV, authors identify security as a critical challenge to overcome. IoV is the future of intelligent vehicular communication and smart cities [19]. Multidimensional security problems occur within IoV, making security one of the main challenges for ad hoc networks. Available models for trust evaluation and management in IoV do not provide the ultimate solution and thus require improvement [11,20]. Many trust models for vehicle networks have been proposed; we discuss some of the renowned models in this section. Most of the trust models available are based on VANETs or ITS. A few recent works can be found on IoV considering trust [21,22]. The existing models can be classified by trust measuring type and categorized into three: data-centric, entity-centric, and hybrid models.

2.1 Trust Models

Trust is determined by the received messages in data-centric models. In a data-centric model, neighboring nodes share their trust opinions on specific events and calculating the trust by majority estimate [23]. The key downside of such models is, they neglect information relevant to the node [11]. Entity-centric models are based on trust credit building. In these models, the interaction experience is an important characteristic. When measuring trust in real-time, inter-node interaction experience is taken into account [24,25]. In one of the entity-centric trust models, the level of trust is determined by fuzzy logic [25]. Another such model presented by [26] work on prior experience, Certificate authority (CA) and, neighbor opinion. The key issue with these

models is that they presume that the malicious activity cannot be performed when the node is authenticated. The second drawback is the dependency on CA. Overall entity centric models are a very powerful tool for evaluating trust. However, these models miss the useful aspects of data centric.

Hybrid models incorporate properties of data and entity to determine trust. Most of these models evaluate the data trustworthiness and keep track of the node trust. A combination of role-based and experience is one such popular model [27]. Another hybrid model evaluates trust by neighbor opinion and similarity-trust [28]. In a research study, researchers used social-trust while evaluating trust [29]. Some researchers have used probability methods, such as the law of Bayes, the theory of evidence, and the theory of Markov [24,30]. For handling the uncertainty during TM, a couple of hybrid models have been proposed [11,31]. Even though the hybrid models are a combination of data and entity, their dynamic integration is still missing [11]. However, to the depth of study, there is no such trust model that uses all the available information during the event. All the models evaluate trust based on specific predefined parameters and scenarios.

2.2 Machine Learning in Vehicular Networks

Machine learning has notable coherence with IoV due to its ability to generate big data. Significant research work has been conducted so far on VANET using machine learning. A research study investigated different aspects of detecting misbehaving vehicles by machine learning and found machine learning an effective method for vehicular network security [14]. The VANET and machine learning have strong coherence, explored in a comparative study between machine learning and VANETS [15]. Researchers in their work used machine learning to detect DDOS attacks in vehicular networks, the study concluded with positive results [32]. Another research work on VANET security worked on false node position attacks and applied a machine-learning algorithm to solve the problem [33]. Most of the studies have shown promising results.

2.3 Context Awareness

The main aim of using context-awareness is to add flexibility by making maximum use of the available data. Authors in a review study elaborate on the potential need for an AI approach for the trust evaluation in vehicular networks; coherence between VANET security and AI solutions exists [20]. A context is a form of knowledge that relates to the problem-solving ability of humans [34]. AI techniques are suitable for context development [35].

The proposed TM framework relies on a hybrid approach using both data and entity properties. On the other hand, it is also worth mentioning that all the available models are for VANETS/ITS. In contrast, our model is a novel trust model for IoV that works on context adaption and machine learning. To the best of our knowledge, no such trust model is presented in the field yet. Our proposed trust evaluation framework is based on context-awareness.

3 Proposed TM Framework

The proposed IoV TM framework is intended to fill the gaps in trust evaluation. The framework works by establishing a context for an event using a cognitive approach. Fig. 2 shows the proposed TM framework. The framework has three key components: input parameters, context building, and trust evaluation. The framework proposed designs on the best practices of VANET, implemented by notable trust models [24,25,27,28,36]. The framework components are derived from the generic context-aware flow model [34,37,38]. Once a critical incident alert is received from nearby vehicles, next, it requires the sender's authentication. The is responsible for carrying out

the authentication process using the public key infrastructure (PKI). Since it needs cryptography and exceeds the scope of our work, we have already considered existing solutions.

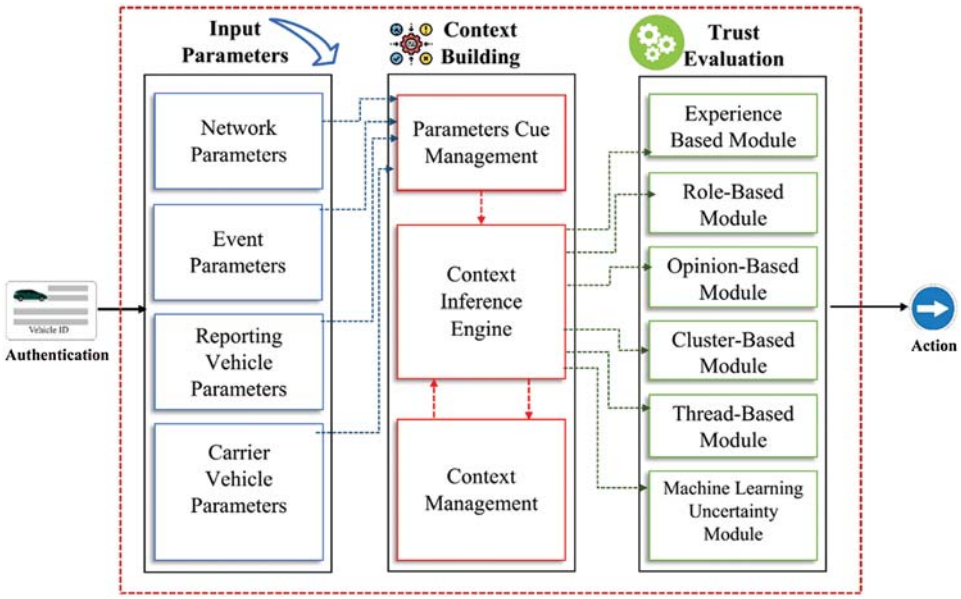

Figure 2: Proposed TM framework with three main modules: input parameters, context building, and trust evaluation

3.1 Parameter Input Layer

After the authentication process, the second task is parameter management, as shown in Fig. 2. Information about an event is filtered out to obtain parameters from the received message token. For ease, the framework classifies all the possible parameters. The information obtained from the node is formalized in "cues," the cues are fed into the context layer for context building. Parameter prioritization is the main task since some parameters have a more valid source and weight than others.

3.2 Context Building Layer

This layer is responsible for building a context around the road event. Context building is the responsibility of the inference engine. The immediately available data is called a low-level context that is transformed into a high-level context. Context data is interconnected information set mostly containing uncertainty. The uncertainty must be handled before submitting it to the context inference process [34]. First, to create a context, the raw data is used, and it is a prerequisite for the development of the context [35]. The perimeter module is responsible for providing available information in the form of readable "cues" to the context module. Context offers complete information to evaluate trust in an event. The context management module is responsible for handling context information obtained from the previous layer.

3.3 Trust Evaluation Layer

The responsibility of this layer is to calculate the trust level. Since the proposed framework is based on the cognitive context approach, the inference engine and trust evaluation modules con-

tinuously exchanged information. The trust evaluation layer consists of different modules. In the proposed TM framework, the trust evaluation process is adaptive. The most used approaches are experience-based, role-based, opinion-based, cluster-based, thread-based, as illustrated in Fig. 2. Different scenarios require different evaluation modules to evaluate the trust. The proposed trust framework matches the most suitable trust evaluation module with an event's scenario using context-awareness.

3.4 Trust Metric

It is essential to define trust metrics before moving towards the trust framework. All existing models have taken into consideration different paraments as metrics. Experience is one of the most used parameters by many models [25,27,28]. Different models also use parameters such as time, location, distance, and others. The goal of our work is to use the maximum available parameters to evaluate trust. The set of trust metrics is made adaptive for this purpose.

4 Trust Evaluation Process

The proposed TM framework evaluates trust based on a critical road event. Trust evaluation revolves around the road-event. The event is denoted by Event ID (Ev_ID). The reporting vehicle that has evident the event itself is Reporter-vehicle (Rp_veh). The vehicles that are not evident in the event still carry the message for hopping or beaconing they are denoted as Carrier-vehicle (Cr_veh). The road event is illustrated in Fig. 3. Local database and centralized data repositories are denoted as Local-database (Loc_DB) and Centralized-database (Cnt_DB). Tr_{ω} denotes the trust level value.

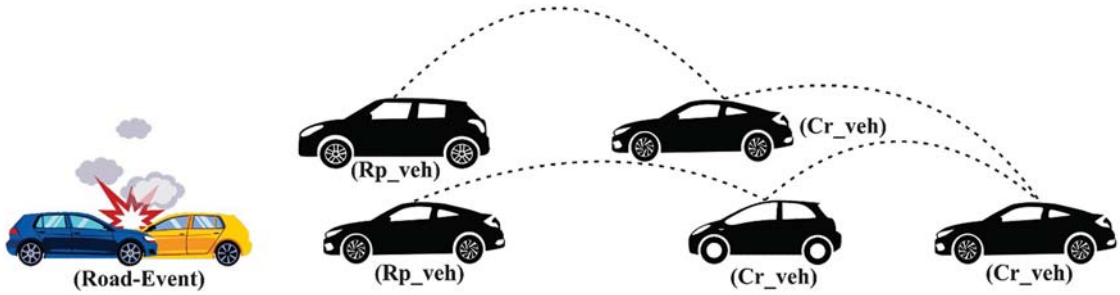

Figure 3: Illustration of road event, with the participation of reporting and carrier vehicles, in hopping

The trust level of a specific event is represented by Ev_ID_Tr_{ω}, and the trust level value of any node is represented by Veh_ID_Tr_{ω}. The unique ID identifies every vehicle in the network. The trust level value is updated after the completion of the event in both local and centralized databases.

4.1 Assumptions

The following assumptions are made to ensure the proper functioning of the proposed TM framework:

- All the vehicles in the network are equipped with OBUFog.
- All vehicles have a uniform communication platform.
- A third-party CA manages the PKI.

4.2 Context Ontology

Ontology is one of the promising methods for context building, which is based on formal logic. With the help of ontology, the context information is built around a road-event. An ontology is an explicit, systematic definition of concepts in a discourse domain. A brief ontology of TM framework is shown in Fig. 4, which illustrates the hierarchical classes and instances of the concept. It is not obligatory to store all relationships with ontology; existing triplets can generate new facts. Together with a collection of individual class instances, an ontology forms a knowledge-base [12].

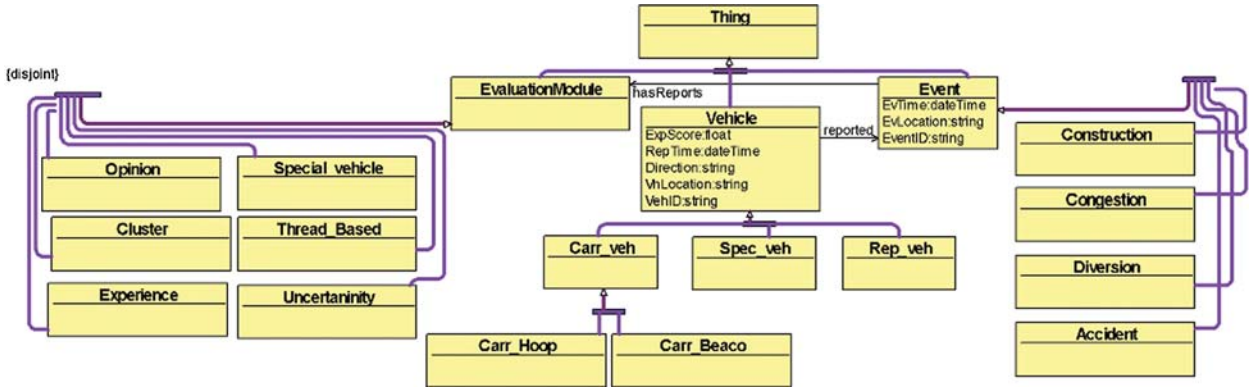

Figure 4: Hierarchical taxonomy, classes, and instances of IoV TM ontology

The taxonomic relationship of ontology includes the following classes: *Vehicle*, *Evaluation-Module*, and *Event*. All the trust evaluation modules are subclasses of class *EvaluationModule*, namely: *ExperienceModule*, *SpecialVehicle*, *Opinion*, *ClusterBased*, *ThreadBased*, and *Uncertainty*. Rep_veh, Carr_veh, and Special_veh are the instances of the class vehicle. The class is disjoint to avoid conceptual overlapping by the reasoner. The instances are associated with the vehicular ID, event ID, location, time, and other data properties.

4.3 Trust Level Threshold

The Trust level (Tr$\ell\omega$) is measured between 0 and 1, an untrustworthy report is denoted as 0, and the highest level of trust is represented by 1 [27,39]. All the values between 0 and 1 are considered as different levels of trust. Initially, all the vehicles are assigned with Tr$\ell\omega$ 0 in Cnt_DB by CA. Unlike common nodes, Tr$\ell\omega$ of special vehicles (ambulance, police, fire brigade) initialized with 0.5. Likewise, the trust of an event Ev_ID_Tr$\ell\omega$ is evaluated and managed during the event. The centralized and local database also store and update event trust value for future verification and trust management. A reported event's trust is also measured between 0 and 1, where 1 represents the highest trust level and 0 for untrusted. The weight allocation Tab. 1 represents: initial trust, previous trust (experience), and trust reward.

The accumulated trust value is the combination of multiple trust values obtained from different modules. The Tr$\ell\omega$1 is the mean trust value of all reporting vehicles obtained by Eq. (1). Reporting vehicles for an event, include general and special vehicles.

$$\mathrm{Tr}lv1 = \frac{\mathrm{Rp\_veh\_Tr}lv \quad (1+2+3\ldots\mathrm{n})}{n} \tag{1}$$

Table 1: Trust weight allocation table

Module	Trust score allocation
Experience-based	Initial node experience (trust score) = 0 Initial special node (trust score) = 0.5 After true report Rep_vehicle= +0.1 Special_vehicle= +0.1
Role-based	Initial special_vehicle experience (trust score) =0.5 After true report Special_vehicle= +0.1
Opinion-based(beaconing)	After true report Carrier_vehicle= +0.05 (beaconing)
Cluster-based	After true report Rep_vehicle= +0.1 Special_vehicle= +0.1
Thread-based(hopping)	After true report Rep_vehicle= +0.1 Carrier vehicle= +0.01 (hopping)
Uncertainty	After true report Rep_vehicle= +0.1 Special_vehicle= +0.1 Carrier_vehicle= +0.01

Carrier vehicles have two types based on hopping and beaconing. Eq. (2) is used to obtain the mean trust $Tr\ell\omega 2$ from carrier vehicles involved in beaconing, whereas carrier vehicles involved in hopping participate in the thread module, discussed in the related section.

$$\mathrm{Tr}lv2 = \frac{\mathrm{Cr\_veh\_\_bec\_Tr}lv \quad (1+2+3\ldots\mathrm{n})}{n} \tag{2}$$

$$\mathrm{Tr}lv3 = \frac{\mathrm{Spe\_veh\_\_Tr}lv \quad (1+2+3\ldots\mathrm{n})}{n} \tag{3}$$

In certain situations where the special vehicle is involved, the mean trust value $Tr\ell\omega 3$ of all Spe_veh can be obtained by Eq. (3). Since the TM framework is adaptive and context-based, the TM might use different trust modules each time. The accumulated trust value of an event Ev_-ID_$Tr\ell\omega$ is obtained by Eq. (4).

$$\mathrm{Ev\_ID\_Tr}lv = \mathrm{Tr}lv_{\mathbf{1}} + \mathrm{Tr}lv_{\mathbf{2}} + \mathrm{Tr}lv_{\mathbf{3}} \tag{4}$$

Eq. (3) serves as the fundamental method for evaluating the trust during the modules: experience, role-base, and opinion-based trust evaluation, each with related specifications. At this point, it is necessary to mention that Eq. (3) involves only those vehicles having a higher or equal experience level than 0.5. Those vehicles with less than 0.5 trust experiences are filtered out and used in other inferencing modules, depending on the context.

4.4 Cluster Module

The cluster-based module is used only for those vehicles that follow the same route daily, In these situations the cluster approach is the most appropriate. The urban traffic mostly follows a pattern by the same vehicle daily. Cluster lists are managed on Cnt_DB and Loc_Db. The reports are broadcasted to all the vehicles in the specific cluster. In combination with other modules, the cluster module is used to determine the trust level according to the context.

4.5 Thread Basedl Hopping

This module is likely to be used where there are hopping in higher numbers than reports and opinions. It is one of the effective techniques used by some models. The basic concept of this module is to use multiple threads of hops. The trust level depends on the thread level (thr_*lev*). This module requires at least two *Rp_vhs.* The level of the thread increases with the intersection of two threads of a single report. The Cr_*vh*, when receives the report with the same thread, considers it as thr_*lev* 1. The level of a thread increases only if a new thread is found. An increment at each level consequently increases the trust level of the report by 0.2.

4.6 Uncertainty Using Statistical Bayesian Machine Learning

Mostly, uncertainty occurs in scenarios where the number of nodes is small. Uncertainty is one of the challenges of evaluating trust. Some TM models vaguely discuss uncertainty in their methodology, such as [30,39]. Using a simple probability is one of the approaches used to handle uncertainty, which is unrealistic. Some approaches include Dempster Shafer theory. The proposed TM framework uses the BML approach to deal with uncertainty. Though BML is one of the rarely used machine learning techniques, it is a constructive statistical method that matches the uncertainty in IoV. Using BML allows combining multiple prior evidence and matches the nature of the problem under discussion. The Bayes rule helps to measure the likelihood of a message being true or false. The experience property must be less than 0.5, as used in Eq. (5). The probability of a report being false can be obtained by Eq. (5). In some circumstances, Rp_vh with less experience is considered under uncertainty. Eq. (6) calculates the trustworthiness of a report.

$$\mathrm{P}(\mathrm{rep\_}\textit{flase}\,|\mathrm{exp\_} < 0.5) = \frac{\mathrm{P}(\mathrm{exp\_}\langle 0.5|\mathrm{rep\_}\textit{flase}).\mathrm{P}(\mathrm{rep\_}\textit{flase})}{P(\mathrm{exp\_} < 0.5)} \tag{5}$$

$$\mathrm{P}(\mathrm{rep\_}\textit{true}\,|\mathrm{exp\_} < 0.5) = 1 + \mathrm{P}(\mathrm{rep\_}\textit{flase}\,|\,\mathrm{exp\_} < 0.5) = \frac{\mathrm{P}(\mathrm{exp\_}\langle 0.5|\mathrm{rep\_}\textit{flase}).\mathrm{P}(\mathrm{rep\_}\textit{flase})}{P(\mathrm{exp\_} < 0.5)} \tag{6}$$

The TM framework performs one step further to be more accurate and use additional available information to infer the trust level of a report. The framework uses BML with multiple evidence; this lets the system infer cognitively when more contextual information is available. Eq. (7) uses multiple evidence BML by adding the direction of the node in Eq. (6).

$$\mathrm{P}(\mathrm{rep\_}\textit{flase}\,|\mathrm{exp\_} < 0.5 \wedge \mathrm{dir\_}\textit{from}) = \frac{\mathrm{P}(\mathrm{exp}_{<0.5} \wedge \mathrm{dir}_{\textit{from}}|\mathrm{rep}_{\textit{flase}}).\mathrm{P}(\mathrm{rep}_{\textit{flase}})}{P(\mathrm{dir}_{\textit{from}} \wedge \ \mathrm{exp}_{<0.5})} \tag{7}$$

The co-occurrence of multiple evidence is calculated by Eq. (7). The P (exp_<0.5 $\wedge$ dir_from) is obtained by Eq. (8).

$$\mathrm{P}(\mathrm{dir\_}\textit{from} \wedge \mathrm{exp\_}\langle 0.5|\mathrm{rep\_}\textit{flase}) = \mathrm{P}(\mathrm{dir\_}\textit{from}\ \ |\mathrm{rep\_}\textit{flase})\ \ \mathrm{P}(\mathrm{exp\_}\langle 0.5|\mathrm{rep\_}\textit{flase}) \tag{8}$$

$$\begin{aligned} P(exp_{<0.5}dir_{from}) = {} & P(exp\_0.5\,|rep\_flase)\;\; P(dir\_from\;\;|rep\_flase)\;\; P(rep\_flase) \\ & + P(exp\_0.5\;\;|rep\_true)P(dir\_from\;\;|rep\_true)P(rep\_true) \end{aligned} \tag{9}$$

$$\begin{aligned} P(rep\_false|exp_{<}0.5 \wedge dir\_from) = {} & \frac{P(rep_{\_flase}).P(exp_{\_<0.5}|rep_{\_flase}).}{P(rep_{\_flase})P(exp_{\_<0.5}|rep_{\_flase})P(dir_{\_from}|rep_{\_flase})} \\ & + \frac{P(dir_{\_from}\;\;|rep_{\_flase})}{P(rep_{\_true})P(exp_{<0.5}|rep_{true})P(dir_{\_from}|rep_{\_true})} \end{aligned} \tag{10}$$

Thus, Eq. (10) is obtained by employing Eqs. (8) and (9) to Eq. (7). The uniqueness of the presented framework is a context where we can add further evidence to infer trust.

Alg. 1 shows the algorithm for a reported event, where a new event report is received. The event is matched with the previous event list, synchronized if the event is previously available; otherwise, a new event is created. Furthermore, the algorithm explains the management of the overall report.

Algorithm 1: Trust Evaluation Algorithm

Pseudocode of event trust evaluation algorithm

```
Initialize
  Event Message received
  Ev_ID retrieved
  Ev_ID_Trlv = 0
  Number of nRp_veh= 0
  Number of nCr_veh =0
If (Ev_ID != exists) than
            start Ev_ID as new event
   else
      merge Veh_ID_Trlv retrieved from Cnt_DB and Loc_DB
      merge Cr_veh_Trlv retrieved from Cnt_DB and Loc_DB
 end If
 If (message receive form Rp_veh) than
      nRp_veh ← nRp_veh+1
   else
      nCr_veh ← nCr_veh+1
 end If
 If (nRp_veh>2) && (Rp_veh_exp>0.5) than
      opt for experience module
   elseIf (special Rp_veh in system) than
      opt for role-based module
   elseIf (nCr_veh >nRp_veh) &&
            (Cp_veh_exp>0.5) than
```

(Continued)

4.7 Message Token

For the TM framework, a token is designed that contains all related information and the message itself. The token is divided into two parts in Tab. 2: the header contains all information

```
24.            opt for Opinion module
25.       elseIf (vehicles share same path frequently) than
26.            opt for Cluster module
27.       elseIf (nCr_veh >nRp_veh) &&
28.                (Cp_veh with high hopping) than
29.            opt for thread-based module
30.       elseIf (uncertain condition) than
31.            opt for uncertainty module
32.    endIf
33.    Ev_ID_Trlv ← (Rp_veh(mean)+Cr_veh(mean) + Spe_veh(mean)+ trust value)
34.    If (Ev_ID_Trlv>0.5) than
35.            perform action,
36.            update in Cnt_DB and Loc_DB
37.            broadcast Ev_ID is trustworthy with Ev_ID_Trlv
38.    else
39.       discard event
40.       update in Cnt_DB and Loc_DB
41.       broadcast Ev_ID is untrustworthy with Ev_ID_Trlv
42.     End
```

related to vehicle and message. The "message" portion only contains information related to road-event. The token is associated and identified with "vehicle ID". The critical messages can be categorized into four categories: accident, traffic congestion, work in progress, and diversion, defined in the event description.

Table 2: Message token

Header									
Vehicle ID	Event ID	Report	Time	Location	Hop	Beaconing	Direction/ Indirect report	Average Speed	Vehicle type
Message									
Event Location		Event Description			Time viewed			Opinion	

4.8 Simulation

The simulation is conducted using MATLAB R2020a and Protege−5.5.0 with the "HermiT 1.4.3 456" reasoner. Depending on the simulation model's scenario, the number of nodes in each random event varies from 2 to 50. The special nodes are set to a maximum of 10%, rest of the 90% nodes are general vehicles. The node trust is initialized by 0 experience, and the special nodes with trust experience by 0.5. A significant concern about simulations relates to outcome variation; outcomes at each attempt may vary due to the experiment's random design. There can be a considerable variation between the same simulation instances in the wireless topology and the network's design. General nodes include reporting and carrier vehicles. In the road network,

road incidents occur at random in the experiment. Each scenario runs 100 iterations to exhaust the simulation.

The framework is tested using scenario-based simulation. The scenarios are divided into three categories to get maximum performance and exhaust the simulation. 1. Heavy traffic: These scenario patterns are often found during rush hours or congestion in urban traffic. These scenarios take up to 50 nodes into consideration. Numerous reports of an incident can be found in these scenarios, making it easy to determine any reported event's level of trust. Most of the trust models perform well in these scenarios. 2. Moderate traffic: 11 to 25 nodes, taken into consideration in these scenarios. These scenarios are typically found during low rush hours in urban areas or on highways. The amount of information available in these situations is also moderate. The proposed framework takes full advantage of the available data, unlike other models that work under limited information. 3. Low traffic: This depicts a traffic pattern found on highways, towns, and rural areas. 2 to 10 nodes are involved in this type of scenario. The lack of information makes these the most critical scenarios. Most of the trust models fail in these scenarios due to the little information available. These scenarios contain maximum uncertainty, which is a significant issue during the trust evaluation.

5 Performance Analysis and Discussion

The module distribution by generating random road events up to 50 nodes can be observed in Fig. 5a. The experience-based module is more likely to occur, and the reason might be the experience property of all the vehicles; this is a significant finding in understanding the type of vehicle involved in the trust evaluation process. The variation of the trust evaluation module can be observed in Fig. 5a. With the smaller number of nodes involved, the opinion module is the highest. In comparison, the moderate node involvement experience module is highly observed. Another notable finding is that the thread-based module requires a higher number of nodes, shows in Fig. 5a. Nonetheless, we believe that it is well justified that uncertainty is high with low node density, which reveals the relations between less information and uncertainty. Depicted in Fig. 5b, involving 10 nodes in the different events, show the "opinion" is with the highest occurrence followed by the experience, the reports with uncertainty are also high. Fig. 5c shows the increment in the number of nodes up to 25 involved in an event. Experience and opinion are almost equal, whereas uncertainty is decreasing. Finally, Fig. 5d shows that the uncertainty is almost inversely proportional to the number of nodes involved in the event.

Fig. 6a shows the trust level evaluated under the experience module. One of the essential features of this framework is the confidence score. Even in the case of high trust, there might be a low confidence score. This feature makes the report more elaborative. Fig. 6b shows the thread module outcomes; a gradual trend during the trust-building phase can be observed. The trust is directly proportional to the thread level. Here it is significant to explain that the level of a thread is not the hop level, which can be observed in Fig. 6b. The results in Fig. 6c show the opinion-based trust evaluation; the confidence line in Fig. 6c supports the legitimacy of trust value. A significant aspect is noted here the confidence score has no coherence with the level of trust. The behavior of "confidence" as an independent variable helps the system make better decisions during trust evaluation. The involvement of special vehicles makes the event more legitimate. A relatively higher trust level can be observed in Fig. 6d, where a special vehicle is involved in trust evaluation. The more special vehicles involved, the higher the level of trust that can be achieved. Fig. 6e summarizes the findings by the uncertainty module. The number of discarded reports is low, and a gradual decrease is observed with an increase in the number of nodes. The use of

big data will probably improve the module's precision over time due to the increased information availability.

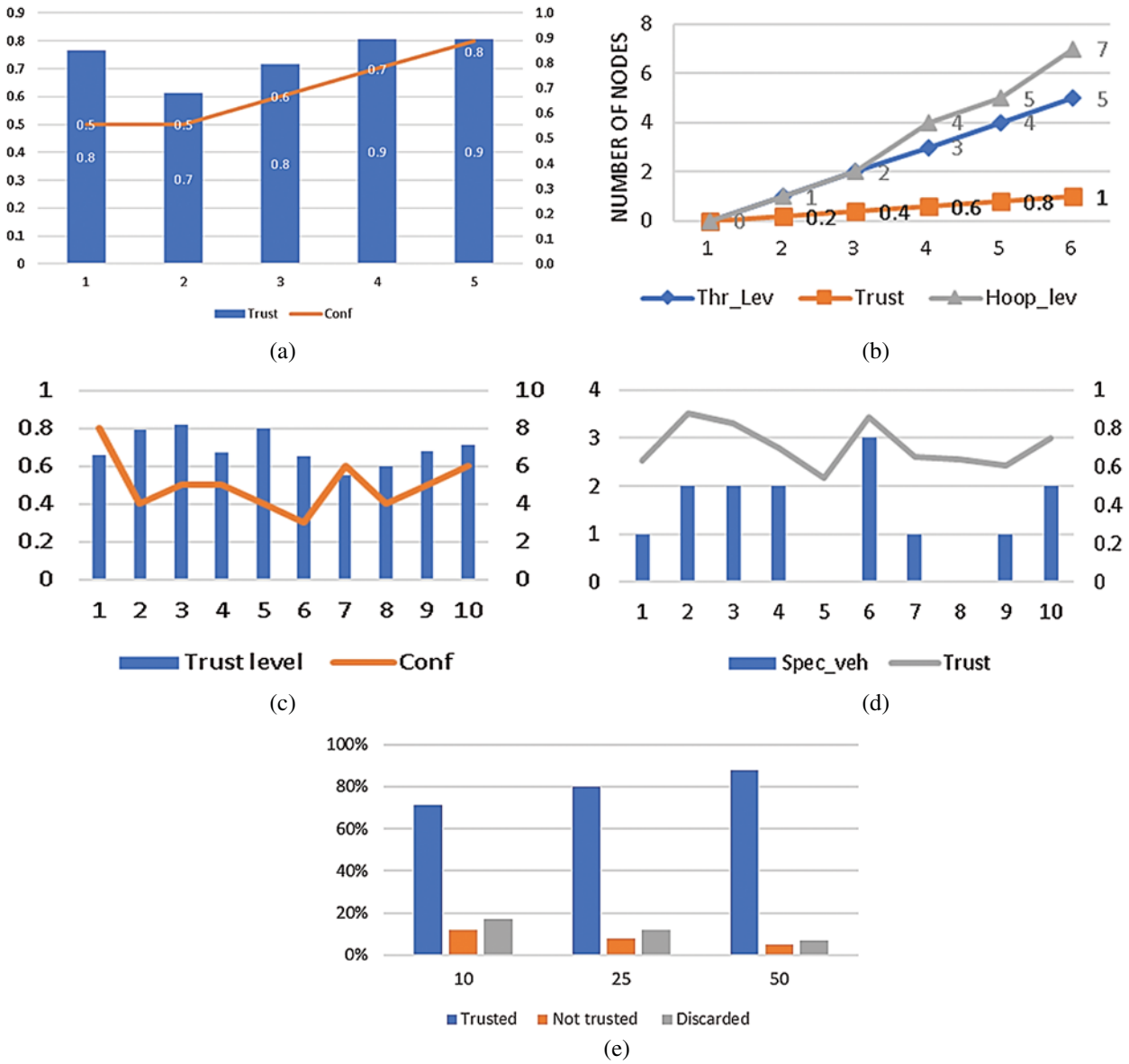

Figure 5: Trust evaluation module and node variation. (a) Relationship of the number of events and nodes under different modules. (b, c, d) Relationship of node variation and different modules

5.1 Limitations

The following limitations must be considered for this TM framework:

- The experiment is conducted using a limited number of nodes, and a large-scale experiment will further improve the accuracy of the results.

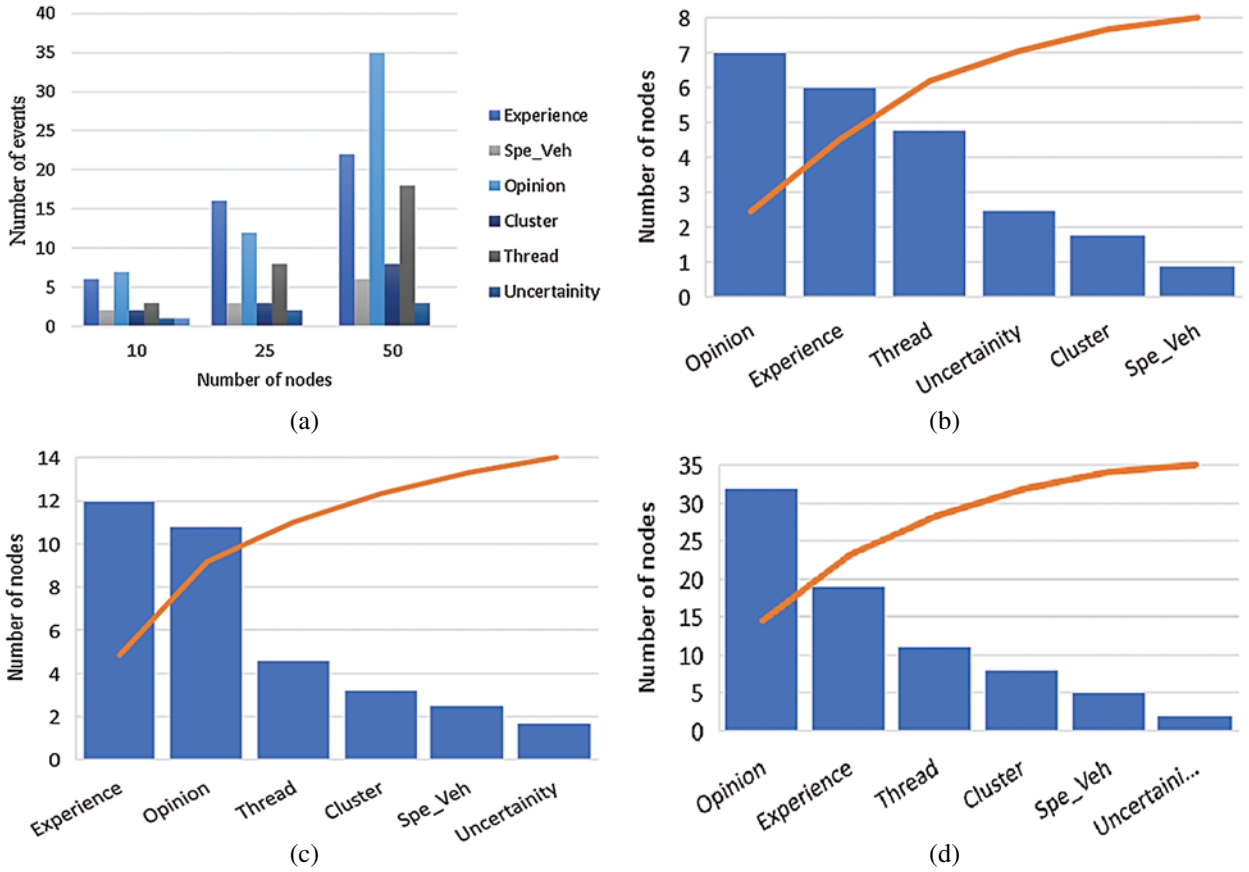

Figure 6: Level of trust and confidence score under different trust evaluation modules. (a) Trust and confidence under experience. (b) Trust under thread-based evaluation module. (c) Opinion module trust and confidence. (d) Special vehicle involvement and trust

- The simulation has shown promising results. An on-road experiment still needs to be conducted.
- The framework does not take the human factor into account.
- The analysis of big data and its involvement in trust evaluation will improve accuracy. A machine learning model is presented in future work that needs to be implemented for further investigation.

5.2 A High-level Machine Learning Inference Model as Future Research Direction

In a short time, the IoV can produce big data; every node generates multiple sensor data. Given this study's limited scope, a high-level machine-learning model as future work is illustrated by Fig. 7. The process begins with data inputs from centralized DB. The second phase is the preprocessing involving: data quality assessment, data cleaning, finding relations, normalization, and feature scaling to specify a range of variables. A mix of supervised and unsupervised learning is suitable to achieve maximum knowledge extraction [40]. The use of regression is ideal for continuous variable prediction. Linear support vector machine (LVSM) is the most suitable because of the trust threshold value [41].

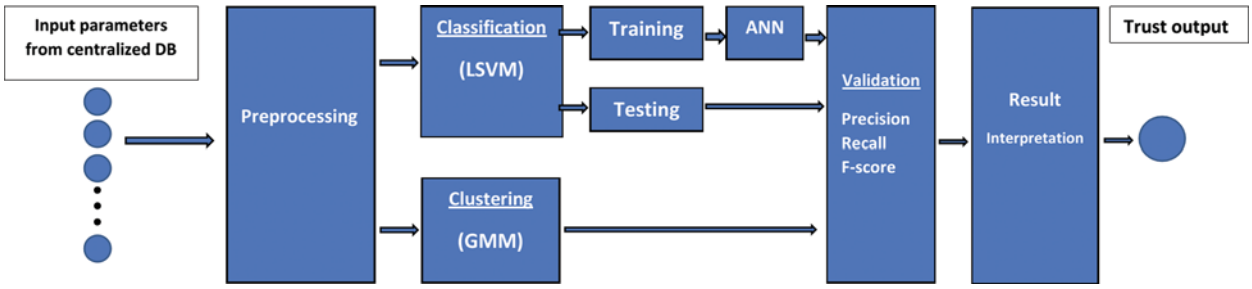

Figure 7: A high-level machine learning model for the inference of trust as a future research direction

An artificial neural network (ANN) is recommended to automate huge sensor data. Similarities in road events are the main reason to use ANN. Malicious node detection is a crucial issue in IoV; the clustering technique is more appropriate and efficient to solve this issue. For clustering, the Gaussian mixture model (GMM) is highly recommended [42]. The reason behind this is the two parameters description method [43]. The training and testing are the subsequent phases to be carried out for regression by the adapting 70:30 general rule. To achieve maximum accuracy of the model, precision, recall, and F-1 score are recommended in the validation phase.

6 Conclusion

Soon, IoV will play a significant role in smart cities and ITS. Many areas of IoV need to be standardized before implementing it as real-time road networks. Trust management is a primary component of vehicle network security, helping prevent a breach of security. In this article, a TM framework is presented for IoV to ensure secure on-road vehicle communication. The proposed trust framework is based on context-awareness, thus use maximum available information resources. The framework works well in critical scenarios where other models fail. The framework intelligently chooses between different trust evaluation modules, thereby allowing full use of available information to determine the received message's trustworthiness. The results indicate that the framework will contribute to trust management security in the vehicle network. The use of the Bayesian method of machine learning was effective when dealing with uncertainty. Our presented trust framework shows promising results. To the best of our knowledge, the work is novel, and no cognitive trust management scheme for IoV has been proposed. The proposed framework is equally beneficial for IoT security.

Acknowledgement: We would like to acknowledge the multinational collaboration made in this research.

Funding Statement: The work is partially funded by CGS Universiti Teknologi PETRONAS, Malaysia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. Zhou, X. Dong, Z. Cao and A. V. Vasilakos, "Secure and privacy preserving protocol for cloud-based vehicular DTNs," *IEEE Transactions on Information Forensics Security and Communication Networks*, vol. 10, no. 6, pp. 1299–1314, 2015.

[2] Y. Xie, X. Su, Y. He, X. Chen, G. Cai *et al.* "Stm32-based vehicle data acquisition system for internet-of-vehicles," *presented at the 16th IEEE Int. Conf. on Computer and Information Science (ICIS)*, China, 2017.

[3] K. M. Alam, M. Saini and A. El Saddik, "Toward social internet of vehicles: Concept, architecture, and applications," *IEEE Access*, vol. 3, no. 1, pp. 343–357, 2015.

[4] Y. Fangchun, W. Shangguang, L. Jinglin, L. Zhihan and S. Qibo, "An overview of internet of vehicles," *China Communications*, vol. 11, no. 10, pp. 1–15, 2014.

[5] S. Sharma and B. Kaushik, "A survey on internet of vehicles: Applications, security issues & solutions," *Vehicular Communications*, vol. 20, no. 2, pp. 100182, 2019.

[6] C. Chen, T. Xiao, H. Zhao, L. Liu and Q. Pei, "GAS: A group acknowledgment strategy for popular content distribution in internet of vehicle," *Vehicular Communications*, vol. 17, no. 1, pp. 35–49, 2019.

[7] H. Hasrouny, A. E. Samhat, C. Bassil and A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, no. 1, pp. 7–20, 2017.

[8] X. Wang, J. Jiang, S. Zhao and L. Bai, "A fair blind signature scheme to revoke malicious vehicles in VANETs," *Computers, Materials & Continua*, vol. 58, no. 1, pp. 249–262, 2019.

[9] T. A. Butt, R. Iqbal, S. C. Shah and T. Umar, "Social internet of vehicles: Architecture and enabling technologies," *Computers & Electrical Engineering*, vol. 69, no. 3, pp. 68–84, 2018.

[10] X. Duan, Y. Zhao, K. Zheng, D. Tian, J. Zhou *et al.* "Cooperative channel assignment for VANETs based on dual reinforcement learning," *Computers, Materials & Continua*, vol. 66, no. 2, pp. 2127–2140, 2021.

[11] X. Yao, X. Zhang, H. Ning and P. Li, "Using trust model to ensure reliable data acquisition in VANETs," *Ad Hoc Networks*, vol. 55, no. 4, pp. 107–118, 2017.

[12] L. Cui, W. Gang, S. Xiaofeng, Z. Feng and Z. Liang, "An efficient certificateless aggregate signature scheme designed for VANET," *Computers, Materials & Continua*, vol. 63, no. 2, pp. 725–742, 2020.

[13] A. Kofod-Petersen and J. Cassens, "Using activity theory to model context awareness," *presented at the Int. Workshop on Modeling and Retrieval of Context*, Edinburgh, UK, 2005.

[14] J. Grover, N. K. Prajapati, V. Laxmi and M. S. Gaur, "Machine learning approach for multiple misbehavior detection in VANET," *in presented at the Int. Conf. on Advances in Computing and Communications*, India, 2011.

[15] S. Ftaimi and T. Mazri, "A comparative study of machine learning algorithms for VANET networks," presented at the the *3rd Int. Conf. on Networking, in Information Systems & Security*, Morocco, 2020.

[16] M. A. Hossain, R. M. Noor, K. -L. A. Yau, S. R. Azzuhri, M. R. Z'aba *et al.* "Comprehensive survey of machine learning approaches in cognitive radio-based vehicular ad hoc networks," *IEEE Access*, vol. 8, no. 1, pp. 78054–78108, 2020.

[17] J. Zhang, K. Zheng, D. Zhang and B. Yan, "AATMS: An anti-attack trust management scheme in VANET," *IEEE Access*, vol. 8, no. 2, pp. 21077–21090, 2020.

[18] M. Bocquet, J. Brajard, A. Carrassi and L. Bertino, "Bayesian inference of chaotic dynamics by merging data assimilation, machine learning and expectation-maximization," *ArXiv Mathematical Sciences*, vol. 2, no. 1, pp. 55–80, 2020.

[19] M. Wazid, A. K. Das, V. Bhat and A. V. Vasilakos, "LAM-Ciot: Lightweight authentication mechanism in cloud-based IoT environment," *Journal of Network and Computer Applications*, vol. 150, no. 2, pp. 102496, 2020.

[20] S. Sumithra and R. Vadivel, "An overview of various trust models for VANET security establishment," presented at the *9th Int. Conf. on Computing*, in *Communication and Networking Technologies (ICCCNT)*, India, 2018.

[21] U. Javaid, M. N. Aman and B. Sikdar, "A scalable protocol for driving trust management in internet of vehicles with blockchain," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11815–11829, 2020.

[22] P. K. Singh, R. Singh, S. K.Nandi, K. Z. Ghafoor, D. B. Rawat *et al.* "Blockchain-based adaptive trust management in internet of vehicles using smart contract," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 7, pp. 1–15, 2020.
[23] U. F. Minhas, J. Zhang, T. Tran and R. Cohen, "Towards expanded trust management for agents in vehicular ad-hoc networks," *International Journal of Computational Intelligence: Theory and Practice (IJCITP)*, vol. 5, no. 1, pp. 03–15, 2010.
[24] T. Gazdar, A. Belghith and H. Abutair, "An enhanced distributed trust computing protocol for VANETs," *IEEE Access*, vol. 6, pp. 380–392, 2018.
[25] S. A. Soleymani, A. H. Abdullah, M. Zareei, M. H. Anisi, C. Vargas-Rosales *et al.* "A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing," *IEEE Access*, vol. 5, no. 1, pp. 15619–15629, 2017.
[26] F. G. Mármol and G. M. Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 934–941, 2012.
[27] F. Ahmad, V. N. Franqueira and A. Adnane, "TEAM: A trust evaluation and management framework in context-enabled vehicular ad-hoc networks," *IEEE Access*, vol. 6, no. 1, pp. 28643–28660, 2018.
[28] S. Ahmed, S. Al-Rubeaai and K. Tepe, "Novel trust framework for vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9498–9511, 2017.
[29] R. Hussain, W. Nawaz, J. Lee, J. Son and J. T. Seo, "A hybrid trust management framework for vehicular social networks," *presented at the Int. Conf. on computational social networks*, Viet Nam, 2016.
[30] D. B. Rawat, G. Yan, B. B. Bista and M. C. Weigle, "Trust on the security of wireless vehicular Ad-hoc networking," *Ad Hoc & Sensor Wireless Networks*, vol. 24, no. 3–4, pp. 283–305, 2015.
[31] Z. Wei, F. R. Yu and A. Boukerche, "Trust based security enhancements for vehicular ad hocnetworks," *presented at the 4th ACM Int. Symp.on Development and Analysis of Intelligent Vehicular Networks and Applications*, Canada, 2014.
[32] A. M. Alrehan and F. A. Alhaidari, "Machine learning techniques to detect DDoS attacks on VANET system: a survey," *presented at the 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, 2019.
[33] P. K. Singh, S. Gupta, R. Vashistha, S. K. Nandi and S. Nandi "Machine learning based approach to detect position falsification attack in vanets," *presented at the Int. Conf. on Security & Privacy*, India, 2019.
[34] F. Paganelli, G. Bianchi and D. Giuli, "A context model for context-aware system design towards the ambient intelligence vision: Experiences in the eTourism domain," *in Universal Access in Ambient Intelligence Environments: Springer*, pp. 173–191, 2007.
[35] A.Schmidt, "Ubiquitous computing-computing in context," Ph.D. Thesis, Computing Department, Lancaster University Lancaster University, U.K., 2003.
[36] T. Biswas, A. Sanzgiri and S. Upadhyaya, in "Building Long Term Trust in Vehicular Networks," *Presented at the IEEE 83rd Vehicular Technology Conf. (VTC Spring)*, China, 2016.
[37] Ö. Yürür, C. H. Liu, Z. Sheng, V. C. Leung, W. Moreno *et al.* "Context-awareness for mobile sensing: A survey and future directions," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 68–93, 2016.
[38] C. Bettini, O. Brdiczka, K. Henricksen, J. Indulska, D.Nicklas *et al.* "A survey of context modelling and reasoning techniques," *Pervasive and Mobile Computing*, vol. 6, no. 2, pp. 161–180, 2010.
[39] X. Ya, Z. Shihui and S. Bin, "Trusted GPSR protocol without reputation faking in VANET," *the Journal of China Universities of Posts and Telecommunications*, vol. 22, no. 5, pp. 22–55, 2015.
[40] M. Alloghani, D. Al-Jumeily, J. Mustafina, A. Hussain and A. J. Aljaaf, "A systematic review on supervised and unsupervised machine learning algorithms for data science," *Supervised and Unsupervised Learning for Data Science*, pp. 3–21, 2020.
[41] Z. F. Hussain, H. R. Ibraheem, M. Alsajri, A. H. Ali, M. A. Ismail *et al.*, "A new model for iris data set classification based on linear support vector machine parameter's optimization," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, pp. 1079–1084, 2020.

[42] J. V. Covioli and G. Coppotelli, *In* "on the use of Gaussian Mixture Models for Automated Modal Parameters Estimation," in *AIAA Scitech 2021 Forum*, Virginia, USA, 2021.

[43] R. Touati, M. Mignotte and M. Dahmane, "Anomaly feature learning for unsupervised change detection in heterogeneous images: A deep sparse residual model," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 13, no. 1, pp. 588–600, 2020.