IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received 22 May 2022, accepted 3 July 2022, date of publication 7 July 2022, date of current version 18 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3189349

RESEARCH ARTICLE

CTMF: Context-Aware Trust Management Framework for Internet of Vehicles

ABDUL REHMAN[1], MOHD FADZIL HASSAN[2], (Senior Member, IEEE), YEW KWANG HOOI[3], MUHAMMAD AASIM QURESHI[4], SAURABH SHUKLA[5], ERWIN SUSANTO[6], SADDAF RUBAB[7], AND ABDEL-HALEEM ABDEL-ATY[8]

[1]Department of Information Technology, Balochistan University of Information Technology, Engineering and Management Sciences (BUITEMS), Quetta 87300, Pakistan
[2]Center for Research in Data Science (CeRDaS), Universiti Teknologi PETRONAS, 32610 Seri Iskandar, Perak Darul Ridzuan, Malaysia
[3]High Performance Cloud Computing Centre (HPC3), Universiti Teknologi PETRONAS, 32610 Seri Iskandar, Perak Darul Ridzuan, Malaysia
[4]Department of Computer Sciences, Bahria University Lahore Campus, Lahore 54000, Pakistan
[5]Insight SFI Centre of Data Analytics, Unit of Semantic Web Data Science Institute (DSI), National University of Ireland Galway (NUIG), Galway, H91 TK33 Ireland
[6]School of Electrical Engineering, Telkom University, Bandung 40257, Indonesia
[7]Department of Computer Engineering, College of Computing and Informatics, University of Sharjah, Sharjah 27272, United Arab Emirates
[8]Department of Physics, College of Sciences, University of Bisha, Bisha 61922, Saudi Arabia

Corresponding author: Abdul Rehman (abdul_18000023@utp.edu.my)

This work was supported by Universiti Teknologi PETRONAS, Malaysia, under Grant YUTP-FRG 1/2021 (015LC0-370).

ABSTRACT Secure communication is the top concern of the Internet of Vehicles (IoV). The trust between nodes can have a considerable impact on ensuring IoV security. Therefore, the trustworthiness of a received message must be evaluated before acting upon it. A malicious node can broadcast bogus events to obtain network control. False reports and malicious vehicles render the network unreliable during emergencies. In this study, a unique trust framework is presented that considers most of the aspects of trust in IoV to accurately identify malicious nodes and events. Previous studies have proposed some trust models for VANETs, which have many deficiencies in serving IoV. In particular, they lack dynamism and practical implementations. All the existing models have two things in common, first they work on fixed parameters, and second, they use static scenarios. In contrast, the proposed framework is based on a context-awareness cognitive approach with artificial intelligence (AI) properties. The framework cognitively learns the environment from the received report and creates a context around an event. In addition to trust management (TM), the proposed framework offers a novel process for detecting and screening malicious nodes using anomaly outliers. The performance of the framework was examined using an experimental simulation. The proposed framework was compared with top benchmarks in the field. The results show inclining performance indicators. The proposed trust-management framework has the potential to serve as a component of IoV security.

INDEX TERMS Internet of Vehicles (IoV), trust management (TM), vehicular ad hoc network (VANET), context awareness.

I. INTRODUCTION

High-speed wireless communication has revolutionized the Internet of Things (IoT). Currently, every other field is merging in IoT; likewise, vehicular communication has shifted from vehicular ad hoc networks (VANETs) to the Internet of Vehicles (IoV) [1]. IoV is in the development phase and has not been applied to on-road traffic; however, it is soon expected to be part of on-road traffic. For IoV, communication security is a high-priority requirement. The information shared among nodes is highly sensitive; if breached, it can result in traffic accidents and life threats to humans. Owing to Internet connectivity and wireless networks, IoV is always vulnerable to serious security threats; the internet has increased the attack surface for cyber threats. Malicious nodes in a network can maneuver all vehicles by sending fake messages, resulting in catastrophic outcomes [2]. Under these circumstances, trust plays a vital role in enhancing

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen.

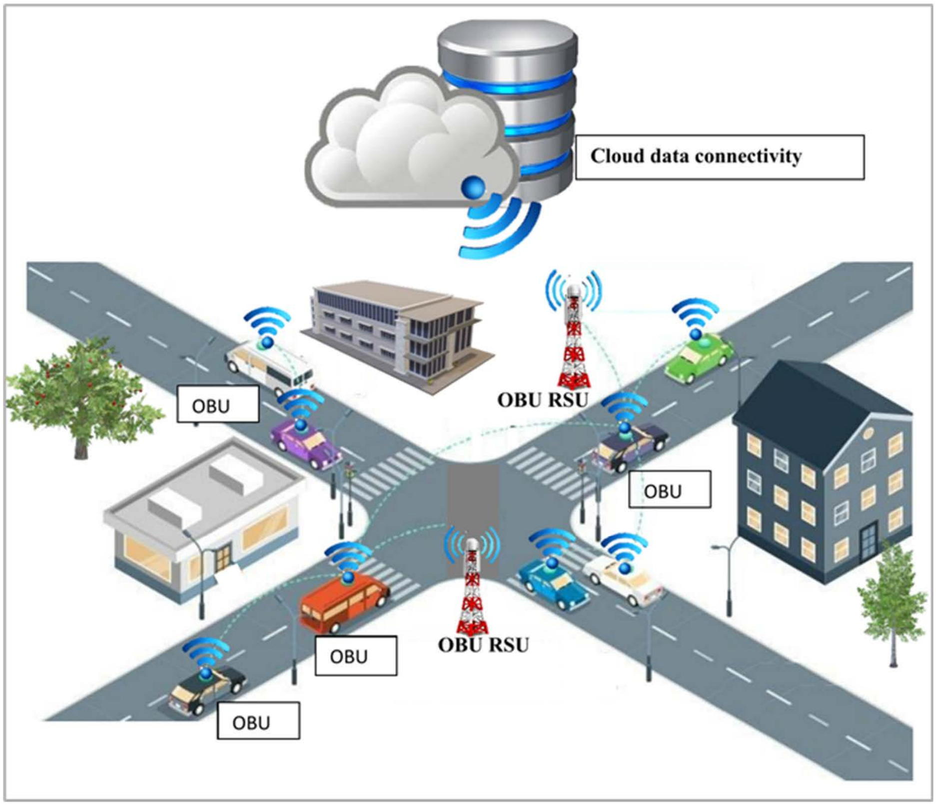


FIGURE 1. Overview of the presented IoV architecture, where all nodes are equipped with OBU and local data repository, linked to a central cloud-based system using BTSRsu.

wireless network security. Trust has always been a part of vehicular network security [3]. Good trust management has been proven to improve security while nodes communicate vital messages [3], [4]. Trust management aims to ensure the legitimacy of the received report regarding a critical road event. Over the last decade, some fundamental work has been conducted on trust management in VANETs. However, existing models have two significant problems: First, existing models are not dedicated to IoV and lack essential requirements [5]–[8]. Second, the models are designed to work on fixed notions and lack flexibility and adaption, which is the utmost requirement of IoV. In addition, IoV requires intelligent solutions to handle its diversity, which can be covered by an artificial intelligence (AI) solution [10], [10]. Context-awareness is an AI approach that deals with making systems flexible and dynamic. Context-aware trust management framework (CTMF) is presented to achieve IoV trust. Unlike other models, CTMF emphasizes building all the available information around an event, which helps to infer trust accurately. The novel feature of the presented framework includes the use of context-aware in trust management, three-layer malicious node detection, confidence scoring, and multilevel uncertainty handling. These unique features make the proposed trust-management framework much more effective.

A. IoV ARCHITECTURE

Prior to discussing the details of the proposed framework, it is essential to discuss the IoV architecture owing to a lack of standards. The generic IoV architecture is shown in Figure 1. Accordingly, all the nodes are equipped with essential circuitry called an on board unit (OBU) and a local data repository (LDR). Roadside units (RSUs) form the major VANET infrastructure where all nodes can connect and communicate. The cloud provides a centralized IoV communication center. Cloud services also manage a central data repository (CDR). A base transceiver station (BTS) can be used as an RSU, and the internet forms the backbone of IoV communication. The LDR and CDR were synchronized after a frequent period.

The remainder of this paper is organized as follows; we discuss the background literature on the trust model for IoV in Section 2. In Section 3, we present the proposed framework and its essentials. In Section 4, we provide a detailed description of the trust evaluation. In Section 5, we present the simulation and analysis of the proposed trust-management framework. In Section 6, the model is validated by benchmarking with related models. Finally, Section 7 presents the conclusions of the study

II. RELATED WORK

Security has been identified as a critical concern in research on the future challenges of IoV. A variety of security issues have been raised with the development of IoV [11], making security one of the primary challenges. However, existing IoV trust evaluation and management approaches cannot provide practical remedies [4], [12]–[14]. Several trust evaluation methods have been proposed for vehicle communication, and some foundational approaches are discussed here. Most trust models are based on VANETs/ITS, and there is a dearth of recent works on IoV [15]–[17]. A few concept-level works on IoV trust using blockchain technology were recently presented [16], [18]. Blockchain-based models present several technical drawbacks, such as high computational requirements in terms of time and space, proof of work, scalability, and centralized nature. The downside of the blockchain makes it incompatible with IoV. Different types of trust measuring models can be employed to classify all available models. Data-centric, entity-centric, and hybrid models are the most frequently used classifications of trust models in VANETs. Several models were presented for each category.

A. DATA CENTRIC MODELS

Data centric models are based on node information used to infer the trustworthiness of a report [19]. Most early trust models were data-centric. According to some scholars, data centric models are more appropriate for trust evaluation [20], [21]. In an earlier data-centric model [22], researchers focused on trust-based scalability by assigning different roles and using their experiences. In data-centric models [23], [24], neighboring vehicles share opinions about an event and compute the trust of the maximum votes. The principal problem of the data-centric approach is that it ignores information related to the vehicle [12]. Besides, distributed attacks using opinions are another drawback of these models. Opinion formulation methods using such models are not defined in detail.

B. ENTITY CENTRIC MODELS

The second form of the model is based on building trust against the nodes. In the methodology, experience is an indispensable feature. In some entity-centric models, intravehicular communication is considered while measuring trust in real time [7], [25]. Entity-centric techniques are more effective and valuable than data-centric techniques [12]. In an entity-centric trust approach, the trust level was measured using fuzzy logic [25]. The fuzzy logic based misbehavior detection scheme is an effective way to detect malicious nodes [26]. An alternative approach works on previous experience, certificate authority (CA), and opinions to construct node trust [15]. Other key methods [27], [28] utilize a mixture of authentication from CA and encryption. The main drawback of these models is that it is impossible to assume malicious behavior once a node has been verified. The second disadvantage is reliance on CA. Overall, entity-centric models are great for assessing trust, and they overlook the benefits of data-centric models.

C. HYBRID MODELS

Hybrid models combine the characteristics of both data and entities to establish the trustworthiness of a received message. These models are the most renowned and well formulated. Generally, there is an association between the data trust and entity trust modules. One such model is a combination of role-based methods and experience [8]. Another hybrid approach measures trust through neighbor opinions and similarity [29]. Typically, the implementation of a ''long-term trust establishment'' approach in a hybrid model ensures message protection [30]. Some researchers have utilized probability approaches, such as Bayes' law, evidence theory, and Markov chain theory [7], [20], [31]–[34]. Another hybrid model is based on pre-assigned trust and utility theory [12]; enormous computation in real time is the disadvantage of this trust model.

Blockchain based trust models are now an active research area. A research study discussed that blockchains could be useful for building lightweight authentication systems during trust management [28], [35]; their result reveals that the lightweight authentication approach is appropriate and secure for dynamic networks. In order to meet the criteria of IoT/IoV, authentication must be dynamic and efficient [36]. Therefore, researchers are working on lightweight authentication [37]. A research work suggested a lightweight authentication method for IoT security and similar networks [38]. In a recent authentication-based framework, the researchers have considered the blockchains for IoV [39]. However, the blockchains in IoT-based networks are still dubious; there are many challenges associated with blockchains, especially in networks like IoT [40]. Another recent work on trust using blockchain was conducted and found workable [41]. The main problem with this study was dependency on RSUs.

Although hybrid models incorporate data and entities, they lack dynamic integration [12]. However, based on the complexity of the research, no such trust model employs all available information during the event. All the models assess trust based on a set of factors and scenarios. Likewise, the suggested TM framework adopts a hybrid approach to trust evaluation because it uses as much information as possible. Meanwhile, all the existing models are for VANETS/ITS, which is a novel trust model for IoV that operates on context adaptation; no such trust model has yet been reported in the field.

D. CONTEXT-AWARENESS

The fundamental goal of implementing context awareness involves increasing flexibility by maximizing the usage of available data [42]. In a review study [4], the authors explained the potential requirement of an artificial intelligence (AI) method for trust measurement in vehicular communication. A well-known study has discussed the existence of rationality between VANET security and AI [4]. Rationality exists between contextual awareness and human reasoning [43]. A context is a type of information that pertains to human problem-solving abilities [44]. Context awareness is a concept related to human nature to understand one's surroundings. AI methods are suitable for context aware systems [45]. The AI community has immense potential to apply various techniques to work on context awareness [43]. The context model must be able to adapt to change and infer a novel context [44]. As IoV is a new field, very few studies have been conducted. Some context-based trust models are

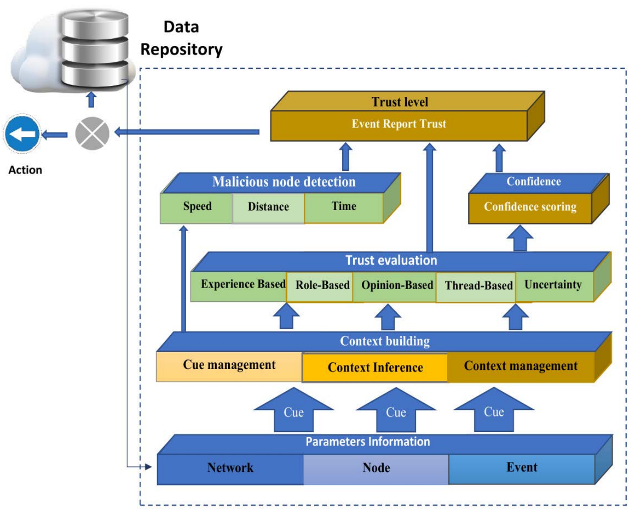


FIGURE 2. CTMF with four modules: parameters information, context building, trust evaluation, and malicious node detection.

presented, such as [2], [8], [19], [26], [42]. The main problem with these models is; that they have not Partially used context and are unable to provide comprehensiveness in terms of context. The proposed TM framework is novel for IoV security. The framework aims to incorporate flexibility to satisfy the dynamic requirements of IoV. Most renowned VANET TM models do not provide a complete solution for IoV.

III. PROPOSED TM FRAMEWORK

An IoV TM framework was presented to solve the shortcomings of existing models for successful trust evaluation. Figure 2 illustrates the proposed TM framework, which comprises four major modules: parameter module, context, module, the trust evaluation module, and malicious node detection. The basis of the proposed framework is the VANET best practices used by renowned trust models [7], [8], [25], [29], [30], [46]. The framework components were built on generic "context-aware" flow models [44], [47], [48]. Each component of the TM framework is discussed in detail below:

A. PARAMETER INPUT LAYER

Parameter management is the first task of trust evaluation, as shown in Figure 2. Information about an event is filtered to retrieve the parameters from the received messages. The framework categorizes all potential parameters for ease of use. The categorization scheme is discussed in the next section. Accordingly, the node's information is organized into "cues," which are then supplied to the context layer for context construction. As, certain elements have a more reliable source and weight than other elements, the fundamental challenge is to prioritize them.

B. CONTEXT LAYER

A low-level context is data that is immediately available and translated into a high-level context. The road-event context was established in this layer. Typically, context data or parameters are interconnected pieces of information with a degree of uncertainty. Context acquisition is the first step during parameter cue management in any context-building process, where data are fed for further processing. The perimeter module delivers information to the context module in the form of easily comprehensible "cues." The last step is context awareness, which presents the context data in an actionable format. A system related to a context requires a quantitative set of developed usable contexts. The deliverable of this layer is the context developed using the available set of parameters. The context provides complete information to evaluate trust in an event. Ontology is used for context building, which is based on formal logic and is one of the potential ways for context construction. Context information is structured around a road event with the support of an ontology. The context of ontological details is discussed in the following section.

TABLE 1. The nomenclature used in the article.

Symbol	Meaning
$\boldsymbol{\theta}$	Theta
$\boldsymbol{\varphi}$	Phi/Fi denotes latitude
λ	Lambda denotes longitude
μ	Mu denotes mean
σ^2	Variance
σ	Standard deviation
pv	Vehicle parameter
$\boldsymbol{R}$	Radius of Earth
$\boldsymbol{a}$	Square of half cord
$\boldsymbol{c}$	Angular distance
d	Geo distance

C. TRUST EVALUATION LAYER

The layer determines the degree of trust. Owing to the use of the context cognitive method, there is continuous information exchange between the inference engine and trust evaluation module. The trust evaluation layer comprises various modules. The best practices were used to align the evaluation modules with suitable scenarios using context-awareness. The commonly employed methods are experience, role, opinion, and thread-based methods, which have been investigated in the literature. Distinct situations require distinct evaluation modules to calculate trust. Each road event had different available parameters. Using context awareness, CTMF links an appropriate trust evaluation module with an event. Table 1 describes the symbols used in the article.

D. PROXIMITY

A simple distance formula can be used for theoretical concepts, but it does not work for real-time calculations. The

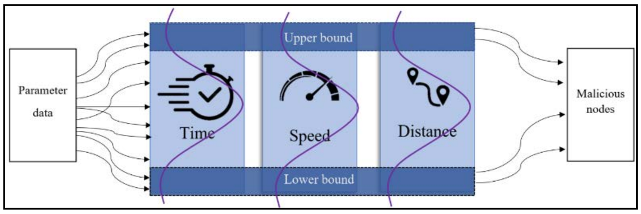


FIGURE 3. Malicious node detection.

framework uses the 'Haversine' formula, which allows the measurement of the distance between two geographical points [49]. The latitude is denoted by φ, longitude λ, and R denotes the Earth's radius (6,371 km). All angles were converted in radians to pass to functions, and Equation 1 was used for the conversion. Equation 2 computes the square of half the chord length between two points. Equation 3 shows the angular distance between two points in radians. Equation 4 calculates the distance between two geographical points on the map.

$$\lambda\frac{\theta}{180}.\begin{cases}\varphi_1,\varphi_2\\ \Delta\varphi\\ \Delta\end{cases} \tag{1}$$

$$\lambda a = sin^2\left(\frac{\Delta\varphi}{2}\right) + cos\varphi_1.cos\varphi_2.sin^2\left(\frac{\Delta}{2}\right) \tag{2}$$

$$c = 2.atan2(\sqrt{a}, \sqrt{(1-a)}) \tag{3}$$

$$d = R.c \tag{4}$$

E. MALICIOUS VEHICLE DETECTION BY ANONYMITY OUTLIERS

In vehicular networks and trust management, malicious node detection is crucial for single out suspicious nodes [50]. Previous models also considered the identification of malicious nodes. Anonymity is effective for detecting malicious vehicles and suspicious reports in a system; anonymity is effective [51]. Standard deviation (SD) is a powerful tool for determining anomalies in systems [52]. Generally, nodes that do not correspond to a certain limit are referred to as outliers. An outlier is a data point that deviates from well-structured data. The proposed framework focuses on identifying malicious nodes that affect the quality of trust values. This module uses SD to detect the expected malicious vehicles in the network. SD expresses how much the data are different from the mean of the distribution.

The malicious-node detection module uses three parameters: time, speed, and distance. Nodes that fall out of the lower or upper limits are considered malicious. These three parameters allow filtering out malicious nodes in the information to make the system secure. The $\sigma 2$ denotes the average of the squared difference from the mean (μ). In Equation 5, μ denote the speed, time, and distance. The μ, σ^2, σ were independently calculated for each parameter, and Equation 5 was used to calculate the mean of each parameter. Equation 6 was used to calculate the variance, and Equation 7 was used to calculate the SD of the three parameters discussed above. The upper and lower bounds were set to ± 2 SD of the mean. Figure 3 illustrates the malicious node detection module, in which the three parameters were evaluated for SD. Vehicles that fall within these bounds are considered malicious.

$$\mu = \frac{\sum parameter}{number\ of\ vehicles} \tag{5}$$

$$\sigma^2 = \frac{\sum(pv_i-\mu)^2}{n} \tag{6}$$

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(pv-\mu)^2} \tag{7}$$

F. TRUST PARAMETERS

The first step in context-building involves categorizing the parameters. The categorization aims to manage cues for context building, and Table 2 summarizes all possible parameters. The first category comprises general parameters, such as experience, number of reports, and opinions. Table 2 also lists its type and availability. The parameters related to network topology are specified in the second category. The parameters contain information related to a single event, as listed in Table 2. Different paraments in Table 2 are based on the category type used by most of the trust models. As the event changes, all the parameter values are refreshed for the next event. The third category details parameters related to the road events under consideration. The last category describes parameters related to the sender vehicle.

G. TRUST EVALUATION PROCESS

The TM framework uses a critical road incident as the central point of trust evaluation. The event is represented by Event ID (Evn_ID). The node that reports the event is denoted as (Rep_veh). The carrier vehicles that hop or beacon the message are denoted as (Carr_veh). Local and centralized databases were designated as local databases (Locl_DB) and centralized databases (Cent_DB), respectively. Trslv represents trust value. Thus, the trust level of a particular event is represented by (Ev_ID_Trslv), and the trust level of a vehicle is denoted by (Veh_Trslv). Lastly, the trust level value was synchronized with local and centralized data repositories.

H. CONTEXT ONTOLOGY

An ontology is a context-building approach that offers the highest range of features and AI support. With ontology, it is not compulsory to store all relations explicitly; the present triplets can generate new facts. An ontology is an explicit, methodical explanation of the observations in a certain domain. An ontology, a collection of individual class instances, creates a knowledge base [53]. Here, the ontology should be explicitly defined as not a set of instructions; instead, it is a set of interrelated concepts used for inferencing. The taxonomical association of ontology comprises the following classes: Vehicle, Evaluation_Module, and Event. All the trust evaluation components are subclasses of class Evaluation_Module, namely Experience_Module, Special_Vehicle, Opinion, Cluster_Based, Thread_Based,

TABLE 2. List of parameters.

Category	Parameters	Type	Availability
General	Experience (interaction)	level (value)	maybe
	Number of reporters	number	maybe
	Opinion	true/false or level	maybe
	Distance	value (between node and event)	always
	Type of event	level/type	always
	Hopping	single, multi (value)	always (vary)
	Position	geolocation	always
	Traffic type	urban, rural, highway	always
	Time	event time, reporting time	always
	Proximity	to the event, to vehicle	always
Network	Total number of nodes	value	always
	Number of reporter nodes	value	always
	Direct report	true/false	always
	RSU	true/false	sometimes
	Centralized connectivity	true/false	sometimes
Road-event	Location	geographical coordinates	always
	Time	value	always
	Type	awareness critical highly critical accident congestion work in progress natural disaster	always
Vehicle	Type of node	general, special (role-based)	always
	Experience	number value	always
	Proximity	number value	sometimes
	Direction	towards, from	always
	Speed	number value	always

and Uncertainty. Rep_veh, Carr_veh, and Special_veh are members of the vehicle class. The class is disjointed to prevent abstract intersection by the reasoner. A brief ontology diagram is illustrated in Figure 4, which illustrates the categorized classes and instances of the model. The instances contained are linked with the node ID, event ID, location, time, and direction.

I. TRUST LEVEL THRESHOLD

Trust (Trslv) was evaluated between 0 and 1, untrusted was represented as 0, and maximum trust was represented as 1 [8], [54], [55]. Initially, all vehicles were allotted as Trs$lv = 0$ and special vehicles as 0.5. Central and local databases store and update event trust information for future authentication and trust evaluation. Multiple trust values are combined to form the trust value of an event. The weight allocation in Table 3 represents the initial trust, experience, and trust rewards. Table 3 explains the reward a vehicle will get after it reports a true event. This trust credit reward will be added to the vehicle's experience.

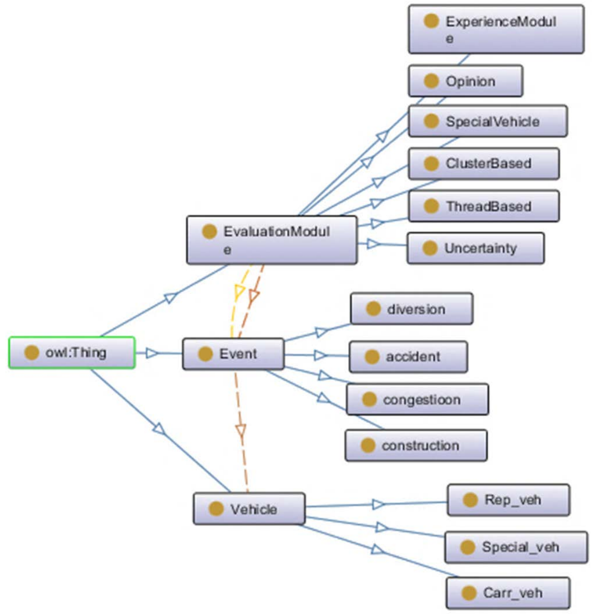


FIGURE 4. Hierarchical taxonomy, classes, and instances of IoV TM ontology.

TABLE 3. Trust weight allocation.

Module	Trust score allocation
Experience	Vehicle experience (trust value) initialized = 0 Special vehicle (trust value) initialized = 0.5 On trust verification Rep_veh= +0.1 Spcl_veh= +0.1
Role	Spcl_veh experience (trust value) initialized =0.5 On trust verification Spcl_veh= +0.1
Opinion (beaconing)	After trued report Carr_veh= +0.05 (beaconing)
Cluster	On trust verification Rep_veh= +0.1 Spcl_veh= +0.1
Thread (hopping)	On trust verification Rep_veh= +0.1 Carr_veh= +0.01 (hopping)
Uncertainty	After trued report Rep_veh= +0.1 Spcl_veh= +0.1 Carr_veh= +0.01

Trust value is an aggregate of multiple trusts derived from distinct modules. Trslv_1 denotes the average trust score of all Rep_vehs obtained using Equation 8. Moreover, Rep_*vehs* for an event consists of a general vehicle.

$$\mathrm{Tr}lv1 = \frac{\mathrm{Rep\_veh\_Tr}lv(1+2+3\ldots\mathrm{n})}{n} \tag{8}$$

Equation 9 is applied to obtain the average trust Trslv_2 from the carrier nodes that participated in beaconing.

$$\mathrm{Tr}lv2 = \frac{\mathrm{Carr\_veh\_\_bec\_Tr}lv(1+2+3\ldots\mathrm{n})}{n} \tag{9}$$

$$\mathrm{Tr}lv3 = \frac{\mathrm{Spcl\_veh\_\_Tr}lv(1+2+3\ldots\mathrm{n})}{n} \tag{10}$$

In particular, in scenarios in which special nodes participate, the mean trust Trslv_3 of all Spcl_*veh* can be acquired using Equation 10. Since CTMF is context oriented, it may use a different module for the next event. The combined trust value of an event, Eve_ID_Trslv, is acquired using Equation 11.

$$\mathrm{Eve\_ID\_Trs}lv = \mathrm{Trs}lv_1 + \mathrm{Trs}lv_2 + \mathrm{Trs}lv_3 \tag{11}$$

Equation 11 provides the primary method for modules, namely experience, role, and opinion trust evaluation, each with associated conditions. Specifically, Equation 11 implies that nodes have a greater or equivalent experience than 0.5. The nodes with less experience than 0.5 trust were filtered out and used in different modules for context building and inference.

J. THREAD BASED/HOPPING

The module is utilized in scenarios where hopping is greater than reports and opinions. The primary concept is to leverage multiple hop threads. The trust level did not depend on the thread level (thrd_*lev*). The thread module requires a minimum of two *Rep_vehs*. The thread rises with the intersection of the two threads during an event. Carrr_*veh*, obtains the identical thread, thrd_*lev* is 1, and the thread increment depends on the encounter of a new thread. An increment in each thread also increased the trust level of the message by 0.2.

K. UNCERTAINTY BY MULTIPLE EVIDENCE BAYESIAN INFERENCE

Uncertainty is the lack of information needed to compute trust results. Some trust models ambiguously discuss uncertainty, such as those in [20], [32], [55]. One technique for dealing with uncertainty is to employ a basic probability, which is unrealistic. The proposed TM framework adopts the multiple-evidence Bayesian inference (MEBI) method to deal with uncertainty. The reason for using MEBI is that it allows the system to combine various pieces of past evidence, which corresponds to the nature of the problem. The Bayesian rule measures the chance of a report being legitimate or bogus. According to Equation 12, the experience parameter should be less than 0.5. Moreover, Equation 12 is used to determine the likelihood of a false message. As mentioned previously, under some conditions, Rep_veh with less experience is regarded as uncertain. Equation 13 determines the legitimacy of the message.

$$P(rep\_flase|exp\_ < 0.5) = \frac{P(exp\_ < 0.5|rep\_flase).P(rep\_flase)}{P(exp\_ < 0.5)} \tag{12}$$

$$\begin{aligned} P(rep\_true|exp\_ < 0.5) &= 1 + P(rep\_flase|exp\_ < 0.5) \\ &= \frac{P(exp\_ < 0.5|rep\_flase).P(rep\_flase)}{P(exp\_ < 0.5)} \end{aligned} \tag{13}$$

The proposed methodology has gone one step further to be more precise and leverages additional accessible data to infer a report's trust level. When more contextual information is provided, the framework leverages MEBI, which allows the system to cognitively infer. Equation 14 employs MEBI using the direction of the node in Equation 13.

$$P(rep\_flase|exp\_ < 0.5 \wedge dir\_from) = \frac{P(exp_{<0.5} \wedge dir_{from}|rep_{flase}).P(rep_{flase})}{P(dir_{from} \wedge exp_{<0.5})} \tag{14}$$

The conjunction of several pieces of evidence is shown in Equation 14. P (exp_<0.5 ∧ dir_from) can be obtained using Equation 15, as shown at the bottom of the next page.

Accordingly, Equation 17, as shown at the bottom of the next page, is obtained by employing Equations 15 and 16, as shown at the bottom of the next page, in Equation (14). The distinctiveness of CTMF is that it combines additional information to compute trust.

Algorithm 1. presents the trust evaluation procedure for an event when a new critical message is obtained. If the same report is already available, it is synced with the prior event list. Otherwise, a different event is generated. In addition, the algorithm elaborates on the management of the entire event.

L. CONFIDENCE SCORE

The confidence score is a novel element of the proposed TM framework. Since the suggested framework utilizes all available data, the confidence score is calculated using a combination of both the involved and discarded reports. Discarded reports were only considered if they were not ambiguous. The weights for the confidence measures are listed in Table 4. Nodes with less experience are excluded from the trust evaluation process; if those nodes are not malicious or ambiguous, they are expected to be true nodes and can be used as secondary evidence. Equation 18 is used to calculate the conf_score for a report; the mean of all involved and discarded nodes is used for the conf_score. The complete process of conf_score computation is described in Algorithm 1. The conf_score is an independent quantity that is not directly related to the trust value. Being independent makes the conf_score a key feature of trust evaluation. Accordingly, there may be a scenario where the trust level of a report is high; however, the confidence score is low, and vice versa.

$$\mathrm{Conf\_score} = \frac{\sum \mathrm{Rep\_inv} + \mathrm{Sep\_inv} + \mathrm{Carr\_inv} + \mathrm{Rep\_dis} + \mathrm{Carr\_dis}}{\mathrm{n}} \tag{18}$$

IV. PERFORMANCE EVALUATION METRICS

The effectiveness of the proposed trust framework should be assessed. The following are the specifications for the performance evaluation of the CTMF. Several indicators are utilized to assess the performance of the TM framework.

TABLE 4. Wight for confidence measure.

Vehicle type	Status in trust evaluation	Confidence score weight
Reporting	Involved	1
Special	Involved	1
Carrier	Involved	0.5
Reporting	Discarded	0.5
Carrier	Discarded	0.1

TABLE 5. Performance metrics, indicators, and descriptions.

Indicator	Description	Measurable quantity
Level of trust	Highest level of trust value achieved against a report, under various traffic circumstances	Measured from 0 to 1
Events evaluated	Number of maximum events evaluated out of received reports	Number of evaluated reports
Critical situation	The least information available ranging from ranging from 2 to 10 nodes	Number of events evaluated for trust in low information density
Confidence level	Degree of confidence on evacuated trust	Number of involved and discarded nodes attaining certain properties
Malicious node detection	Maximum number of malicious vehicles detection during an event	Number of malicious nodes detected.
Trust under different traffic patterns	Level of trust obtained under different types of road traffic.	Number of events evaluated in urban low and high traffic. Number of events evaluated in rural/highway low and high traffic.

The key performance evaluator was the trust level. Trust is determined to be between 0 and 1, where 1 indicates the maximum level of trust and 0 predicts a non-trustable report. Most values >= 0.5 are considered trustworthy. The second critical measure involves the number of events evaluated. The real test of the TM framework is when low information makes it difficult to evaluate trust, causing the discarding of a report. The third measure is critical road events with the least amount of information available; most trust models exhaust at this point. The fourth measure set for evaluating the performance of this TM framework was the level of confidence in the inferred report. The confidence level is an independent variable that increases the legitimacy of the report. The fifth performance measure is the ability to accurately detect the maximum number of malicious nodes. The final measure of TM framework performance is managed trust under different traffic scenarios, such as urban and rural/highway traffic patterns. The performance evaluation matrix and its properties are summarized in Table 5. In addition to these key measures, a confusion matrix analysis is also performed in the following section to further investigate the performance of the proposed TM framework relative to other models.

A. CONFUSION MATRIX

A confusion matrix is a measure to assess the performance of algorithms, and it seems that the TM is suitable to be evaluated using a confusion matrix. When discussing TM, the confusion matrix is, and more importantly, classifies the reports into two. Legitimate reports and reports by malicious nodes are represented by Equations 19 and 20.

$$\text{Legitimate reports} = \text{TP} + \text{FN} \tag{19}$$

$$\text{Malicious reports} = \text{FP} + \text{TN} \tag{20}$$

It is important to note that type-I error false negatives (FPs) are the most alarming for TM; they indicate false reports by malicious nodes that the system cannot detect. Therefore, the framework must have minimum false negatives (FN) and FP and high true positives (TP) and true negatives (TN). TP: These are events in which the system predicted a true report and the events occurred. True TN: The events predicted by the system as false reports and the events that did not occur in reality. FP: These are events in which the system predicted the reported event as true but the event did not occur. FN: The events predicted by the system were false, but the event did occur in reality. Also known as a "Type II error."

Accuracy: From all the tests (positive and negative), Equation 21 shows how many tests the system predicted accurately. A higher accuracy indicates a better performance. Error rate (ERR): Equation 22 expresses the error rate, where the number of incorrect predictions by the system is divided by the total number. Precision: Precision expresses the proportion of reports the model identifies as relevant and is

$$P(dir\_from \wedge exp\_ < 0.5|rep\_flase) = P(dir\_from|rep\_flase)P(exp\_ < 0.5|rep\_flase) \tag{15}$$

$$\begin{aligned} P\left(\exp_{<0.5} \wedge dir_{from}\right) &= P(exp\_0.5 \wedge |rep\_flase)P(dir\_from|rep\_flase)P(rep\_flase) \\ &\quad + P(exp\_0.5|rep\_true)P(dir\_from|rep\_true)P(rep\_true) \end{aligned} \tag{16}$$

$$\begin{aligned} P(rep\_flase|exp\_ < 0.5 \wedge dir\_from) &= \frac{P(rep\_flase).P(exp\_ < 0.5|rep\_flase).}{P(rep\_flase)P(exp\_ < 0.5|rep\_flase)P(dir\_from|rep\_flase)} \\ &\quad + \frac{P(dir\_from|rep\_flase)}{P(rep\_true)P(exp_{<0.5}|rep_{true})P(dir\_from|rep\_true)} \end{aligned} \tag{17}$$

Algorithm 1: Trust Evaluation Algorithm

The event trust evaluation algorithm

```
Initialization
 Event report obtained
 Evn_ID obtained
 Evn_ID_Trslv = 0
 Total nRep_veh=0
 Total nCrr_veh =0
 Total nSpec_veh =0
If (Evn_ID! = found) then
     Start Evn_ID as new session
  else
   Combine Veh_Trslv obtained from
Cent_DB and Locl_DB
   Combine Cr_veh_Trslv obtained from
Cent_DB and Locl_DB
end If
If (report obtain form Rep_veh) then
     nRep_veh ← nRep_veh+1
  else
     nCrr_veh ← nCrr_veh+1
end If
If (nRep_veh>2) && (Rep_veh_exp>0.5) then
       establish experience module
  else If (special Rep_veh in system) then
       establish role-based module
  else If (nCrr_veh >nRep_veh) &&
       (Crr_veh_exp>0.5) then
     establish opinion module
  else If (ncRep_veh >=1) then
     establish cluster module
  else If (nCrr_veh >(nRep_veh >1)) &&
     (Crr_veh with high hopping) then
     establish thread-based module
  else If (uncertain situation) then
     establish uncertainty module
end If Evn_ID_Trslv ← trust value
     (opted modules)
If (Evn_ID_Trslv > 0.5) then
  take action,
  Synch in Cent_DB and Locl_DB
  Forward Evn_ID is trustworthy with
Evn_ID_Trslv
 else
  reject event
  synch with Cent_DB and Locl_DB
broadcast Evn_ID is trusted with
Evn_ID_Trlv
end If
End
```

articulated in Equation 23. More specifically, when the system predicts yes, how often is it correct? Recall: The number of relevant reports selected. Recall is defined by Equation 24. F1 score: in Equation 25, a high F1 score indicates that the TM system has low false positives and low false negatives; therefore, the TM system correctly identifies real threats, and the network is undisturbed by false reports. The F1 score ranges from 0 to 1, where 1 is considered perfect and 0 indicates the worst performance.

$$ACC\cdot = \frac{TP + TN}{Total} \tag{21}$$

Algorithm 2: Confidence Score Algorithm

Pseudocode of confidence score computing algorithm

```
Initialize
 Event report received
 Ev_ID retrieved
 Ev_ID_ conf_score = 0
 Rep_inv =1, Spe_inv =1, Carr_inv =1,
 Rep_dis =1, Carr_dis =1
  Execute
 Rep_inv ← Rep_inv x 1
 Spe_inv ← Spe_inv x 1
 Carr_inv ← Carr_inv x 0.5
 n ← count(Rep_inv+ Spe_inv+ Carr_inv+
 Rep_dis+ Carr_dis)
If (Rep_dis_experience < = 0.5 && Rep_dis !=
malicious) then
      Rep_dis ← Rep_dis x 0.5
    else
  Rep_dis ← 0
  end If
  If (Carr _dis_experience <= 0.5 && Carr
  dis != malicious) then
  Carr _dis ← Carr _dis x 0.1
     else
       Carr _dis ← 0
  end If
   Ev_ID_conf_score = ∑Rep_inv+Sep_inv+Carr_inv+Rep_dis+Carr_dis / n
End
```

$$ERR\cdot = \frac{FP + FN}{Total} \tag{22}$$

$$PRE\cdot = \frac{TP}{FP + TP} \tag{23}$$

$$REC\cdot = \frac{TP}{FN + TP} \tag{24}$$

$$F1 = 2\frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} = \frac{TP}{TP + \frac{1}{2}(FP + FN)} \tag{25}$$

B. SIMULATION SETUP

The simulation setup comprises an area with a radius of approximately 5 km for urban traffic and 10 km for rural/highway traffic. While the nodes are moving, accidents or road blockages were generated at random locations. The primary tool used for the simulation is MATLAB R2020, a powerful tool used by other related models. Secondly, the framework employed Protege-5.5.0 0 with the "HermiT 1.4.3 456" reasoner, an open-source environment was used for ontology design.

Depending on the scenario, the number of nodes in each random event ranged from 2 to 50. The special vehicles were limited to 10% of the total vehicles, and the remaining 90% were general nodes. The trust experience of the starting nodes is initialized as 0, and the trust experience of the special nodes is initialized as 0.5. Outcome variation is a significant concern with simulations; because of the experiment's random design, results may differ from attempt to attempt. There are considerable differences between the simulation instances in the wireless topology and network architecture.

TABLE 6. Experiment parameter description.

Parameter	Description	Default Value
Experience	Initial node experience	0.0
Experience Special node	Initial special node	0.5
True report reward	True report reward, general and special vehicle	0.1
True report reward (opinion)	True report (beaconing) True report (hopping) True report (uncertainty)	0.05 0.01 0.01
Trust	Trust threshold	>=0.5
Simulation area	Urban, rural, and highway	
Vehicles	The simulation is conducted by varying the number of vehicles	1-2, 10, 25, 50
Special vehicles	Number of special vehicles varies in the network	Maximum 10 %
Malicious nodes	In an only related test	10 %
Event duration	Time for which the event is valid	90 s
Area	Urban /city traffic Rural/highway traffic	5 km 10 km

Reporting and carrying vehicles are examples of the general nodes. In the experiment, road events occurred randomly on the road network, as reported by nodes. Some experimental sets go up to 100 iterations to obtain significantly accurate results to complete the simulation. In addition to the above, malicious node detection was performed by including a maximum of 20% of malicious nodes for comparison and benchmarking.

A scenario-based simulation was used to test the framework. The scenarios were categorized into three groups to obtain maximum performance and exhaust the simulation: 1. Heavy traffic is common in urban traffic during busy hours or traffic jams. Up to 50 nodes were considered for these traffic situations. In certain cases, there were several reports of an incident, which made it simpler to assess the trustworthiness of any given event. In these settings, most trust models perform reasonably well. 2. Moderate traffic is represented by 11–25 nodes in these scenarios. These circumstances are most common on highways or during "low rush hours in urban areas." In such instances, a normally limited set of information is available. Unlike other models that use a defined set of information, this framework uses all accessible data. 3. Less traffic: this traffic pattern can be observed on highways, in cities, and in rural areas. In this scenario, 2–10 nodes were involved. These are the most critical scenarios, owing to a lack of information. These situations feature the greatest ambiguity, which is a significant issue in the trust-assessment process. The remaining simulation specifications are listed in Table 6.

C. ASSUMPTIONS

The following assumptions were made to ensure the accurate execution of the presented TM framework:

- OBU is embedded in each vehicle in the network.
- All vehicles use a common communication platform.
- All OBUs use IEEE 802.11p as the standard communication protocol.
- All OBUs are dedicated short-range communications (DSRC) channel enabled
- Public key infrastructure (PKI) is controlled by a third-party centralized authority (CA), which is completely reliable and provides key management standards.
- All cellular BTS provides support to vehicular network as RSU.

V. RESULTS AND DISCUSSION

The simulation results are presented in this section. The experiment was conducted using different competitive models to measure the performance of the framework compared to other works. Following the presentation of the results, a comprehensive discussion is provided on the synthesized findings.

A. VALIDATION OF THE PROPOSED FRAMEWORK

The proposed TM framework was validated by comparing it with existing renowned models using a benchmarking technique. Moreover, validation determines how well the framework performs compared to existing studies. Table 7 enlists the specification used for validation.

B. BENCHMARKING

The benchmarking aims to verify the performance of the proposed trust management framework compared to existing approaches, Table 8 state the selected studies for benchmarking. The following three studies were chosen for benchmarking: trust evaluation and management (TEAM), an enhanced distributed trust computing protocol (EDTCP), and a novel trust framework (NTF).

The results are compared with selected studies using the simulation-based experiment. A simulation of the road event depicting the maximum possible traffic scenarios was generated. The trust is evaluated using all four frameworks, including the proposed framework. The results are compared to analyze the performance of the proposed framework in contrast with the other three frameworks in the following sections.

C. CONTEXT COGNITIVE MODULE ALLOCATION

Table 9 presents the results under different traffic conditions, and the events are adapted by different modules based on the availability of information. The opinion is highly adapted up to 37% in low urban traffic, and the second module is "experience" with 30%. The remaining modules range from 6 to 8%. In contrast, low traffic in rural traffic has highly attained the experience module 39% followed by opinion with 29%.

TABLE 7. Specification used in the models selected for validation.

Model	CA	Authentication	RSU	Experience	Cluster	Opinion/ Beaconing	Hopping	Special nodes	decentralized	Credit allocation	Node Initialization	Uncertainty
[8]	✓	×	×	✓	×	×	×	✓	×	×	✓	×
[7]	×	×	×	✓	×	×	×	×	×	×	×	×
[29]	×	✓	×	✓	×	✓	×	×	×	×	×	×
Proposed (CTMP)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

TABLE 8. Different modules adapted under different traffic conditions.

S. no	Model	Title
1	[8]	TEAM: A trust evaluation and management framework in context-enabled vehicular ad-hoc networks
2	[7]	An enhanced distributed trust computing protocol for VANETs
3	[29]	Novel trust framework for vehicular networks

TABLE 9. Different modules adapted under different traffic conditions.

Traffic		Experience (%)	Spe_Veh (%)	Opinion (%)	Cluster (%)	Thread (%)	Uncertainty (%)
urban	low	30	7	37	6	12	8
	high	27	9	36	7	16	5
rural	low	39	4	29	3	15	10
	high	27	6	34	4	21	8

The other modules range from 3 to 14%. In Table 9, the high urban traffic contains a highly utilized opinion module 36% and experience of 27%. The remaining modules range from 5 to 16%. In contrast, higher traffic in rural has an opinion of 34%, experience 27%, and a rise in thread module as 21%. Others range from 4 to 8%.

The results in Table 9 confirm that the selection is a good choice for a framework to be context-based because of the clear variation due to changes in traffic conditions. If the TM and evaluation frameworks are fixed, they will miss out on the critical aspects. To further develop the argument in Table 9, low rural traffic has a significant number of carrier nodes, which is the reason why the opinion module has 29% usage. In this condition, ignoring neighbor opinions will undoubtedly lead to imperfect and incomplete trust evaluations. Similarly, other modules have significant unique information that, if missed, impacts the quality of trust in a report. Thus, this argument is fairly justified in that the

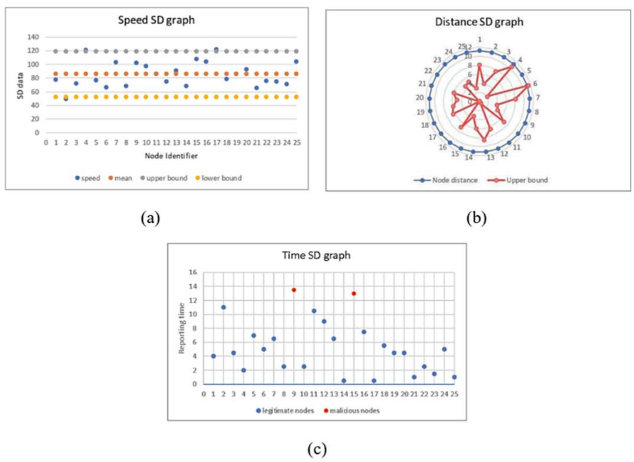


FIGURE 5. (a) Malicious node detection under SD and using node speed. (b) Malicious node detection under SD and using node distance to the event. (c) Malicious node detection under SD and using reporting time.

context-aware cognitive approach allows the TM framework to take complete advantage of the available information.

D. MALICIOUS NODE DETECTION

The framework adopts a three-layer process based on SD to separate the expected malicious node from the system. These three layers are based on three parameters: speed, time, and distance. Figure 5 (a) illustrates the observations of the speed layer of the malicious node detection module with the upper and lower bounds based on the SD. Data-points 2 and 17 fall out, indicating that these two nodes are malicious. Figure 5 (b) shows the results from the distance layer of the malicious node detection module, where data points 4 and 6 lie outside the upper bond of the distance and point as specious nodes. Most vehicles report events within a limited SD and are considered to be legitimate. Figure 5 (c) illustrates the time base SD from the beginning of an event. The red nodes are out of the upper bound, and the blue nodes represent nodes within limits. Data points 8 and 15 were designated as malicious. The upper and lower bonds were set to two SD. Moreover, the nodes that are out of the upper and lower SD bounds are considered malicious. Some models use

TABLE 10. Malicious nodes detection.

variance	256.133	75.84888889	28.46222
mean	88	13.46666667	9.266667
SD	16.0042	8.709126758	5.335
lower bound	55.9917	-3.95158685	-1.40333
upper bound	120.008	30.88492018	19.93667
Identifier	Speed	Distance	Time
1	102	17	10
2	60	14	14
3	102	15	9
4	85	4	3
5	100	25	15
6	89	12	8
7	55	9	10
8	84	8	6
9	104	7	4
10	91	17	11
11	108	2	1
12	72	17	14
13	74	1	1
14	105	35	20
15	89	19	13

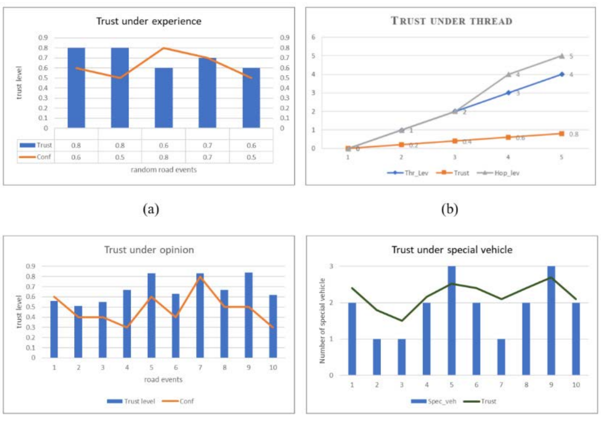


FIGURE 6. (a) Trust and confidence under experience module. (b) Trust under thread module. (c) Trust and confidence under the opinion module. (d) Trust and confidence under special vehicle module.

simple means to determine the malicious nodes; this method is not comprehensive, and using SD makes the system more reliable.

The findings in Table 10 indicate the performance of the malicious node detection module, where nodes 7 and 14 were identified as malicious based on the window between the upper and lower bounds. Here, it is crucial to note that, as an example, node 14 is more likely to be malicious because it falls out of two quantities, whereas node 7 falls out of one quantity, and both nodes will still be marked as malicious.

E. TRUST EVALUATION

The following results represent the trust evaluation under the different modules. Figure 6 (a) illustrates trust evaluation during the experience module. Along with the trust level, the confidence level is also illustrated in Figure 6 (a), and

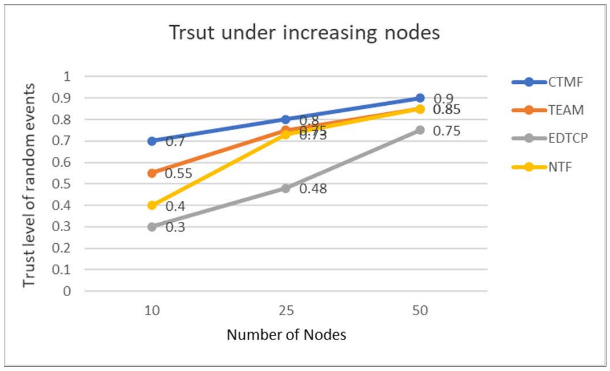


FIGURE 7. Impact of node increment on trust evaluation.

the confidence level is plotted between 0 and 1 for this graph to facilitate easy understanding. The thread module that shows the trust evaluation is shown in Figure 6 (b). The line graph in Figure 6 (b) corresponds to the thread, trust, and hop levels. The threads are evaluated against an incremental number of nodes. The thread module outputs demonstrate a steady progression over the trust-building phase. The thread level is directly related to the amount of trust. It is crucial to remember that a thread's level is not the same as that of the hop. The results in Figure 6 (c) show ten random road events under the opinion module. Confidence level values were mounted on trust values. The confidence level was independent of trust value. The performance of the "confidence score" as an independent variable aids the algorithm in making a better trust evaluation. The presence of a special node adds legitimacy to an event. The results of evaluating trust while involving a special vehicle in a road event are expressed in Figure 6 (d). The number of special vehicles was evaluated based on the trust level. Figure 6 (d) presents the impact of the relation of a special node with the trust level. The more special nodes that are engaged, the better the level of trust attained. The confidence score is a critical element of this framework. A low confidence score may occur, even when there is a high trust level.

Table 11 presents the trust level with a confidence score. The last two columns are critical, primarily because the unique feature of the proposed framework is depicted. The highly trusted and highly non-trusted are based on the confidence score. For instance, the event "E2" has a high trust level but low confidence, whereas "E1" is vice versa. The same is the case with non-trusted reports, they might be either highly untrusted or just untrusted, e.g., "E6" and "E10".

F. BENCHMARKING RESULTS AND DISCUSSION

In trust management, the volume of contextual information increases with an increase in nodes. Accordingly, the node density directly affects the design of the TM framework. Some TM frameworks are designed in monotonous patterns; these frameworks cannot perform in the fluctuation of information, which leads to the miscalculation of trust.

In Figure 7, the comparative results of the trust evaluation are presented, including the TM framework. The experiment

TABLE 11. Trust level with confidence scoring.

Event identifier	Trust level	Confidence level	Trusted	Non-trusted	Highly trusted	Highly non-trusted
E 1	0.7	8.0	1	0	1	0
E 2	0.9	3.0	1	0	0	0
E 3	0.8	7.0	1	0	1	0
E 4	0.5	4.0	1	0	0	0
E 5	0.8	5.0	1	0	0	0
E 6	0.2	8.0	0	1	0	1
E 7	0.6	3.0	1	0	0	0
E 8	0.4	7.0	0	1	0	1
E 9	0.5	4.0	1	0	0	0
E 10	0.3	3.0	0	1	0	0
E 11	0.2	5.0	0	1	0	0
E 12	0.7	7.0	1	0	1	0
E 13	0.8	8.0	1	0	1	0
E 14	0.7	8.0	1	0	1	0
E 15	0.6	6.0	1	0	1	0
E 16	0.2	7.0	0	1	0	1
E 17	0.7	8.0	1	0	1	0
E 18	0.5	5.0	1	0	0	0

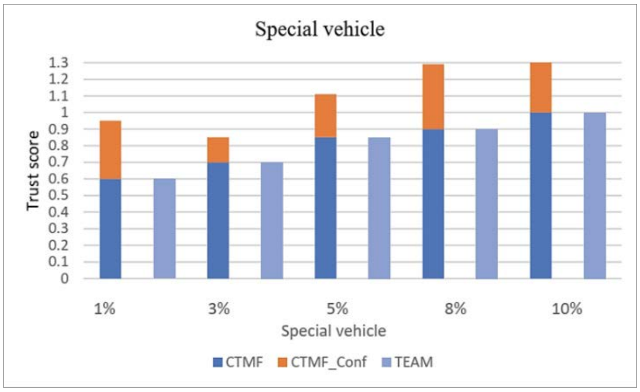


FIGURE 8. The impact of the involvement of special vehicles on trust.

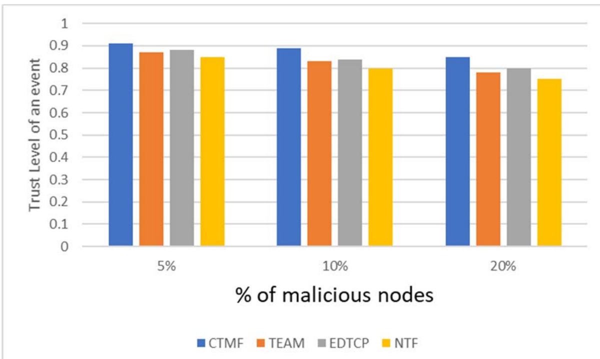


FIGURE 9. Trust level evaluation while involving malicious nodes.

was based on an increasing number of nodes for an event. The node increment frequencies are 10, 25, and 50. The data analysis in Figure 8 aims to assess the impact of an increasing number of nodes during an event. It is clearly observed that the trust level can be easily assessed with better accuracy by most models at a higher number of nodes, including the proposed method. These frameworks encounter the problem of low node engagement. At the lower nodes, the performance of CTMF is still the highest. TEAM also performs well at mid and high nodes but lacks low, dense traffic handling. The performance of EDTCP and NTF was significantly low. The reason behind the relatively better performance of CTMF under low nodes is contextual information, better handling of uncertainty, and local data management.

The trust in the special vehicle was simulated, and the related results are presented in Figure 8. The confidence level of CTMF was also mounted on top of the trust level. Special vehicle involvement is in percentage and ranges from 1 to 10% of all event nodes. The use of special vehicles was performed only by the proposed CTMF and TEAM models. Figure 9 depicts the trust evaluation, where special vehicles are part of the event. The CTMF inflicts a significant difference when including the confidence scoring of each trust evaluation, and the confidence score bars are stacked on the CTMF trust bars in Figure 8. Confidence scoring increases the authenticity and reliability of trust values.

Table 12 summarizes all models for urban and rural traffic with low and high densities. The table presents the data on the discarded and used event reports. The percentage of handled reports was highest for CTMF which is 95.75%. TEAM, EDTCP, and NTF correspond to 92.25%, 87.75%, and 90%,

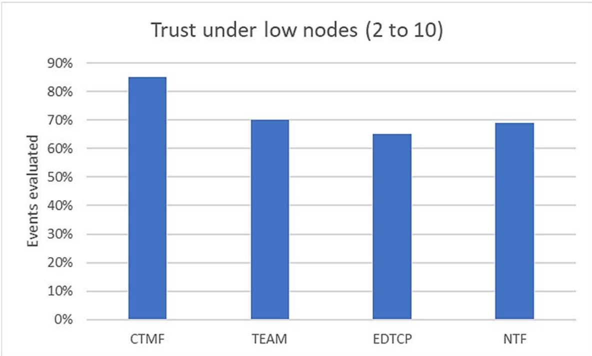


FIGURE 10. Trust evaluation under very low nodes.

respectively. None of the three models under comparison had a mechanism related to uncertainty handling. Simultaneously, CTMF handles all reports with low available information under the uncertainty module. The uncertainty module enables the minimization of the TM framework information loss risk. The results clearly depict enhanced performance with the use of uncertainty handling. Moreover, Table 12 also presents the traffic patterns and their correlations with available information and trust evaluation. In short, the density of traffic has a favorable effect on the trust evaluation process.

G. MALICIOUS NODES PRESENCE

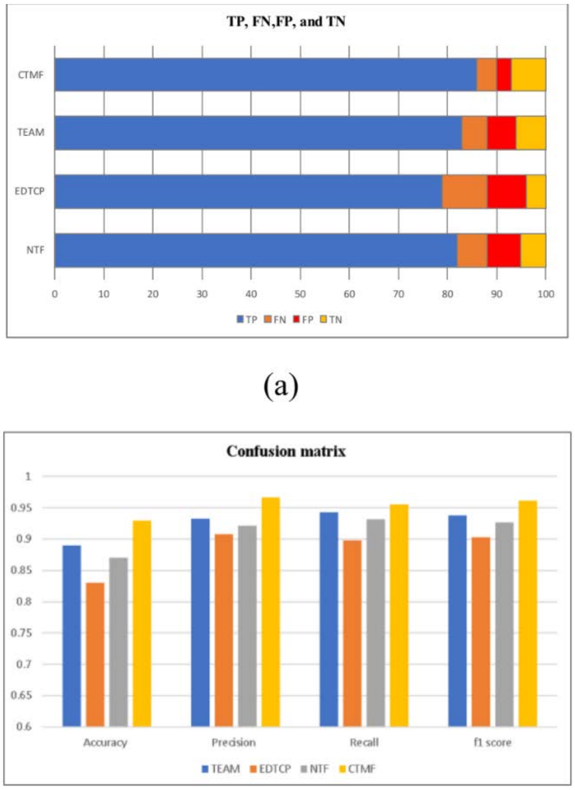
Figure 9 shows the trust evaluation in the presence of malicious vehicles. The malicious vehicles are included in the ratios of 5%, 10%, and 20% of all network nodes. Malicious nodes were included to assess the impact of the presence of malicious nodes on an event. Accordingly, CTMF performed better than TEAM, EDTCP, and NTF. The reason for better performance is contextual information; the CTMF completely exploits the available information to single out malicious nodes, whereas others miss certain critical information.

H. CRITICAL EVENT

Under extreme conditions, the trust level accuracy can be observed in the bar graph in Figure 10, where the nodes vary from 2 to 10. Low nodes can create information scarcity, thereby making it difficult for a TM system to perform. Under extreme conditions, the performance of CTMF was better than that of the others. The proposed framework utilizes the maximum available information, uncertainty handling, and local data management, which make CTMF perform better than TEAM, EDTCP, and NTF under extreme conditions.

I. CONFUSION MATRIX

The results of the validation using the confusion matrix are presented in this section. The experiment was performed under controlled conditions by marking a 90:10 ratio of legitimate to malicious reports. The first result of all four models is shown in Figure 11 (a). The results contained the identified reports as TP, FN, FP, and TN. The confusion matrix second



(a)

(b)

FIGURE 11. (a) Confusion matrix basic indicators. (b) Confusion matrix indicators.

set of results states the accuracy, precision, recall, and f1 score of all four models in The results in Figure 11 (a) reveal some interesting facts. For the TM models, the most crucial figure is the FP, which is the most severe indicator. FP depicts false reports sent by a malicious node that the system cannot detect. CTMF has the minimum FP score, followed by TEAM and the other two models. TN, another vital indicator, must be high because it is also reported by malicious nodes and identified by the trust system. CTMF operates better than the others by detecting the TNs, which may be due to a practical malicious node detection module. Figure 11 (b) presents the second set of results for all four models. Accuracy indicates the correctness of the reports inferred by the models. The presented model CTMF has reasonably better accuracy than the others with a score of 0.93, TEAM with 0.90, NTF with 0.88, and EDTCP with 0.83. Precision expresses how exact and accurate the model is out of the inferred trusted reports and how many of them actually turned out to be true. Vehicles in the IoV system may lose critical reports if the precision is not high. Figure 11 (b) displays that the precision of the proposed framework is ~0.97, followed by TEAM with ~0.94. The CTMF uses context information that allows the framework to dynamically manage all the information, which is the primary reason for its higher precision. Recall computes the number of actual true reports the framework infers. A higher recall rate is desirable when there is high cost associated with

TABLE 12. Handled and discarded reports.

Model	Reports	Uncertain	Urban traffic		Rural traffic		Mean	Mean of handled
			high	low	high	low		
CTMF	Handled		91	86	87	84	87	95.75
	Uncertain	handled	6	9	9	11	8.75	
		discarded	3	5	4	6	4.5	
TEAM	Handled	N/A	93	92	91	93	92.25	92.25
	discarded	N/A	7	8	9	7	7.75	
EDTCP	Handled	N/A	90	87	88	86	87.75	87.75
	discarded	N/A	10	13	12	14	12.25	
NTF	Handled	N/A	93	87	91	89	90	90
	discarded	N/A	7	13	9	11	10	

FN reports. Although FN is less significant for trust models than other indicators, it is still an indispensable factor. The CTFM attained a slightly better recall rate than the other methods. The final and most important indicator is the f1score which shows the overall correct identification by the system. CTMF had an f1score of 0.96, which is quite promising. The remaining three models varied from 0.94 0.90. Figure 11 (b).

VI. CONCLUSION AND FUTURE WORK

In IoV communication, trust is a significant solution for reducing the risk of network attacks. This study proposes a dynamic trust management framework to fully utilize the available information by using context awareness, which was missing in earlier solutions. The proposed models also detect malicious vehicles in a network by using a unique outlier technique. A comparison with the top existing models resulted in a better performance using the proposed framework. This trust framework is expected to provide complete support for IoV security in terms of trust management. In future work, the proposed trust framework can be tested for the IoT and other ad hoc networks. Furthermore, machine learning and big data can be used as supportive tools for long-term trust management. The comparative study analysis indicated that the current trust models cannot sufficiently to satisfy the dynamic trust evaluation criteria. In contrast, given IoV dynamics, the proposed model was structured to ensure optimum trust. Moreover, the proposed trust model is equally useful for other related IoT security solutions.

REFERENCES

[1] A. Hbaieb, S. Ayed, and L. Chaari, "A survey of trust management in the internet of vehicles," *Comput. Netw.*, vol. 203, Sep. 2022, Art. no. 108558.

[2] F. A. Ghaleb, M. A. Maarof, A. Zainal, B. A. S. Al-Rimy, A. Alsaeedi, and W. Boulila, "Ensemble-based hybrid context-aware misbehavior detection model for vehicular ad hoc network," *Remote Sens.*, vol. 11, no. 23, p. 2852, Dec. 2019.

[3] N. Fan and C. Q. Wu, "On trust models for communication security in vehicular ad-hoc networks," *Ad Hoc Netw.*, vol. 90, Jul. 2019, Art. no. 101740.

[4] S. Sumithra and R. Vadivel, "An overview of various trust models for VANET security establishment," in *Proc. 9th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2018, pp. 1–7.

[5] J. Zhang, K. Zheng, D. Zhang, and B. Yan, "AATMS: An anti-attack trust management scheme in VANET," *IEEE Access*, vol. 8, pp. 21077–21090, 2020.

[6] J. Guo, X. Li, Z. Liu, J. Ma, C. Yang, J. Zhang, and D. Wu, "TROVE: A context-awareness trust model for VANETs using reinforcement learning," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6647–6662, Jul. 2020.

[7] T. Gazdar, A. Belghith, and H. Abutair, "An enhanced distributed trust computing protocol for VANETs," *IEEE Access*, vol. 6, pp. 380–392, 2018.

[8] F. Ahmad, V. N. L. Franqueira, and A. Adnane, "TEAM: A trust evaluation and management framework in context-enabled vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 28643–28660, 2018.

[9] A. Haydari and Y. Yilmaz, "Real-time detection and mitigation of DDoS attacks in intelligent transportation systems," in *Proc. 21st Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2018, pp. 157–163.

[10] A. Alharthi, Q. Ni, and R. Jiang, "A privacy-preservation framework based on biometrics blockchain (BBC) to prevent attacks in VANET," *IEEE Access*, vol. 9, pp. 87299–87309, 2021.

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

[12] X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in VANETs," *Ad Hoc Netw.*, vol. 55, pp. 107–118, Feb. 2017.

[13] T. Qiu, D. Luo, F. Xia, N. Deonauth, W. Si, and A. Tolb, "A greedy model with small world for improving the robustness of heterogeneous Internet of Things," *Comput. Netw.*, vol. 101, pp. 127–143, Jun. 2016.

[14] E. K. Duarte, L. A. L. F. D. Costa, M. Erneberg, E. P. D. Freitas, B. Bellalta, and A. Vinel, "SafeSmart: A VANET system for faster responses and increased safety in time-critical scenarios," *IEEE Access*, vol. 9, pp. 151590–151606, 2021.

[15] A. Theodouli, K. Moschou, K. Votis, D. Tzovaras, J. Lauinger, and S. Steinhorst, "Towards a blockchain-based identity and trust management framework for the IoV ecosystem," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2020, pp. 1–6.

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

[17] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat, and S. Nandi, "Blockchain-based adaptive trust management in internet of vehicles using smart contract," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3616–3630, Jun. 2021.

[18] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs," *IEEE Access*, vol. 7, pp. 56656–56666, 2019.

[19] F. A. Ghaleb, A. Zainal, M. A. Maroof, M. A. Rassam, and F. Saeed, ''Detecting bogus information attack in vehicular ad hoc network: A context-aware approach,'' *Proc. Comput. Sci.*, vol. 163, pp. 180–189, Jan. 2019.

[20] 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 Netw.*, vol. 24, nos. 3–4, pp. 283–305, 2015.

[21] R. A. Shaikh and A. S. Alzahrani, ''Intrusion-aware trust model for vehicular ad hoc networks,'' *Secur. Commun. Netw.*, vol. 7, no. 11, pp. 1652–1669, Nov. 2014.

[22] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, ''A trust-based message propagation and evaluation framework in VANETs,'' in *Proc. Int. Conf. Inf. Technol. Converg. Services*, 2010, pp. 1–8.

[23] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, ''Towards expanded trust management for agents in vehicular ad-hoc networks,'' *Int. J. Comput. Intell., Theory Practice*, vol. 5, no. 1, pp. 3–15, 2010.

[24] M. Raya and J.-P. Hubaux, ''Securing vehicular ad hoc networks,'' *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[25] S. A. Soleymani, ''A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing,'' *IEEE Access*, vol. 5, pp. 15619–15629, 2017.

[26] F. A. Ghaleb, F. Saeed, E. H. Alkhammash, N. S. Alghamdi, and B. A. S. Al-Rimy, ''A fuzzy-based context-aware misbehavior detecting scheme for detecting rogue nodes in vehicular ad hoc network,'' *Sensors*, vol. 22, no. 7, p. 2810, Apr. 2022.

[27] X. Li, J. Liu, X. Li, and W. Sun, ''RGTE: A reputation-based global trust establishment in VANETs,'' in *Proc. 5th Int. Conf. Intell. Netw. Collaborative Syst.*, Sep. 2013, pp. 210–214.

[28] J. Cui, D. Wu, J. Zhang, Y. Xu, and H. Zhong, ''An efficient authentication scheme based on semi-trusted authority in VANETs,'' *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2972–2986, Mar. 2019.

[29] S. Ahmed, S. Al-Rubeaai, and K. Tepe, ''Novel trust framework for vehicular networks,'' *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9498–9511, Oct. 2017.

[30] T. Biswas, A. Sanzgiri, and S. Upadhyaya, ''Building long term trust in vehicular networks,'' in *Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring)*, May 2016, pp. 1–5.

[31] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, ''A job market signaling scheme for incentive and trust management in vehicular ad hoc networks,'' *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3657–3674, Aug. 2015.

[32] O. A. Wahab, H. Otrok, and A. Mourad, ''A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles,'' *Comput. Commun.*, vol. 41, pp. 43–54, Mar. 2014.

[33] Y. Chen and Y. Wei, ''A beacon-based trust management system for enhancing user centric location privacy in VANETs,'' *J. Commun. Netw.*, vol. 15, no. 2, pp. 153–163, Apr. 2013.

[34] M. H. M. Adnan, M. F. Hassan, I. Aziz, and I. V. Paputungan, ''Protocols for agent-based autonomous negotiations: A review,'' in *Proc. 3rd Int. Conf. Comput. Inf. Sci. (ICCOINS)*, Aug. 2016, pp. 622–626.

[35] S. Jangirala, A. K. Das, and A. V. Vasilakos, ''Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment,'' *IEEE Trans. Ind. Informat.*, vol. 16, no. 11, pp. 7081–7093, Nov. 2020.

[36] S. Challa, A. K. Das, P. Gope, N. Kumar, F. Wu, and A. V. Vasilakos, ''Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems,'' *Future Gener. Comput. Syst.*, vol. 108, pp. 1267–1286, Jul. 2020.

[37] H. Vasudev, D. Das, and A. V. Vasilakos, ''Secure message propagation protocols for IoVs communication components,'' *Comput. Electr. Eng.*, vol. 82, Mar. 2020, Art. no. 106555.

[38] M. Wazid, A. K. Das, K. V. Bhat, and A. V. Vasilakos, ''LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment,'' *J. Netw. Comput. Appl.*, vol. 150, Jan. 2020, Art. no. 102496.

[39] Z. Yang, R. Wang, D. Wu, B. Yang, and P. Zhang, ''Blockchain-enabled trust management model for the Internet of Vehicles,'' *IEEE Internet Things J.*, early access, 2021.

[40] S. Singh, A. S. M. S. Hosen, and B. Yoon, ''Blockchain security attacks, challenges, and solutions for the future distributed IoT network,'' *IEEE Access*, vol. 9, pp. 13938–13959, 2021.

[41] C. Pu, ''A novel blockchain-based trust management scheme for vehicular networks,'' in *Proc. Wireless Telecommun. Symp. (WTS)*, Apr. 2021, pp. 1–6.

[42] F. A. Ghaleb, M. A. Maarof, A. Zainal, M. A. Rassam, F. Saeed, and M. Alsaedi, ''Context-aware data-centric misbehaviour detection scheme for vehicular ad hoc networks using sequential analysis of the temporal and spatial correlation of the consistency between the cooperative awareness messages,'' *Veh. Commun.*, vol. 20, Dec. 2019, Art. no. 100186.

[43] A. Kofod-Petersen and J. Cassens, ''Using activity theory to model context awareness,'' in *Proc. Int. Workshop Modeling Retr. Context*. Cham, Switzerland: Springer, 2005, pp. 1–17.

[44] 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*. Cham, Switzerland: Springer, 2007, pp. 173–191.

[45] A. Schmidt, ''Ubiquitous computing-computing in context,'' Ph.D. Thesis, Comput. Dept., Lancaster Univ., Lancaster, U.K., 2003.

[46] A. Amin, S. Basri, M. F. Hassan, and M. Rehman, ''Software engineering occupational stress and knowledge sharing in the context of global software development,'' in *Proc. Nat. Postgraduate Conf.*, Sep. 2011, pp. 1–4.

[47] O. Yurur, C. H. Liu, Z. Sheng, V. C. M. Leung, W. Moreno, and K. K. Leung, ''Context-awareness for mobile sensing: A survey and future directions,'' *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 68–93, 1st Quart., 2016.

[48] C. Bettini, O. Brdiczka, K. Henricksen, J. Indulska, D. Nicklas, A. Ranganathan, and D. Riboni, ''A survey of context modelling and reasoning techniques,'' *Pervasive Mobile Comput.*, vol. 6, no. 2, pp. 161–180, 2010.

[49] C. C. Robusto, ''The cosine-haversine formula,'' *Amer. Math. Monthly*, vol. 64, no. 1, pp. 38–40, Jan. 1957.

[50] F. A. Ghaleb, F. Saeed, M. Al-Sarem, B. A. Saleh Al-Rimy, W. Boulila, A. E. M. Eljialy, K. Aloufi, and M. Alazab, ''Misbehavior-aware on-demand collaborative intrusion detection system using distributed ensemble learning for VANET,'' *Electronics*, vol. 9, no. 9, p. 1411, Sep. 2020.

[51] P. Oberoi, ''Survey of various security attacks in clouds based environments,'' *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 9, pp. 405–410, Sep. 2017.

[52] I. Agrafiotis, A. Erola, J. Happa, M. Goldsmith, and S. Creese, ''Validating an insider threat detection system: A real scenario perspective,'' in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2016, pp. 286–295.

[53] L. Cui, W. Gang, S. Xiaofeng, Z. Feng, and Z. Liang, ''An efficient certificateless aggregate signature scheme designed for VANET,'' *Comput., Mater. Continua*, vol. 63, no. 2, pp. 725–742, 2020.

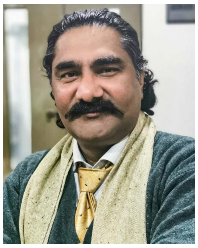
[54] K. C. Abdelaziz, N. Lagraa, and A. Lakas, ''Trust model with delayed verification for message relay in VANETs,'' in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Aug. 2014, pp. 700–705.

[55] X. Ya, Z. Shihui, and S. Bin, ''Trusted GPSR protocol without reputation faking in VANET,'' *J. China Universities Posts Telecommun.*, vol. 22, no. 5, pp. 22–55, Oct. 2015.

ABDUL REHMAN received the Ph.D. degree in information technology from Universiti Teknologi PETRONAS, Malaysia. He is currently working on Internet of Vehicles (IoV) information security. He has conducted and published significant research work in IoV trust managnent. His research interests include vehicular communication, information security, context-awareness, and the design of intelligent systems.

MOHD FADZIL HASSAN (Senior Member, IEEE) received the B.Sc. degree *(cum laude)* in computer information systems from Colorado State University, USA, in 1999, and the M.Sc. degree in artificial intelligence and the Ph.D. degree in informatics from The University of Edinburgh, U.K., in 2001 and 2007, respectively. He was the Former Dean of the Centre for Graduate Studies, Universiti Teknologi PETRONAS (UTP), where he is currently the Director of the Institute of Autonomous Systems. He is also an Alumnus of the Malay College Kuala Kangsar (MCKK). He is actively involved in research works focusing on these areas and has secured numerous research grants as a principal investigator namely, FRGS, ERGS, PRGS, and Technofund from the Malaysian Government. He is also actively involved with international collaborative research works particularly with universities from the Middle East, South Korea, and the ASEAN region. He has been involved in authoring more than 100 indexed publications. His research interests include the area of artificial intelligence, multi-agent systems, and service-oriented architecture (SOA). He was an Executive Committee Member of the IEEE Computer Society Malaysia, in 2018.

YEW KWANG HOOI received the Ph.D. degree from Universiti Teknologi PETRONAS, Malaysia. He is currently a Senior Lecturer with the Department of Computer and Information Sciences, Universiti Teknologi PETRONAS. His research interests include semantic web, knowledge representation, and formal language.



MUHAMMAD AASIM QURESHI received the Ph.D. degree in algorithms. He is currently a Seasoned Academician and a Researcher with 20 years of professional experience. He has more than 30 publications to his credit. His current research interests include artificial intelligence, algorithms, machine learning, and fuzzy logics. He has supervised numerous projects and theses related to virtual/augmented reality, recommender systems, sentiment analysis, and robot navigation. At many national and international conferences, he has been the session chair. He was an invited speaker at different research events. He is also a reviewer of numerous international conferences and journals.

SAURABH SHUKLA received the B.Tech. degree from Dr. A. P. J. Abdul Kalam Technical University, Lucknow, Uttar Pradesh, India, in 2008, the M.Tech. degree from the Indian Institute of Information Technology (IIIT), Allahabad, India, in 2010, in the research area of an intelligent systems, and the Ph.D. degree from Universiti Teknologi PETRONAS (UTP), Malaysia, in August 2020, in the research area of the healthcare Internet of Things (IoT). He joined as a Postdoctoral Researcher with the Insight SFI Centre of Data Analytics, Unit of Semantic Web, Data Science Institute (DSI), National University of Ireland Galway (NUIG), in October 2020. He is currently working on Cooperative Energy Trading Systems (CENTSs) Project for an efficient peer-to-peer energy trading systems in a smart grid (SG) networks. He has academic experience of more than seven years and published around 20 papers in various international journals and conferences. His research interests include the healthcare Internet of Things, fog computing (FC), cloud computing, machine learning, and blockchain.

ERWIN SUSANTO received the bachelor's degree in electrical engineering and the master's degree in control systems from the Sepuluh Nopember Institute of Technology, Surabaya, Indonesia, in 1998 and 2006, respectively, and the Ph.D. degree from Kumamoto University, Japan, in 2012. He is currently an Assistant Professor in control systems lectures with the School of Electrical Engineering, Telkom University. He has some journals and conference publications in control engineering topics. His research interests include both theory and application of control systems, and smart and automation systems. Since 2014, he has been receiving some research grants from the Indonesia Ministry of Research and Technology-Higher Education. He is an Editor of *National Journal* and a reviewer of some international conferences.

SADDAF RUBAB received the Doctor of Philosophy (Ph.D.) degree focused in information technology from Universiti Teknologi PETRONAS, Malaysia. She worked with NUST, Pakistan. She is currently affiliated with the Department of Computer Engineering, College of Computing and Informatics, University of Sharjah. She is also an experienced Researcher with a demonstrated history of working in the higher education industry. She has skilled in data science, artificial intelligence, cognitive science, grid computing, and operations research.

ABDEL-HALEEM ABDEL-ATY received the B.Sc. and M.Sc. degrees in physics from the Department of Physics, Al-Azhar University, Egypt, in 2004 and 2009, respectively, and the master's and Ph.D. degrees in theoretical physics (quantum information) from Universiti Teknologi PETRONAS, Malaysia, in 2011 and 2015, respectively. His Ph.D. study was supported by a scholarship from Universiti Teknologi PETRONAS. In 2017, he received a scholarship as a Visiting Researcher at the University of Oxford, U.K. In 2017, he was elected as a Junior Associate Member of the African Academy of Science, Kenya. He is especially working in theories of quantum measurement, nanomechanical modeling, highly non-classical light, practical information security, and optical implementations of quantum information tasks. His current research interests include quantum resources, optical and atomic implementations of quantum information tasks and protocols, quantum computing, mathematical modeling, computational intelligence, and machine learning. In 2015, he received the Sultana Nahar's Prize for the Best Ph.D. Thesis in Egypt.