Received August 3, 2025; revised November 8, 2025; accepted February 1, 2026.

Trust Management in the Internet of Vehicles: A Survey of the State-of-the-Art

Yingxun Wang[1,2], Adnan Mahmood[3] (Member, IEEE), Mohamad Faizrizwan Mohd Sabri[2], Hushairi Zen[4] (Senior Member, IEEE)

[1]Faculty of Computer and Information Engineering, Qilu Institute of Technology, Jinan 250200, P.R.China
[2]Faculty of Engineering, Universiti Malaysia Sarawak, Kota Samarahan 94300, Sarawak, Malaysia
[3]School of Computing, Macquarie University, Sydney, NSW 2109, Australia
[4]Faculty of Engineering and Technology, i-CATS University College, Kuching 93350, Sarawak, Malaysia

CORRESPONDING AUTHORS: Yingxun Wang (e-mail: wyx8586@qlit.edu.cn), Adnan Mahmood (e-mail: adnan.mahmood@mq.edu.au)

ABSTRACT The Internet of Vehicles (IoV) represents a transformative paradigm within the context of Intelligent Transportation System (ITS) with the aim to enhance road safety, traffic efficacy, environmental sustainability, and user convenience. However, as IoV networks increase in scale and complexity, ensuring trustworthy interactions among vehicles, infrastructure, and service providers becomes paramount. This paper, therefore, presents a comprehensive review of trustworthiness management for an IoV network. Firstly, the transition of Vehicular Ad hoc Networks (VANETs) to IoV followed by an examination of the notion of trust in various domains has been explored. Subsequently, the characteristics of trust, salient constituents of trust, key trust attributes, trust evaluation parameters, and trust-based attacks in the context of an IoV network have been delineated. Moreover, the five key processes involved in the trust management, i.e., trust formation, trust propagation, trust aggregation, trust update, and trust decision, have been investigated vis-à-vis the state-of-the-art. Furthermore, the advanced trust management models, i.e., conventional and artificial intelligence-based ones, have been analyzed in-depth. Finally, simulation tools and datasets employed in IoV-based trust management models have been introduced, along with an outline of key open research directions in this domain.

INDEX TERMS Internet of Vehicles, Trust Constituents, Trust-based Attacks, Trust Management, Vehicular Ad hoc Networks.

I. INTRODUCTION

OVER the last decade, significant and rapid advancements in the promising paradigms of the Internet of Things (IoT) and Artificial Intelligence (AI) have transformed conventional Vehicular Ad hoc Networks (VANETs) into Internet of Vehicles (IoV). This transformation has significantly narrowed the gap between connected and autonomous driving and their practical implementation. IoV is a novel concept in the Intelligent Transportation System (ITS) with a wide variety of both safety-critical and non-safety applications. By integrating mobile ad hoc networks with the IoT, IoV results into a Vehicle-to-Everything (V2X) network. It is noteworthy to mention here that researchers have lately been focusing to secure IoV networks from both external and internal attacks. Accordingly, the development of reliable trust models for accurate trust assessments is indispensable for improving the security of such networks [1], [2].

VANETs, as a vital part of ITS, integrate the mobile internet and IoT. It represents a distinctive form of Mobile Ad hoc Networks duly characterized by openness, high mobility, and dynamic topological changes in a network [3], [4], [5]. Hence, researchers from both academia and industry have expressed an increased interest in the development of VANETs, particularly, driven by the advancements in long-term evolution and Fifth-Generation (5G) mobile communication technologies. Consequently, the concept of 5G–ITS is now being discussed in the research literature since the deployment of 5G can significantly enhance IoV network capabilities by providing more robust and low-latency communication [6], [7], [8].

However, VANETs have certain transmission challenges, i.e., poor wireless channel stability, rapid network topology changes, short link lifetimes, and node distributions constrained by road structures. Therefore, the transition of VANETs to IoV becomes inevitable. IoV manifests a highly dynamic communication network that facilitates interactions

between vehicles via Vehicle-to-Vehicle (V2V) communication, vehicles and roadside infrastructure via Vehicle-to-Infrastructure (V2I) communication, vehicles and vulnerable pedestrians via Vehicle-to-Pedestrian (V2P) communication, and vehicles and backbone network via Vehicle-to-Network (V2N) communication, thereby realizing V2X communication [9], [10]. The components of an IoV encompass On-Board Units (OBUs), communication networks, cloud platforms, big data centers, and application services [11]. Amongst them, OBUs are wireless communication devices installed in vehicles and are primarily responsible for facilitating the exchange of data between vehicles, and vehicles and supporting infrastructure, e.g., toll systems, traffic signals, and roadside units. OBUs, in fact, serve as an information collection and processing center of an IoV network, and encompasses in-vehicle sensors, communication modules, in-vehicle computing platforms, navigation systems, and in-vehicle infotainment systems [12]. It is pertinent to mention that a core function of the IoV is the rapid transmission of information via various wireless communication technologies, including but not limited to, terahertz communication, dedicated short-range communication, 5G, Wi-Fi, and bluetooth [13].

To realize the primary objectives of an IoV network, i.e., enhancing traffic safety [14], [15], optimizing traffic efficiency [16], [17], reducing energy consumption [18], and minimizing environmental pollution [19], it is indispensable to ensure (a) security and privacy to mitigate both external and internal attacks so that the malicious entities cannot jeopardize such a network [20], [21], (b) precise environmental perception for autonomous driving and traffic monitoring via in-vehicle sensors and sensing technologies [22], (c) comprehensive data storage, analysis, and real-time processing capabilities by means of edge and cloud computing [23], [24], (d) wireless communication technologies in a bid to facilitate efficient V2X communication [25], (e) intelligent routing protocols to optimize the data transmission paths [26], and (f) energy management and optimization schemes to enhance energy efficiency by optimizing routes and control systems [27].

Nevertheless, compared with other research objectives, security is of utmost importance in an IoV network. If an IoV network is not secure, it would have fatal consequences for both individuals in vehicles and exposed pedestrians. According to one of the estimates of the World Health Organization, road traffic accidents result in the deaths of about 1.35 million individuals annually, thereby making this as one of the top ten global causes of mortality [28], [29]. Although considerable advancements have already been made in the recent years in the development and deployment of the IoV-related technologies, connected vehicles still confront significant security challenges and any security breach could jeopardize the entire IoV network [15]. Furthermore, conventional cryptography-based mechanisms are inadequate for addressing internal attacks in an IoV network [30]. Therefore, trust's concept has recently emerged as one of the promising solutions for dealing with internal attacks in highly dynamic and distributed networks.

A. SELECTION OF THE RELEVANT PAPERS

The papers selected for this paper are representative papers sourced from renowned scholarly journals, e.g., IEEE Transactions on Intelligent Transportation Systems (T – ITS), IEEE Transactions on Vehicular Technology (TVT), IEEE Transactions on Services Computing (TSC), IEEE Transactions on Network and Service Management (TNSM), IEEE Transactions on Computational Social Systems (TCSS), IEEE Transactions on Dependable and Secure Computing (TDSC), ACM Transactions on Cyber-Physical Systems (TCPS), ACM Computing Surveys, IEEE Internet of Things Journal (IoT – J), Vehicular Communications, and IEEE Access, along with reputed conferences, e.g., IEEE International Conference on Computer Communications (INFOCOM), IEEE Global Communications Conference (GLOBECOM), IEEE International Conference on Trust, Security, and Privacy in Computing and Communications (TrustCom).

A comprehensive search pertinent to the keywords of 'trust', 'trustworthiness', and 'trustworthy' in conjunction with the 'Internet of Vehicles', 'IoV', 'Vehicular Ad hoc Networks', and 'VANETs' from various digital libraries has been conducted, including but not limited to, IEEE Xplore, ACM Digital Library, Elsevier's ScienceDirect, SpringerLink, and Google Scholar. Subsequently, the selected papers were categorized based on their publication venues, i.e., journal or conference. Finally, papers that aligned with the scope of our research were selected by taking into consideration factors, i.e., novelty of the proposed methodology, employed trust attributes and trust aggregation mechanisms, trust evaluation parameters, trust-based attack, simulation tools and datasets.

B. MOTIVATIONS AND CONTRIBUTIONS

A trust management framework employs data- and entity-based trust attributes to ascertain trust values of vehicles for effectively mitigating the propagation of fraudulent messages within an IoV network. It operates through three primary functions (a) systematically identifying and eliminating vehicles propagating malicious misinformation, (b) maintaining secure and dependable traffic flow management, and (c) implementing adaptive weight allocation for trust attributes through either conventional methodologies or learning mechanism-based approaches to accurately quantify their respective impacts on trust evaluation. Moreover, the framework further incorporates dynamic trust threshold derived from calculated trust attributes to precisely detect malicious vehicles. Current implementation challenges primarily revolve around determining optimal parameter configurations, particularly in establishing precise quantification of contribution trust attribute weights and stability-related trust threshold. Furthermore, comprehensive performance

validation remains crucial, requiring rigorous evaluation of the trust management framework's resilience against diverse trust-based attacks through the implementation of adversarial attack scenarios, thereby ensuring robust defense trust mechanisms against sophisticated security breaches in an IoV network.

From Table 1, we can observe that most existing surveys do not comprehensively cover all aspects of trust management in IoV networks. To address this gap, this paper offers a detailed in-depth investigation pertinent to the notion of trust. It further taxonomizes the state-of-the-art IoV-based trust management approaches into conventional and AI-based ones, and critically evaluates the same vis-à-vis the specific salient trust attributes they employ and the trust-based attacks they consider. Hence, the main contributions of this paper are outlined as follows:

- We conduct a detailed in-depth investigation pertinent to the notion of trust, trust characteristics, trust constituents, trust attributes, trust evaluation parameters, and the trust-based attacks.
- The trust management process is categorized into five key stages, i.e., trust formation, trust propagation, trust aggregation, trust update, and trust decision, thereby allowing for a critical comparative review of the existing literature.
- Trust management models at the forefront of current research are broadly categorized into two main groups, i.e., conventional-based trust management models and artificial intelligence-based trust management models. The main research content of the referred trust management models are critically evaluated vis-à-vis the specific trust attributes they employ and the trust-based attacks they consider. Furthermore, we discuss numerous significant research directions pertinent to trust management in an IoV network.

C. ORGANIZATION OF THE PAPER

Section II focuses on the promising notion of trust, the underlying characteristics of trust, key constituents of trust, trust attributes, trust evaluation parameters, and trust-based attacks in IoV networks. Section III describes the five key processes involved in the trust management, i.e., trust formation, trust propagation, trust aggregation, trust update, and trust decision. Section IV offers a comparative analysis of the latest trust management models, i.e., conventional and artificial intelligent-based ones. Finally, Section V discusses the simulation tools and datasets employed in the IoV-based trust models, whereas, Section VI discusses the key open research directions pertinent to IoV-based trust management. Finlay, Section VII concludes the paper. In essence, this particular paper offers a comprehensive overview of the domain to its readers and serves as an entry point for them to explore the same. The taxonomy of this paper is illustrated in Figure 1.

II. TRUST IN THE INTERNET OF VEHICLES

As discussed earlier, the conventional cryptography-based schemes primarily cater for external attacks in an IoV network, however, they remain susceptible to internal attacks [41]. Accordingly, trust has lately emerged as one of the promising solutions for handling internal attacks in highly dynamic and distributed networks [42]

A. THE NOTION OF TRUST

Trust, in essence, is subjective in nature and is, therefore, defined differently across diverse disciplines, i.e., sociology, management science, psychology, medical science, economics, and computer science [43]. At its core, trust is a belief of an individual (trustor) in another individual's (trustee) ability to perform a certain task or tasks [31]. Figure 2 presents an overview of trust across diverse disciplines.

The notion of trust, as employed in this paper, is as follows:

"Trust is a probability of a trustee, i.e., the one who is trusted, to provide a specific service (or services) pertinent to a particular application to a trustor, i.e., the one who trusts, at a given instance of time in a reasonable manner".

Similarly, the notion of trust value, as utilized in this paper, is as follows:

"Trust value, also referred to as the degree of trust or credibility, is a quantitative measure used to assess trustworthiness of a trustee. It is generally represented in the range of [0, 1] with 0 signifying untrustworthiness and 1 manifesting trustworthiness".

B. THE CHARACTERISTICS OF TRUST

To precisely ascertain vehicle trustworthiness in an IoV network, it is pertinent to take into account the following salient underlying characteristics of trust [38], [43]:

- *Subjective* – Subjective trust is ascertained by taking into consideration the direct interaction with a trustee, i.e., it is, in essence, a direct observation made by a trustor pertinent to a trustee.
- *Objective* – Objective trust, as opposed to subjective trust, is computed by compiling feedback about a trustee from its immediate neighbors (peers) in an IoV network.
- *Dynamic* – Trust is a dynamic construct that varies vis-à-vis time mainly due to various contextual factors. This dynamic behavior of trust should be carefully observed in order to ascertain a wide variety of complex trust-based attacks instigated by the malicious vehicles.
- *Asymmetry* – Trust is intrinsically both asymmetric and unidirectional, i.e., the confidence vested by a trustor A in a trustee B does not automatically entail a reciprocated trust from a trustee B towards a trustor A. These two forms of reliance are separate and autonomous.

TABLE 1. Comparison of Existing Surveys vis-à-vis This Survey

Refs.	Main Focus	Trust Attributes	Trust Attacks	Trust Management Process	Trust Evaluation Parameters	Simulation Tools and Datasets
[31]	Classification of IoV-based trust management approaches in terms of AI (clustering, reinforcement learning, fuzzy logic, game theory), and emerging technologies (cloud / fog / edge computing, blockchain, and SDN).	×	◐	◐	×	◐
[32]	Surveyed IoV-based trust management approaches with the key focus being weights quantification, threshold quantification, misbehavior detection, and attack resistance.	✓	✓	×	×	×
[33]	Taxonomized the VANETs-based trust management approaches in the form of conventional-, network-, data-, situation and location-, and AI-based ones.	×	✓	◐	×	◐
[34]	Classified VANETs-based trust establishment and management approaches in terms of cryptography, recommendation, fuzzy logic, consensus, game theory, blockchain, infrastructure, and machine learning ones, and emerging technologies.	×	×	×	×	×
[35]	A systematic literature review to investigate the state-of-the-art IoV-based trust management approaches, the effectiveness of the same, and the suitability of context awareness for trust establishment.	×	×	×	×	◐
[36]	Taxonomized the VANETs-based trust management approaches in the form of emerging technologies (cloud / fog / edge computing, SDN, and blockchain) and AI (clustering, reinforcement learning, fuzzy logic, and game theory).	×	✓	◐	×	×
[37]	A systematic literature review of blockchain-based trust management approaches for IoV across four aspects – trust computation, blockchain scalability, emerging technologies, and security and privacy.	✓	✓	◐	×	×
[38]	Classified the machine learning-driven IoV-based trust management approaches in terms of supervised learning, unsupervised learning, and reinforcement learning.	✓	×	◐	×	×
[39]	Reviewed the state-of-the-art VANETs-based trust management approaches and discussed the impact of decentralization on integrity, security, and privacy.	×	✓	×	×	×
[40]	Cataloged trust management approaches for Connected Autonomous Vehicles (CAVs) in the form of traditional and machine learning (supervised, unsupervised, semi-supervised, and advanced) ones, and reviewed the later vis-à-vis CAVs-specific scenarios.	×	×	◐	×	×
This Survey	Conducted a detailed in-depth investigation pertinent to the notion of trust. Taxonomized the state-of-the-art IoV-based trust management approaches into conventional and AI-based ones and critically evaluated the same vis-à-vis the specific trust attributes they employ and the trust-based attacks they consider.	✓	✓	✓	✓	✓

This article has been accepted for publication in IEEE Open Journal of Intelligent Transportation Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJITS.2026.3663495.

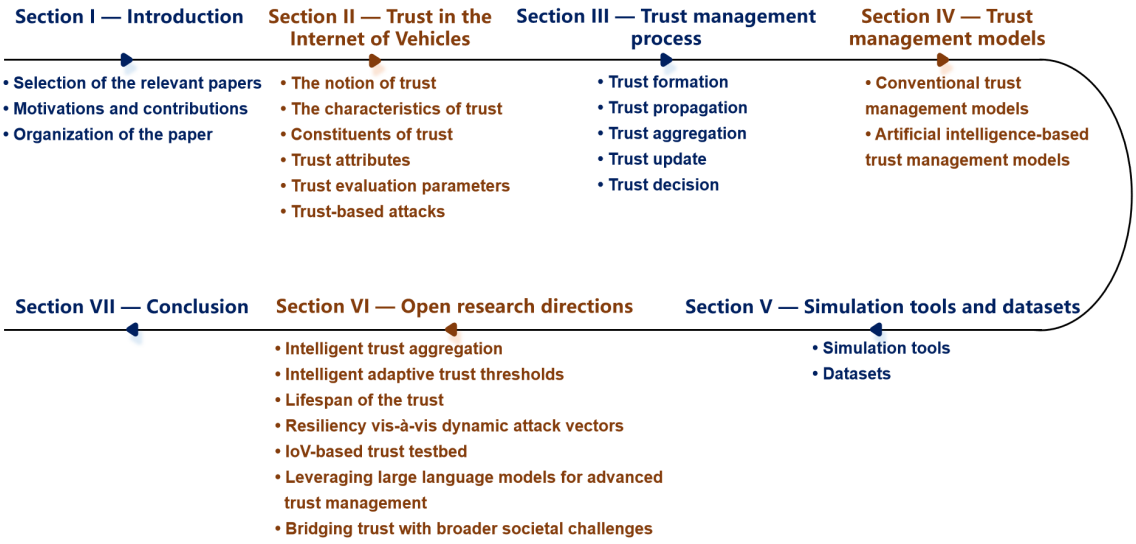

FIGURE 1. **Taxonomy of This Survey.**

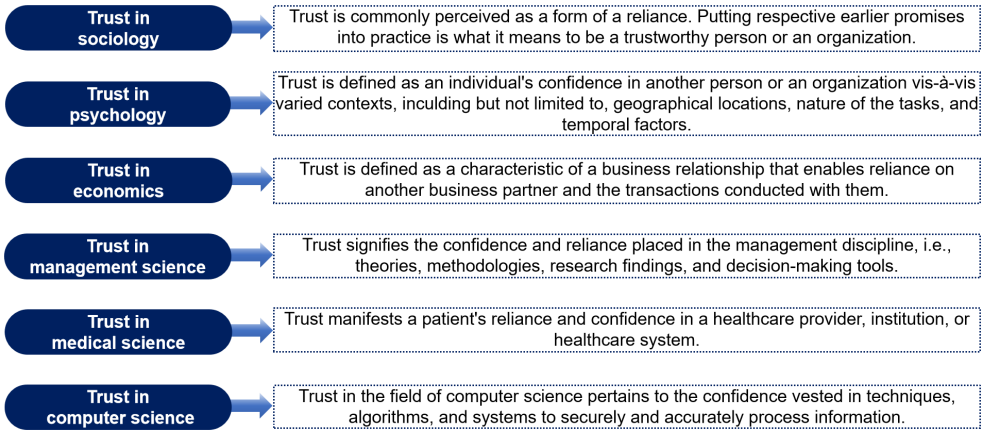

FIGURE 2. **The Notion of Trust in Different Domains.**

- *Local* – When the trust value is confined to a trustor and a trustee, it indicates a vehicle-vehicle relationship based on trust, wherein one vehicle assesses the reliability of another vehicle based on local information, e.g., self-observation and past experiences. However, this value lacks generalizability within an IoV network [31].
- *Global* – Global trust contains assigning a unique and universally recognized trust value to every vehicle in an IoV network. This trust value is predominantly determined by aggregating all the local information of a vehicle.
- *Trust Decay* – The reliability of a trust value assigned to a trustee in an IoV network is likely to decay over time, i.e., the older the estimate, the less credible and less accepted it would be.
- *Context Specific* – The level of trust among vehicles in an IoV network varies according to contextual factors, i.e., the network environment, vehicles' types, and operating scenarios.
- *History Dependent* – The trust of a trustee in an IoV network evolves over time. Trustworthiness of a vehicle at any given time instance is, in fact, its accumulated trust, i.e., the historical trust is also considered albeit to a certain extent.

C. CONSTITUENTS OF TRUST

Trust has two key constituents, i.e., direct trust and indirect trust. The same are delineated as follows:

1) DIRECT TRUST (DT)

Direct trust is established based on a trustor's direct interactions and empirical observations of a targeted vehicle (the trustee) [44]. Although direct trust typically holds greater weight compared to indirect trust, both of them are usually integrated to provide a comprehensive assessment of a vehicle's trustworthiness within an IoV network [45]. So far, numerous methods have been employed in the research

TABLE 2. Methodology for Direct Trust Calculation

Reference	Method	Definition
[46] [47] [48] [49] [50] [51]	Positive and negative interactions	It takes into account both the positive and total interactions, with direct trust is determined by the ratio of positive interactions to total interactions.
[52] [53] [54] [55]	Bayesian inference	The Bayesian inference method, based on the Beta distribution, is employed for the computation of direct trust.
[43] [56] [57] [58] [59] [60] [61]	Trust parameter weight summation	The proposed approach involves the aggregation of multiple trust parameters, each assigned with varying weights, to derive a measure of direct trust.

FIGURE 3. Trust Attributes in Trust Models.

literature for quantifying the direct trust, the details of which are presented in Table 2.

A trustor i's direct trust towards a trustee j at a time instance k has been determined in [43] by considering both the Packet Delivery Ratio (PDR) at time instance k and a weighted aggregation of PDR values from previous time instances. The direct trust has been quantified in [46] by taking into account positive and negative interactions pertinent to a trustor-trustee pair. Moreover, a Bayesian approach based on beta distribution has been employed in [52] to quantify the direct trust.

2) INDIRECT TRUST (IDT)

The indirect trust, also known as recommendation trust, pertinent to a trustee is assessed through the aggregated recommendations from a trustor's one-hop neighbors [47].

D. TRUST ATTRIBUTES

The computation of the aforementioned trust constituents (direct trust and indirect trust) takes into account various trust attributes (parameters) as depicted in Figure 3.

- *Packet Delivery Ratio* – The packet delivery ratio quantifies the degree of association between a trustor and a trustee, thereby reflecting the extent to which messages are successfully received and subsequently disseminated by a trustee [43], [61], [62], [63], [64], [65], [66], [67].
- *Similarity* – The similarity between a trustor and a trustee is usually quantified by considering either the extent of similar content accessed or the similar services provided by them throughout their respective trajectory within an IoV network [46], [49], [50], [59], [68], [69], [70], [71].
- *Familiarity* – Familiarity demonstrates the level of acquaintance between a trustor and a trustee in an IoV network, i.e., a high degree of familiarity indicates a trustor to have a considerable prior knowledge to a trustee [43], [57], [63], [68], [69], [72], [73].
- *Timeliness* – The timeliness of an interaction between a trustor and a trustee is determined by considering the time on which their respective interaction has transpired vis-à-vis the current time instance [57], [63], [74], [75], [76], [77]. Timeliness is of the utmost essence since an outdated information can result into obsolete decisions and which could have severe consequences for entities in an IoV network [65].
- *Cooperativeness* – Cooperativeness reflects the extent to which a trustee interacts with the other vehicles in order to realize a particular service (or services) in a honest manner, i.e., vehicles that act cooperatively are relied upon by the other vehicles and, therefore, consequently obtain higher privileges in an IoV network [1], [43], [68], [78], [79].
- *Context* – Context is essential for determining a trustee's trustworthiness within an IoV network. In essence, context facilitates to understand the underlying dynamics, wherein a trustee operates, including but not limited to, its respective geographical location, ambient traffic, and weather conditions hence resulting in a more accurate trust assessment [69], [80].
- *Reward* – Reward, as an attribute, is employed to award or penalize a trustee depending on its behavior within an IoV network. For instance, if a trustee continuously acts in a cooperative manner, it is awarded a certain factor that augments its respective trust. On the contrary, if a trustee acts selfishly or carry out any sort of a misconduct, its respective trust is decayed or penalized to a considerable degree [54], [79].

This article has been accepted for publication in IEEE Open Journal of Intelligent Transportation Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJITS.2026.3663495.

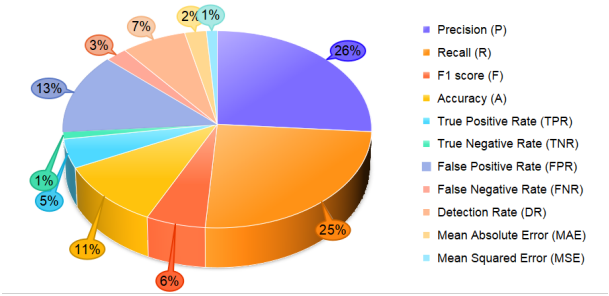

FIGURE 4. Frequency of the Trust Evaluation Parameters.

E. TRUST EVALUATION PARAMETERS

Trust evaluation is integral to the trust management process, for providing a key basis to verify the reliability and efficacy of various trust management schemes [81]. To date, the advanced trust management models for IoV networks have primarily relied on particular trust parameters for evaluation purposes, including but not limited to, Precision, Recall, F1 score, Accuracy, True Positive Rate, True Negative Rate, False Positive Rate, False Negative Rate, Detection Rate, Mean Absolute Error, and Mean Squared Error. The trust evaluation parameters discussed are elaborated in detail in Table 3.

The results of the statistical analysis (Figure 4) clearly demonstrate the prevalence of commonly employed trust evaluation parameters. Precision (26%), Recall (25%), FPR (13%), and Accuracy (11%) are widely adopted for evaluating trust models in existing literature. This finding underscores their relative efficacy in assessing general trust models.

F. TRUST-BASED ATTACKS

The concept of trust has attracted substantial scholarly attention in the recent years. Nevertheless, trust is also susceptible to a variety of attacks. In general, trust-based attacks are generally classified into two main categories, i.e., self-interest-based trust attacks and reputation-based trust attacks. The self-interest-based trust attacks include self-promoting attacks, opportunistic service attacks, on-off attacks, zig-zag attacks, selective behavior attacks, and newcomer attacks (whitewashing attacks), whereas, the reputation-based trust attacks comprise ballot stuffing attacks (good-mouthing attacks), bad-mouthing attacks, time dependent attacks, and collusion attacks [57]. Owing to the dynamic and decentralized characteristic of an IoV network, a malicious vehicle often operates deceptively to gain the trust of neighboring nodes, and once it finds itself in an advantageous position, it can initiate malign activities. To put it another way, a malicious vehicle disguises to provide superior services with the intention of establishing a higher reputation within an IoV network. However, once its reputation is established, it begins to deliver subpar services. More importantly, malicious vehicles may engage in trust-based attacks at specific time instances while functioning normally at other times [110], [111], [112]. Therefore, detecting such attacks poses a significant challenge.

1) SELF-INTEREST-BASED TRUST ATTACKS

- *Self-Promoting Attacks* – Misbehaving vehicles often enhance their reputation to obtain major privileges, thereby jeopardizing the entire IoV network to serve their own malicious objectives [57], [89]. Accordingly, a vehicle exhibiting malicious behavior can create sophisticated Sybil identities (pseudonymous) to manipulate trust for deceiving conventional reputation mechanisms [47], [63].
- *On-Off Attacks* – It is pertinent to highlight that intelligent malicious vehicles adopt a strategic approach by switching between trustworthy and untrustworthy modes. Such an intermittent behavior enables the malicious vehicles to cause harm while remaining undetected in a bid to avoid expulsion from an IoV network. Therefore, by alternately presenting good and bad behaviors, the possibility of classifying such vehicles as malicious is ultimately reduced [1], [43], [47], [71], [75], [83], [89], [92], [103], [95], [113], [114], [115].
- *Zig-Zag Attacks* – Attackers may engage in intermittent malicious behavior to evade detection. For instance, they might choose to intermittently spoof incoming messages before switching to launch a bad-mouth attack, thereby resulting in a zig-zag attack. Whilst their exist similarities between zig-zag attacks and on-off attacks, nevertheless, zig-zag attacks's fluctuation pattern lack regularity [86].
- *Selective Behavior Attacks* – Analogous to gray hole attacks, in selective behavior attacks, misbehaving vehicles exhibit deceptive behavior towards certain nodes, while maintaining honest behavior towards others. Consequently, this may lead to conflicting trust scores assigned to a vehicle by its peers based on direct and/or indirect observations. Nevertheless, by this means, i.e., when a untrustworthy vehicle does not intentionally prioritize high-computation services, it can still uphold its legitimate reputation within an IoV network [93], [108], [116].
- *Newcomer Attacks* – In a newcomer attack, by registering a fresh identity, a malicious vehicle eliminates its undesirable historical record. To mitigate this attack, newcomer vehicles are initially assigned a low trust value and an adaptive attenuation factor is incorporated to impede rapid escalation of the trust value, thereby necessitating consistent performance over an extended duration for trust accumulation [115], [117]. The newcomer attack bears resemblance to the whitewashing attack.

TABLE 3. Trust Evaluation Parameters in Trust Management Models (Precision – P, Recall – R, F1 Score – F, Accuracy – A, True Positive Rate – TPR, True Negative Rate – TNR, False Positive Rate – FPR, False Negative Rate – FNR, Detection Rate – DR, Mean Absolute Error – MAE, Mean Squared Error – MSE)

References	Trust Evaluation Parameters	Definition
[1] [2] [49] [50] [54] [60] [82] [68] [71] [72] [75] [81] [83] [84] [85] [86] [87] [88] [89] [90] [91] [92] [93]	P	Precision signifies the proportion of predicted positives that are actually positive.
[1] [49] [50] [54] [60] [82] [68] [71] [72] [75] [81] [83] [84] [85] [86] [87] [88] [89] [90] [91] [92] [93] [94] [95] [96]	R	Recall, also known as TPR, denotes the proportion of actual positives that are correctly predicted.
[1] [2] [51] [68] [71] [81] [83] [84] [86] [87]	F	F1 score represents the weighted harmonic mean of precision and recall.
[47] [55] [79] [73] [77] [81] [97] [98] [99] [100] [94] [101] [102] [103]	A	Accuracy depicts the proportion of all predictions that are correct. It is commonly employed for assessing the overall performance of trust-based models.
[95]	TNR	TNR, also called specificity, implies the proportion of actual negatives that are correctly predicted.
[2] [50] [58] [60] [71] [75] [89] [97] [96] [104] [105] [106]	FPR	FPR suggests the proportion of actual negatives that are incorrectly predicted as positives.
[2] [71] [75] [104] [105]	FNR	FNR represents the proportion of actual positives that are incorrectly predicted as negatives.
[46] [57] [104] [106] [107] [108] [109]	DR	The detection rate reflects the probability of detecting malicious behaviors, thereby indicating their likelihood of being identified.
[50] [51]	MAE	MAE calculates the average magnitude of errors between the actual and predicted values within a given dataset.
[51]	MSE	MSE quantifies the average squared difference between the actual values and their corresponding predicted values in a given dataset.

2) REPUTATION-BASED TRUST ATTACKS

- *Bad-Mouthing Attacks* – In case of a bad-mouthing attack, attackers manipulate messages similarly to those in simple attacks, whereby false recommendations are sent by the attacker when a vehicle requests recommendations from a bad-mouthing attacks attacker, leading to inaccurate trust evaluation and misjudged decisions [51], [118]. The bad-mouthing attacks often manifest as coordinated groups, wherein multiple malicious vehicles collaborate to undermine the credibility of a specific honest vehicle [1], [46], [47], [54], [57], [60], [71], [75], [81], [89], [103], [105], [119].
- *Ballot Stuffing Attacks* – In a ballot stuffing attack (good-mouthing attack), malicious vehicles work together to offer positive recommendations for another malicious vehicle, thereby enhancing its reputation. Furthermore, if these malicious vehicles are selected as cluster heads, it could have severe implications for the safety and dependability of the IoV network, posing a lethal threat to both occupants of the vehicles and vulnerable pedestrians [46], [47], [51], [56], [57], [71], [75], [89], [95].
- *Time Dependent Attacks* – In time dependent attacks, the attacker exhibits temporal variability in their behavior, demonstrating proficiency to gain trust from vehicles within the IoV network for a certain duration while engaging in unfair rating practices at other times. Consequently, erroneous information and ratings are disseminated among neighboring vehicles during the course of the attack [93], [108].

The trust-based attacks delineated in this particular section can manifest across the network layer, application layer, and the data layer of an IoV ecosystem. Specifically, (a) self-promoting attacks, on-off attacks, and zig-zag attacks transpire on the network layer since adversaries manipulate the routing behaviors, message dissemination, and communication reliability in a bid to distort the perceived trust levels, (b) selective behavior attacks and opportunistic service attacks transpire on the application layer, wherein adversaries provide strategically timed or inconsistent services by exploiting application-level interactions, and (c) bad-mouthing attacks and ballot stuffing attacks transpire on the data layer, wherein adversaries inject falsified feedbacks to manipulate the trust assessments in order to influence the trust decision process. This, therefore, highlights the multi-dimensional impact of trust-based attacks and necessitates

This article has been accepted for publication in IEEE Open Journal of Intelligent Transportation Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJITS.2026.3663495.

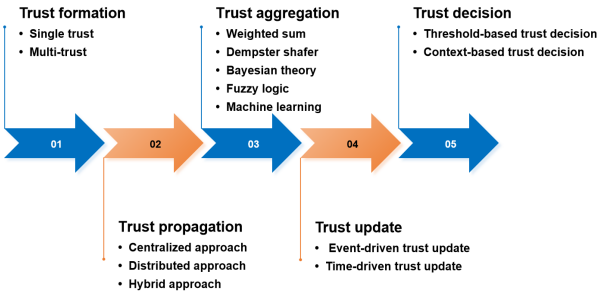

FIGURE 5. Trust Management Process.

layered defenses to holistically secure IoV environments [120] [121].

III. TRUST MANAGEMENT PROCESS

This section outlines the five critical phases of the trust management process, i.e., trust formation, trust aggregation, trust propagation, trust update, and trust decision. A visual representation illustrating the inter-dependencies among these processes is presented in Figure 5.

A. TRUST FORMATION

The process of trust formation typically involves the consideration of trust parameters which can be derived from either a single parameter (single trust) or multiple parameters (multi-trust):

1) SINGLE-TRUST ATTRIBUTE

The single trust attribute takes into account only one specific attribute utilized in determining the total trust. In other words, when it comes to a single trust, evaluation predominantly relies on only one metric [77].

2) MULTI-TRUST ATTRIBUTES

The multi-trust attributes present the notion of trust as a multidimensional concept, wherein multiple factors (attributes) influencing trust are aggregated to form a single trust value. Furthermore, the consideration of numerous attributes facilitates the acquisition of more precise and reliable trust [47], [58], [80], [94], [122], [123], [124].

B. TRUST PROPAGATION

Trust propagation involves disseminating the evaluated trust of a trustee in an IoV network so that its trust can be collectively, and not individually, ascertained by all the vehicles interacting with it. This not only helps in reaching a more precise trust of a trustee but also facilitates in mitigating any trust-based attacks instigated by the same. Trust propagation typically falls within three primary categories:

1) CENTRALIZED APPROACH

The centralized approach relies on a central vehicle that not only collects trust-related information for trust computation purposes but also disseminates the said information. As a result, this particular approach exhibits susceptibility to failure owing to a single point of failure [58], [85], [90], [125].

2) DISTRIBUTED APPROACH

In case there is no centralized authority, vehicles themself assume the responsibility for trust computation as well as trust propagation. While effectively addressing the problem of single point of failure inherent in the centralized approach, this methodology presents challenge pertinent to biased dissemination of trust within an IoV network [43], [47], [81], [86], [87], [88], [122], [126], [127].

3) HYBRID APPROACH

The hybrid approach is commonly employed to mitigate the challenges associated with both centralized and distributed approaches. Additionally, this approach classifies propagation into two distinct types, i.e., locally distributed and globally centralized, as well as, locally centralized and globally distributed [53], [56], [59], [62], [70], [75], [128].

C. TRUST AGGREGATION

Trust aggregation aims to aggregate trust parameters to derive a single trust value, thereby significantly influencing the outcome of trust evaluation. Over the years, numerous techniques for aggregating trust have been thoroughly discussed in the existed research literature, i.e., weighted sum techniques [117], Dempster Shafer Theory (DST) [68], bayesian theory [129], fuzzy logic [97], and Machine Learning (ML) [106]. The detailed description of these trust aggregation technologies is presented as follows:

1) WEIGHTED SUM TECHNIQUES

This technique presents a straightforward approach to aggregate trust parameters by assigning each of them with either a static or a dynamic weight, thereby resulting in a single trust value [1], [2], [46], [54], [58], [82], [64], [86], [101], [128], [130].

2) DEMPSTER SHAFER THEORY (DST)

Dempster Shafer Theory, also refers to as belief theory or evidence theory, integrates multiple pieces of evidence so as to enable the combination of data from diverse independent sources to generate a belief level within the range of [0,1]. However, in the presence of malicious entities, conflicting uncertainties in DST can potentially confound the judgments made by legitimate entities, thereby compromising the reliability of decisions [57], [68], [71], [96], [131].

3) BAYESIAN THEORY

Bayesian theory is a probabilistic framework that acquires empirical knowledge by employing historical statistical data instead of relying on expert knowledge. It quantifies uncertainty by treating probabilities as degrees of belief, where prior probability is combined with observed data (likelihood) to form a posterior probability. The trust in bayesian theory is represented as a beta-distributed random variable within the range of [0,1] [129], [132], [133].

4) FUZZY LOGIC

Fuzzy logic is a mathematical framework that handles imprecision, uncertainty, and partial truth by extending the traditional binary logic. Unlike boolean logic, which requires inputs of either 0 or 1, fuzzy logic offers a more practical approach that mirrors human reasoning. As a result, fuzzy logic is capable of addressing uncertainty and ambiguity in the concept of trust [61], [91], [94], [134].

5) MACHINE LEARNING (ML)

This particular technique typically involves two steps, i.e., unsupervised learning (clustering) and multiclass supervised learning (classification) to categorize nodes into distinct classes. ML approach is generally suitable for models with a relatively higher number of trust parameters, however, it can incur significant computational costs and delays [69], [72], [74], [99], [135], [136].

D. TRUST UPDATE

The process of trust update generally encompasses event-driven and time-driven trust update, and the same are delineated as follows:

1) EVENT-DRIVEN TRUST UPDATE

In an event-driven approach, trust is updated vis-à-vis each transaction. However, this sort of trust update results in an increased traffic overhead owing to frequent transactions within an IoV network [43], [48], [49], [52], [88].

2) TIME-DRIVEN TRUST UPDATE

In a time-driven approach, trust is accumulated and updated via trust aggregation schemes after a predefined duration of time. Nevertheless, the temporal synchronization in this context remains an ongoing challenge [61], [127], [130], [137].

E. TRUST DECISION

The underlying objective of the trust decision is to predict the trustworthiness of a trustee based on its trust value, thereby ascertaining whether it can be considered trustworthy or not.

1) THRESHOLD-BASED TRUST DECISION

In a threshold-based trust decision approach, the trust value of a trustee is either compared with a static or a dynamically adaptive threshold to facilitate the trustworthy decision process in a highly dynamic IoV network [46], [68], [86], [88], [96], [114], [122], [128], [138], [139].

2) CONTEXT-BASED TRUST DECISION

This trust decision approach employs the contextual information, including but not limited to, location, temporal factor, and energy status, so as to systematically formulate policies that can facilitate in determining whether a vehicle is classified as malicious or not [130], [140].

Table 4 summarizes the trust management processes employed in the advanced trust management models.

IV. TRUST MANAGEMENT MODELS: DISCUSSION AND ANALYSIS

In the last decade, numerous trust management models have been proposed for IoV networks to address the increasingly intricate internal security challenges and diverse applications' requirements [1], [2], [43], [50], [99], [117]. This section, therefore, provides an in-depth analysis of the two salient categories relevant to this context, i.e., Conventional Trust Management Models (Con-TMM) and Artificial Intelligence-based Trust Management Models (AI-TMM).

A. CONVENTIONAL TRUST MANAGEMENT MODELS (Con-TMM)

A Dual-model Consensus-based Anti-risk Confidence Allocation (DCACA) trust management scheme in an IoV network has been put forward in [1] so as to analyze and identify internal inappropriate behaviors of vehicles. The dual-model consensus mechanism incorporates a real-time consensus collection mechanism and a matrix-based consensus mechanism, thereby significantly enhancing the detection capability of malicious behaviors by aggregating and analyzing trust opinions from various vehicles. Additionally, an anti-risk confidence allocation mechanism has been designed to exclude negative trust opinions originating from malicious vehicles. Furthermore, to ensure evaluation accuracy, the trust management scheme employed a confidence-based weighting method for aggregating direct trust, indirect trust, and global trust.

A trust model for VANETs aimed at mitigating attacks (message manipulation attacks and bad-mouthing attacks) originating from legitimate network participants has been envisaged in [60]. Trust evaluation encompasses local trust and RSUs-based trust. The local trust and social evaluation involve estimating the social relationships between vehicles through their respective trajectories and interaction history, in conjunction with social recommendations from neighboring vehicles. To achieve an accurate and comprehensive assessment of trust, the model utilizes RSUs to aggregate weights

This article has been accepted for publication in IEEE Open Journal of Intelligent Transportation Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJITS.2026.3663495.

TABLE 4. Trust Management Processes in the IoV-based Trust Management Models (*Note: Single-Trust Attribute – STA, Multi-Trust Attributes – MTAs, Dempster Shafer Theory – DST, Machine Learning – ML*)

Reference	Trust Formation	Trust Aggregation	Trust Propagation	Trust Update	Trust Decision
[1]	MTAs	Weighted sum	Distributed	Event-driven	Threshold-based
[2]	MTAs	Weighted sum	Centralized	Event-driven	Threshold-based
[50]	MTAs	Weighted sum	Hybrid	Event-driven	Threshold-based
[51]	MTAs	ML	Distributed	Event-driven	Threshold-based
[52]	MTAs	Weighted sum	Distributed	Event-driven	Threshold-based
[53]	MTAs	Weighted sum	Hybrid	Event-driven	Threshold-based
[54]	MTAs	Weighted sum	Distributed	Event-driven	Threshold-based
[56]	MTAs	Weighted sum	Distributed	Event-driven	Threshold-based
[59]	MTAs	Information entropy	Hybrid	Hybrid	Threshold-based
[60]	MTAs	Weighted sum	Centralized	Event-driven	Threshold-based
[61]	MTAs	Fuzzy logic	Distributed	Time-driven	Threshold-based
[67]	MTAs	Weighted sum	Distributed	Event-driven	Threshold-based
[68]	MTAs	DST	Distributed	Event-driven	Threshold-based
[70]	MTAs	Weighted sum	Hybrid	Event-driven	Threshold-based
[71]	MTAs	DST	Hybrid	Event-driven	Threshold-based
[72]	MTAs	ML	Distributed	Event-driven	Threshold-based
[75]	MTAs	Weighted sum	Hybird	Event-driven	Threshold-based
[78]	MTAs	ML	Distributed	Distributed	Threshold-based
[79]	MTAs	ML	Distributed	Distributed	Threshold-based
[86]	MTAs	Weighted sum	Distributed	Distributed	Threshold-based
[87]	MTAs	Weighted sum	Distributed	Hybrid	Threshold-based
[90]	MTAs	Weighted sum	Centralized	Event-driven	Threshold-based
[97]	MTAs	Fuzzy logic	Distributed	Time-driven	Threshold-based
[99]	MTAs	ML	Distributed	Event-driven	Threshold-based
[94]	STA	Fuzzy logic	Distributed	Time-driven	Threshold-based
[102]	MTAs	Weighted sum	Distributed	Event-driven	Threshold-based
[103]	MTAs	Weighted sum	Distributed	Event-driven	Threshold-based
[95]	MTAs	Bayesian	Distributed	Time-driven	Threshold-based
[96]	MTAs	DST	Distributed	Event-driven	Threshold-based
[104]	STA	Fuzzy logic	Distributed	Event-driven	Threshold-based
[106]	MTAs	ML	Distributed	Hybrid	Threshold-based
[108]	MTAs	DST	Distributed	Event-driven	Threshold-based
[117]	MTAs	ML and Weighted sum	Distributed	Time-driven	Threshold-based
[123]	MTAs	Fuzzy logic	Distributed	Event-driven	Threshold-based
[128]	MTAs	Weighted sum	Hybrid	Event-driven	Threshold-based
[130]	MTAs	Weighted sum	Distributed	Time-driven	Threshold-based
[134]	MTAs	Fuzzy logic	Distributed	Event-driven	Threshold-based
[137]	MTAs	Honey-bee algorithm	Centralized	Time-driven	Threshold-based
[138]	MTAs	Weighted sum	Centralized	Event-driven	Threshold-based
[139]	MTAs	Weighted sum	Distributed	Event-driven	Threshold-based
[141]	MTAs	ML	Centralized	Event-driven	Threshold-based
[142]	MTAs	ML	Distributed	Event-driven	Threshold-based
[143]	MTAs	Weighted sum	Hybird	Event-driven	Context-based
[144]	MTAs	ML	Distributed	Event-driven	Threshold-based
[145]	MTAs	ML	Distributed	Event-driven	Threshold-based

derived from eigenvector centrality and social indicators within the local trust network.

An incentive-based mechanism has been proposed in [70] to facilitate decentralized and reliable service management for information dissemination within VANETs. This mechanism evaluates message credibility by leveraging the trustworthiness of the sender and incorporates a negative feedback function to prevent malicious vehicles' attacks. Furthermore, a reward and punishment mechanism, rooted in repeated game theory, has been designed to incentivize vehicles for active information sharing. Additionally, to ensure consistent trust management storage and reduce reliance on centralized institutions, a blockchain-based distributed trust management mechanism has been presented, wherein RSUs serve as blockchain nodes and are responsible for calculating vehicles' trust values and maintaining their respective trust value list.

A trusted RSU-based task offloading mechanism has been established in [75] to detect simple attacks, recommendation attacks, and on-off attacks with the objective of securing information service operations in the context of an IoV network. This infrastructure trust management model includes the Quality of Service (QoS) trust and social trust, wherein QoS trust considers connectivity trust and timeliness trust, whereas, the social trust among RSUs is established through unselfish trust, neighbor recommendation, and cooperation trust. Moreover, a delay-optimized vehicle task offloading model has been developed to provide a quantitative analysis of the latency resulting from task delegation processes. Furthermore, an algorithm based on trusted RSU service is designed to realize the offloading of networked vehicles' task.

A Multi-Dimensional Trust (MDT) model for VANETs has been put forward in [86] to effectively counter common trust-based attacks, such as, simple attacks, recommendation attacks, and zig-zag attacks. This model comprises four stages, i.e., (a) data collection, (b) trust aggregation, (c) data filtering, and (d) trust update. This particular model takes into consideration various trust attributes of vehicles and employs the entropy weighting method for dynamic weight adjustment of the said attributes for ultimately achieving a comprehensive trust evaluation. Furthermore, the model utilizes the median absolute deviation to eliminate abnormal evaluation results more effectively against both complex and dynamic intelligent attacks.

A distributed Hybrid Trust Management framework (HTMS-V) has been proposed in [97] to identify potential internal attacks in VANETs, i.e., false message injection attacks, on-off attacks, and collusion attacks. HTMS-V integrates both direct trust and indirect trust by leveraging direct interaction data and trust recommendations from one-hop neighbors. Moreover, the said framework enhances the subjective logic trust model with a distance-based weighted voting mechanism to improve trust accuracy. Furthermore, the said framework incorporates inter-node distance and equips each vehicle with a trust evaluation and decision module to address certain challenges, i.e., incomplete trust variables, erroneous trust evaluations, and potential collusion attacks in distributed environments.

A Cross-Domain dynamic Trust inheritance mechanism (CDTE) for VANETs has been envisaged in [103] to update the trust value of a vehicle in real time. The mechanism's architecture contains three layers, i.e., central management layer, edge node layer, and vehicle node layer. It first integrates direct trust and recommended trust to ascertain the single trust value of a vehicle, and then calculates its global trust value through a trust feedback strategy consisting of active trust feedback and passive trust feedback, thereby ensuring to punish malicious vehicles and reward reliable ones. Moreover, to address the trust discontinuity problem in cross-domain scenarios, the RSUs can rapidly retrieve and refresh a vehicle's historical trust records upon its first entry into a new domain.

A RSU-assisted Trust-based Routing protocol for VANETs (RTRV) has been presented in [113] which incorporates trust criteria to ensure secure routing for establishing reliable and efficient communication paths. An enhanced monitoring procedure for trust management has been introduced for leveraging the common neighbor between the current node and the next hop node to select the monitoring node. Additionally, it employs a dual-observer (sender and monitor node) monitoring mechanism to observe the behavior of the next hop while utilizing RSU in trust management. This approach enhances resistance against good-mouthing attacks, bad-mouthing attacks, on-off attacks, gray hole (selective forwarding) attacks, collusion attacks, and newcomer attacks.

A content distribution model based on Entity Trust (ET) and Social Trust (ST) has been proposed in [134] so as to enhance the quality of service in a SIoV network. The model segregates the trust evaluation into ET and ST. ET describes the communication capability of vehicle equipment, e.g., OBUs, antennas, the processing units, and the receiving and sending units, which is assessed based on historical communication (direct and indirect trustworthy ratio) between vehicles. On the contrary, the evaluation of ST stems from the process of establishing new social connections and receiving feedback from acquaintances. Subsequently, fuzzy comprehensive evaluation has been employed for assessing ET and ST, thereby establishing an overall trust framework that effectively regulates the driving application functions and social behavior within SIoV network. Additionally, this model improves blocking rules of content distribution too.

The analysis of Table 5 reveals that the state-of-the-art conventional trust management models have a relatively small number of trust parameters because of the ongoing challenge in implementing a dynamic weighting mechanism. However, this reduced set of trust parameters presents drawbacks in evaluating the efficiency of the trust model.

TABLE 5. Conventional Trust Management Models (Con-TMM)

Ref.	Trust Attributes							Trust Attacks							
	PDR	Sim	Fam	Timeliness	Coop	Context	Reward	SPA	OOA	ZZA	SBA	NA	BMA	BSA	TDA
[1]	✓	-	-	-	✓	✓	-	-	✓	-	-	-	✓	-	-
[43]	✓	-	✓	✓	✓	✓	-	✓	✓	-	-	-	-	-	-
[52]	✓	-	-	-	-	✓	-	-	-	-	-	-	✓	-	-
[54]	✓	-	-	-	-	✓	✓	-	-	-	-	-	✓	-	-
[56]	✓	-	-	-	-	✓	-	-	-	-	-	-	✓	✓	-
[57]	✓	-	-	-	-	✓	-	✓	-	-	-	-	✓	-	-
[60]	✓	-	-	-	✓	✓	-	✓	-	-	-	-	✓	-	-
[63]	✓	-	✓	✓	-	-	-	-	-	-	-	-	-	-	-
[67]	✓	-	-	✓	-	-	-	-	-	-	-	-	-	-	-
[68]	-	✓	✓	-	✓	-	✓	-	✓	-	-	-	-	-	-
[70]	-	✓	-	-	-	-	-	-	-	-	-	-	✓	-	-
[71]	-	✓	-	-	-	-	-	-	✓	-	-	-	✓	✓	-
[75]	-	✓	-	✓	✓	✓	-	-	✓	-	-	-	✓	✓	-
[86]	✓	-	-	-	-	✓	-	-	-	✓	-	-	✓	✓	-
[93]	-	✓	-	-	-	-	-	-	-	-	✓	-	-	-	✓
[95]	✓	-	-	-	-	✓	-	-	✓	-	-	✓	✓	✓	-
[97]	✓	-	-	-	-	✓	-	-	✓	-	-	-	✓	✓	-
[103]	✓	-	-	-	-	✓	-	-	✓	-	-	-	✓	-	-
[108]	✓	-	-	-	-	✓	-	✓	-	-	✓	-	-	-	✓
[117]	✓	-	-	-	-	✓	-	✓	✓	-	-	✓	-	-	-
[128]	✓	-	-	-	-	✓	-	-	-	-	-	-	-	-	-
[134]	✓	-	-	-	✓	✓	-	-	-	-	-	-	-	-	-

Packet Delivery Ratio – PDR, Similarity – Sim, Familiarity – Fam, Cooperativeness – Coop
Self-Promoting Attack – SPA, On-Off Attack – OOA, Zig-Zag Attack – ZZA, Selective Behavior Attack – SBA
Newcomer Attack – NA, Bad-Mouthing Attack – BMA, Ballot Stuffing Attack – BSA, Time Dependent Attack – TDA

B. ARTIFICIAL INTELLIGENCE-BASED TRUST MANAGEMENT MODELS (AI-TMM)

Due to the limitations inherent in conventional trust management models, i.e., limited number of trust parameters and challenges pertinent to dynamic weights, numerous Artificial Intelligence-based Trust Management Models (AI-TMM) have been introduced in the research literature [50], [51], [72], [74], [99], [144], [146].

To address the inability of the current trust models to select appropriate recommendation nodes and dynamically adapt the recommendation trust's weight, a trust model based on IoV topological structure has been put forward in [50]. The model contains three layers, i.e., local trust management, cluster trust management, and global trust management. Prior to calculating of recommendation trust, a fuzzy C-means algorithm has been employed to filter out malicious recommendation values, followed by assessing the reliability of recommendation trust values through degrees of similarity and dissimilarity.

A trust framework utilizing artificial neural networks has been envisaged in [51] to provide a reliable basis for trust assessment in a Social Internet of Things (SIoT) network. Several key trust metrics, i.e., direct trust, reliability and benevolence, credible recommendations, and context-based degree of relationships, have been taken into account. Furthermore, a knowledge graph embedding approach has been employed to estimate the social similarity among IoT entities.

Machine learning approaches have been introduced in [72] to resolve challenges concerning intelligent weighting and the establishment of optimal detection thresholds for malicious behavior identification in an IoV network. A feature matrix that incorporates four key trust parameters, i.e., packet delivery ratio, familiarity, timeliness, and interaction frequency, has been established by (a) treating all trust parameters calculated by each trustor for a trustee as a single feature and (b) taking into account the collective average of the said four parameters calculated by all trustors for a trustee. Moreover, various machine learning algorithms have been applied for labeling each generated feature matrix. Finally, support vector machine, weighted k-nearest neighbor, and subspace k-nearest neighbor classifiers have been employed to categorize vehicles as either trustworthy or untrustworthy.

A time-aware trust model, leveraging machine learning techniques to determine and predict the behavior of entities in a SIoT network has been envisaged in [78]. The trust model encompasses four trust parameters, i.e., friendship

similarity, community-of-interest, cooperativeness, and co-work similarity. Machine learning has been utilized to aggregate the said trust parameters and to classify objects as trustworthy or untrustworthy. Moreover, change in the trust values vis-à-vis time has been analyzed to determine the impact of each trust parameter on an object's aggregated trust. A somewhat similar SIoT-based trust model encompassing direct trust and indirect trust has been presented in [79], wherein objects have been classified as trusted, neutral, or untrusted.

A hybrid optimization-based Deep Maxout Network (DMN) for classifying attacks in VANETs has been suggested in [90]. Cluster head selection and routing are performed using the fractional aquila optimizer algorithm which combines fractional calculus and aquila optimization techniques [147]. Moreover, the selection process takes into account the impact of distance, trust factors, energy levels, and entropy weighted models. The trust factors encompass direct trust, indirect trust, and recent and historical trust. Attack detection is segregated into two stages, i.e., feature selection and classification. The feature selection uses congruence coefficients to select key attributes. Finally, according to whether the nodes are malicious or normal, DMN is used to classify the nodes.

A hierarchical trust evaluation method based on data transmission success rate, network reliability and real time performance, and nodes' historical behaviors to determine the total trustworthiness of nodes has been proposed in [99]. The proposed training model considers the issue of non Independent and Identically Distributed (non-IID) data affecting Federated Learning (FL) model convergence speed and, accordingly, introduced a Federated Adaptive (FedAdp) weighting algorithm encompassing initialization, local update, and global update processes to enhance or attenuate the positive or negative contributions from the participating nodes.

A trust-based client selection framework for federated learning has been developed in [102] in a bid to address the issue pertinent to malicious or unreliable clients' updates in the context of an IoV network. By incorporating contextual information, reputation scores, and resource availability, the said framework adaptively aggregates clients trust levels to prioritize reliable contributions and suppress adversarial influence. This framework encompasses several key components, i.e., central server, clients, communication network, trust evaluation module, and client selection module to ensure that only the most reliable clients participate in the FL training process. The central server sends the global model to all the clients who train and evaluate local models, and return updates and trust metrics. The trust evaluation module calculates and updates trust scores of each client, whereas, the client selection module opts for the most trustworthy ones. The central server aggregates updates from the selected clients to update the global model and repeats the process until it converges.

A Q-Learning based Adaptive Trust Threshold control strategy (QART) has been proposed for VANETs in [106] to enhance the accuracy and efficiency of malicious vehicle detection. Firstly, an error degree has been defined to quantify the likelihood of false alarms and which serves as a foundation for determining an adaptive trust threshold. Subsequently, QART leverages reinforcement learning's reward and punishment mechanisms to balance detection efficiency and false alarm rates. Finally, a dynamic update control method has been developed to incorporate the latest trust evaluation results for timely and adaptive decision-making.

A Verifiable Discrete Trust Model (VDTM) for the Social Internet of Vehicles has been proposed in [144] in a bid to address the risks associated with data leakage and trustworthiness when sharing social information, thereby ensuring secure information sharing. Consistent FL has been employed to verify both forward and reverse trust for enhancing authentication across different shared sessions. Moreover, key-based authentication has been implemented to ensure session integrity during information sharing.

An entity centric trust framework based on decision tree and artificial neural networks has been proposed in [145] so as to enhance the security of an IoV network. This framework took into consideration direct trust, recommended trust, multifaceted entities-based role, and distance-based (euclidean) measures for calculating and evaluating trust amongst the vehicles. Moreover, decision tree classification has been employed to establish rules for trust computation and artificial neural networks have been utilized to enable self-training of vehicular nodes in order to ensure reliable message propagation.

Table 6 depicts a comparative analysis of the most recent AI-based trust management models.

V. SIMULATION TOOLS AND DATASETS

This section delineates simulation tools and datasets for assessing the performance of trust-based models in an IoV network.

A. SIMULATIONS TOOLS

The simulation method is predominantly employed to evaluate the trust models in an IoV network. The state-of-the-art simulation tools in this context include, but are not limited to, Veins [52], Network Simulator 3 (NS-3) [49], Opportunistic Network Environment (ONE) [81], NetLogo simulator [94], MATLAB, and Python [46].

1) VEINS

Veins is a traffic simulation framework which integrates Simulation of Urban Mobility (SUMO) and OMNeT++ with a primary focus on simulating urban traffic flows and vehicular communications. Accordingly, researchers can manipulate several parameters, e.g., traffic signals, vehicles' behaviors, and communication protocols, to evaluate traffic

This article has been accepted for publication in IEEE Open Journal of Intelligent Transportation Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJITS.2026.3663495.

TABLE 6. Artificial Intelligence-based Trust Management Models (AI-TMM)

Ref.	Trust Attributes							Trust Attacks							
	PDR	Sim	Fam	Timeliness	Coop	Context	Reward	SPA	OOA	ZZA	SBA	NA	BMA	BSA	TDA
[50]	✓	✓	-	-	-	-	-	-	-	-	-	-	-	-	-
[51]	✓	-	-	-	-	✓	-	-	-	-	-	-	-	-	-
[72]	✓	-	✓	✓	-	-	-	-	-	-	-	-	-	-	-
[74]	✓	-	-	✓	-	-	-	✓	-	-	✓	-	-	-	-
[78]	-	✓	-	-	✓	-	-	-	-	-	-	-	-	-	-
[79]	-	✓	-	-	✓	-	✓	-	-	-	-	-	✓	✓	-
[90]	✓	-	-	-	-	-	-	✓	-	-	-	-	-	-	-
[99]	✓	-	-	✓	-	✓	-	-	✓	-	-	-	-	-	-
[100]	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	-
[102]	✓	-	-	-	-	✓	-	-	-	-	-	-	✓	✓	-
[106]	✓	-	-	-	-	✓	-	-	-	-	-	✓	✓	✓	-
[145]	✓	✓	-	✓	-	-	-	-	-	-	-	-	-	-	-
[148]	✓	-	-	-	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
[149]	✓	-	-	✓	✓	-	-	-	-	-	-	-	-	-	-
[150]	✓	-	-	-	-	-	-	✓	-	-	-	-	-	-	-

Packet Delivery Ratio – PDR, Similarity – Sim, Familiarity – Fam, Cooperativeness – Coop
Self-Promoting Attack – SPA, On-Off Attack – OOA, Zig-Zag Attack – ZZA, Selective Behavior Attack – SBA
Newcomer Attack – NA, Bad-Mouthing Attack – BMA, Ballot Stuffing Attack – BSA, Time Dependent Attack – TDA

management strategies, optimize flow dynamics, analyze congestion causes, and assess the impact of the same in an IoV network. The results can be visually presented using intuitive tools to facilitate decision-making processes and enhance traffic planning capabilities. Existing literature suggests that numerous studies on trust management have utilized Veins to validate their proposed trust management models [2], [52], [86], [87], [88], [97], [113], [115], [117], [122].

2) NETWORK SIMULATOR 3 (NS-3)

NS-3 is an open-source network simulation tool which utilizes the discrete event simulation method and provides support for various network protocols, e.g., transmission control protocol and user datagram protocol. Researchers can define the network topology and simulation parameters using tool command language scripts that offer a high degree of flexibility [151]. NS-3 thus enables the creation of realistic simulation scenarios and is, therefore, widely employed to validate trust management models [48], [49], [58], [91], [123], [137], [152]. Moreover, there is a gradual transition among researchers towards more contemporary simulation tools NS-3.

3) OPPORTUNISTIC NETWORK ENVIRONMENT (ONE)

ONE is a simulation environment which enables creating dynamic networking scenarios and facilitates the testing of numerous routing protocols. Also, it offers visualization tools that portrays a comprehensive depiction of nodes movement and data transmission processes. The flexibility and scalability inherent in ONE has encouraged researchers over the years to validate their respective trust management models in dynamic IoV scenarios [54], [60], [82], [68], [81].

4) NETLOGO SIMULATOR

NetLogo simulator is an integrated development environment for multi-agent simulation well-suited for modeling complex systems [153]. It enables the simultaneous movement of thousands of agents, thereby facilitating the exploration of individual microscopic entities and their respective interactions that give rise to macroscopic phenomena. NetLogo simulator has also been instrumental in studying trust management within IoV networks by enabling the simulation of agent-based trust dynamics and communication protocols [59], [94], [101].

5) OTHERS

In addition to the above, MATLAB and Python have also been extensively utilized to simulate and validate IoV-based trust management models. MATLAB offers capabilities in numerical analysis, numerical and symbolic computation, engineering and scientific plotting, and digital image processing. It is, therefore, widely employed by researchers for purposes of model creation, algorithm development, and data analysis. Moreover, MATLAB provides a dedicated Simulink platform for designing and deploying IoV applications. Accordingly, it has gained significant popularity within trust management community. Similarly, Python serves as a commonly used tool for simulating dynamic networks. To summarize, both MATLAB and Python have emerged as

preferred choices in the research literature for validating the performance of various IoV-based trust management models [43], [46], [51], [55], [57], [58], [70], [72], [74], [75], [89], [90], [128], [134].

B. DATASETS

Datasets are indispensable for validating IoV-based trust management models. Whilst there are no dedicated IoV-based trust datasets, i.e., with exception of the one envisaged in [154], a detailed analysis of the advanced reveals that both Epinions dataset and CRAWDAD dataset have been extensively employed for the said purpose [155], [156].

1) EPINIONS DATASETS

Epinions is a publicly available trust dataset that encompasses six key parameters, i.e., userid, productid, categoryid, rating, usefulness, and timestamp. In the Epinions dataset, a data entry of $[1, 2, 3, 4, 5, 6]$ denotes that user 1 rated product 2 in category 3 with a rating of 4 (usefulness of the rating being 5) at timestamp 6. The Epinions dataset, while not originally designed as an IoV dataset, has been appropriately transformed into one by certain researchers to evaluate the effectiveness and reliability of trust management models in an IoV network [69], [107].

2) COMMUNITY RESOURCE FOR ARCHIVING WIRELESS DATA AT DARTMOUTH (CRAWDAD) DATASET

CRAWDAD is a dataset for the research community interested in wireless networks and mobile computing. This particular dataset was originally conceived as part of the SIGCOMM conference and hence encompasses traces of participants' devices, including but not limited to, their respective proximity, opportunistic message creation and dissemination (with interaction logs in terms of successful and unsuccessful interactions), and the social profiles (list of friends and interest groups). Over the past few years, the CRAWDAD dataset has been widely employed in the research literature for assessing the effectiveness and reliability of trust management models in an IoV network [63], [72], [78].

VI. OPEN RESEARCH DIRECTIONS

Whilst the notion of trust in IoV networks has gained considerable research attention from both academia and industry over the last decade, there are still a number of prevailing issues which mandates careful consideration. This section, therefore, is an effort pertinent to outline numerous key open research directions to IoV-based trust management.

A. INTELLIGENT TRUST AGGREGATION

Trust aggregation involves aggregating several context-dependent trust attributes (parameters) into a single optimal trust value to ascertain the vehicles's trustworthiness in an IoV network. Accordingly, conventional trust-based mechanisms primarily employ static weights for the said purpose. However, static weights cannot realize the impact of the influential trust attributes in the trust aggregation process [46], [113]. Owing to the same, learning-based trust aggregation methods have recently been explored in the existed research literature [72], [74]. Nevertheless, learning-based trust mechanisms require substantial data and are prone to data bias too. It is, therefore, indispensable to design intelligent trust aggregation mechanisms that are not only robust but can further take into consideration the underlying dynamic context for determining optimal trust values in an IoV network [38].

B. INTELLIGENT ADAPTIVE TRUST THRESHOLDS

Existing trust-based management mechanisms primarily rely on predefined trust thresholds to distinguish the trustworthy vehicles from the untrustworthy ones. Accordingly, a vehicle with trust above the predefined threshold is deemed trustworthy and the one below the predefined threshold is viewed as untrustworthy [47], [52]. Therefore, an optimal and intelligent trust threshold is indispensable for not only detecting the malicious vehicles but to subsequently evict them as soon as possible from an IoV network. This is particularly of the essence since (a) an excessively high predefined threshold risks false-positive elimination of legitimate vehicles, or (b) an overly low threshold permits malicious vehicles to achieve adversarial objectives. An adaptive trust threshold is thus one of the possible solutions for addressing this issue, however, the same would also result in an excessive network management overhead since it involves monitoring and adaptively adjusting the threshold for each vehicle at regular intervals. Therefore, there is a dire need of envisaging intelligent adaptive threshold mechanisms so as to tackle this critical challenge [39], [82].

C. LIFESPAN OF THE TRUST

Owing to the highly dynamic and distributed characteristics of an IoV network, vehicles interact with and subsequently assign trust to numerous other vehicles during the course of their respective trajectory. Accordingly, it is not possible for a particular vehicle to store the trust of all the vehicles it has interacted with primarily due to the onboard storage constraints. Moreover, a vehicle might interact with another vehicle merely once, thereby making it highly impractical to keep a record of such an interaction after a certain duration of time. Therefore, intelligent lifespan- and decay-related mechanisms should be envisaged for (a) not only ascertaining the lifetime of the trust vis-à-vis context but (b) to also decay the same by an optimal proportion in case of no recent further interactions [157], [158].

D. RESILIENCY vis-à-vis DYNAMIC ATTACK VECTORS

Whilst trust remains an optimal solution for mitigating internal attacks within an IoV network, it remains suscep-

tible to a variety of trust-based attacks, i.e., on-off attacks, self-promoting attacks, opportunistic attacks, ballot stuffing attacks (good-mouthing attacks), and bad-mouthing attacks. Such attacks are incited by the dishonest vehicles to attain considerable privileges so as to jeopardize the entire IoV network for their malign objectives. It becomes even more critical if and when an attacker (malicious vehicle) launches multiple dynamic attacks vis-à-vis dynamic contexts to avoid detection and subsequent eviction from an IoV network. It is, therefore, vital importance to devise intelligent threat models that have the potential to identify the underlying vulnerabilities within an IoV network that are exploited by the attackers to instigate such sort of sophisticated attacks [52].

E. IoV-BASED TRUST TESTBED

An IoV-based trust testbed is paramount for evaluating trust models in this particular domain. Whilst numerous trust models have already been envisaged and subsequently evaluated via a wide range of simulation techniques, these simulations often do not reflect the real-world realistic environment pertinent to an IoV network. Also, existing trust models take into consideration multiple static trust attributes and are evaluated via standardized metrics, however, they lack a comprehensive and realistic trust testbed that can ascertain their respective performance vis-à-vis dynamic contexts and subsequently compare their respective performance vis-à-vis several other prevailing trust models. Hence, designing of an IoV-based trust testbed that not only takes into account the underlying environmental considerations but can also intelligently evaluate the complex interactions between the dynamic network entities is imperative for strengthening the resiliency of an IoV network [159].

F. LEVERAGING LARGE LANGUAGE MODELS FOR ADVANCED TRUST MANAGEMENT

The emergence of Large Language Models (LLMs) offers a promising opportunity for strengthening the IoV-based trust management. Owing to their sophisticated natural language understanding and contextual reasoning capabilities, complex, multi-modal data, including but not limited to, vehicular sensor readings, traffic reports, and drivers and passengers intent, can be intelligently interpreted vis-à-vis varied IoV environments. A critical research gap lies in investigating how LLMs can dynamically adjust trust evaluation policies in response to the unstructured incident reports and real-time risk assessments. Nevertheless, integrating LLMs in resource-constrained and latency-sensitive IoV settings mandates designing lightweight LLM architectures for the on-board units and the development of secure, privacy-preserving mechanisms for querying cloud-based LLMs [160], [161].

G. BRIDGING TRUST WITH BROADER SOCIETAL CHALLENGES

A critical challenge lies in envisaging IoV-based trust management mechanisms that simultaneously adhere to both sustainability and ethical governance. For advancing sustainability, the IoV-based mechanisms should efficaciously filter out untrustworthy nodes and minimize redundant communications to reduce energy consumption. At the same time, ethical compliance mandates IoV-based trust mechanisms that not only safeguard privacy but also ensure fairness in reputation formation and transparency in trust decisions. Satisfying these dual objectives necessitates lightweight and explainable trust architectures that can operate under real-time constraints while also balancing resource efficacy with accountable, unbiased decision-making across varied IoV environments [162], [163].

VII. CONCLUSION

This paper offers an in-depth analysis of trust management in the context of an IoV network. It begins with a discussion of evolution of IoV followed by an exploration of the notion of trust across several different domains. This paper then examines the key aspects of trust in an IoV network, i.e., salient trust characteristics, trust constituents, trust attributes, trust evaluation parameters, and trust-based attacks. It also delves into the various processes involved in trust management, i.e., trust formation, trust propagation, trust aggregation, trust update, and trust decision. Moreover, this paper highlights the key research of existing IoV-based trust management models, i.e., conventional and artificial intelligence ones. Furthermore, it introduces the simulation tools and datasets employed to evaluate the performance of IoV-based trust models, thereby providing an in-depth synthesis of the current state of trust management in IoV networks. Although current research has made considerable progress in this domain, several critical open challenges remain. Future efforts are expected to increasingly adopt distributed technologies, e.g., federated learning and blockchain, to build decentralized and transparent trust frameworks. Interestingly, large language models show strong potential for extracting rich behavioral patterns from unstructured vehicular data thus enabling more refined trust assessment. Concurrently, hypergraph theory provides a natural structure for representing complex multi-node interactions beyond simple pairwise relationships, thereby leading to a more comprehensive and accurate representation of trust dynamics in IoV networks.

REFERENCES

[1] C. Cheong, Y. Song, Y. Cao, Y. Zhang, H. Wang, and Q. Ni, "DCACA: Dual-Model Consensus-Based Anti-Risk Confidence Allocation Trust Management in IoVs," *IEEE Internet of Things Journal*, vol. 12, no. 2, pp. 1890–1906, 2024.

[2] X. Dang, G. Zhang, K. Sun, and Y. Li, "A Trust Model for VANETs Using Malicious-Aware Multiple Routing," *Computers & Security*, vol. 148, pp. 104–145, 2025.

[3] R. Di Pietro, S. Guarino, N. Verde, and J. Domingo-Ferrer, "Security in Wireless Ad-Hoc Networks – A Survey," *Computer Communications*, vol. 51, pp. 1–20, 2014.

[4] S. Hossain, S.-M. Senouci, B. Brik, and A. Boualouache, "A Privacy-Preserving Self-Supervised Learning-Based Intrusion Detection System for 5G-V2X Networks," *Ad Hoc Networks*, vol. 166, p. 103674, 2025.

[5] M. Jamil, M. Farhan, F. Ullah, and G. Srivastava, "A Lightweight Zero Trust Framework for Secure 5G VANET Vehicular Communication," *IEEE Wireless Communications*, vol. 31, no. 6, pp. 136–141, 2024.

[6] G. Rathee, A. Kumar, C. A. Kerrache, and C. T. Calafate, "A Trust Management Solution for 5G-Based Future Generation Internet of Vehicles," *Computer Networks*, vol. 248, p. 110501, 2024.

[7] B. Vidhya, H. Harshene, and N. Abimathi, *Introduction to Next Generation Networks 5G and Beyond*. John Wiley & Sons, Ltd, 2025, ch. 1, pp. 1–18.

[8] H. Zhang and M. Li, "Towards an Intelligent and Automatic Irrigation System Based on Internet of Things with Authentication Feature in VANET," *Journal of Information Security and Applications*, vol. 88, p. 103927, 2025.

[9] V. Rishiwal, U. Agarwal, A. Alotaibi, S. Tanwar, P. Yadav, and M. Yadav, "Exploring Secure V2X Communication Networks for Human-Centric Security and Privacy in Smart Cities," *IEEE Access*, vol. 12, pp. 138 763–138 788, 2024.

[10] S. Han, F.-Y. Wang, G. Luo, L. Li, and F. Qu, "Parallel Surfaces: Service-Oriented V2X Communications for Autonomous Vehicles," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 11, pp. 4536–4545, 2023.

[11] M. Gupta, R. B. Patel, S. Jain, H. Garg, and B. Sharma, "Lightweight Branched Blockchain Security Framework for Internet of Vehicles," *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 11, p. e4520, 2023.

[12] B. Ji, X. Zhang, S. Mumtaz, C. Han, C. Li, H. Wen, and D. Wang, "Survey on the Internet of Vehicles: Network Architectures and Applications," *IEEE Communications Standards Magazine*, vol. 4, no. 1, pp. 34–41, 2020.

[13] C. Zhu, X. Xie, C. Ding, Y. Zhou, X. Gao, and J. An, "Terahertz Empowered Vehicular Fog Computing: Opportunities, Feasibility, and Enhancements," *IEEE Wireless Communications*, vol. 31, no. 4, pp. 315–323, 2024.

[14] J. Guo, M. Bilal, Y. Qiu, C. Qian, X. Xu, and K.-K. Raymond Choo, "Survey on Digital Twins for Internet of Vehicles: Fundamentals, Challenges, and Opportunities," *Digital Communications and Networks*, vol. 10, no. 2, pp. 237–247, 2024.

[15] H. Taslimasa, S. Dadkhah, E. C. P. Neto, P. Xiong, S. Ray, and A. A. Ghorbani, "Security Issues in Internet of Vehicles (IoV): A Comprehensive Survey," *Internet of Things*, vol. 22, p. 100809, 2023.

[16] A. Dutta, L. M. Samaniego Campoverde, M. Tropea, and F. De Rango, "A Comprehensive Review of Recent Developments in VANET for Traffic, Safety & Remote Monitoring Applications," *Journal of Network and Systems Management*, vol. 32, no. 4, p. 73, 2024.

[17] P. Rani and R. Sharma, "Intelligent Transportation System for Internet of Vehicles Based Vehicular Networks for Smart Cities," *Computers and Electrical Engineering*, vol. 105, p. 108543, 2023.

[18] G. Sun, Z. Wang, H. Su, H. Yu, B. Lei, and M. Guizani, "Profit Maximization of Independent Task Offloading in MEC-Enabled 5G Internet of Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 11, pp. 16 449–16 461, 2024.

[19] T. Aldhanhani, A. Abraham, W. Hamidouche, and M. Shaaban, "Future Trends in Smart Green IoV: Vehicle-to-Everything in the Era of Electric Vehicles," *IEEE Open Journal of Vehicular Technology*, vol. 5, pp. 278–297, 2024.

[20] X. Lu and W. Song, "Improved Trajectory Data Encryption Method for Internet of Vehicles Using GAN-based Chaotic Logistic Algorithm," *Alexandria Engineering Journal*, vol. 114, pp. 719–727, 2025.

[21] F. Shang and X. Deng, "A Data Sharing Scheme Based on Blockchain for Privacy Protection Certification of Internet of Vehicles," *Vehicular Communications*, vol. 51, p. 100864, 2025.

[22] P. Rani and R. Sharma, "Intelligent Transportation System Performance Analysis of Indoor and Outdoor Internet of Vehicle (IoV) Applications Towards 5G," *Tsinghua Science and Technology*, vol. 29, no. 6, pp. 1785–1795, 2024.

[23] H.-S. Kang, Z.-Y. Chai, Y.-L. Li, H. Huang, and Y.-J. Zhao, "Edge Computing in Internet of Vehicles: A Federated Learning Method Based on Stackelberg Dynamic Game," *Information Sciences*, vol. 689, p. 121452, 2025.

[24] N. Tabassum and C. Reddyy, "Review on QoS and Security Challenges Associated with the Internet of Vehicles in Cloud Computing," *Measurement: Sensors*, vol. 27, p. 100562, 2023.

[25] X. Wang, H. Zhu, Z. Ning, L. Guo, and Y. Zhang, "Blockchain Intelligence for Internet of Vehicles: Challenges and Solutions," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 4, pp. 2325–2355, 2023.

[26] A. K.N. and R. Nagaraj, "Secure Vehicle-to-Vehicle Communication Using Routing Protocol Based on Trust Authentication Secure Sugeno Fuzzy Inference System Scheme," *Recent Patents on Engineering*, vol. 19, no. 1, 2025.

[27] P. Mishra and G. Singh, "Energy Management Systems in Sustainable Smart Cities Based on the Internet of Energy: A Technical Review," *Energies*, vol. 16, no. 19, 2023.

[28] X. Wei, "Enhancing Road Safety in Internet of Vehicles Using Deep Learning Approach for Real-Time Accident Prediction and Prevention," *International Journal of Intelligent Networks*, vol. 5, pp. 212–223, 2024.

[29] Q. Xie, Z. Ding, Q. Xie, X. Tan, D. He, and W. Tang, "Blockchain-Based Traffic Accident Handling Protocol Without Third Party for VANETs," *IEEE Internet of Things Journal*, vol. 11, no. 19, pp. 31 068–31 079, 2024.

[30] P. S. Marwein, S. Nath Sur, X.-Z. Gao, and D. Kandar, "Recent Survey on Internet of Vehicles: Architecture, Applications, Challenges, and Its Solutions," *Journal of Testing and Evaluation*, vol. 52, no. 1, pp. 731–753, 01 2024.

[31] A. Hbaieb, S. Ayed, and L. Chaari, "A Survey of Trust Management in the Internet of Vehicles," *Computer Networks*, vol. 203, p. 108558, 2022.

[32] S. A. Siddiqui, A. Mahmood, Q. Z. Sheng, H. Suzuki, and W. Ni, "A Survey of Trust Management in the Internet of Vehicles," *Electronics*, vol. 10, no. 18, p. 2223, 2021.

[33] H. Che, Y. Duan, C. Li, and L. Yu, "On Trust Management in Vehicular Ad-Hoc Networks: A Comprehensive Review," *Frontiers in the Internet of Things*, vol. 1, p. 995233, 2022.

[34] R. Hussain, J. Lee, and S. Zeadally, "Trust in VANET: A Survey of Current Solutions and Future Research Opportunities," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 5, pp. 2553–2571, 2021.

[35] A. Rehman, M. F. Hassan, K. H. Yew, I. Paputungan, and D. C. Tran, "State-of-the-Art IoV Trust Management: A Meta-Synthesis Systematic Literature Review (SLR)," *PeerJ Computer Science*, vol. 6, p. e334, 2020.

[36] H. Amari, Z. A. E. Houda, L. Khoukhi, and L. H. Belguith, "Trust Management in Vehicular Ad-Hoc Networks: Extensive Survey," *IEEE Access*, vol. 11, pp. 47 659–47 680, 2023.

[37] M. Razafimanjato, M. M. Saad, and D. Kim, "Blockchain-Based Trust Management Systems in the Internet of Vehicles: A Comprehensive Survey," *ICT Express*, 2025.

[38] E. Alalwany and I. Mahgoub, "Security and Trust Management in the Internet of Vehicles (IoV): Challenges and Machine Learning Solutions," *Sensors*, vol. 24, no. 2, 2024.

[39] M. AlMarshoud, M. Sabir Kiraz, and A. H. Al-Bayatti, "Security, Privacy, and Decentralized Trust Management in VANETs: A Review of Current Research and Future Directions," *ACM Computing Surveys*, vol. 56, no. 10, 2024.

[40] Q. Xu, L. Zhang, and Y. Liu, "Enhancing Trust Management System for Connected and Autonomous Vehicles Using Machine Learning Methods: A Survey," *arXiv preprint*, 2025, arXiv:2505.07882.

[41] E. Khezri, H. Hassanzadeh, R. O. Yahya, and M. Mir, "Security Challenges in Internet of Vehicles (IoV) for ITS: A Survey," *Tsinghua Science and Technology*, 2024.

[42] A. O. Philip, S. M U, R. Paul, and R. Saravanaguru, "Towards Intelligent Trust-Based Incident and Evidence Management Models for Internet of Vehicles: A Survey," *Computers and Electrical Engineering*, vol. 117, p. 109284, 2024.

[43] S. A. Siddiqui, A. Mahmood, Q. Z. Sheng, H. Suzuki, and W. Ni, "Trust in Vehicles: Toward Context-Aware Trust and Attack Resistance for the Internet of Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 9, pp. 9546–9560, 2023.

[44] W. Yong-hao, "A Trust Management Model for Internet of Vehicles," in *Proceedings of the 2020 4^{th} International Conference on Cryp-*

tography, Security and Privacy, ser. ICCSP 2020. New York, NY, USA: Association for Computing Machinery, 2020, p. 136–140.

[45] A. Mahmood, W. E. Zhang, Q. Z. Sheng, S. A. Siddiqui, and A. Aljubairy, *Trust Management for Software-Defined Heterogeneous Vehicular Ad Hoc Networks*. Cham: Springer International Publishing, 2019, pp. 203–226.

[46] S. Sagar, A. Mahmood, Q. Z. Sheng, M. Zaib, and F. Sufyan, "Can We Quantify Trust? Towards a Trust-Based Resilient SIoT Network," *Computing*, vol. 106, no. 2, pp. 557–577, Feb 2024.

[47] J. Chen, X. Wang, and X. Shen, "RTE: Rapid and Reliable Trust Evaluation for Collaborator Selection and Time-Sensitive Task Handling in Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 11, no. 7, pp. 12 278–12 291, 2024.

[48] B. Su and L. Tong, "Transmission Protocol of Emergency Messages in VANET Based on the Trust Level of Nodes," *IEEE Access*, vol. 11, pp. 68 243–68 256, 2023.

[49] B. Li, X. Song, T. Dai, W. Wu, D. Zhu, X. Zhai, H. Wen, Q. Lin, H. Chen, and K. Cai, "Trust Management Strategy for Digital Twins in Vehicular Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 10, pp. 3279–3292, 2023.

[50] S. Sun, X. Fan, and Y. Xiao, "Trust Model Based on Recommendation Filtering in Internet of Vehicles," in *2023 2^{nd} International Conference on Computing, Communication, Perception and Quantum Technology (CCPQT)*, 2023, pp. 364–369.

[51] S. Sagar, A. Mahmood, K. Wang, Q. Z. Sheng, J. K. Pabani, and W. E. Zhang, "Trust–SIoT: Toward Trustworthy Object Classification in the Social Internet of Things," *IEEE Transactions on Network and Service Management*, vol. 20, no. 2, pp. 1210–1223, 2023.

[52] J. Qi, N. Zheng, M. Xu, P. Chen, and W. Li, "A Hybrid-Trust-Based Emergency Message Dissemination Model for Vehicular Ad Hoc Networks," *Journal of Information Security and Applications*, vol. 81, p. 103699, 2024.

[53] T. Cao, J. Yi, X. Wang, H. Xiao, and C. Xu, "Interaction Trust-Driven Data Distribution for Vehicle Social Networks: A Matching Theory Approach," *IEEE Transactions on Computational Social Systems*, vol. 11, no. 3, pp. 4071–4086, 2024.

[54] Y. Wang, Y. Cao, C. Lv, Y. Zhang, B. Zhou, and S. Wan, "PDTM: A Provenance-Driven Dynamic Trust Management Model for IoVs," *Sustainable Energy Technologies and Assessments*, vol. 60, p. 103496, 2023.

[55] F. Huang, Q. Li, and J. Zhao, "Trust Management Model of VANETs Based on Machine Learning and Active Detection Technology," in *2022 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, 2022, pp. 412–416.

[56] S. Shokrollahi and M. Dehghan, "TGRV: A Trust-Based Geographic Routing Protocol for VANETs," *Ad Hoc Networks*, vol. 140, p. 103062, 2023.

[57] A. Mahmood, Q. Z. Sheng, W. E. Zhang, Y. Wang, and S. Sagar, "Toward a Distributed Trust Management System for Misbehavior Detection in the Internet of Vehicles," *ACM Transactions on Cyber-Physical Systems*, vol. 7, no. 3, Jul. 2023.

[58] A. Mahmood, S. A. Siddiqui, Q. Z. Sheng, W. E. Zhang, H. Suzuki, and W. Ni, "Trust on Wheels: Towards Secure and Resource Efficient IoV Networks," *Computing*, vol. 104, no. 6, pp. 1337–1358, Jun 2022.

[59] D. Yin and B. Gong, "Auto-Adaptive Trust Measurement Model Based on Multidimensional Decision-Making Attributes for Internet of Vehicles," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 3537771, 2022.

[60] Y. Zhang, Y. Song, Y. Wang, Y. Cao, X. Ren, and F. Yan, "TECS: A Trust Model for VANETs Using Eigenvector Centrality and Social Metrics," in *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2022, pp. 36–43.

[61] H. Li, Q. Shan, J. Zhan, and D. Wang, "A Trust Evaluation Method Based on Environmental Assessment in the Perception Layer of Internet of Vehicles," in *2021 13^{th} International Conference on Communication Software and Networks (ICCSN)*, 2021, pp. 49–54.

[62] B. Akwirry, N. Bessis, H. Malik, and S. McHale, "A Multi-Tier Trust-Based Security Mechanism for Vehicular Ad-Hoc Network Communications," *Sensors*, vol. 22, no. 21, 2022.

[63] S. A. Siddiqui, A. Mahmood, Q. Z. Sheng, H. Suzuki, and W. Ni, "A Time-Aware Trust Management Heuristic for the Internet of Vehicles," in *2021 IEEE 20^{th} International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2021, pp. 1–8.

[64] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, and F. Hussain, "MARINE: Man-in-the-Middle Attack Resistant Trust Model in Connected Vehicles," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3310–3322, 2020.

[65] D. Wang, X. Chen, H. Wu, R. Yu, and Y. Zhao, "A Blockchain-Based Vehicle-Trust Management Framework Under a Crowdsourcing Environment," in *2020 IEEE 19^{th} International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2020, pp. 1950–1955.

[66] Y. Yu, Z. Jia, W. Tao, B. Xue, and C. Lee, "An Efficient Trust Evaluation Scheme for Node Behavior Detection in the Internet of Things," *Wireless Personal Communications*, vol. 93, no. 2, pp. 571–587, Mar 2017.

[67] A. Jain, A. Kumar, Mahadev, J. K. Chaudhary, and S. Singh, "Trust-Based Reliability Scheme for Secure Data Sharing With Internet of Vehicles Networks," *Internet Technology Letters*, vol. 8, no. 2, p. e70000, 2025.

[68] C. Cheong, Y. Song, Y. Cao, Y. Zhang, B. Cai, and Q. Ni, "Multidimensional Trust Evidence Fusion and Path-Backtracking Mechanism for Trust Management in VANETs," *IEEE Internet of Things Journal*, vol. 11, no. 10, pp. 18 619–18 634, 2024.

[69] Y. Wang, A. Mahmood, M. F. M. Sabri, H. Zen, and L. C. Kho, "MESMERIC: Machine Learning-Based Trust Management Mechanism for the Internet of Vehicles," *Sensors*, vol. 24, no. 3, 2024.

[70] H. Han, M. Zhang, Z. Xu, X. Dong, and Z. Wang, "Decentralized Trust Management and Incentive Mechanisms for Secure Information Sharing in VANET," *IEEE Access*, vol. 12, pp. 124 414–124 427, 2024.

[71] N. Shamaeian and D. Pesch, "Evidence Theory-Based Trust Management for the Social Internet of Vehicles," in *2024 IEEE 49^{th} Conference on Local Computer Networks (LCN)*, 2024, pp. 1–7.

[72] S. A. Siddiqui, A. Mahmood, Q. Z. Sheng, H. Suzuki, and W. Ni, "Towards a Machine Learning Driven Trust Management Heuristic for the Internet of Vehicles," *Sensors*, vol. 23, no. 4, 2023.

[73] S. A. Siddiqui, A. Mahmood, W. E. Zhang, and Q. Z. Sheng, "Machine Learning Based Trust Model for Misbehaviour Detection in Internet-of-Vehicles," in *Neural Information Processing*, T. Gedeon, K. W. Wong, and M. Lee, Eds. Cham: Springer International Publishing, 2019, pp. 512–520.

[74] D. Wang, Y. Yi, S. Yan, N. Wan, and J. Zhao, "A Node Trust Evaluation Method of Vehicle-Road-Cloud Collaborative System Based on Federated Learning," *Ad Hoc Networks*, vol. 138, p. 103013, 2023.

[75] M. Mao, T. Hu, and W. Zhao, "Reliable Task Offloading Mechanism Based on Trusted Roadside Unit Service for Internet of Vehicles," *Ad Hoc Networks*, vol. 139, p. 103045, 2023.

[76] J. Chen and X. Wang, "TCNS: An Efficient Trusted Cooperative Node Selection Model for Internet of Vehicles," in *2021 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, 2021, pp. 1–6.

[77] I. A. Rai, R. A. Shaikh, and S. R. Hassan, "A Hybrid Dual-Mode Trust Management Scheme for Vehicular Networks," *International Journal of Distributed Sensor Networks*, vol. 16, no. 7, p. 1550147720939372, 2020.

[78] S. Sagar, A. Mahmood, M. Sheng, M. Zaib, and W. Zhang, "Towards a Machine Learning-driven Trust Evaluation Model for Social Internet of Things: A Time-aware Approach," in *MobiQuitous 2020 - 17^{th} EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, ser. MobiQuitous '20. New York, NY, USA: Association for Computing Machinery, 2021, p. 283–290.

[79] S. Sagar, A. Mahmood, Q. Z. Sheng, and W. E. Zhang, "Trust Computational Heuristic for Social Internet of Things: A Machine Learning-based Approach," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[80] I. Alam, M. Manjul, V. Pathak, V. Mala, A. Mangal, H. K. Thakur, and D. K. Sharma, "Efficient and Secure Graph-Based Trust-Enabled Routing in Vehicular Ad-Hoc Networks," *Mobile Networks and Applications*, pp. 1–21, 2024.

[81] Y. Song, Y. Cao, C. Cheong, D. He, K.-K. Raymond Choo, and J. Wang, "CAT: A Consensus-Adaptive Trust Management Based on the Group Decision Making in IoVs," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 7730–7743, 2024.

[82] Y. Wang, Y. Zhang, Y. Song, Y. Cao, L. Zhang, and X. Ren, "Appeal-Based Distributed Trust Management Model in VANETs Concerning Untrustworthy RSUs," in *2023 IEEE Wireless Communications and Networking Conference (WCNC)*, 2023, pp. 1–6.

[83] C. Cheong, Y. Song, Y. Zhang, Y. Cao, C. Leow, and X. Wang, "A Path-Backtracking-Based Trust Management Scheme for VANETs," 06 2024, pp. 1–6.

[84] I. Memon, R. A. Shaikh, and H. Shaikh, "Retraction Note: Dynamic Pseudonyms Trust-based Model to Protect Attack Scenario for Internet of Vehicle Ad-Hoc Networks," *Multimedia Tools and Applications*, vol. 83, no. 3, p. 13395, 2024.

[85] M. H. Junejo, A. A.-H. B. A. Rahman, R. A. Shaikh, K. M. Yusof, and S. Sadiah, "Trust Model for Reliable Grouping-Based Communications in Vehicular Ad-Hoc Networks," *IEEE Access*, vol. 11, pp. 124 584–124 596, 2023.

[86] J. Qi, N. Zheng, M. Xu, X. Wang, and Y. Chen, "A Multi-Dimensional Trust Model for Misbehavior Detection in Vehicular Ad Hoc Networks," *Journal of Information Security and Applications*, vol. 76, p. 103528, 2023.

[87] S. Zhang, R. He, Y. Xiao, and Y. Liu, "A Three-Factor Based Trust Model for Anonymous Bacon Message in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 9, pp. 11 304–11 317, 2023.

[88] H. El-Sayed, H. Alexander, P. Kulkarni, M. A. Khan, R. M. Noor, and Z. Trabelsi, "A Novel Multifaceted Trust Management Framework for Vehicular Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 11, pp. 20 084–20 097, 2022.

[89] R. Magdich, H. Jemal, and M. B. Ayed, "A Resilient Trust Management Framework Towards Trust Related Attacks in the Social Internet of Things," *Computer Communications*, vol. 191, pp. 92–107, 2022.

[90] G. Kaur and D. Kakkar, "Hybrid Optimization Enabled Trust-Based Secure Routing with Deep Learning-based Attack Detection in VANET," *Ad Hoc Networks*, vol. 136, p. 102961, 2022.

[91] A. K. Fabi and S. M. Thampi, "A Psychology-Inspired Trust Model for Emergency Message Transmission on the Internet of Vehicles (IoV)," *International Journal of Computers and Applications*, vol. 44, no. 5, pp. 480–490, 2022.

[92] F. Ahmad, F. Kurugollu, C. A. Kerrache, S. Sezer, and L. Liu, "NOTRINO: A NOvel Hybrid TRust Management Scheme for INternet-of-Vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 9244–9257, 2021.

[93] M. Mao, P. Yi, T. Hu, Z. Zhang, X. Lu, and J. Lei, "Hierarchical Hybrid Trust Management Scheme in SDN-Enabled VANETs," *Mobile Information Systems*, vol. 2021, no. 1, p. 7611619, 2021.

[94] H. Xia, F. Xiao, S.-s. Zhang, C.-q. Hu, and X.-z. Cheng, "Trustworthiness Inference Framework in the Social Internet of Things: A Context-Aware Approach," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, 2019, pp. 838–846.

[95] J. Zhang, K. Zheng, D. Zhang, and B. Yan, "AATMS: An Anti-Attack Trust Management Scheme in VANET," *IEEE Access*, vol. 8, pp. 21 077–21 090, 2020.

[96] A. Bhargava and S. Verma, "DUEL: Dempster Uncertainty-Based Enhanced- Trust Level Scheme for VANET," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 15 079–15 090, 2022.

[97] H. Byeon, M. E. Seno, A. K. Srivastava, A. AlGhamdi, I. Keshta, M. Soni, K. D. V. Prasad, D. Abdurakhimova, and M. W. Bhatt, "Trust Management Scheme for Securing Vehicular Ad Hoc Networks Against Malicious Nodes and False Message Anomaly," *Transactions on Emerging Telecommunications Technologies*, vol. 36, no. 4, p. e70110, 2025.

[98] T. Jing, Y. Liu, X. Wang, and Q. Gao, "Joint Trust Management and Sharing Provisioning in IoV-Based Urban Road Network," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 6942120, 2022.

[99] N. Wan and D. Wang, "A Novel Federated Learning Framework Based on Trust Evaluation in Internet of Vehicles," *Adhoc & Sensor Wireless Networks*, vol. 58, no. 3/4, p. 321, 2024.

[100] A. Haddaji, S. Ayed, and L. Chaari, "Federated Learning with Blockchain Approach for Trust Management in IoV," in *Advanced Information Networking and Applications*, L. Barolli, F. Hussain, and T. Enokido, Eds. Cham: Springer International Publishing, 2022, pp. 411–423.

[101] H. Xia, S.-s. Zhang, Y. Li, Z.-k. Pan, X. Peng, and X.-z. Cheng, "An Attack-Resistant Trust Inference Model for Securing Routing in Vehicular Ad Hoc Networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 7108–7120, 2019.

[102] A. Raza and E. Badidi, "A Trust-Based Client Selection Framework for Federated Learning in the Internet of Vehicles," in *2025 International Wireless Communications and Mobile Computing (IWCMC)*, 2025, pp. 1180–1185.

[103] Y. Ren, Z. Li, Y. Yang, H. Yu, Y. Zhao, and X. Wei, "A Dynamic Trust Evaluation Scheme Based on Cross-Domain Trust Inheritance for VANETs," *Ad Hoc Networks*, vol. 175, p. 103872, 2025.

[104] M. Choukhairi, Y. Fakhri, and M. Amnai, "TTIDS : A Time-Driven Trust Based Intrusion Detection System for IoT Networks," in *2022 9^{th} International Conference on Wireless Networks and Mobile Communications (WINCOM)*, 2022, pp. 1–8.

[105] D. Jegatheesan and C. Arumugam, "SIoV-FTFSA-CAOA: A Fuzzy Trust-Based Approach for Enhancing Security and Energy Efficiency in Social Internet of Vehicles," *Wireless Networks*, vol. 30, no. 4, pp. 2061–2080, 2024.

[106] X. Liu, L. Liang, Z. Tan, J. Chen, and G. Li, "An Adaptive Trust Threshold Based on Q-Learning for Detecting Intelligent Attacks in Vehicular Ad-Hoc Networks," *Ad Hoc Networks*, vol. 175, p. 103865, 2025.

[107] C. A. Kerrache, N. Lagraa, R. Hussain, S. H. Ahmed, A. Benslimane, C. T. Calafate, J.-C. Cano, and A. M. Vegni, "TACASHI: Trust-Aware Communication Architecture for Social Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 5870–5877, 2019.

[108] J.-M. Chen, T.-T. Li, and J. Panneerselvam, "TMEC: A Trust Management Based on Evidence Combination on Attack-Resistant and Collaborative Internet of Vehicles," *IEEE Access*, vol. 7, pp. 148 913–148 922, 2019.

[109] 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. 28 643–28 660, 2018.

[110] D. S. B. Naik and V. Dondeti, "Trust-Based Secure Federated Learning Framework to Mitigate Internal Sttacks for Intelligent Vehicular Networks," *Peer-to-Peer Networking and Applications*, vol. 18, no. 2, p. 10, 01 2025.

[111] Y. Zhang, C. Jiang, and P. Zhang, "Security-Aware Resource Allocation Scheme Based on DRL in Cloud–Edge–Terminal Cooperative Vehicular Network," *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 95–104, 2024.

[112] X. Li, X. Yin, and J. Ning, "Trustworthy Announcement Dissemination Scheme With Blockchain-Assisted Vehicular Cloud," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 1786–1800, 2023.

[113] M. Azizi and S. Shokrollahi, "RTRV: An RSU-Assisted Trust-Based Routing Protocol for VANETs," *Ad Hoc Networks*, vol. 154, p. 103387, 2024.

[114] G. Du, Y. Cao, J. Li, Y. Zhuang, X. Chen, Y. Li, and J. Chen, "A Blockchain-Based Trust-Value Management Approach for Secure Information Sharing in Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 333–344, 2024.

[115] R. Su, Y. Jin, and Y.-Q. Song, "Assessing Trustworthiness of V2X Messages: a Cooperative Trust Model Against CAM- and CPM-Based Ghost Vehicles in IoV," in *Proceedings of the 10^{th} International Conference on Vehicle Technology and Intelligent Transport Systems*, May 2024, pp. 276–283.

[116] W. Mo, W. Liu, G. Huang, N. N. Xiong, A. Liu, and S. Zhang, "A Cloud-Assisted Reliable Trust Computing Scheme for Data Collection in Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 7, pp. 4969–4980, 2022.

[117] S. Shokrollahi and M. Dehghan, "CTVAN: A Cooperation-Based RSU-Assisted Trust Management Model for Reliable Communication in VANETs," *Cluster Computing*, vol. 28, no. 4, p. 227, Feb. 2025.

[118] A. Alnasser, H. Sun, and J. Jiang, "Recommendation-Based Trust Model for Vehicle-to-Everything (V2X)," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 440–450, 2020.

[119] C. Zhang, L. Zhu, C. Xu, K. Sharif, K. Ding, X. Liu, X. Du, and M. Guizani, "TPPR: A Trust-Based and Privacy-Preserving Platoon Recommendation Scheme in VANET," *IEEE Transactions on Services Computing*, vol. 15, no. 2, pp. 806–818, 2022.

[120] Y. Wang, A. Mahmood, M. F. M. Sabri, and H. Zen, "Towards Distinguishing Trust Based Attacks in an IoV Network," *Journal of King Saud University - Computer and Information Sciences*, vol. 37, no. 4, p. 39, 2025.

[121] M. A. Khan and W. Zhang, "Security and Trust Management in the Internet of Vehicles: A Systematic Literature Review," *Sensors*, vol. 24, no. 2, 2024.

[122] Z. Shen, Y. Wang, H. Wang, P. Liu, K. Liu, and J. Zhang, "Trust Mechanism Privacy Protection Scheme Combining Blockchain and Multi-Party Evaluation," *IEEE Transactions on Intelligent Vehicles*, vol. 9, no. 2, pp. 3885–3894, 2024.

[123] F. Honarmand and A. Keshavarz-Haddad, "T-AODV: A Trust-Based Routing Against Black-Hole Attacks in VANETs," *Peer-to-Peer Networking and Applications*, vol. 17, no. 3, pp. 1309–1321, 2024.

[124] I.-R. Chen, F. Bao, and J. Guo, "Trust-Based Service Management for Social Internet of Things Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 6, pp. 684–696, 2016.

[125] D. Suo and S. E. Sarma, "Real-time Trust-Building Schemes for Mitigating Malicious Behaviors in Connected and Automated Vehicles," in *2019 IEEE Intelligent Transportation Systems Conference (ITSC)*, 2019, pp. 1142–1149.

[126] I.-R. Chen, J. Guo, and F. Bao, "Trust Management for SOA-Based IoT and Its Application to Service Composition," *IEEE Transactions on Services Computing*, vol. 9, no. 3, pp. 482–495, 2016.

[127] Z. Chen, R. Ling, C.-M. Huang, and X. Zhu, "A Scheme of Access Service Recommendation for the Social Internet of Things," *International Journal of Communication Systems*, vol. 29, pp. 694–706, 2016.

[128] Y. Lu, G. Zhang, X. Wang, and X. Li, "Trust-Based Reliability Enhancements Provisioning With Resilience Under Information Asymmetry in IoV System," *IEEE Access*, vol. 11, pp. 82 362–82 376, 2023.

[129] H. Gao, C. Liu, Y. Yin, Y. Xu, and Y. Li, "A Hybrid Approach to Trust Node Assessment and Management for VANETs Cooperative Data Communication: Historical Interaction Perspective," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 16 504–16 513, 2022.

[130] S. Wei, X. Li, H. Ji, and H. Zhang, "Anti-attack Trust Evaluation Algorithm Based on Bayesian Inference in VANET," in *Communications and Networking*, F. Gao, J. Wu, Y. Li, H. Gao, and S. Wang, Eds. Cham: Springer Nature Switzerland, 2024, pp. 142–161.

[131] I. Mirzadeh, M. Sayad Haghighi, and A. Jolfaei, "Filtering Malicious Messages by Trust-Aware Cognitive Routing in Vehicular Ad Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 1, pp. 1134–1143, 2023.

[132] W. Fang, W. Zhang, Y. Liu, W. Yang, and Z. Gao, "BTDS: Bayesian-Based Trust Decision Scheme for Intelligent Connected Vehicles in VANETs," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 12, p. e3879, 2020.

[133] Y. Xiao and Y. Liu, "BayesTrust and VehicleRank: Constructing an Implicit Web of Trust in VANET," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2850–2864, 2019.

[134] Y. Zhao, W. Liu, B. Li, X. Zhou, Z. Ning, T. Qiu, and M. Atiquzzaman, "Entity and Sociality Trust-Aware Model for Content Distribution in Social Internet of Vehicles," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 12, pp. 12 511–12 522, 2022.

[135] G. Rjoub, J. Bentahar, and O. A. Wahab, "Explainable Trust-Aware Selection of Autonomous Vehicles Using LIME for One-Shot Federated Learning," in *2023 International Wireless Communications and Mobile Computing (IWCMC)*, 2023, pp. 524–529.

[136] P.-C. Zhao, Y.-H. Huang, D.-X. Zhang, L. Xing, H.-H. Wu, and J.-P. Gao, "CCP-Federated Deep Learning Based on User Trust Chain in Social IoV," *Wireless Networks*, vol. 29, no. 4, pp. 1555–1566, 2023.

[137] A. Fabi and S. M. Thampi, "A Trust Management Framework Using Forest Fire Model to Propagate Emergency Messages in the Internet of Vehicles (IoV)," *Vehicular Communications*, vol. 33, p. 100404, 2022.

[138] S. Yadav, K. Singh, A. K. Yadav, M. Shariq, S. A. Chaudhry, A. K. Das, and M. Manjul, "Efficient and Reliable Information Sharing for Internet of Vehicles using Trust and Blockchain," *IEEE Transactions on Vehicular Technology*, pp. 1–13, 2025.

[139] L. Nagaraju and I. Saini, "Trust-Centric Detection of Roadside Unit Misbehaviour in VANETs," in *2025 International Wireless Communications and Mobile Computing (IWCMC)*, 2025, pp. 361–366.

[140] W. Li, H. Song, and F. Zeng, "Policy-Based Secure and Trustworthy Sensing for Internet of Things in Smart Cities," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 716–723, 2018.

[141] S. Aalibagi, H. Mahyar, A. Movaghar, and H. E. Stanley, "A Matrix Factorization Model for Hellinger-Based Trust Management in Social Internet of Things," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 4, pp. 2274–2285, 2022.

[142] C. Marche and M. Nitti, "Trust-Related Attacks and Their Detection: A Trust Management Model for the Social IoT," *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 3297–3308, 2021.

[143] I. García-Magariño, S. Sendra, R. Lacuesta, and J. Lloret, "Security in Vehicles with IoT by Prioritization Rules, Vehicle Certificates, and Trust Management," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 5927–5934, 2019.

[144] M. M. Alshahrani, "A Verifiable Discrete Trust Model (VDTM) Using Congruent Federated Learning (CFL) for Social Internet of Vehicles," *IEEE Open Journal of Vehicular Technology*, vol. 5, pp. 1441–1456, 2024.

[145] H. El-Sayed, H. A. Ignatious, P. Kulkarni, and S. Bouktif, "Machine Learning Based Trust Management Framework for Vehicular Networks," *Vehicular Communications*, vol. 25, p. 100256, 2020.

[146] I. U. Din, K. H. Khan, A. Almogren, and M. Guizani, "Machine Learning for Trust in Internet of Vehicles and Privacy in Distributed Edge Networks," *IEEE Internet of Things Journal*, pp. 1–1, 2025.

[147] L. Abualigah, D. Yousri, M. Abd Elaziz, A. A. Ewees, M. A. Al-qaness, and A. H. Gandomi, "Aquila Optimizer: A Novel Meta-Heuristic Optimization Algorithm," *Computers & Industrial Engineering*, vol. 157, p. 107250, 2021.

[148] 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 of Things Journal*, vol. 7, no. 7, pp. 6647–6662, 2020.

[149] J. Guo, A. Liu, K. Ota, M. Dong, X. Deng, and N. N. Xiong, "ITCN: An Intelligent Trust Collaboration Network System in IoT," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 1, pp. 203–218, 2022.

[150] D. Zhang, F. R. Yu, R. Yang, and L. Zhu, "Software-Defined Vehicular Networks With Trust Management: A Deep Reinforcement Learning Approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 2, pp. 1400–1414, 2022.

[151] G. F. Riley and T. R. Henderson, "The NS-3 Network Simulator," in *Modeling and Tools for Network Simulation*. Springer, 2010, pp. 15–34.

[152] M. Najafi, L. Khoukhi, and M. Lemercier, "Decentralized Prediction and Reputation Approach in Vehicular Networks," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 7, p. e4456, 2022.

[153] U. Wilensky, "NetLogo," 1999, online; Accessed 10-March-2021.

[154] Y. Wang, A. Mahmood, M. F. M. Sabri, and H. Zen, "TM–IoV: A First-of-Its-Kind Multilabeled Trust Parameter Dataset for Evaluating Trust in the Internet of Vehicles," *Data*, vol. 9, no. 9, 2024.

[155] S. Sagar, A. Mahmood, Q. Z. Sheng, W. E. Zhang, Y. Zhang, and J. K. Pabani, "Understanding the Trustworthiness Management in the Social Internet of Things: A Survey," *Computer Networks*, vol. 251, p. 110611, 2024.

[156] B. Farahbakhsh, A. Fanian, and M. H. Manshaei, "TGSM: Towards Trustworthy Group-based Service Management for Social IoT," *Internet of Things*, vol. 13, p. 100312, 2021.

[157] B. Huber and F. Kandah, "DECAY: Dynamic Evaluation and Component Analysis for Enhancing Trust Management," in *2024 IEEE International Conference on Consumer Electronics (ICCE)*, 2024, pp. 1–6.

[158] A. Mahmood, "Trust on Wheels – Towards Trust Management in the Internet of Vehicles," Ph.D. dissertation, Macquarie University, Sydney, New South Wales, Australia, 2021.

[159] A. Drobot, T. Zhang, M. L. Buonarosa, F. Kargl, S. Schwinke, and B. Sikdar, "The Internet of Vehicles (IoV) – Security, Privacy, Trust, and Reputation Management for Connected Vehicles," *IEEE Internet of Things Magazine*, vol. 6, no. 2, pp. 6–16, 2023.

[160] Z. Shu, X. Sun, and H. Cheng, "When llm meets hypergraph: A sociological analysis on personality via online social networks," in

Proceedings of the 33^{rd} ACM International Conference on Information and Knowledge Management, ser. CIKM '24. New York, NY, USA: Association for Computing Machinery, 2024, p. 2087–2096.

[161] S. Huang, H. Li, Y. Gu, X. Hu, Q. Li, and G. Xu, "HyperG: Hypergraph-Enhanced LLMs for Structured Knowledge," in *Proceedings of the 48^{th} International ACM SIGIR Conference on Research and Development in Information Retrieval*, ser. SIGIR '25. New York, NY, USA: Association for Computing Machinery, 2025, p. 1218–1228.

[162] S. A. Md Mahmudul Islam, "Existence of Trust-Field in Vehicular Ad Hoc Networks: Empirical Evidence," *arXiv preprint*, 2024, arXiv:2407.13923.

[163] P. G. Muhammet Anil Yagiz, "LENS-XAI: Redefining Lightweight and Explainable Network Security through Knowledge Distillation and Variational Autoencoders for Scalable Intrusion Detection in Cybersecurity," *arXiv preprint*, 2025, arXiv:2501.00790.

YINGXUN WANG is associated with the Faculty of Computer and Information Engineering, Qilu Institute of Technology, Jinan, Shandong, People's Republic of China as an Associate Professor. Her research interests encompass the Internet of Things (primarily, the Internet of Vehicles), trust management, and heterogeneous wireless networking. She has, over the years, published extensively in leading international journals, including but not limited to, IEEE Transactions on Automation Science and Engineering and IEEE Communications Letters. Yingxun has additionally secured competitive funding of RMB 2.5 million.

ADNAN MAHMOOD (PhD, Member – IEEE) is a Senior Lecturer with the School of Computing, Macquarie University, Sydney, Australia. Adnan's research interests include the Internet of Things, the Internet of Vehicles, Trust Management, Software Defined Networks, and the Next Generation Heterogeneous Wireless Networks, amongst other topics. His extensive publication list includes refereed book chapters; journal articles published in prestigious venues, including but not limited to, the ACM Computing Surveys, IEEE Transactions on Services Computing, IEEE Transactions on Knowledge and Data Engineering, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Network and Service Management, ACM Transactions on Sensor Networks, ACM Transactions on Cyber-Physical Systems, Scientific Reports (Nature Portfolio), and Advanced Intelligent Systems; and papers in highly reputed international conferences, including but not limited to, the International Joint Conference on Artificial Intelligence, AAAI Conference on Artificial Intelligence, International Conference on Web Services, and International Conference on Service-Oriented Computing.

MOHAMAD FAIZRIZWAN MOHD SABRI (PhD) is a Senior Lecturer with the Faculty of Engineering, Universiti Malaysia Sarawak, Malaysia. His research interest lies in control systems, electrified mobility, energy management, and energy efficiency. Over the years, he has been involved in several high impact research projects pertinent to hybrid electric vehicle control, smart grid communication, neural network-based process control, FPGA-based designs, industrial IoT systems, spatial AI green energy management, and trust management in IoV networks. Faizrizwan holds a BEng. Electric and Electronics from Nagasaki University, Japan, an MEng. in Electronics from La Trobe University, Australia, and a PhD in Electrical Engineering from Universiti Teknologi Malaysia, Malaysia.

HUSHAIRI ZEN (PhD, Senior Member – IEEE) is a Professor and Dean of the Faculty of Engineering and Technology, i–CATS University College, Sarawak, Malaysia, wherein he provides academic leadership for engineering education, programme development, quality assurance, and industry engagement. Prior to this, he served as the Director, Centre of Competency for IoT, Universiti Malaysia Sarawak, Malaysia as part of which he led the design and implementation of state-of-the-art IoT solutions. Professor Zen's scholarly and professional interests span IoT architecture, sensor networks, data driven monitoring, and AI-enabled engineering applications with an ongoing emphasis on impactful, industry relevant research and regional collaborations in Sarawak, Malaysia.