Journal of King Saud University Computer and Information Sciences https://doi.org/10.1007/s44443-026-00554-4

Article in Press

Trust management in the internet of vehicles: a survey of learning-based mechanisms

Received: 27 Oct 2025

Accepted: 03 Feb 2026

Published online: 14 February 2026

Cite this article as: Voon, S., Mahmood, A., Kho, L. *et al.* Trust management in the internet of vehicles: a survey of learning-based mechanisms. *J. King Saud Univ. Comput. Inf. Sci.* (2026). https://doi.org/10.1007/s44443-026-00554-4

Sze Voon, Adnan Mahmood, Lee Kho, Sze Ngu, Annie Joseph, Ade Marzuki & Mohamad Sabri

Trust Management in the Internet of Vehicles: A Survey of Learning-based Mechanisms

Sze Sin Voon[1,2*], Adnan Mahmood[2], Lee Chin Kho[1], Sze Song Ngu[1], Annie Joseph[1], Ade Syaheda Wani Marzuki[1], Mohamad Faizrizwan Mohd Sabri[1]

[1]Faculty of Engineering, Universiti Malaysia Sarawak, Kota Samarahan, 94300, Sarawak, Malaysia.
[2]School of Computing, Macquarie University, Sydney, 2109, NSW, Australia.

*Corresponding author(s). E-mail(s): 24020011@siswa.unimas.my;
Contributing authors: adnan.mahmood@mq.edu.au; lckho@unimas.my; ssngu@unimas.my; jannie@unimas.my; maswani@unimas.my; msmfaizrizwan@unimas.my;

Abstract

The rapid advancements in information and communication technologies have resulted in the emergence of the Internet of Vehicles (IoV) as an indispensable constituent of intelligent transportation systems. This thus enables vehicles to exchange real-time data for improving road safety, traffic efficacy, and users' convenience. However, as vehicles increasingly rely on this interconnected network, robust trust management frameworks are essential to defend against threats that could undermine network integrity and consequently compromise road safety. Trust management in IoV involves evaluating the trustworthiness of vehicles through various parameters, including but not limited to, packet delivery ratio, familiarity, and timeliness, in order to filter out malicious vehicles and ensure reliable data exchange. While conventional methods provide basic security measures, they have limitations in detecting insider threats particularly as IoV environments scale and diversify. Therefore, intelligent learning-based mechanisms, i.e., machine learning, deep learning, and reinforcement learning, have become crucial for addressing these limitations since they are able to continuously adapt to complex dynamic threats within IoV networks. This survey offers a comprehensive review of these learning-based approaches in the context of IoV-based trust management so as to assess their respective efficaciousness in mitigating

trust-related attacks. It also discusses the adaptability, scalability, and robustness of such learning-based frameworks thus highlighting their potential to meet the evolving challenges of IoV ecosystems. This survey concludes with delineating current challenges and proposes future directions for developing more adept and scalable IoV-based trust management mechanisms.

Keywords: Internet of Things, Internet of Vehicles, Intelligent Transportation Systems, Trust Management, Network Security.

1 Introduction

The rapid proliferation of information and communication technologies and the Internet of Things (IoT) has led to an accelerated transformation of the traditional Vehicular Ad hoc Networks (VANETs) into the Internet of Vehicles (IoV). IoV is a state-of-the-art networking paradigm envisaged to meet the services' needs, including but not limited to, traffic management [1], collision avoidance [2], and autonomous driving [3] via Vehicle-to-Everything (V2X) communication [4]. As depicted in Figure 1, V2X communication encompasses Vehicle-to-Vehicle (V2V) communication, Vehicle-to-Infrastructure (V2I) communication, Vehicle-to-Network (V2N) communication, and Vehicle-to-Pedestrian (V2P) communication, thereby enabling comprehensive connectivity in highly dynamic networks [5]. However, the increasing number of V2X links in such dynamic networks also results in potential attack surfaces [6].

Unlike conventional cryptographic techniques that are capable of tackling external attacks, trust can mitigate internal attacks in IoV networks. Trust can be described as a trustor's belief in a trustee's ability in carrying out an action or a set of actions in a manner that meets a trustor's expectations [7]. Trust, accordingly, is indispensable for ensuring safe and efficient communication amongst vehicles in an IoV network. Thus, several dimensions of trust, encompassing but not limited to, security, integrity, reliability, and behavioral consistency should be addressed to realize the future advancement of the IoV [8]. Security measures are intended to protect vehicles and their respective communications from malicious attacks while preserving data availability and confidentiality. Integrity ensures the data of a vehicle is correct and unaltered [9]. The reliability of a vehicle is defined as its ability to perform its specified functions without being attacked [10]. Behavioral consistency is the degree to which a vehicle behaves consistently over time and is crucial to maintain trust amongst network entities [11].

Trustworthy relationships enable vehicles to cater solely to the service requests originating from honest entities within an IoV network, thereby reducing the risk of exposure to malicious actors [12]. Trustworthy communication ensures that vehicles can depend on one another for accurate and timely information, and which is crucial for mitigating accidents and ensuring passenger safety [13]. Moreover, establishing trust aids in identifying and eradicating malicious entities that may attempt to jeopardize the whole IoV network for their own malevolent purposes [14]. IoV networks are

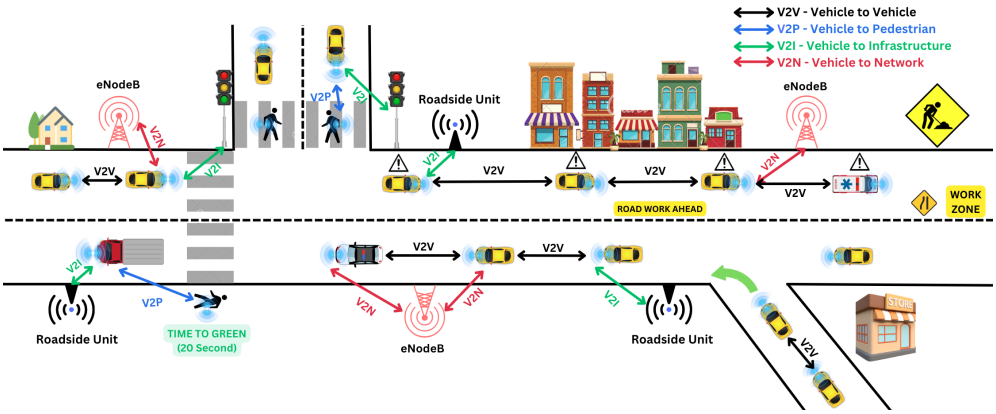

Fig. 1 An overview of V2X communication in an IoV network.

inherently open, dynamic, and rely on sensitive communication, thereby making them vulnerable to a number of malicious attacks which can put the lives of pedestrians, passengers and drivers at risk [15]. Therefore, trust management-related challenges, including but not limited to, trust quantification, trustworthiness threshold, lifetime of the trust score, strategies pertinent to trust decaying factors, incentivization of intelligent selfish vehicles, and the dire need for realistic trust-based IoV testbeds mandate careful deliberation [16, 17].

1.1 State-of-the-Art Surveys on Trust Management in IoV

Over the past decade or so, researchers from both industry and academia have documented surveys pertinent to IoV-based trust management. In [18], trust management mechanisms are segregated vis-à-vis their respective methodologies, i.e., conventional (recommendation-based, infrastructure, etc.) and emerging (machine learning and neural networks). However, it does not delineate the parameters for ascertaining trust scores and discussion around trust-based attacks. Moreover, a comprehensive survey of IoV-based trust management is delineated in [19] with a particular focus on trust properties, metrics and computation. The survey classifies the existing trust-based mechanisms into entity-based, data-based, and hybrid ones. It also addresses security in V2X communication, deliberates on the trust challenges, and explores blockchain, cloud and learning-based mechanisms. Nevertheless, an in-depth discussion of deep learning-based mechanisms is not included. A holistic overview of trust management in VANETs is presented in [20] encompassing trust-based mechanisms and their respective classification (entity-based, data-based, and hybrid schemes), challenges, and future research directions. The trust-based mechanisms are further classified based on various technologies, i.e., cloud, software-defined networking, fog computing, blockchain, and artificial intelligence. Nevertheless, it lacks coverage of trust parameters and trust-based attacks.

Table 1 Comparison of state-of-the-art surveys of IoV-based trust management.

References	Year	Trust Parameters	Trust-based Attacks	Machine Learning	Deep Learning	Reinforcement Learning	Open Research Directions
[18]	2021	×	×	✓	✓	✓	✓
[19]	2022	✓	×	✓	×	✓	✓
[20]	2023	×	✓	✓	×	✓	✓
[21]	2024	×	×	✓	×	×	✓
[22]	2024	✓	×	✓	×	✓	✓
[23]	2025	×	×	✓	✓	✓	✓
This Survey	2025	✓	✓	✓	✓	✓	✓

Remarks: ✓Addressed, ×Not Addressed.

Additionally, [21] reviews the decentralized approaches in VANETs by focusing on trust management to enhance security and privacy. The survey highlights the limitations of conventional cryptographic mechanisms and offers insight into the origin of trust and trust-based services. Trust management mechanisms are categorized into trust-based services, subject trust, and origin of trust, with the concept of trust further classified into two dimensions, i.e., content trust and entity trust. However, this survey discussed general security attacks instead of trust-based attacks and lacks a discussion on parameters employed for trust evaluation and learning-based mechanisms. Finally, [22] presents a comprehensive review of IoV and categorizes trust management mechanisms into conventional (fuzzy logic, cryptography, blockchain, and Bayesian inference-based) and machine learning-based ones. Several IoV-based security attacks and their respective potential solutions are explored with the key intent to enhance security in the highly dynamic IoV environment. Nonetheless, the discussion does not discuss trust-related attacks, e.g., opportunistic service attacks, on-off attacks, ballot stuffing attacks, and trust management mechanisms which incorporates deep learning.

In [23], the authors propose a comprehensive survey of trust management systems for Connected Autonomous Vehicles (CAVs), focusing on overcoming the limitations of traditional trust management systems in dynamic vehicular networks by incorporating machine learning. The survey organizes existing research using a conceptual three-layer framework, i.e., trust data layer, trust computation layer, and trust incentive layer, demonstrating how various machine learning techniques such as supervised, unsupervised, reinforcement learning, graph neural networks, and federated learning can enhance trust modeling. A six-dimensional taxonomy is introduced to assess key aspects of trust management such as effectiveness, flexibility, reliability, efficiency, security, and privacy. The paper further categorizes existing trust management systems studies by application scenarios and highlights open challenges and future directions, serving as a structured and insightful reference for advancing trust and intelligence in CAV systems. The overall comparison of the referred surveys is summarized in Table 1.

1.2 Main Contributions of the Survey

This survey provides a thorough overview of IoV-based trust management, with a primary focus on learning-based mechanisms, i.e., machine learning, deep learning, and

reinforcement learning. It further reviews several trust parameters that are indispensable for evaluating the trustworthiness of any particular vehicle in an IoV network. Moreover, it delineates the trust-based attacks that have the potential to jeopardize the entire IoV network. This survey further addresses the limitations of the conventional IoV-based trust management mechanisms and subsequently highlights the state-of-the-art learning-based trust management mechanisms and comparison in an IoV network context. In essence, this survey aims to advance the understanding of learning-based trust management mechanisms for academic and industrial researchers so that a more secure and reliable IoV network can be envisaged.

1.3 Paper Selection Strategy

The papers opted for this survey are of high quality and have been selected from reputed transactions, e.g., IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Sustainable Computing, IEEE Transactions on Vehicular Technology, ACM Transactions on Cyber Physical Systems, and ACM Transactions on Internet Technology; journals, e.g., Vehicular Communications, IEEE Communications Journal, and IEEE Internet of Things Journal, and proceedings from reputed international conferences. Search strings, i.e., "trust management", "trust" + "Internet of Vehicles", and "IoV" are involved in the process of paper selection from the databases, including but not limited to, Elsevier Science Direct, Springer Nature Link, ACM Digital Library, IEEE Xplore, and Google Scholar. Subsequently, the papers are sort listed in accordance to their respective quality with the key factor being the novelty of the underlined methodology.

1.4 Organization of the Survey

The remaining parts of this survey are organized as follows. Section 2 delineates an overview of IoV-based trust management. Section 3 deliberates the limitations of conventional IoV-based trust management mechanisms. Section 4 presents the learning-based trust management mechanisms in an IoV network context. Finally, Section 5 discusses the open research directions, whereas, Section 6 concludes this particular survey.

2 Overview of Trust Management in IoV

This section delineates the notion of trust, the trust parameters that are employed in a bid to assess vehicles' trustworthiness and the trust-based attacks in an IoV networks context.

2.1 Trust in IoV

Researchers in both academia and industry have employed cryptographic-based mechanisms in order to tackle external attacks in IoV networks over the past decade or so. However, cryptographic-based mechanisms are unable to address internal attacks and are suspectable to internal attacks [24]. Accordingly, trust emerged as one of the promising paradigms for addressing internal attacks in such highly dynamic and

distributed networks. It is pertinent to mention that the notion of trust is defined differently across various disciplines. For example, in the context of social, trust manifests a degree of belief or confidence in a person's ability to carry out social exchanges in an amicable manner [25, 26]. In the context of business and economics, trust acts as a pivotal catalyst for enhancing engagement, communication, and organizational performance, thereby attracting the interest of economists and practitioners alike [27]. Trust, in essence, can be classified as either a quantitative or qualitative attribute of a trustee ascertained by a trustor subjectively or objectively for carrying out a particular task or tasks within a specific context at any given instance of time [6]. Trust, in the context of IoV networks, is quantified via employing context-dependent parameters to ascertain the trustworthiness of a trustee [28, 29].

IoV-based trust mechanisms can be classified into 3 salient types, i.e., data-centric trust models, node-centric trust models, and hybrid trust models. Data-centric trust models assess trust by primarily taking into consideration the received messages (data) instead of evaluating the trustworthiness of the message sender [30–32]. For instance, [33, 34] evaluates the trustworthiness of data based on the intrinsic properties of data and launches mitigation against the underlying attacks when abnormal data is observed. Node-centric trust models identify and subsequently remove malicious nodes (vehicles) by primarily ascertaining their respective reputations [35]. For example, [36] focuses on evaluating the trust of individual vehicles via direct trust parameters, i.e., packet delivery ratio, location proximity, interaction frequency, and indirect trust (recommendations provided by the one-hop neighbors). Last but not least, hybrid trust models combine key features of both data-centric and node-centric trust models [37, 38]. For reference, [39] evaluates node-centric trustworthiness and eliminates malicious vehicles via a threshold range based on distance between the evaluator and the sender, and subsequently assesses data-centric trustworthiness via information quality, role-oriented trust, and effective distance of messages from the sender to the evaluator.

Therefore, trust is indispensable in the context of IoV networks since it guarantees secure and reliable communication, and fosters users' confidence amidst underlying vulnerabilities [40]. If an IoV network is not secure, malicious entities will have the opportunity to jeopardize the entire IoV network for their respective malicious gain, thereby risking the lives of not only passengers but vulnerable pedestrians. Trust, therefore, in tandem with other emerging and promising technological paradigms, can play a pivotal role in maintaining the security of an IoV ecosystem [41].

2.2 Trust Parameters

There are several trust parameters (attributes) that trust models commonly employ to quantify a trustee's trust in an IoV network. Trust can be divided into either direct or indirect trust. Direct trust represents a direct opinion of a trustee by a trustor according to the quality of their respective interactions [42]. In contrast, indirect trust reflects the opinions of a trustor's one-hop neighbors pertinent to a trustee [43]. The direct and indirect trust within an IoV network is illustrated in Figure 2. Some commonly used trust-based parameters in the research literature are further discussed as follows:

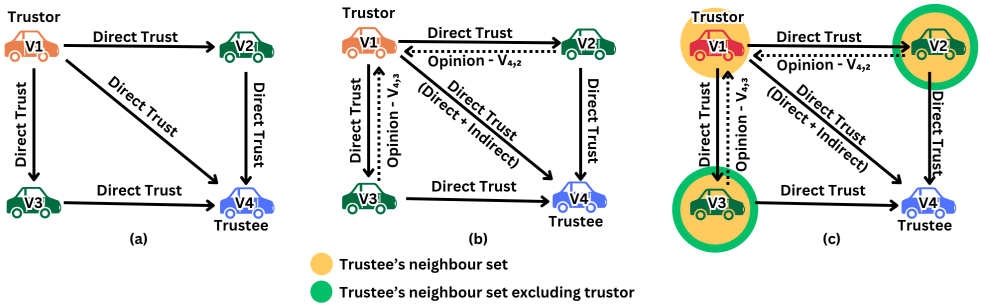

Fig. 2 Direct and indirect trust – (a) shows direct trust, (b) includes both direct and indirect trust (recommendations), and (c) depicts a trustee's set of neighbors.

2.2.1 Packet Delivery Ratio

The packet delivery ratio (PDR) manifests the number of message (packets) successfully received by a trustee j ($P_{i,j}$) to the number of packets sent by a trustor i (P_j) at time instance t. In other words, the PDR indicates the interaction quality between a trustor-trustee pair at different time instances [44–46].

$$PDR_{i,j,t} = \frac{P_{i,j,t}}{P_{j,t}} \tag{1}$$

2.2.2 Similarity

The similarity reflects the degree to which a trustor-trustee pair exhibit similar characteristics, i.e., in terms of trajectory or content [47, 48]. Trajectory similarity can be quantified using the cosine similarity formula, which considers the alignment between the trajectory vectors of the trustor i and the trustee j. Specifically, it measures the cosine corresponding to the angle between their respective movement vectors, thereby reflecting the degree to which their trajectories are similar [49]. The formula is delineated as follows:

$$Traj.Similarity_{i,j,t} = \frac{\vec{i_t} \cdot \vec{j_t}}{\|\vec{i_t}\| \cdot \|\vec{j_t}\|} \tag{2}$$

where, $\vec{i_t}$ and $\vec{j_t}$ represent the trajectory vectors of the trustor i and trustee j at time instance t respectively. The numerator $\vec{i_t} \cdot \vec{j_t}$ is the dot product of both the trajectory vectors, while the denominator $\|\vec{i_t}\| \cdot \|\vec{j_t}\|$ is the product of their magnitudes.

Other than that, content similarity can be ascertained via the Pearson Correlation Coefficient by taking into consideration the information shared by a trustor i and a trustee j at time instance t [50].

$$Cont.Similarity_{i,j,t} = \frac{\sum_{t=1}^{T} TV_t^i \cdot TV_t^j}{\sqrt{\sum_{t=1}^{T}(TV_t^i)^2} \cdot \sqrt{\sum_{t=1}^{T}(TV_t^j)^2}} \tag{3}$$

wherein, TV_t^i and TV_t^j refer to the normalized trust vector of trustor i and trustee j at time t respectively.

2.2.3 Familiarity

Familiarity implies the extent to which a trustor is conversant with a trustee. It is generally calculated by taking the proportion of common neighbors between a trustor i and a trustee j ($C_{i,j}$) at time instance t relative to the sum of neighbors of the trustor i (N_i) at time t. This is of the essence, as a high degree of familiarity facilitates disseminating messages over a broader area of an IoV network [51, 52].

$$Familiarity_{i,j,t} = \frac{C_{i,j,t}}{N_{i,t}} \tag{4}$$

2.2.4 Timeliness

Timeliness delineates the recency of an interaction between a trustor i and a trustee j and which can be ascertained by using the power-law distribution [53]. This parameter ensures that older interactions are given lower trust in contrast to the most recent interactions [54, 55]. This is expressed as:

$$Timeliness_{i,j} = \eta_{sc}(t_o - t_{i,j})^{-\epsilon}, \tag{5}$$

where, $t_o - t_{i,j}$ denotes the delay between the latest time instance t_o and the time $t_{i,j}$, at which the interaction occurs between trustor i and trustee j. ϵ denotes the power-law exponent and η_{sc} represents a preset scaling constant.

2.2.5 Location Proximity

Location proximity is indispensable in trust quantification since a trustor-trustee pair should be in the same vicinity (communication range) for interaction-related purposes [56]. The conventional Euclidean distance formula is inadequate and, therefore, the *Haversine* formula is generally employed to measure the geographical distance between two points [57].

$$d_{i,j} = 2r \cdot \arcsin\left(\sqrt{\sin^2\left(\frac{\Delta\phi}{2}\right) + \cos(\phi_i)\cos(\phi_j)\sin^2\left(\frac{\Delta\lambda}{2}\right)}\right) \tag{6}$$

wherein, d represents the distance between the two geographical points, and r suggests the radius of the Earth with a mean value of 6,371 km. The ϕ and λ are the latitudes and longitudes of the two geographical points expressed in radians respectively. $\Delta\phi = \phi_j - \phi_i$ and $\Delta\lambda = \lambda_j - \lambda_i$ denotes the difference in latitude and longitude between a trustor i and a trustee j respectively.

2.2.6 Interaction Frequency

Interaction frequency is the frequency at which a trustor i and a trustee j interact with one another in an IoV network. It is determined by considering the overall number of interactions between a trustor i and a trustee j ($I_{i,j}$) at time instance t to the sum of interactions between the trustor and all its immediate neighbors (I_i) at the said time instance. More frequent interaction signifies a solid and dependable relation between a trustor and trustee in order to carry out actions in a bid to realize a particular service [58, 59].

$$InteractionFrequency_{i,j,t} = \frac{I_{i,j,t}}{I_{i,t}} \tag{7}$$

2.2.7 Cooperativeness

Cooperativeness refers to how cooperative or egoistic a trustee is. If a vehicle is remarkably cooperative, it will contribute to realizing the key goals of an IoV network [60, 61]. The cooperativeness is delineated as the ratio of the total number of vehicles in interaction with trustee j at time instance t ($V_{j,t}$) to the sum of vehicles in the network ($|V-1|$) [62].

$$Cooperativeness_{j,t} = \frac{V_{j,t}}{|V-1|} \tag{8}$$

2.3 Trust-based Attacks in IoV

Numerous trust management mechanisms have been presented to quantify trust and maintain the security, integrity, and reliability of IoV networks. However, these mechanisms remain susceptible to various attacks that can undermine the trustworthiness of vehicles within the network [63]. The attacks encompass, but are not limited to, on-off attacks, opportunistic service attacks, selective behavior attacks, and ballot-stuffing attacks. The self-promoting attacks, on-off attacks, opportunistic service attacks, and selective behavior attacks primarily stem from self-interest, while ballot-stuffing and bad-mouthing attacks fall under reputation-based attacks [64]. The attacks are described as follows:

2.3.1 Self-promoting Attack

Self-promoting attack occurs when a misbehaving vehicle continually boosts its reputation in order to obtain prominent privileges in an IoV network, ultimately exploiting these privileges to launch attacks and violate the system's reputation rules. To carry out this attack, a malicious vehicle can artificially boost its trustworthiness by creating sophisticated Sybil (pseudonymous) identities [65, 66].

2.3.2 On-off Attack

During an on-off attack, a malicious vehicle randomly alternates between cooperative and malicious actions for preserving a credible reputation in an IoV network, ensuring

a higher chance of gaining privileges [67, 68]. Therefore, by fluctuating between high and low reputation in a zigzag pattern, the malicious vehicle can reduce the probability of being identified as malicious due to low reputation value [69, 70].

2.3.3 Opportunistic Service Attack

In the context of an opportunistic service attack, it happens when a malevolent vehicle initially operates honestly to establish a strong reputation within an IoV network [71]. Once it identifies an optimal opportunity to launch an attack, it starts to act opportunistically to provide bad or misleading services. Since vehicles in an IoV environment interact to support both safety and non-safety services, malicious vehicles with high reputations can also collaborate with other malicious vehicles in order to execute complex attacks [72, 73].

2.3.4 Selective Behavior Attack

In case of a selective behavior attack, an adversarial vehicle strategically provides excellent service for certain tasks while neglecting or undermining others [74]. For example, a malicious vehicle may prioritize low computation services to conserve resources while intentionally underperforming in more resource-intensive tasks. Such behavior is deemed malicious as it disrupts an IoV network's cooperative nature, yet the vehicle can still maintain a reasonable reputation despite its deliberate avoidance of computationally intensive services [75, 76].

2.3.5 Bad-mouthing Attack

A bad-mouthing attack in an IoV network occurs when malicious nodes deliberately provide false or negative feedback about legitimate nodes to undermine their reputation and trustworthiness [77]. The main goal of such attack is to diminish the chances of benign nodes attaining significant privileges within the network. Such attack is often carried out collectively, with a group of adversarial vehicles collaborating to erode the trustworthiness of specific benign vehicles [78, 79].

2.3.6 Ballot Stuffing Attack

In a ballot-stuffing attack, the adversarial vehicles conspire to artificially boost the trust level of a specific vehicle in an IoV network, creating an illusion of trustworthiness to honest vehicles. This attack aims to enhance the malicious vehicles' reputation, increasing their chances of acquiring significant privileges within the network. Consequently, this attack compromises the network's reliability and security, potentially endangering the passengers and vulnerable pedestrians [80, 81].

3 Conventional Trust Management Mechanisms in IoV

This section explains conventional trust management mechanisms and discusses their key limitations in highly dynamic IoV networks. Some conventional mechanisms

emphasize specific parameters. For example, the recommendation-based trust model relies on feedback from other nodes such as pedestrian, vehicles and Road Side Units (RSU) to share their experiences with other nodes [82, 83]. The role-based trust model manages trust based on the roles of individuals or entities, ensuring secure communication and access control [84]. Moreover, the context-aware trust model uses contextual data to assess the reliability of nodes in the IoV [85]. Over time, recommendation, role, and context-awareness have become parameters in IoV, with additional parameters being explored to address the expanding range of conditions. However, conventional trust management mechanisms in IoV typically assign a static weight or predefined rules to various parameters. They are fixed throughout the trust evaluation process, making them less adaptive to the highly dynamic IoV environments.

One of the most commonly used static weights is the mean, which is determined by summing all the values in a sample and then dividing that total by the number of values present in the sample [86]. It is often employed as a weighting method in conventional mechanisms due to its simplicity. For instance, in [87], the mean is used as a weighting method by averaging the old trust metric and the trust metrics from various trustors, thereby aggregating them into a single global trust for each vehicle. Meanwhile, [88] calculates the average of the neighbor's trust, the friend's trust and the historical trust of the receiving vehicle from the perspective of the sending vehicle. Besides that, the authors in [89] also employ the weighted mean method to assess the positive or negative correlation of parameters with the trust level value of vehicles. Although more recent feedback is given higher weight in [90], distinguishing it from other weighted mean methods that treat all feedback equally, the weighted average approach is still used for reputation aggregation. However, conventional aggregation approaches often assign equal or fixed weightings to vehicles, which can result in inaccurate evaluations in trust management due to the variations in driving behaviors, perspectives and distances between vehicles [91].

The subjective logic-based method is also employed for trust management in IoV. This method is a reasoning system that functions based on personal beliefs, where the term *opinion* is used to represent each subjective belief [92]. For example, selective logic is employed to ascertain the reputation values of the vehicles [93] and to calculate trust by considering opinions on the level of belief and disbelief of vehicles as well as uncertainty in the behavior of a vehicle based on predefined base rates [94]. In order to accommodate varying weights in opinion formulation, conventional subjective logic has evolved into multi-weight subjective logic to improve weighting operations [95]. For instance, a three-weight subjective logic selects more reliable data and enhances data credibility by fusing probabilistic beliefs through positive and negative interactions [96]. Another paper [97] also employs three-valued subjective logic in modeling and assessing subjective trust within vehicular social networks by treating vehicle interactions as social connections. The authors provide a framework that enables subjective and objective trust assessment in IoV by leveraging subjective logic to improve efficiency and accuracy in the evaluation of vehicular trustworthiness.

Moreover, game theory also represents a conventional method for trust management mechanisms. For instance, game theory is applied in [98] by utilizing a bargaining game to establish an incentive-based pricing framework, where vehicles and RSUs

improve their trust values, resulting in optimized content delivery based on their trust scores. In [99], the authors leverage game theory in trust management by applying evolutionary strategies to model potential attackers and assess the effectiveness of reputation systems. This approach allows optimal tactics identification for all participants while offering a measurable evaluation of the reputation management system's performance. Game theory can also be used to establish reliable interactions and secure cooperation between vehicles in IoV. For example, in a hedonic coalition game, the trust levels are used to form coalitions and can be calculated using a decentralized Bayesian inference approach [100]. Other than that, fuzzy logic is also a conventional mechanism that can be considered. For example, fuzzy logic is applied in [101] to address uncertainty and imprecision of data in vehicular networks by evaluating the sender's credibility based on parameters such as experience, plausibility, and accuracy of the message. This evaluation helps to determine whether messages should be trusted or dismissed. The authors in [102] apply fuzzy logic in the context of IoV trust management to assess the trustworthiness of vehicles based on behavioral information, establish their access privileges and message credibility while also taking into account their mobility, and enhance security with mutual authentication.

While conventional trust management mechanisms in IoV have established a strong foundation, they encounter several limitations that diminish their performance in dynamic and complex vehicular networks. One of the issues is the dependence of trust models on static weightings and rigid models, which often fail to adapt to changing contexts. It is recommended to increase the weight assigned to more critical parameters [103], although the priority of parameters may vary depending on the situation. This inflexibility results in inaccurate trust evaluations, especially in environments where vehicle behaviors and network conditions continuously evolve. Furthermore, traditional mechanisms exhibit limited scalability when managing large volumes of data and interactions in rapidly evolving settings, rendering IoV networks susceptible to various attacks [104]. Although traditional models can detect certain malicious actions based on historical data or fixed rules, they struggle with more sophisticated attacks. Even enhanced mechanisms may still rely on static rules or thresholds that can be exploited by sophisticated attackers, such as self-promoting attacks and selective behavior attacks [105].

4 Learning-based Trust Management Mechanisms in IoV

This section begins with an overview of learning-based mechanisms and proceeds to discuss their application in trust management, highlighting various models that leverage learning-based mechanisms to improve trust evaluation.

4.1 Introduction to Learning-based Mechanisms

Several learning-based mechanisms are increasingly utilized in trust management to improve evaluation processes within the IoV framework. The primary learning methods include machine learning, deep learning, and reinforcement learning. These techniques greatly enhance trust assessment by allowing systems to gather insights

from data, adjust to varying circumstances, and enhance the accuracy and dependability of decisions, ultimately resulting in more secure and efficient vehicle networks. A visual representation that shows the comparison of machine learning, deep learning, and reinforcement learning is shown in Figure 3.

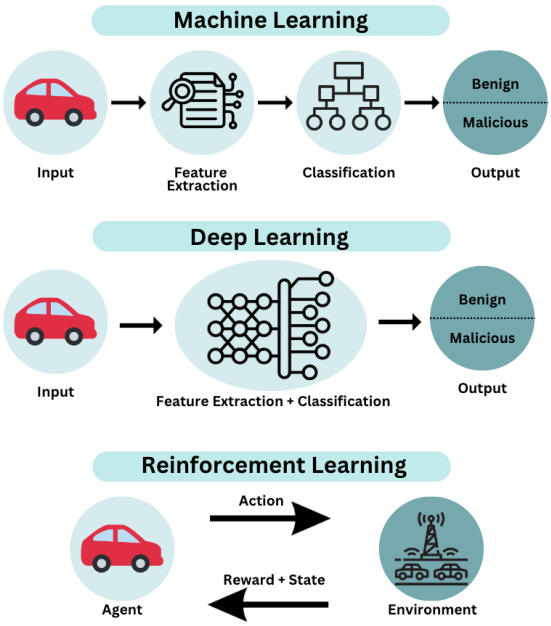

Fig. 3 Comparison of machine learning-, deep learning-, and reinforcement learning-based mechanisms in IoV.

4.1.1 Machine Learning

Machine learning involves the study and establishment of algorithms that predict outcomes based on data. These algorithms serve to bridge gaps in understanding complex patterns and relationships within the data [106]. Machine learning allows computers to mimic and adapt human-like behavior, enabling systems to learn from each interaction and action before leveraging this experience to enhance future performance [107]. Machine learning is primarily divided into two domains, i.e., supervised and unsupervised learning [108]. Most practical machine learning mechanisms involve three main supervised algorithms or their variants, which are K-Nearest Neighbors (KNN), Support Vector Machine (SVM), and Decision Tree [109]. On the contrary, examples of unsupervised algorithms include K-means clustering, the Gaussian Mixture Model, and the Hidden Markov Model.

4.1.2 Deep Learning

Deep learning, a subfield of machine learning, has developed into a crucial tool in modern computing applications due to its ability to perform sophisticated tasks after learning complex concepts [110]. There is a crucial difference between conventional machine learning and deep learning. Conventional machine learning relies on handcrafted feature extraction and multiple algorithms to make decisions. However, deep learning is more powerful because it can automatically learn and represent features on multiple levels [111]. Deep learning is a prominent and emerging area within machine learning, since it involves a cascade of layers that perform non-linear processing to learn multi-level data representations [112]. Each layer may contain hundreds or even thousands of neural units, with those between the input and output layers referred to as hidden layers and their respective units as hidden nodes [113].

4.1.3 Reinforcement Learning

Reinforcement learning, derived from animal learning theory, autonomously develops optimal policies through trial-and-error and continuous interaction with dynamic environments, with its self-improving and online learning characteristics making it a core technology for intelligent agents [114]. A feedback mechanism that identifies when the autonomous agent has selected the correct action is crucial for effective learning; this is achieved via a reward (or cost) function that evaluates actions taken in specific system states [115]. In other words, reinforcement learning is a machine learning technique that enables an agent to decide on actions in an unknown environment by observing, analyzing, and selecting actions based on expected maximum returns, learning to take optimal actions by representing the environment as a Markov decision process [116, 117]. Reinforcement learning is highly flexible and beneficial in immediate and competitive settings. It allows a self-governing agent to make optimal consecutive decisions without much or any prior understanding of the surroundings [118].

4.2 State-of-the-Art Machine Learning-based Trust Management Mechanisms in IoV

In [119], a machine learning mechanism was envisaged for 76 vehicles, wherein the authors ascertained trust by encompassing interaction frequency, timeliness, PDR and familiarity before recording them into a feature matrix. Then, they used unsupervised learning algorithms to classify the vehicles into trustworthy and untrustworthy clusters. Various supervised learning classifiers including KNN, SVM, and ensemble classifiers are trained to obtain an optimal decision boundary to identify malicious vehicles. The proposed model showed outstanding results, with high accuracy, recall, precision, and F1-score, outperforming six other models. The authors in [120] present a trust model that incorporates both indirect and direct trust. In order to label the feature matrix after extraction, clustering is done using 3 unsupervised learning algorithms, i.e., fuzzy c-means, agglomerative clustering and k-means. After that, KNN and Random Forest (RF) classifiers are employed for training purposes, determining the decision boundary for malicious node detection. The proposed model is evaluated

using precision, recall, and F1-score parameters. The evaluation results are exceptionally high. Notably, the performance of the proposed model surpasses that of five other trust models, achieving the highest performance.

The model in [121] evaluates trust by merging the reputation features with other trust parameters including message freshness, message similarity, sender proximity, and event location to improve the accuracy of the model. It utilizes ensemble learning that combines multiple weak learners alongside the Gini criterion for feature selection to improve predictions regarding vehicle trustworthiness and detect malicious vehicles. Apart from precision, recall and F1-score, the model was evaluated using Area Under Curve (AUC), confusion metrics and time measurement and the results illustrate that the proposed model achieved the highest performance across all metrics when it was compared with two other models. Furthermore, [122] a trust management mechanism was presented for CAVs, which is also an important component of IoV. The proposed model considered multidimensional trust factors to ensure a comprehensive trust evaluation. These factors include spatiotemporal logic features like frequency and position trust factors, behavioral analysis features such as content duplication and speed trust factors, as well as traffic flow features such as the time headway trust factor. Shallow machine learning classifiers including XGBoost, AdaBoost, RF and KNN were used for per-minute predictions. The model is evaluated using accuracy, recall, precision, and F1-score to compare different learning mechanisms in detecting malicious vehicles. The model proposed in [123] incorporates parameters such as discrepancies in distance and velocity along both x- and y-directions prior to conducting plausibility checks related to location and movement validity. Multiple classifiers, including KNN, SVM, NB, RF and Ensemble learning mechanisms, were trained to detect malicious vehicles. However, the results showed low consistency when the model was evaluated with metrics such as precision, recall and F1-score under different types of attacks.

In [124], a federated learning-based trust management mechanism is proposed to enhance node reliability in IoV network. The node trust evaluation is performed by assessing a vehicle's reputation score based on key parameters, i.e., honesty score, model accuracy, and interaction timeliness. The federated learning process leverages a capacity metric to evaluate interaction behaviors, enabling the identification of trustworthy nodes. The system's performance is evaluated through metrics including variations in packet transmission rates and network latency under varying malicious node proportions, demonstrating its effectiveness in maintaining network stability and security. In [125], federated learning is used to enable vehicles to collaboratively train a global model for trust evaluation without sharing raw data. Each vehicle trains a local trust model based on its own observations and transmits only secured model updates to a central aggregator. This approach ensures the confidentiality and integrity of the updates during transmission and aggregation. Trust is implicitly managed by allowing only secure and tamper-resistant updates to contribute to the global model, thereby preserving privacy and defending against potential attacks. The model is evaluated using response time, latency, resource utilization efficiency, and network scalability, demonstrating its suitability for secure and efficient deployment in IoV environments. In outline, the comparison of case studies on machine learning-based trust management mechanisms is presented in Table 2.

Table 2 Comparison of machine learning-based trust management mechanisms in IoV.

References		[119]	[120]	[121]	[122]	[123]	[124]	[125]
Parameters	Interaction Frequency	✓			✓			
	Timeliness	✓		✓			✓	
	PDR	✓	✓				✓	✓
	Familiarity	✓	✓					
	Similarity		✓	✓	✓			
	Location Proximity			✓	✓	✓		
	Reputation			✓			✓	
	Velocity Discrepancies				✓	✓		
	Neighbor Nodes Amount				✓			
	Vehicle Density Variance				✓			
	Behavioral Consistency							✓
	Context-awareness		✓		✓			
Learning Algorithms	KNN	✓	✓		✓	✓		
	SVM	✓				✓		
	RF		✓		✓	✓		
	NB					✓		
	Ensemble Learning	✓		✓		✓		
	K-means	✓	✓					
	Fuzzy C-Means		✓					
	XGBoost				✓			
	Federated Learning						✓	✓
	AdaBoost				✓			
Evaluation Metrics	Accuracy	✓			✓			
	Precision	✓	✓	✓	✓	✓		
	F1-score	✓	✓	✓	✓	✓		
	Recall	✓	✓	✓	✓	✓		
	AUC			✓				
	Confusion Matrix			✓				
	Response Time							✓
	Network Latency						✓	✓
	Transmission Efficiency						✓	✓
	Network Scalability							✓

4.3 State-of-the-Art Deep Learning-based Trust Management Mechanisms in IoV

In [126], the trustworthiness of driverless cars is evaluated by monitoring compromised on-board unit components, including cameras, LiDAR and radar. These vehicles can be categorized as trustworthy or untrustworthy using a deep learning-based model, specifically a Deep Neural Network (DNN). The trust degree evaluation is based on the parameters, including the vehicle's acceleration or deceleration, relative speed, phase time, and location proximity. After training the DNN model using trust degree as input, the performance of the proposed model is assessed through Receiver Operating Characteristic (ROC) curves, AUC, recall, and precision. The results illustrate that the DNN outperforms alternative models like SVM and Long Short-Term Memory (LSTM) networks. Moreover, the application of a DNN model facilitates the identification of malicious nodes within smart transport ecosystems by training on extensive datasets sourced from sustainable cities [127]. The proposed model computes vehicle trust degrees based on three primary parameters including experience, performance, and behavior, which are represented by interaction frequency, PDR, and

reputation, respectively. The research includes detecting cyber attacks such as Whitewash and Brute Force attacks but it does not explicitly address trust-related attacks. The attributes including accuracy, F1-score, recall, and precision are used to ascertain the effectiveness of the proposed model. These metrics provide insights into its effectiveness in identifying malicious nodes while ensuring privacy and security in smart transportation systems.

The authors in [128] propose a trust model that verifies data trustworthiness using various parameters including experience derived from past interactions and plausibility. The plausibility is calculated by the location verification which includes distance-based and time-based verification after the authentication and lifetime verification (timeliness) process of the message. In this context, deep learning is applied at the stage of experience measurement to extract features and automatically classify vehicular data, enhancing the accuracy of trust assessments. It operates within a modified Deep Metric Learning (DML)-based Chaotic Henry Gas Solubility Optimization (CHGSO) framework to manage multi-class classification and resolve uncertainties. In the process of performance evaluation, the attributes including PDR, average latency and throughput are used to assess the efficiency of the proposed model. Furthermore, authors in [129] utilize parameters including the total count of relay nodes, vehicle mistrust scores, and trust derived from both experience and recommendations. The trust value of each intermediate (relay) node is then calculated via a fuzzy system based on two parameters, i.e., the density of the network and the relay's distance metric. With input from the fuzzy trust level recommendation, the vehicles are classified into three categories namely normal, abnormal, and malicious. After that, the malicious behaviors of vehicles are predicted by employing a Deep Belief Network (DBN). The performance of the proposed model outperformed other models while evaluated using several attributes, including detection rate, end-to-end delay, communication overhead, processing delay, detection time, network accuracy, PDR, and throughput ratio.

The trust model proposed in [130] calculates the trust degree of vehicles using several vital parameters, i.e., direct trust, indirect trust, recent trust, and historical trust. Direct trust is computed by taking account energy depletion and message-forwarding behavior, while indirect trust relies on feedback from neighboring vehicles. Recent trust combines direct and indirect trust, whereas historical trust is derived from an exponential averaging of past trust scores to reflect long-term reliability. The model incorporates deep learning through the Deep Maxout Network (DMN) to classify the vehicles as benign or malicious. The DMN is optimized by the Fractional Aquila Spider Monkey Optimization Algorithm to enhance the accuracy of detecting attacks. The performance of the proposed model is ascertained using metrics such as precision, recall, network energy, and trust with different feature sizes. Moreover, the authors in [131] present a multidimensional trust evaluation model where each trustor assesses trustees based on historical interactions, reliability, and long-term behavior, supplemented by ancillary factors such as environmental context and sensor performance. Final trust values are categorized as trusted, average, or malicious, with malicious nodes being blocked and logged. At the core of the system is an Improved Long Short-Term Memory (I-LSTM) neural network tailored for anomaly detection

Table 3 Comparison of deep learning-based trust management mechanisms in IoV.

References		[126]	[127]	[128]	[129]	[130]	[131]	[132]
Parameters	Acceleration	✓						
	Relative speed	✓						
	Location	✓		✓	✓	✓		
	Experience		✓	✓	✓		✓	✓
	PDR		✓					
	Reputation		✓					✓
	Timeliness			✓				
	Relay Count				✓			
	Mistrust value				✓			
	Recommendation				✓	✓		
	Network Density				✓			
	Context						✓	✓
	Energy Depletion					✓		
Evaluation Metrics	Accuracy		✓		✓		✓	✓
	F1-score		✓					✓
	Recall	✓	✓			✓		✓
	Precision	✓	✓			✓		✓
	ROC	✓						
	Detection Time				✓		✓	✓
	AUC	✓						
	PDR			✓	✓			
	Average Latency			✓				
	Throughput			✓	✓			
	Detection Rate				✓		✓	✓
	Processing Delay				✓			✓
	Communication Overhead				✓			
	End-to-end Delay				✓			
	Network Energy					✓		
	Trust Variation					✓		
	Sensitivity							✓
Learning Algorithms	Deep Belief Learning				✓			
	Deep Neural Network	✓	✓			✓		
	Deep Metric Learning			✓				
	Deep Maxout Learning					✓		
	Long Short-term Memory						✓	✓

in autonomous vehicle environments, with evaluation results showing the highest performance in terms of accuracy, risk detection rate, and response time across varying conditions compared to existing methods. A hybrid intrusion detection and prevention system for VANETs is proposed in [132], where trust evaluation is based on a thresholded trust score produced by a DNN-BiLSTM model trained on optimized behavioral features extracted using an autoencoder. The trust score reflects node behavior over time aligning with experience-based evaluation while routing decisions incorporate contextual information such as signal strength and vehicle distance. Deep learning enables high-accuracy anomaly detection and the system is analyzed using metrics including accuracy, precision, recall, F1-score, specificity, sensitivity, detection rate, false positive/negative rates, transmission time, and convergence rate, demonstrating strong performance compared to existing methods. In brief, the comparison of deep learning-based trust management mechanisms is presented in Table 3.

4.4 State-of-the-Art Reinforcement Learning-based Trust Management Mechanisms in IoV

The proposed reinforcement learning-based trust mechanism in [133] enhances trust management through direct and indirect evidence. The direct trust evidence is derived from positive and negative interactions between the trustor and trustee within specific contexts. In contrast, the indirect trust evidence is obtained from the trust values of vehicles showing similar behaviors in a given context, which are fine-tuned using a regression model to estimate indirect trust value under diverse contexts. This mechanism dynamically adjusts the thresholds for trust and weights assigned to different types of evidence by employing Q-learning algorithms, effectively identifying and filtering out malicious vehicles. The performance of the model is evaluated using metrics including simulation run time and average reward, apart from common metrics such as accuracy, recall, precision, and F1-score. The model shows the highest performance and fastest convergence compared to other selected models. Furthermore, the authors in [134] consider both internal and external information when calculating final trust values within an IoV environment. The calculation also includes the entropy of trust values related to a given request to ensure a more reliable trust assessment. The Q-learning algorithm is employed to adjust the strategy dynamically while continuously receiving feedback on the accuracy of the trust evaluation results. The feedback loop enables the model to adapt to different contexts, enhancing the precision rate of the trust management mechanism. This ability leads to the fastest convergence and a high precision rate, while also maintaining strong consistency, thereby significantly enhancing the overall trust evaluation performance and ensuring more reliable and adaptive decision-making compared to other existing models.

The trust management mechanism proposed in [135] combines the reputation update policies, which include weak and robust trust policies and employs deep reinforcement learning to optimize reputation updates. Feedback is integrated through the Dempster-Shafer theory after the reputation scores are calculated to increase the accuracy of malicious vehicles. Utilization of deep reinforcement learning enables trust management mechanisms to adjust the reputation policy dynamically, maximizing rewards and ensuring the robustness of trust management in IoV scenarios. The trust management mechanism in [136] focuses solely on direct trust in order to simplify the model and reduce communication costs. Both control and data packets are considered in direct trust with their respective forwarding ratios used to determine each vehicle's trust value. Q-learning is employed in this mechanism by utilizing cumulative trust values for the long-term reward, also considered as the Q-value, to ensure secure communication between vehicles. The metrics included to evaluate the performance are loss function, convergence performance, and Expected Transmission Count (ETX) delay. Trust evaluation in [137] combines direct and indirect trust values by using the Bayesian approach for direct trust and Yager's rule for indirect trust. The overall trust value is computed by fusing the trust values and making adjustments through the confidence factor to enhance the reliability of the observations. A Q-learning algorithm is then utilized for dynamic updates to trust values based on continuous observations and feedback to ensure adaptability in numerous IoV contexts. The authors also show the robustness of the proposed model against trust-based

Table 4 Comparison of reinforcement learning-based trust management mechanisms in IoV.

References		[133]	[134]	[135]	[136]	[137]	[138]	[139]
Parameters	Context-awareness	✓	✓					
	Positive Evidence Ratio	✓					✓	
	Reputation	✓	✓	✓	✓		✓	✓
	Entropy		✓					
	Regularity of Trust Value		✓					
	Time of Event		✓			✓		✓
	PDR				✓	✓		
	Confidence					✓	✓	
	Role-based							✓
Evaluation Metrics	Accuracy	✓				✓		
	Precision	✓	✓					✓
	Recall	✓						
	F1-score	✓						
	Average Reward	✓		✓		✓		
	Loss				✓			
	Convergence Performance				✓			
	ETX Delay				✓			
	Execution Time	✓				✓		✓
	Detection Rate						✓	✓
Learning Algorithms	Q-learning	✓	✓		✓	✓		✓
	Deep Reinforcement Learning			✓			✓	
Trust-related Attacks	Bad-mouthing Attacks	✓				✓		
	Ballot-stuffing Attacks	✓				✓		

attacks, specifically Ballot-stuffing and Bad-mouthing attacks. The authors evaluate their framework's performance by comparing it with others, focusing on response time, network adaptability, average hop counts, and packet reception.

The trust management mechanism proposed in [138] integrates both objective and subjective evaluations, where objective trust is based on a vehicle's interaction performance, considering the proportion of positive and negative interactions, and subjective trust incorporates confidence values derived from historical trust records and opinions from neighboring vehicles, weighted by message quality and the raters' reputations. Furthermore, the authors employ a GenAI-enhanced deep reinforcement learning algorithm to optimize trust-aware consensus by dynamically selecting the primary node and block size based on node reputation, throughput, and delay, thereby ensuring a reliable and efficient consensus process in the IoV environment. The trust model is evaluated by tracking trust value changes of different vehicle types and comparing detection accuracy against baseline models under varying thresholds and misbehavior probabilities. In [139], trust evaluation is performed by integrating four sources of trust, i.e., direct, indirect, role-based, and global. Direct trust is derived from recent interaction experiences, indirect trust considers the recommendations from neighboring vehicles, role-based trust is obtained from the trustor's belief in the trustee's assigned role, and global trust is evaluated based on the RSUs broadcasting trust values within their communication range. To enhance trust-based decision-making under dynamic conditions, the authors further introduce a Q-learning-based adaptive threshold control strategy, where each vehicle acts as an agent and autonomously adjusts its trust threshold according to the current error degree and trust state. The effectiveness of the model is assessed based on metrics like false-positive rate and detection rate under various conditions, including different learning rates, vehicular

densities, malicious vehicle proportions, as well as varying punishment and reward factors. In outline, the comparison of reinforcement learning-based trust management mechanisms is presented in Table 4, which highlights the key parameters, evaluation metrics, learning algorithms and trust-related attacks.

5 Open Research Directions

Although the advancement of learning-based trust management mechanisms in the IoV has promised an avenue for enhancing its reliability and security, several challenges hinder their effectiveness. Addressing these challenges is crucial for future efficient and robust trust management mechanisms in IoV. The following sections discuss the limitations and future research directions in this field, including but not limited to, robustness against trust-based attacks, practical implementation and assessment, data diffusion and collaborative learning in high-density environments, and motivating selfish vehicles.

5.1 Robustness Against Trust-based Attacks

Developing trust management mechanisms that are robust against numerous attacks is a major challenge in IoV. Due to the fast-changing and open characteristics of IoV, it is vulnerable to malicious behavior that can influence the trust evaluation process [140]. Implementing a trust management mechanism that is resilient to attacks is crucial for ensuring the safety and reliability of the IoV [141]. Although some researchers include various attack detection and mitigation strategies, these often encompass limited trust-based attack models. For instance, the authors prove the effectiveness of their trust management system in resisting against two specific trust-based attacks in [137], namely the Ballot-stuffing and the Bad-mouthing attack attack. Future research should focus on creating more comprehensive mechanisms to detect these attacks effectively, ensuring the integrity and reliability of trust management in IoV [142].

5.2 Practical Implementation and Assessment

Despite significant advancements in learning-based trust management mechanisms for IoV, their real-world application and testing remain limited. Demonstrating the effectiveness and scalability of these trust management algorithms in actual, practical scenarios presents significant difficulties [143, 144]. The limited access to high-quality datasets, primarily attributable to privacy concerns and the reluctance of business stakeholders to share data with academic institutions, constitutes a substantial challenge to the practical implementation and evaluation of learning-based trust management mechanisms [145]. Therefore, developing high-quality synthetic datasets that reflect real-world IoV environments and scalable testing frameworks capable of replicating these conditions will be critical for training, evaluating, and accurately assessing the performance of trust management models [146].

5.3 Data Diffusion and Collaborative Learning in High-density IoV Environment

The massive data streams from vehicles need to be effectively collected, processed, and analyzed. Robust storage solutions and advanced data processing techniques are required to ensure data quality for the training process [147]. Moreover, inadequate computing resources can lead to inaccurate handling of high-dimensional data, resulting in imprecise buffering decisions [148]. In high-density IoV environments, achieving effective collaborative learning with minimal overhead is crucial due to the bandwidth constraints and the necessity for quick data dissemination and accurate trust assessments [149]. Therefore, research into more suitable learning-based trust management models that can operate efficiently in bandwidth-constrained environments, and developing advanced data processing algorithms will be crucial for handling the highly dynamic data in IoV networks [150].

5.4 Motivating Selfish Vehicles

Motivating and encouraging honest behavior in IoV has become a significant challenge in getting vehicles with malicious intent to act cooperatively [151]. Although learning-based mechanisms can alleviate the problem of dynamic thresholds and achieve high accuracy in detecting malicious vehicles, their performance may be compromised if there are many selfish nodes in the network [152]. Furthermore, the potential for selfish behavior could reduce the willingness of participants to collaborate within the IoV [153]. Hence, it is important to explore effective methods to curb selfish behaviors as a future direction to ensure the security and availability of IoV because selfish vehicles might decline information reporting tasks to minimize overhead [154].

5.5 Adaptive Trust Models for Diverse IoV Scenarios

The diversity of scenarios within IoV leads to significant challenges in developing effective trust management mechanisms [155]. Each environment, such as urban, suburban, and rural environments has different characteristics, e.g., communication infrastructure, traffic density and vehicle behavior patterns, which can influence the trust evaluation process significantly.Trust management models are often not flexible enough to adapt to rapidly evolving vehicular environments [156]. Since a trust management model establishes trust among the vehicles according to the information like context information from the vehicles [157], focus on developing adaptive trust models capable of dynamically adjusting to various IoV environments. This adaptability is essential for ensuring consistency and reliability in trust assessments across all scenarios in highly dynamic networks [158].

5.6 Cold Start

As the cold start is among the most extensively studied issues in trust management, it is a significant challenge that warrants attention [159]. This challenge emanates when a node enters a network without prior interactions with other entities, making it hard to evaluate its trustworthiness. In many existing trust management mechanisms, this

issue is addressed by assigning an arbitrary initial trust score or some may overlook this issue [160]. This scenario poses problems when a vehicle enters an unfamiliar environment without any previous encounters with other vehicles [161]. There will be a risk of eliminating an honest vehicle from the network if the initial trust score is set too low or a delay in detecting malicious vehicles if the initial score is too high [162]. Therefore, future research should resolve the cold start challenge to enhance trust management accuracy in IoV.

6 Conclusion

In conclusion, this survey provides a comprehensive review of trust management mechanisms in IoV, with a focus on learning-based mechanisms including machine learning, deep learning, and reinforcement learning. It also includes an analysis of the trust parameters used for calculating trust scores of vehicles and examines various trust-related attacks that pose threats to IoV networks. Through a comparative analysis of existing learning-based trust management mechanisms, their potential to enhance the accuracy, adaptability, and robustness of trust management systems can be identified. Integration of adaptive trust models and more robust attack detection mechanisms with emerging technologies like learning-based approaches has the potential to significantly improve trust management in IoV systems leading to safer and more efficient vehicular communication systems. However, several challenges still need to be addressed, including but not limited to, robustness against trust-based attacks, practical implementation and assessment, data diffusion and collaborative learning in high-density environments, and motivating selfish vehicles. Therefore, future research should be dedicated to overcome the challenges in order to ensure the reliability and security of IoV in diverse and dynamic environments.

Funding

The corresponding author would like to sincerely acknowledge the generous support of the MoHE's FRGS Grant No. FRGS/1/2023/ICT07/UNIMAS/021 for funding the research-at-hand.

References

[1] Alladi, T., Kohli, V., Chamola, V., Yu, F.R.: Securing the Internet of Vehicles: A Deep Learning-based Classification Framework. IEEE Networking Letters **3**(2), 94–97 (2021)

[2] Gu, C., Ma, B., Hu, D.: A Dependable and Efficient Decentralized Trust Management System Based on Consortium Blockchain for Intelligent Transportation Systems. IEEE Transactions on Intelligent Transportation Systems (2024)

[3] Omeiza, D., Webb, H., Jirotka, M., Kunze, L.: Explanations in Autonomous Driving: A survey. IEEE Transactions on Intelligent Transportation Systems **23**(8), 10142–10162 (2021)

[4] Manogaran, G., Rawal, B.S.: Machine Learning-based Trust Model for Secure Internet of Vehicle Data Exchange. In: 2020 IEEE Globecom Workshops (GC Wkshps), pp. 1–6 (2020). IEEE

[5] Wang, J., Shao, Y., Ge, Y., Yu, R.: A Survey of Vehicle to Everything (V2X) Testing. Sensors **19**(2), 334 (2019)

[6] Srivastava, S., Agarwal, D., Chaurasia, B.K., Adhikari, M.: Blockchain-based Trust Management for Data Exchange in Internet of Vehicle Network. Multimedia Tools and Applications **84**(8), 4837–4855 (2025)

[7] Truong, N.B., Lee, H., Askwith, B., Lee, G.M.: Toward a Trust Evaluation Mechanism in the Social Internet of Things. Sensors **17**(6), 1346 (2017)

[8] Surapaneni, P., Bojjagani, S., Khan, M.K.: DYNAMIC-TRUST: Blockchain-Enhanced Trust for Secure Vehicle Transitions in Intelligent Transport Systems. IEEE Transactions on Intelligent Transportation Systems (2025)

[9] Hossain, M.M., Hasan, R., Zawoad, S., *et al.*: Trust-IoV: A Trustworthy Forensic Investigation Framework for the Internet of Vehicles (IoV). In: IEEE International Congress on Internet of Things (ICIOT), pp. 25–32 (2017)

[10] Lu, Y., Zhang, G., Wang, X., Li, X.: Trust-Based Reliability Enhancements Provisioning with Resilience Under Information Asymmetry in IoV System. IEEE Access (2023)

[11] Zavvos, E., Gerding, E.H., Yazdanpanah, V., Maple, C., Stein, S., *et al.*: Privacy and Trust in the Internet of Vehicles. IEEE Transactions on Intelligent Transportation Systems **23**(8), 10126–10141 (2021)

[12] Sagar, S., Mahmood, A., Sheng, M., Zaib, M., Zhang, W.: 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, pp. 283–290 (2020)

[13] Dhibi, N., Makhlouf, A.M., Zerai, F.: Reputation-based Security for IoV Environment. International Association of Engineers (IAENG) International Journal of Computer Science **52**(4) (2025)

[14] Jain, A., Kumar, A., Mahadev, Chaudhary, J.K., Singh, S.: Trust-Based Reliability Scheme for Secure Data Sharing With Internet of Vehicles Networks. Internet Technology Letters **8**(2), 70000 (2025)

[15] Mahmood, A., Sheng, M., Zhang, W.E., Yongchareon, S.: Trust Management in the Internet of Vehicles, (2023). CRC Press

[16] Mahmood, A., Sheng, Q.Z., Siddiqui, S.A., Sagar, S., Zhang, W.E., Suzuki, H., Ni, W.: When Trust Meets the Internet of Vehicles: Opportunities, Challenges, and Future Prospects. In: 2021 IEEE 7^{th} International Conference on Collaboration and Internet Computing (CIC), pp. 60–67 (2021). IEEE

[17] Seno, M.E., Zaidi, A., Gupta, B., Avacharmal, R., Yogi, K.S., Tiwari, M., Reegu, F.A., Shavkatov, N., Soni, M.: A Hybrid Trust Management Strategy for Reliable Cyber-Physical System in Intelligent Transportation. IEEE Transactions on Intelligent Transportation Systems (2025)

[18] Hussain, R., Lee, J., Zeadally, S.: Trust in VANET: A Survey of Current Solutions and Future Research Opportunities. IEEE Transactions on Intelligent Transportation Systems **22**(5), 2553–2571 (2021) https://doi.org/10.1109/TITS.2020.2973715

[19] Hbaieb, A., Ayed, S., Chaari, L.: A Survey of Trust Management in the Internet of Vehicles. Computer Networks **203**, 108558 (2022)

[20] Amari, H., Abou El Houda, Z., Khoukhi, L., Belguith, L.H.: Trust Management in Vehicular Ad-hoc Networks: Extensive Survey. IEEE Access **11**, 47659–47680 (2023)

[21] AlMarshoud, M., Sabir Kiraz, M., H. Al-Bayatti, A.: Security, Privacy, and Decentralized Trust Management in VANETs: A Review of Current Research and Future Directions. ACM Computing Surveys **56**(10), 1–39 (2024)

[22] Alalwany, E., Mahgoub, I.: Security and Trust Management in the Internet of Vehicles (IoV): Challenges and Machine Learning Solutions. Sensors **24**(2), 368 (2024)

[23] Xu, Q., Zhang, L., Liu, Y.: Enhancing Trust Management System for Connected Autonomous Vehicles Using Machine Learning Methods: A Survey (2025). https://arxiv.org/abs/2505.07882

[24] Tangade, S., Manvi, S.S., Lorenz, P.: Trust Management Scheme based on Hybrid Cryptography for Secure Communications in VANETs. IEEE Transactions on Vehicular Technology **69**(5), 5232–5243 (2020)

[25] Hatamleh, I.H.M., Safori, A.O., Habes, M., Tahat, O., Ahmad, A.K., Abdallah, R.A.-Q., Aissani, R.: Trust in Social Media: Enhancing Social Relationships. Social Sciences **12**(7), 416 (2023)

[26] Sagar, S., Mahmood, A., Wang, K., Sheng, Q.Z., Pabani, J.K., Zhang, W.E.: Trust–SIoT: Toward Trustworthy Object Classification in the Social Internet of

Things. IEEE Transactions on Network and Service Management **20**(2), 1210–1223 (2023)

[27] Mądra-Sawicka, M.: Trust Building Strategy Among Food Listed Companies in the Digital Economy Era. In: Trust, Organizations and the Digital Economy, pp. 245–257 (2021). Routledge

[28] Rehman, A., Hassan, M.F., Yew, K.H., Paputungan, I., Tran, D.C.: State-of-the-Art IoV Trust Management a Meta-synthesis Systematic Literature Review (SLR). PeerJ Computer Science **6**, 334 (2020)

[29] Din, I.U., Khan, K.H., Almogren, A., Guizani, M.: Machine Learning for Trust in Internet of Vehicles and Privacy in Distributed Edge Networks. IEEE Internet of Things Journal (2025)

[30] Ahmad, F., Franqueira, V.N., Adnane, A.: TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-hoc Networks. IEEE Access **6**, 28643–28660 (2018)

[31] Zhang, J.: A Survey on Trust Management for Vanets. In: 2011 IEEE International Conference on Advanced Information Networking and Applications, pp. 105–112 (2011). IEEE

[32] Zhang, J.: A Survey on Trust Management for VANETs. In: 2011 IEEE International Conference on Advanced Information Networking and Applications, pp. 105–112 (2011). https://doi.org/10.1109/AINA.2011.86

[33] Sharma, P., Liu, H.: A Machine-learning-based Data-centric Misbehavior Detection Model for Internet of Vehicles. IEEE Internet of Things Journal **8**(6), 4991–4999 (2020)

[34] Wu, A., Ma, J., Zhang, S.: RATE: a RSU-aided Scheme for Data-centric Trust Establishment in VANETs. In: 2011 7^{th} International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1–6 (2011). IEEE

[35] Alazemi, F., Al-Mulla, A., Al-Akhras, M., Alawairdhi, M., Al-Masri, M., Omar, H., Alshareef, H.: A Trust Management Model in Internet of Vehicles. International Journal of Data and Network Science **7**(2), 745–756 (2023)

[36] Tripathi, K.N., Jain, G., Yadav, A.M., Sharma, S.C.: Entity-centric Combined Trust (ECT) Algorithm to Detect Packet Dropping Attack in Vehicular Ad Hoc Networks (VANETs). In: Next Generation Information Processing System: Proceedings of ICCET 2020, Volume 2, pp. 23–33 (2021). Springer

[37] Kerrache, C.A., Calafate, C.T., Cano, J.-C., Lagraa, N., Manzoni, P.: Trust Management for Vehicular Networks: An Adversary-Oriented Overview. IEEE Access **4**, 9293–9307 (2016)

[38] Alriyami, Q., Adnane, A., Smith, A.K.: Evaluation Criterias for Trust Management in Vehicular Ad-hoc Networks (VANETs). In: 2014 International Conference on Connected Vehicles and Expo (ICCVE), pp. 118–123 (2014). IEEE

[39] Ahmad, F., Kurugollu, F., Kerrache, C.A., Sezer, S., Liu, L.: NOTRINO: A Novel Hybrid Trust Management Scheme for Internet-of-Vehicles. IEEE Transactions on Vehicular Technology **70**(9), 9244–9257 (2021)

[40] Razafimanjato, M., Yang, H., Park, S., Kim, S., Kim, D.: Blockchain and AI-Enabled Trust Management Model for Internet of Vehicles. In: 2025 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), pp. 0442–0447 (2025). IEEE

[41] Ismail, S., Hammad, E., Iqbal, R.: Towards Holochain-Based Adaptive Trust Management in Social Internet of Vehicles. In: 2025 IEEE 15^{th} Annual Computing and Communication Workshop and Conference (CCWC), pp. 00878–00884 (2025). IEEE

[42] Rehman, A., Hassan, M.F., Hooi, Y.K., Qureshi, M.A., Chung, T.D., Akbar, R., Safdar, S.: Context and Machine Learning Based Trust Management Framework for Internet of Vehicles. Computers, Materials and Continua **68**(3), 4125–4142 (2021)

[43] Cheong, C., Song, Y., Cao, Y., Wang, H., Ni, Q., et al.: DCACA: Dual-Model Consensus-Based Anti-Risk Confidence Allocation Trust Management in IoVs. IEEE Internet of Things Journal (2024)

[44] Li, H., Shan, Q., Zhan, J., Wang, D.: 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), pp. 49–54 (2021). IEEE

[45] Wang, D., Chen, X., Wu, H., Yu, R., Zhao, Y.: 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), pp. 1950–1955 (2020). IEEE

[46] Yu, Y., Jia, Z., Tao, W., Xue, B., Lee, C.: An Efficient Trust Evaluation Scheme for Node Behavior Detection in the Internet of Things. Wireless Personal Communications **93**, 571–587 (2017)

[47] Siddiqui, S.A., Mahmood, A., Zhang, W.E., Sheng, Q.Z.: Machine Learning Based Trust Model for Misbehaviour Detection in Internet-of-Vehicles. In: Neural Information Processing: 26^{th} International Conference, International Conference on Neural Information Processing (ICONIP) 2019, Sydney, NSW, Australia, December 12–15, 2019, Proceedings, Part IV 26, pp. 512–520 (2019).

Springer

[48] Abidi, R., Azzouna, N.B., Trojet, W., Hoblos, G., Sahli, N.: A Study of Mechanisms and Approaches for IoV Trust Models Requirements Achievement. The Journal of Supercomputing **80**(3), 4157–4201 (2024)

[49] Mahmood, A., Siddiqui, S.A., Zhang, W.E., Sheng, Q.Z.: A Hybrid Trust Management Model for Secure and Resource Efficient Vehicular Ad Hoc Networks. In: 2019 20^{th} International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), pp. 154–159 (2019). IEEE

[50] Mao, M., Yi, P., Hu, T., Zhang, Z., Lu, X., Lei, J.: Hierarchical Hybrid Trust Management Scheme in SDN-Enabled VANETs. Mobile Information Systems **2021**(1), 7611619 (2021)

[51] Wang, Y., Zen, H., Sabri, M.F.M., Wang, X., Kho, L.C.: Towards Strengthening the Resilience of IoV Networks—A Trust Management Perspective. Future Internet **14**(7), 202 (2022)

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

[53] Vegni, A.M., Leoni, C., Loscri, V., Benslimane, A.: A Reputation-based Trustworthiness Concept for Wireless Networking in Vehicular Social Networks. IEEE Communications Magazine (2023)

[54] Shen, X., Ma, R.: A Blockchain Solution for the Internet of Vehicles with Better Filtering and Adaptive Capabilities. Sensors **25**(4), 1030 (2025)

[55] Huang, X., Yu, R., Kang, J., Zhang, Y.: Distributed Reputation Management for Secure and Efficient Vehicular Edge Computing and Networks. IEEE Access **5**, 25408–25420 (2017)

[56] Chen, J., Wang, X., Shen, X.S.: RTE: Rapid and Reliable Trust Evaluation for Collaborator Selection and Time-Sensitive Task Handling in Internet of Vehicles. IEEE Internet of Things Journal (2023)

[57] Rehman, A., Hassan, M.F., Hooi, Y.K., Qureshi, M.A., Shukla, S., Susanto, E., Rubab, S., Abdel-Aty, A.-H.: CTMF: Context-aware Trust Management Framework for Internet of Vehicles. IEEE Access **10**, 73685–73701 (2022)

[58] Rathee, G., Ahmad, F., Kurugollu, F., Azad, M.A., Iqbal, R., Imran, M.: CRT-BIoV: A Cognitive Radio Technique for Blockchain-enabled Internet of Vehicles. IEEE Transactions on Intelligent Transportation Systems **22**(7), 4005–4015 (2020)

[59] Jayasinghe, U., Lee, G.M., Um, T.-W., Shi, Q.: Machine Learning based Trust Computational Model for IoT Services. IEEE Transactions on Sustainable Computing **4**(1), 39–52 (2018)

[60] Rehman, G.-U., Ghani, A., Zubair, M., Naqvi, S.H.A., Singh, D., Muhammad, S.: IPS: Incentive and Punishment Scheme for Omitting Selfishness in the Internet of Vehicles (IoV). IEEE Access **7**, 109026–109037 (2019)

[61] Khan, S., Imtiaz, N., Biswas, A.K., Bin Siddique, Z., Khan, Q.A.: An Expert Hybrid Federated Learning and Trust Management for Security, Efficiency, and Power Optimization in Smart Health Systems. IEEE Access (2025)

[62] Siddiqui, S.A., Mahmood, A., Sheng, Q.Z., Suzuki, H., Ni, W.: Trust in vehicles: Toward Context-aware Trust and Attack Resistance for the Internet of Vehicles. IEEE Transactions on Intelligent Transportation Systems (2023)

[63] Wang, Y., Mahmood, A., Mohd Sabri, M.F., Zen, H.: Towards Distinguishing Trust based Attacks in an IoV Network. Journal of King Saud University Computer and Information Sciences **37**(4), 1–15 (2025)

[64] Wang, J., Yan, Z., Wang, H., Li, T., Pedrycz, W.: A Survey on Trust Models in Heterogeneous Networks. IEEE Communications Surveys and Tutorials **24**(4), 2127–2162 (2022)

[65] Yan, K., Ma, W., Yang, Q., Sun, S., Wang, W.: Info-Chain: Reputation-Based Blockchain for Secure Information Sharing in 6G Intelligent Transportation Systems. IEEE Internet of Things Journal (2023)

[66] Bangui, H., Buhnova, B., Kusnirakova, D., Halasz, D.: Trust Management in Social Internet of Things Across Domains. Internet of Things **23**, 100833 (2023)

[67] Gai, F., Zhang, J., Zhu, P., Jiang, X.: Trust on the Ratee: A Trust Management System for Social Internet of Vehicles. Wireless Communications and Mobile Computing **2017**(1), 7089259 (2017)

[68] Shokrollahi, S., Dehghan, M.: TGRV: A Trust-based Geographic Routing Protocol for VANETs. Ad Hoc Networks **140**, 103062 (2023)

[69] Du, G., Cao, Y., Li, J., Zhuang, Y., Chen, X., Li, Y., Chen, J.: A Blockchain-Based Trust-Value Management Approach for Secure Information Sharing in Internet of Vehicles. IEEE Internet of Things Journal **11**(1), 333–344 (2023)

[70] Ahmed, W., Di, W., Mukathe, D.: Blockchain-Assisted Privacy-Preserving and Context-Aware Trust Management Framework for Secure Communications in VANETs. Sensors **23**(12), 5766 (2023)

[71] Nabi, M.M., Shah, M.A.: A Fuzzy Approach to Trust Management in Fog Computing. In: 2022 24^{th} International Multitopic Conference (INMIC), pp. 1–6 (2022). IEEE

[72] Singh, C., Juneja, N., Kaur, S., *et al.*: A Case Study of Trust Management for Authorization and Authentication in IoT Devices Using Layered Approach. In: Society 5.0 and the Future of Emerging Computational Technologies, pp. 45–62 (2022). CRC Press

[73] Mahmood, A., Siddiqui, S.A., Sheng, Q.Z., Zhang, W.E., Suzuki, H., Ni, W.: Trust on Wheels: Towards Secure and Resource Efficient IoV Networks. Computing **104**(6), 1337–1358 (2022)

[74] Sagar, S., Mahmood, A., Sheng, Q.Z.: Towards Resilient Social IoT Sensors and Networks: A Trust Management Approach, (2024). Springer

[75] Lenard, T., Collen, A., Benyahya, M., Nijdam, N.A., Genge, B.: Exploring Trust Modelling and Management Techniques in the Context of Distributed Wireless Networks: A Literature Review. IEEE Access (2023)

[76] Yin, R., Ma, X., Yuan, H., Zhai, M., Guo, C.: A Distributed Adaptive Routing Against Selective Forwarding Attack in Scale-free Network Considering Cascading Failure. Journal of Complex Networks **11**(3), 021 (2023)

[77] Ayed, S., Hbaieb, A., Chaari, L.: Blockchain and Trust-based Clustering Scheme for the IoV. Ad Hoc Networks **142**, 103093 (2023)

[78] Ayobi, S., Wang, Y., Rabbani, M., Dorri, A., Jelodar, H., Huang, H., Yarmohammadi, S.: A Lightweight Blockchain-based Trust Model for Smart Vehicles in Vanets. In: Security, Privacy, and Anonymity in Computation, Communication, and Storage: 13^{th} International Conference, SpaCCS 2020, Nanjing, China, December 18-20, 2020, Proceedings 13, pp. 276–289 (2021). Springer

[79] Kudva, S., Badsha, S., Sengupta, S., La, H., Khalil, I., Atiquzzaman, M.: A Scalable Blockchain Based Trust Management in VANET Routing Protocol. Journal of Parallel and Distributed Computing **152**, 144–156 (2021)

[80] Nath, H.J., Choudhury, H.: Privacy-Preserving Authentication Protocols in Vanet. SN Computer Science **4**(5), 589 (2023)

[81] Zhao, Y., Wang, Y., Wang, P., Yu, H.: PBTM: A Privacy-Preserving Announcement Protocol With Blockchain-Based Trust Management for IoV. IEEE Systems Journal **16**(2), 3422–3432 (2022) https://doi.org/10.1109/JSYST.2021.3078797

[82] Sun, S., Fan, X., Xiao, Y.: Trust Model Based on Recommendation Filtering in Internet of Vehicles. In: 2023 2^{nd} International Conference on Computing,

Communication, Perception and Quantum Technology (CCPQT), pp. 364–369 (2023). IEEE

[83] Tripathi, K.N., Yadav, A.M., Nagar, S., Sharma, S.: ReTrust: Reliability and Recommendation Trust-based Scheme for Secure Data Sharing among Internet of Vehicles (IOV). Wireless Networks **29**(6), 2551–2575 (2023)

[84] Etzel, R., Narine, O., Georgiou, K., Diakogeorgios, T., Usman, J., Ghazizadeh, P.: Effectiveness of Trust-based Authentication in Vehicular Cloud Computing. In: 2023 International Symposium on Networks, Computers and Communications (ISNCC), pp. 1–5 (2023). IEEE

[85] Ghaleb, F.A., Maarof, M.A., Zainal, A., Rassam, M.A., Saeed, F., Alsaedi, M.: Context-aware Data-centric Misbehaviour Detection Scheme for Vehicular Ad Hoc Networks using Sequential Analysis of the Temporal and Spatial Correlation of the Consistency between the Cooperative Awareness Messages. Vehicular Communications **20**, 100186 (2019)

[86] Vetter, T.R.: Descriptive Statistics: Reporting the Answers to the 5 Basic Questions of Who, What, Why, When, Where, and a Sixth, So What? Anesthesia & Analgesia **125**(5), 1797–1802 (2017)

[87] Gazdar, T., Alboqomi, O., Munshi, A.: A Decentralized Blockchain-based Trust Management Framework for Vehicular Ad Hoc Networks. Smart Cities **5**(1), 348–363 (2022)

[88] Chen, X., Wang, L.: A Trust Evaluation Framework using in a Vehicular Social Environment. In: 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 1004–1005 (2017). https://doi.org/10.1109/INFCOMW.2017.8116532

[89] Shen, J., Wang, C., Lai, J.-F., Xiang, Y., Li, P.: CATE: Cloud-Aided Trustworthiness Evaluation Scheme for Incompletely Predictable Vehicular Ad Hoc Networks. IEEE Transactions on Vehicular Technology **68**(11), 11213–11226 (2019) https://doi.org/10.1109/TVT.2019.2938968

[90] Li, Q., Malip, A., Martin, K.M., Ng, S.-L., Zhang, J.: A Reputation-Based Announcement Scheme for VANETs. IEEE Transactions on Vehicular Technology **61**(9), 4095–4108 (2012) https://doi.org/10.1109/TVT.2012.2209903

[91] Cheng, H., Zhang, X., Yang, J., Liu, Y.: PPRT: Privacy Preserving and Reliable Trust-Aware Platoon Recommendation Scheme in IoV. IEEE Systems Journal **17**(3), 4922–4933 (2023) https://doi.org/10.1109/JSYST.2023.3264773

[92] Liu, Y., Li, K., Jin, Y., Zhang, Y., Qu, W.: A Novel Reputation Computation Model Based on Subjective Logic for Mobile Ad Hoc Networks. Future Generation Computer Systems **27**(5), 547–554 (2011)

[93] Zhang, T., Li, L., Liu, D., Si, Q.: A Subjective Logic-based Reputation Management Scheme for Highway Internet of Vehicles. In: Fourth International Conference on Computer Science and Communication Technology (ICCSCT 2023), vol. 12918, pp. 413–422 (2023). SPIE

[94] Mahmood, A., Sheng, Q.Z., Zhang, W.E., Wang, Y., Sagar, S.: Toward a Distributed Trust Management System for Misbehavior Detection in the Internet of Vehicles. ACM Transactions on Cyber-Physical Systems **7**(3), 1–25 (2023)

[95] Kang, J., Yu, R., Huang, X., Wu, M., Maharjan, S., Xie, S., Zhang, Y.: Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks. IEEE Internet of Things Journal **6**(3), 4660–4670 (2019) https://doi.org/10.1109/JIOT.2018.2875542

[96] Liu, Q., Gong, J., Liu, Q.: Blockchain-assisted Reputation Management Scheme for Internet of Vehicles. Sensors **23**(10), 4624 (2023)

[97] Cheng, T., Liu, G., Yang, Q., Sun, J.: Trust Assessment in Vehicular Social Network Based on Three-Valued Subjective Logic. IEEE Transactions on Multimedia **21**(3), 652–663 (2019) https://doi.org/10.1109/TMM.2019.2891417

[98] Li, J., Xing, R., Su, Z., Zhang, N., Hui, Y., Luan, T.H., Shan, H.: Trust Based Secure Content Delivery in Vehicular Networks: A Bargaining Game Theoretical Approach. IEEE Transactions on Vehicular Technology **69**(3), 3267–3279 (2020) https://doi.org/10.1109/TVT.2020.2964685

[99] Tian, Z., Gao, X., Su, S., Qiu, J., Du, X., Guizani, M.: Evaluating Reputation Management Schemes of Internet of Vehicles Based on Evolutionary Game Theory. IEEE Transactions on Vehicular Technology **68**(6), 5971–5980 (2019) https://doi.org/10.1109/TVT.2019.2910217

[100] Halabi, T., Zulkernine, M.: Trust-Based Cooperative Game Model for Secure Collaboration in the Internet of Vehicles. In: 2019 IEEE International Conference on Communications (ICC), pp. 1–6 (2019). https://doi.org/10.1109/ICC.2019.8762069

[101] Soleymani, S.A., Abdullah, A.H., Zareei, M., Anisi, M.H., Vargas-Rosales, C., Khurram Khan, M., Goudarzi, S.: A Secure Trust Model Based on Fuzzy Logic in Vehicular Ad Hoc Networks With Fog Computing. IEEE Access **5**, 15619–15629 (2017) https://doi.org/10.1109/ACCESS.2017.2733225

[102] Miao, T., Shen, J., Lai, C.-F., Ji, S., Wang, H.: Fuzzy-Based Trustworthiness Evaluation Scheme for Privilege Management in Vehicular Ad Hoc Networks. IEEE Transactions on Fuzzy Systems **29**(1), 137–147 (2021) https://doi.org/10.1109/TFUZZ.2020.3030490

[103] Sheikh, M.S., Liang, J., Wang, W.: Security and Privacy in Vehicular Ad Hoc

Network and Vehicle Cloud Computing: A Survey. Wireless Communications and Mobile Computing **2020**(1), 5129620 (2020)

[104] Kapassa, E., Themistocleous, M., Christodoulou, K., Iosif, E.: Blockchain Application in Internet of Vehicles: Challenges, Contributions and Current Limitations. Future Internet **13**(12), 313 (2021)

[105] Masmoudi, M., Amous, I., Zayani, C.A., Sèdes, F.: Trust Attack Prevention Based on Spark-Blockchain in Social IoT: A Survey. International Journal of Information Security, 1–20 (2024)

[106] Gupta, R., *et al.*: A Survey on Machine Learning Approaches and its Techniques. In: 2020 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), pp. 1–6 (2020). IEEE

[107] Alzubi, J., Nayyar, A., Kumar, A.: Machine Learning from Theory to Algorithms: An Overview. In: Journal of Physics: Conference Series, vol. 1142, p. 012012 (2018). IOP Publishing

[108] Badillo, S., Banfai, B., Birzele, F., Davydov, I.I., Hutchinson, L., Kam-Thong, T., Siebourg-Polster, J., Steiert, B., Zhang, J.D.: An Introduction to Machine Learning. Clinical Pharmacology and Therapeutics **107**(4), 871–885 (2020)

[109] Das, K., Behera, R.N.: A Survey on Machine Learning: Concept, Algorithms and Applications. International Journal of Innovative Research in Computer and Communication Engineering **5**(2), 1301–1309 (2017)

[110] Amiri, S., Salimzadeh, S., Belloum, A.S.: A Survey of Scalable Deep Learning Frameworks. In: 2019 15^{th} International Conference on eScience, pp. 650–651 (2019). IEEE

[111] Alom, M.Z., Taha, T.M., Yakopcic, C., Westberg, S., Sidike, P., Nasrin, M.S., Hasan, M., Van Essen, B.C., Awwal, A.A., Asari, V.K.: A State-of-the-Art Survey on Deep Learning Theory and Architectures. Electronics **8**(3), 292 (2019)

[112] Pouyanfar, S., Sadiq, S., Yan, Y., Tian, H., Tao, Y., Reyes, M.P., Shyu, M.-L., Chen, S.-C., Iyengar, S.S.: A Survey on Deep Learning: Algorithms, Techniques, and Applications. ACM Computing Surveys (CSUR) **51**(5), 1–36 (2018)

[113] Dong, S., Wang, P., Abbas, K.: A Survey on Deep Learning and its Applications. Computer Science Review **40**, 100379 (2021)

[114] Qiang, W., Zhongli, Z.: Reinforcement Learning Model, Algorithms and its Application. In: 2011 International Conference on Mechatronic Science, Electric Engineering and Computer (MEC), pp. 1143–1146 (2011). IEEE

[115] Padakandla, S.: A Survey of Reinforcement Learning Algorithms for Dynamically Varying Environments. ACM Computing Surveys (CSUR) **54**(6), 1–25 (2021)

[116] Utic, Z., Ramachandran, K.: A Survey of Reinforcement Learning in Intrusion Detection. In: 2022 1^{st} International Conference on AI in Cybersecurity (ICAIC), pp. 1–8 (2022). IEEE

[117] Wang, X., Wang, S., Liang, X., Zhao, D., Huang, J., Xu, X., Dai, B., Miao, Q.: Deep Reinforcement Learning: A Survey. IEEE Transactions on Neural Networks and Learning Systems (2022)

[118] Nguyen, T.T., Reddi, V.J.: Deep Reinforcement Learning for Cyber Security. IEEE Transactions on Neural Networks and Learning Systems **34**(8), 3779–3795 (2021)

[119] Siddiqui, S.A., Mahmood, A., Sheng, Q.Z., Suzuki, H., Ni, W.: Towards a Machine Learning Driven Trust Management Heuristic for the Internet of Vehicles. Sensors **23**(4), 2325 (2023)

[120] Wang, Y., Mahmood, A., Sabri, M.F.M., Zen, H., Kho, L.C.: MESMERIC: Machine Learning-Based Trust Management Mechanism for the Internet of Vehicles. Sensors **24**(3), 863 (2024)

[121] Alharthi, A., Ni, Q., Jiang, R., Khan, M.A.: A Computational Model for Reputation and Ensemble-Based Learning Model for Prediction of Trustworthiness in Vehicular Ad Hoc Network. IEEE Internet of Things Journal **10**(20), 18248–18258 (2023) https://doi.org/10.1109/JIOT.2023.3279950

[122] Xu, Q., Zhang, L., Qin, X., Zhou, Y.: A Novel Machine Learning-Based Trust Management Against Multiple Misbehaviors for Connected and Automated Vehicles. IEEE Transactions on Intelligent Transportation Systems, 1–16 (2024) https://doi.org/10.1109/TITS.2024.3422423

[123] Sharma, P., Liu, H.: A Machine-Learning-Based Data-Centric Misbehavior Detection Model for Internet of Vehicles. IEEE Internet of Things Journal **8**(6), 4991–4999 (2021) https://doi.org/10.1109/JIOT.2020.3035035

[124] Su, Z., Cheng, R., Li, C., Chen, M., Zhu, J., Long, Y.: Federated Learning and Reputation-based Node Selection Scheme for Internet of Vehicles. Electronics **14**(2), 303 (2025)

[125] Din, I.U., Khan, K.H., Almogren, A., Guizani, M.: Machine Learning for Trust in Internet of Vehicles and Privacy in Distributed Edge Networks. IEEE Internet of Things Journal, 1–1 (2025) https://doi.org/10.1109/JIOT.2025.3547595

[126] Karmakar, G., Chowdhury, A., Das, R., Kamruzzaman, J., Islam, S.: Assessing

Trust Level of a Driverless Car Using Deep Learning. IEEE Transactions on Intelligent Transportation Systems **22**(7), 4457–4466 (2021) https://doi.org/10.1109/TITS.2021.3059261

[127] Khan, S., Khan, S., Sulaiman, A., Al Reshan, M.S., Alshahrani, H., Shaikh, A.: Deep Neural Network and Trust Management Approach to Secure Smart Transportation Data in Sustainable Smart Cities. ICT Express (2024)

[128] Tripathi, K.N., Sharma, S.C.: An Optimal Trust and Secure Model using Deep Metric Learning for Fog-based VANET. Transactions on Emerging Telecommunications Technologies **34**(8), 4805 (2023)

[129] Tripathi, K.N., Yadav, A.M., Sharma, S.: Fuzzy and Deep Belief Network based Malicious Vehicle Identification and Trust Recommendation Framework in VANETs. Wireless Personal Communications **124**(3), 2475–2504 (2022)

[130] Kaur, G., Kakkar, D.: Hybrid Optimization Enabled Trust-based Secure Routing with Deep Learning-based Attack Detection in VANET. Ad Hoc Networks **136**, 102961 (2022)

[131] Renjith, P., Balasubramani, S., Ramesh, K., Patnala, E.: An Initial Risk Assessment for Multimodal with LSTM-Based Trust Evaluation Framework for Autonomous Vehicle Security. Springer Nature Computer Science **6**(2), 1–15 (2025)

[132] Sontakke, P.V., Chopade, N.B.: Hybrid DNN-BiLSTM-aided Intrusion Detection and Trust-clustering and Routing-based Intrusion Prevention System in VANET. Journal of Control and Decision **12**(2), 209–226 (2025)

[133] Jang, S.Y., Park, S.K., Cho, J.H., Lee, D.: CARES: Context-aware Trust Estimation for Realtime Crowdsensing Services in Vehicular Edge Networks. ACM Transactions on Internet Technology **22**(4), 1–24 (2022)

[134] Guo, J., Li, X., Liu, Z., Ma, J., Yang, C., Zhang, J., Wu, D.: TROVE: A Context-Awareness Trust Model for VANETs Using Reinforcement Learning. IEEE Internet of Things Journal **7**(7), 6647–6662 (2020) https://doi.org/10.1109/JIOT.2020.2975084

[135] Gyawali, S., Qian, Y., Hu, R.Q.: Deep Reinforcement Learning Based Dynamic Reputation Policy in 5G Based Vehicular Communication Networks. IEEE Transactions on Vehicular Technology **70**(6), 6136–6146 (2021) https://doi.org/10.1109/TVT.2021.3079379

[136] Zhang, D., Yu, F.R., Yang, R., Zhu, L.: Software-Defined Vehicular Networks With Trust Management: A Deep Reinforcement Learning Approach. IEEE Transactions on Intelligent Transportation Systems **23**(2), 1400–1414 (2022) https://doi.org/10.1109/TITS.2020.3025684

[137] Sarker, O., Shen, H., Babar, M.A.: Reinforcement Learning Based Neighbour Selection for VANET with Adaptive Trust Management. In: 2023 IEEE 22^{nd} International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 585–594 (2023). https://doi.org/10.1109/TrustCom60117.2023.00091

[138] Chen, H., Fu, X., Yuan, Q., Zhuang, Z., Kang, J., Liu, Z., Wang, J., Niyato, D.: Trust Model-Based Consensus Optimization for Vehicle Platooning Networks: A Novel Deep Reinforcement Learning Approach With GenAI. IEEE Transactions on Intelligent Transportation Systems, 1–16 (2025) https://doi.org/10.1109/TITS.2025.3559672

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

[140] Khan, I.A., Keshk, M., Hussain, Y., Pi, D., Li, B., Kousar, T., Ali, B.S.: A Context-aware Zero Trust-based Hybrid Approach to IoT-based Self-driving Vehicles Security. Ad Hoc Networks **167**, 103694 (2025)

[141] Jing, T., Liu, Y., Wang, X., Gao, Q.: Joint Trust Management and Sharing Provisioning in IoV-Based Urban Road Network. Wireless Communications and Mobile Computing **2022**(1), 6942120 (2022)

[142] Lone, F.R., Verma, H.K.: MP-TMD: A Multidimensional Plausibility-driven Cooperative Trust Model for Multiple Misbehaviour Detection in Intelligent Transportation Systems. Cluster Computing **28**(3), 181 (2025)

[143] Mianji, E.M., Fardad, M., Muntean, G.-M., Tal, I.: A Survey on Multiagent Reinforcement Learning Applications in the Internet of Vehicles. In: 2024 IEEE 99^{th} Vehicular Technology Conference (VTC2024-Spring), pp. 1–7 (2024)

[144] Man, S.S., Ding, M., Li, X., Chan, A.H.S., Zhang, T.: Acceptance of Highly Automated Vehicles: The Role of Facilitating Condition, Technology Anxiety, Social Influence and Trust. International Journal of Human–Computer Interaction **41**(6), 3684–3695 (2025)

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

[146] Singh, P.K., Singh, R., Nandi, S.K., Ghafoor, K.Z., Rawat, D.B., Nandi, S.: Blockchain-based Adaptive Trust Management in Internet of Vehicles Using Smart Contract. IEEE Transactions on Intelligent Transportation Systems **22**(6), 3616–3630 (2020)

[147] Ullah, I., Deng, X., Pei, X., Mushtaq, H., Uzair, M.: IoV-SFL: A Blockchain-based Federated Learning Framework for Secure and Efficient Data Sharing in the Internet of Vehicles. Peer-to-Peer Networking and Applications **18**(1), 1–20 (2025)

[148] Ali, E.S., Hasan, M.K., Hassan, R., Saeed, R.A., Hassan, M.B., Islam, S., Nafi, N.S., Bevinakoppa, S.: Machine Learning Technologies for Secure Vehicular Communication in Internet of Vehicles: Recent Advances and Applications. Security and Communication Networks **2021**(1), 8868355 (2021)

[149] Danba, S., Bao, J., Han, G., Guleng, S., Wu, C.: Toward Collaborative Intelligence in IoV Systems: Recent Advances and Open Issues. Sensors **22**(18), 6995 (2022)

[150] Ning, P., Wang, H., Tang, T., Zhang, J., Du, H., Niyato, D., Yu, F.R.: Diffusion-based Deep Reinforcement Learning for Resource Management in Connected Construction Equipment Networks: A Hierarchical Framework. IEEE Transactions on Wireless Communications (2025)

[151] Arshad, Q.-u.-A., Khan, W.Z., Azam, F., Khan, M.K., Yu, H., Zikria, Y.B.: Blockchain-based Decentralized Trust Management in IoT: Systems, Requirements and Challenges. Complex and Intelligent Systems **9**(6), 6155–6176 (2023)

[152] Jyothi, N., Patil, R.: An Optimized Deep Learning-based Trust Mechanism In VANET for Selfish Node Detection. International Journal of Pervasive Computing and Communications **18**(3), 304–318 (2021)

[153] Firdaus, M., Rahmadika, S., Rhee, K.-H.: Decentralized Trusted Data Sharing Management on Internet of Vehicle Edge Computing (IoVEC) Networks using Consortium Blockchain. Sensors **21**(7), 2410 (2021)

[154] Xu, Y., Yu, E., Song, Y., Tong, F., Xiang, Q., He, L.: $\mathcal{R}$-Tracing: Consortium Blockchain-Based Vehicle Reputation Management for Resistance to Malicious Attacks and Selfish Behaviors. IEEE Transactions on Vehicular Technology **72**(6), 7095–7110 (2023)

[155] Tang, F., Kawamoto, Y., Kato, N., Liu, J.: Future Intelligent and Secure Vehicular Network Toward 6G: Machine-learning Approaches. Proceedings of the IEEE **108**(2), 292–307 (2019)

[156] Du, J., Han, G., Lin, C., Martínez-García, M.: LTrust: An Adaptive Trust Model Based on LSTM for Underwater Acoustic Sensor Networks. IEEE Transactions on Wireless Communications **21**(9), 7314–7328 (2022)

[157] Iqbal, R., Butt, T.A., Afzaal, M., Salah, K.: Trust Management in Social Internet of Vehicles: Factors, Challenges, Blockchain, and Fog Solutions. International

Journal of Distributed Sensor Networks **15**(1), 1550147719825820 (2019)

[158] Yin, D., Gong, B.: Auto-Adaptive Trust Measurement Model Based on Multidimensional Decision-Making Attributes for Internet of Vehicles. Wireless Communications and Mobile Computing **2022**(1), 3537771 (2022)

[159] Li, Y., Xie, Y., Liu, Q., Li, J.: DMTAS-VB: Dynamic Model Update-based Trust Assessment Strategy for VANETs Considering Blockchain. IEEE Internet of Things Journal (2025)

[160] Bampatsikos, M., Politis, I., Xenakis, C., CA Thomopoulos, S.: Solving the Cold Start Problem in Trust Management in IoT. In: Proceedings of the 16^{th} International Conference on Availability, Reliability and Security, pp. 1–9 (2021)

[161] Alboqomi, O., Gazdar, T., Munshi, A.: A New Blockchain-based Trust Management Protocol for Vehicular Ad Hoc Networks. In: Proceedings of the 4^{th} International Conference on Future Networks and Distributed Systems, pp. 1–5 (2020)

[162] Siddiqui, S.A., Mahmood, A., Sheng, Q.Z., Suzuki, H., Ni, W.: A Survey of Trust Management in the Internet of Vehicles. Electronics **10**(18), 2223 (2021)