



## REVIEW

# Cyber security analysis of connected vehicles

Maria Drolence Mwanje<sup>1</sup> | Omprakash Kaiwartya<sup>1</sup>  | Mohammad Aljaidi<sup>2</sup> | Yue Cao<sup>3</sup> | Sushil Kumar<sup>4</sup> | Devki Nandan Jha<sup>5</sup> | Abdallah Naser<sup>1</sup> | Jaime Lloret<sup>6</sup> 

<sup>1</sup>Department of Computer Science, Nottingham Trent University, Nottingham, UK

<sup>2</sup>Computer Science Department, Faculty of Information Technology, Zarqa University, Zarqa, Jordan

<sup>3</sup>School of Cyber Science and Engineering, Wuhan University, Wuhan, China

<sup>4</sup>School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India

<sup>5</sup>School of Computing, Newcastle University, Newcastle, UK

<sup>6</sup>Research Institute for Integrated Management of Coastal Areas, Universitat Politècnica de Valencia, Grao de Gandia, Spain

## Correspondence

Omprakash Kaiwartya, Department of Computer Science, Nottingham Trent University, Nottingham, NG11 8NS, UK.

Email: [omprakash.kaiwartya@ntu.ac.uk](mailto:omprakash.kaiwartya@ntu.ac.uk)

## Funding information

Nottingham Trent University UK

## Abstract

The sensor-enabled in-vehicle communication and infrastructure-centric vehicle-to-everything (V2X) communications have significantly contributed to the spark in the amount of data exchange in the connected and autonomous vehicles (CAV) environment. The growing vehicular communications pose a potential cyber security risk considering online vehicle hijacking. Therefore, there is a critical need to prioritize the cyber security issues in the CAV research theme. In this context, this paper presents a cyber security analysis of connected vehicle traffic environments (CyACV). Specifically, potential cyber security attacks in CAV are critically investigated and validated via experimental data sets. Trust in V2X communication for connected vehicles is explored in detail focusing on trust computation and trust management approaches and related challenges. A wide range of trust-based cyber security solutions for CAV have been critically investigated considering their strengths and weaknesses. Open research directions have been highlighted as potential new research themes in CAV cyber security area.

## 1 | INTRODUCTION

The need to transform the transport sector has led to increasing innovations in vehicle technology, such as connected and autonomous vehicles. According to the report published by the statistical research department [1], over 71% of vehicles produced in the UK are connected, and by 2026 there is a projection of 100% connected vehicle production. These connected vehicles are highly equipped with technology, such as sensors that capture the status of the vehicle environment to aid in automatic decision-making. This collected data is processed and communicated to other vehicles and in-vehicle applications, mobile devices, third-party service providers and external infrastructure. On a daily basis, these connected vehicles are estimated to communicate and exchange data worth 25 gigabytes. [2] This data includes biometrics, driver's behaviour, location, and car system/status, used by internal attackers to

influence decision-making. For example, an attacker can hijack a CAV and send false observations to neighbouring vehicles forcing them to change behaviour. Furthermore, when such data is processed it can be linked to personally identifiable information such as driver and passenger details and health information.

However, safety and efficiency-oriented sustainability in transportation via connected vehicles come with a greater risk of online vehicle hijacking [3]. Ranging from unauthorized accessing of wheels, disabling brakes, locking doors, engine disruption to path forging, location and identity manipulation, denial of traffic service, and tracking are a few examples of online vehicle hijacking. We have witnessed security threat in computer networks in terms of unauthorized system and application hijacking in a greater scale targeting individuals, specific organizations or even entire systems of a country. So, there is also necessity to prepare for online vehicle hijacking in CAV

This is an open access article under the terms of the [Creative Commons Attribution-NonCommercial-NoDerivs](https://creativecommons.org/licenses/by-nc-nd/4.0/) License, which permits use and distribution in any medium, provided the original work is properly cited, the use is non-commercial and no modifications or adaptations are made.

© 2024 The Authors. *IET Intelligent Transport Systems* published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology.

environment, concerning trustworthy, ubiquitous, and seamless connected vehicle communications [4].

To support the drive towards secure communication and decision making in self-driving cars, numerous studies have been conducted that elucidate the concept of security in CAV vehicle-to-everything communication. A study by [4] explores the security of CAV in-vehicle components and suggests a secure network architecture. The researchers classify and identify the characteristics of the in-vehicle components with a comprehensive review of the challenges, possible attack entry points, and solutions. The systematic survey is limited as it focuses on the security of in-vehicle components, thus ignoring other components of the V2X communication. Furthermore, there is no validation of the suggested secure network architecture. The authors in [5] provide a systematic review of autonomous vehicle cyber security attacks and defence strategies classified into anomaly detection, intrusion detection, and security architecture. The research focuses on attacks on autonomous components such as the driving and control systems and V2X communications. Researchers [6] explore the vehicular communication cybersecurity challenges and propose a three-layer security framework that identifies security threats in connected and autonomous vehicles. A survey by [7] explores the risks and vulnerabilities in CAVs and provides possible mitigation. Works by [8] provides a comprehensive review of the security challenges in CAVs and classifies attacks into V2X communication, in-vehicle and other attacks. More studies have been conducted to improve cyber security attack prevention and detection techniques in connected and autonomous vehicles.

The research efforts detailed in [9] recommend the deployment of cryptography and non-cryptography mechanisms, such as trust-based techniques, which are a tradeoff between performance and time [10]. The cryptographic mechanisms are strong and efficient against external attacks. However, they are ineffective if authorized CAVs (users) become malicious and require high computational resources, leading to delayed decision-making. To bridge this gap, recent studies focus on building trust-based security models because of their capability to identify internal attackers and the less computational resources.

In this context, this paper focuses on providing a clear understanding of the V2X communication cycle and an extensive review of the trust-based security mechanisms guided by the research questions below.

- What components within the CAV environment support V2X communication?
- What are the current cyber security threats, vulnerabilities and cyber attacks in V2X communication under CAV environments?
- What are the potential metrics and models for measuring trust while driving in a CAV environment?

Below is a summary of the contributions of the paper:

- 1) A review of the CAV communication cycle and the components that support V2X communication.

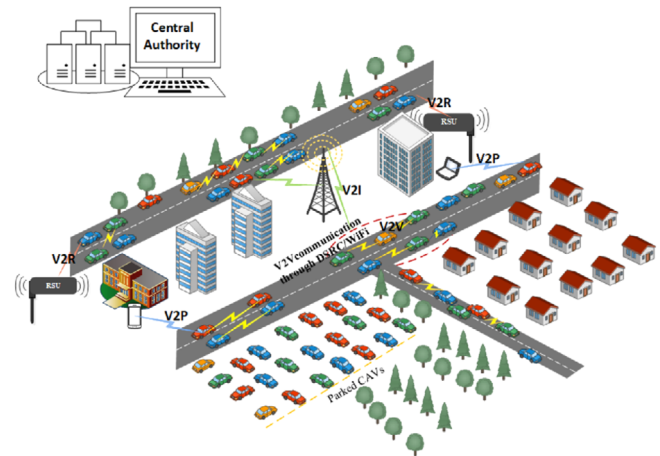


FIGURE 1 A representation of a CAV environment.

- 2) A review of the vulnerabilities and cyber attacks in CAVs with a practical illustration of the replay, DoS, and false injection attacks.
- 3) A critical analysis of the current trust-based security mechanisms in CAVs categorized according to the suggested trust taxonomy.
- 4) A critical review of the current environments such as blockchain, edge and cloud in which CAVs are implemented and the existing research within those environments.
- 5) Finally, we identify the current gaps and establish open issues that require further research.

The rest of the article is organized as follows. Section 2—CAV cyber infrastructure. Section 3—Cyber attacks in CAVs. Section 4—Trust in connected vehicle communication. Sections 5—Related literature on trust-based security for CAV. Section 6—Open research issues in CAV cyber security with the conclusion in Section 7.

## 2 | CAV CYBER INFRASTRUCTURES

The following section provides an overview of the CAV communication infrastructure and its various components that support internal and external communication illustrated in Figure 1. Additionally, Table 1 provides a summary of the attacks against the V2X communication components and the possible mitigation.

### 2.1 | The sensing and perception layer

At the beginning of the communication cycle, data from different sensors is fused together to provide an accurate representation of the vehicle environment. This data is then sent to other vehicles as V2X messages for correct decision-making. Component malfunction, obstacles, and malicious users can influence the accuracy of this data described in the below section.

**TABLE 1** A summary of the CAV V2X communication components vulnerabilities.

Structure	Component	Attacks/threats	Mitigation
Sensing unit	Camera	Camera binding and confusion of controls [11].	Redundancy, machine learning, infra red light filters [11, 16]
	Ultrasonic sensors	Spoofing, jamming, and acoustic quieting [11, 16–18].	Redundancy, machine learning [11, 16–18].
	LiDAR and Radar	LiDAR spoofing and jamming, signal analysis, relay, Radar spoofing and jamming. [11, 13–16, 19].	Redundancy (sensor fusion) randomization of measurements [11, 13–16, 19].
	GPS Receivers	GPS spoofing and jamming, signal analysis [20–23]	Location verification schemes. [20–23]
Remote technologies	IEEE 802.11	Limited/short coverage, high latency (poor performance) in high-density environments, scalability issues, limited bandwidth for safety applications [24, 25].	Protocol/standard improvement-IEEE 802.11bd, congestion control mechanisms [26], Inter-networking with cellular. [27]
	Cellular- LTE	Centralized nature causing delays, LTE channel spoofing [28], message broadcast exposing-eavesdropping [29], de-synchronization attack in LTE [30]	Message reception relay algorithms and congestion management techniques [31], Protocol advancement-(release12-release 19), networking with IEEE 802.p [27], frequency monitoring [28],

### 2.1.1 | Cameras

Cameras support execution of independent tasks in CAVs such as parking, lane departure and traffic light recognition [11]. They offer a high level of accuracy during object detection; however, these infringe on people's privacy, and their operation is affected by light. Attackers can exploit the light limitation in cameras by placing high-emitting light objects along the road that blind the camera and confuse the auto controls [12]. Furthermore, the processing of data captured from the cameras is computationally expensive. To mitigate the attacks on cameras, infrared filters are deployed to control light intensity and multiple cameras for redundancy. [13].

### 2.1.2 | LiDAR and radar

The radio detection and ranging (radar) sensor helps CAVs to identify objects at a distance for feature evaluation such as speed. Radar systems consist of four components: a processor, a receiver, an antenna (transmitting and receiving) and a transmitter. During the operation, electromagnetic waves are released by the vehicle toward the surrounding target. The electromagnetic waves then reflect off the target back to the receiver. The processor can then estimate the surrounding vehicle's angle, position and velocity. Light detection and ranging (LiDAR) technology calculates the distance of identified objects in the environment using laser light pulses. The LiDAR sensor emits these laser light pulses to the surrounding target object which reflects back to the sensor. The distance between the target object and the sensor is calculated based on the light pulse travel time to and back from the LiDAR sensor. Previous studies have investigated the threats to LiDAR and Radar sensors. A study

by [13] investigates the relaying and spoofing signal attacks in LiDAR a huge risk to collision avoidance systems. The authors suggest redundancy and random probing as countermeasures to the threats. Researchers in [11] perform experiments to investigate the accuracy of LiDAR and Radar data and suggest redundancy and randomization as countermeasures. More studies [14, 15] have also evaluated the threats to LiDAR and Radar and can be referred to for further information.

### 2.1.3 | Ultrasonic sensors

Ultrasonic sensors use sound waves to calculate the distance between themselves and surrounding objects. As soon as an object receives the sound waves, they are sent back to the sensor. The distance between the sensor and the environment depends on when the first object echoes back to the sensor and the echoes are ignored [11]. Ultrasonic sensor readings are highly affected by noise, and only the nearest small obstacles are considered [16]. The authors in [17] analyze the security of ultrasonic sensors in autonomous vehicles and suggest the implementation of multiple sensors to check data consistency across all the sensors and physical shift authentication through random probing. Another study by [18] suggests additional countermeasures such as machine learning and strong noise detection to prevent jamming or constant signal attacks in ultrasonic sensors.

### 2.1.4 | GPS

CAVs use global navigation satellite unit sensors (GNSS) to navigate from one point to another. The GNSS use data from the

signals broadcast by the satellite. This data can be accessed and manipulated by malicious users, leading to incorrect directions and routing.

Numerous studies [22, 32–34] have investigated GPS attacks in vehicles such as spoofing, jamming, and provided possible mitigation and detection models. A recent study by [35] suggested a GPS spoofing detection model that learns from historical trajectories. The researchers use vehicle dynamics and entropy reinforcement learning to identify abnormal trajectories. Another study by [22] provides a GPS spoofing model that fuses the inbuilt sensor data to identify location and compares this with the data from the GPS receiver. Besides the above-mentioned threats the presence of obstacles such as tunnels and tall buildings affects the performance of the GPS receivers [21]. In conclusion, studies on CAV sensor attacks recommend redundancy(sensor fusion) [34] and randomization as prevention/mitigation techniques and machine learning models to detect abnormal behaviour.

## 2.2 | V2X communication remote technologies

V2X communication supports the exchange of information between the internal components of the vehicle and the external terminals. This communication is facilitated by VANET technology frequently categorized into vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). Additional categories exist, such as vehicle-to-pedestrian (V2P), vehicle-to-sensors (V2S), vehicle-to-roadside units (V2R) and vehicle-to-ecosystem (V2E) [36]. To support the possibility of exchanging fused sensor data as V2X messages, standardization bodies in different countries have proposed approaches that define the communication syntax and rules.

### 2.2.1 | IEEE 802.11p communication standard

The IEEE 802.11p is the basis of the intelligent transportation system (ITS) G5 and dedicated short-range communication (DSRC) protocols in Europe and United States respectively. These communication standards were published by standardization bodies such as the European Telecommunications Standards Institute (ETSI) in Europe and Institute of Electrical and Electronics Engineers (IEEE) in US. Figure 2 is a summary of how the IEEE 802.11p/bd vehicular communication protocols differ. Additional standards defined by different bodies exist such as ITS Connect in Japan but this paper will focus on ITS G5 and DSRC. These standards operate based on a spectrum band that varies in different countries and supports different applications. The ETSI EN 302 637-2 defines V2V and V2I communications. V2V communication enables vehicles to exchange information with other vehicles within proximity (single-hop neighbour) on the network for informed decision-making. This exchange is a periodic broadcast of a cooperative awareness message (CAM) to other vehicle OBUs informing them of their environment. [37] The CAM contains

data about vehicles' heading, speed, acceleration, and position. According to the European Telecommunication Standard Institute, [38] the CAM basic service at the facilities layer constructs the CAM once its generation is triggered under a specific set of rules. The generation of the CAM is according to a specified format which consists of a header and a body defined in ETSI TS 102 637-2 standard. The CAM is encoded and sent to the network and transport layers for dissemination. This dissemination is a one-to-many (broadcast) defined by the ITS G5A network architecture. Once the CAM is received by other vehicles it is decoded by the CAM basic service and a local dynamic map is generated for storage and update of the status information. Furthermore, the standard categorizes communication between vehicles and infrastructure such as smart road infrastructure and road side units (RSUs) as V2I communication. The infrastructure acts as transceivers to disseminate information about road hazards including traffic density/congestion through decentralized environment notification messages (DENM) [39]. When an event occurs along the road, the road hazard warning application triggers the generation, and broadcast of the DENM according to the defined requirements. These dissemination requirements define the rate at which the DENM is sent out, acceptable latency, priority and destination area. The generated DENM consists of the header and the body. According to the ETSI TS G5 the header includes the protocol version, type of message (message ID), and the time of generation. The body includes details about the event such as severity, cause, effect of the event on traffic flow, event position, and the area of relevance. After the generation of the DENM it is encoded and sent to the network and transport layers for dissemination. Similar to CAM and DENM defined by the C-ITS in Europe, is the basic safety message (BSM) defined by the DSRC IEEE 802.11p standard in US. The BSMs are divided into two parts- periodic and event-driven messages. The key difference between the DENM and event-driven BSM is transmission over multi-hop and single-hop neighbourhood respectively.

### 2.2.2 | LTE/cellular V2X communication

Recent innovations are drifting towards cellular technologies in V2X that provide large coverage, support low latency requirements, and high traffic density scenarios [40]. This cellular network supports four modes of communication- vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P), and vehicle-to-network (V2N) [41] illustrated in Figure 3. The technology was introduced through the third generation partnership project (3GPP) with the 3G network to mark its beginning in V2X. The failure of the 3G technology to meet the V2X communication standards led to the birth of the 4G/LTE network that offers high bandwidth, low latency, high reliability and high throughput. In a 4G LTE Network, communication starts once a vehicle is discovered within the proximity of another. The sender establishes a direct link (side link) through the PC5 interface (mode 1 and mode 2) to support communication in the absence of cellular infrastructure (base station). Currently, there is a shift towards

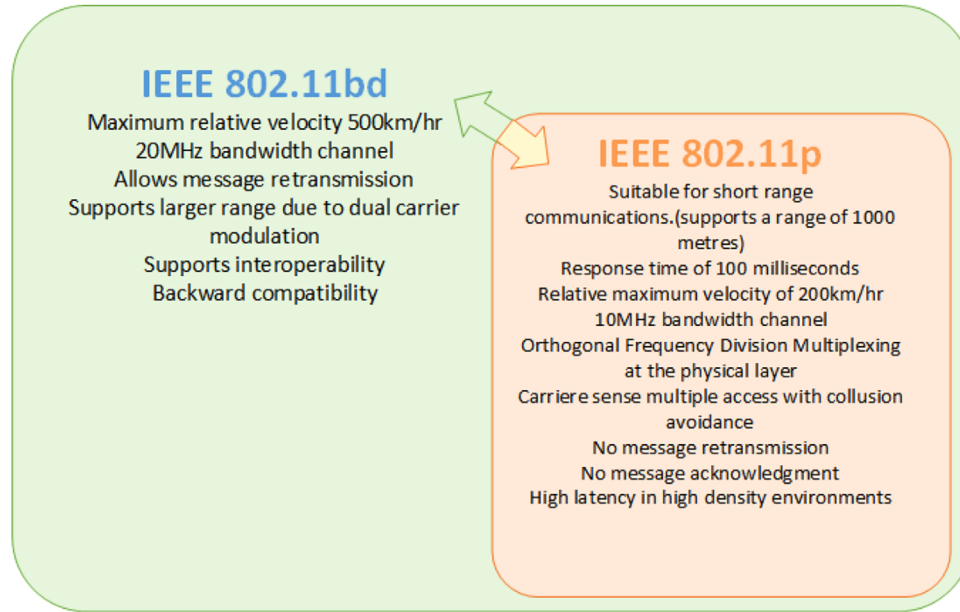


FIGURE 2 Characteristics of the IEEE 802.11p/bd vehicular communication protocols.

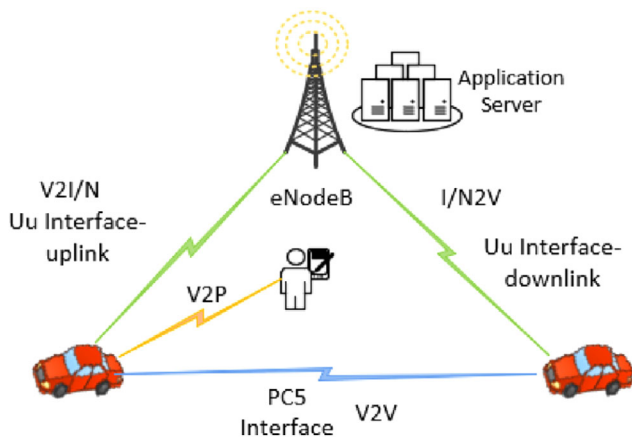


FIGURE 3 Cellular V2X modes of communication.

5G network architecture in V2X communication to attain higher performance demands that support faster mobility with low latency [42]. The 5G LTE supports direct communication through the PC5 interface (mode 3 and 4) and with cellular/network infrastructure (base stations, application servers) using the LTE Uu interfaces (uplink and downlink) illustrated in Figure 3

### 2.2.3 | Hybrid

Previous studies have proved the presence of limitations in both communication modes. Researchers in [43] evaluated the performance of 4G LTE and DSRC in a real-world test-bed. The results show that DSRC outperforms 4G-LTE for real time high-safety applications such as collision avoidance in low-

density traffic. 4G LTE was found to be suitable for non-safety applications. Another study by [44] concludes that the cellular technologies offer better and reliable transmissions over large distances. In summary, the results from the different studies indicate that performance of these protocols varies based on application, coverage and traffic density. [45] To solve the limitations in both technologies a study by [46] investigates the joint use of C-V2X and DSCR in a 5.9 GHz frequency band. The researchers define a function model that describes the transmission and reception of a CAM message in a hybrid environment. From the analysis, there is need for a mutual synchronization model to ensure proper channel allocation and transmission in a hybrid environment. Another study by [47] evaluates the existence of DSCR and C-V2X in vehicular communication. The authors present a function model to relay CAM in environments with both DSRC and C-V2X communication. More studies [27, 48, 49] have been conducted to evaluate the hybrid architectures which can be referred to for further information.

## 3 | CYBER ATTACKS IN CAVs

### 3.1 | Categorization of the general cyber attacks in CAVs based on the key security requirements

To ensure secure V2X communication in CAV technology, researchers have defined different security requirements- confidentiality, integrity, availability, authentication, and non-repudiation. These security requirements have guided the categorization of cyber attacks in V2X communication described in the below section and the possible mitigation methods illustrated in Figure 4.

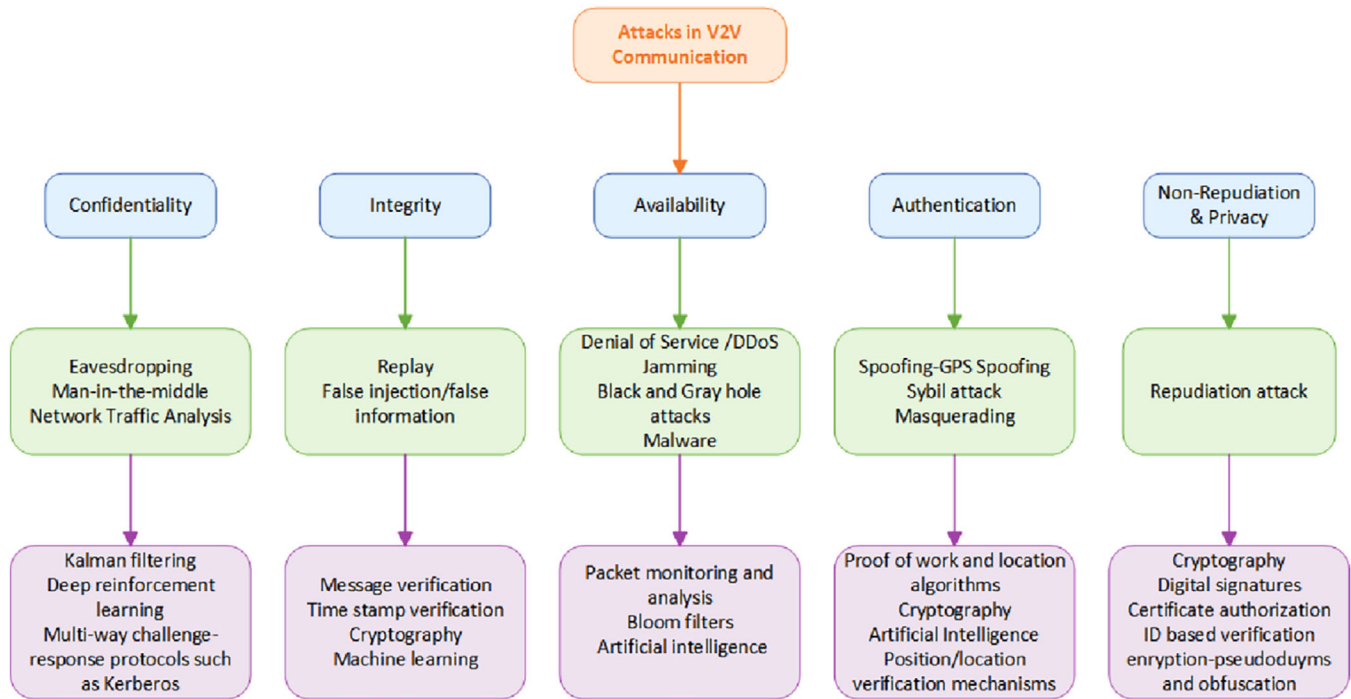


FIGURE 4 A summary of the CAV attacks and mitigation categorized according to the security requirements.

### 3.1.1 | Attacks on authentication

Authentication defines the ability to verify the legitimate sender of the message on the network. The absence of strong authentication mechanisms has birthed the success of threats such as global positioning system (GPS) spoofing, Sybil and masquerading attacks. In a quest to prevent and detect GPS spoofing attacks different studies [20, 22, 23] have suggested position/location verification schemes that deploy various mathematical models. Researchers in [50–54] have explored Sybil attacks in connected vehicles and suggested possible prevention and mitigation techniques. These include encryption, proof of work and location algorithms, position verification, cryptography, and artificial intelligence. Traditional cryptography mechanisms have been a key pillar in identity verification models for vehicular network however these are computationally expensive and are unable to identify internal attackers.

### 3.1.2 | Attacks on integrity

After verification of the sender, then integrity surfaces to verify that the message received has not been modified along the communication channel [55]. Attacks in this category include replay and false injection. Studies in [56–59] have investigated these attacks and suggested prevention algorithms. These include cryptography, message verification, time stamp verification, and machine learning. Most of the suggested mitigation methods suffer from high computation overhead.

### 3.1.3 | Attacks on availability

Availability guarantees that the network resources are accessible to authorized users all the time when the need arises. The common attacks on availability include denial of service attacks (DOS) [60] distributed denial of service attack (DDoS). [61], jamming attacks [62], black and grey hole attacks [63]. Studies have investigated DoS attacks in VANETs and provided possible mitigation and detection mechanisms such as packet detection, monitoring, and analysis [64–67], bloom filters [68], machine learning methods such as kernel support vector machine [69], logistic regression [70], and trust computation [71].

### 3.1.4 | Attacks on non-repudiation

From previous reviews, non-repudiation is also known as the accountability requirement. Any action performed on the network must be accounted for. If vehicle A sends a message to B, then it should be possible to identify A without violating privacy. In a repudiation attack, it is impossible to identify the sender of a message on the network when the need arises. Authors in [72] have proposed an accident reporting system that ensures accountability and privacy. The authors use digital signatures, mutual authentication, and certificate authorization to fulfil these security requirements. More studies [73–75] have made efforts to ensure accountability while maintaining the privacy of identity and location. These studies in general use

digital signatures, cryptography, ID-based verification systems, certificate, and session key update mechanisms.

### 3.1.5 | Attacks on confidentiality

Confidentiality defines the protection of message contents from unauthorized access (users) [55]. The attacks on confidentiality are eavesdropping, man-in-the-middle (MITM) [76], and network traffic analysis. Authors in [77, 78] have investigated eavesdropping attacks and suggested detection models that implement distributed Kalman filtering and deep reinforcement learning. Additional studies in [29] advocate for the use of multi-way challenge-response protocols such as Kerberos to mitigate MITM attacks.

### 3.1.6 | Attacks on privacy

The privacy security requirement guarantees the protection of data such as personal information. It is subdivided into identity and location privacy, where identity privacy ensures the safety of the sender (vehicle) details and location privacy guarantees protection of the sender's position details [79]. The four attributes that relate to privacy in CAVs: are unlinkability, anonymity, pseudonymity, and unobservability. [42, 80] Numerous surveys [81–89] have been conducted regarding the privacy in VANETs. These suggest privacy schemes such as tree-based risk assessment, cryptography, location cloaking [90], encryption-pseudonyms [91], and obfuscation [92].

## 3.2 | Visualization of cyber security attacks in CAVs

This section is a practical illustration of some of the attacks described in Section 3.1 namely replay, false information, and DoS. It aims to provide a clear understanding of these attacks based on datasets that have been generated from previous research. The reason we use these scenario-based datasets [93] except for VeReMi [94] is because they provide cyber attack data simulated in VANET environments. Global and reliable datasets such as KDD-CUP99, ToN-IoT, and NSL-KDD have been simulated in normal network environments leading to bias if used for VANET illustrations/studies. Below is a description of the two datasets used for the illustrations. The vehicular reference misbehaviour dataset (VeReMi) is a misbehaviour detection dataset that was generated using vehicles in network simulation (VEINS) software [94]. VEINS is an open-source VANET simulator that consists of a network simulator OMENeT++ and a traffic simulator SUMO. During traffic generation, the researchers implemented the Luxembourg SUMO traffic (LuST) scenario that consists of real-world traffic data provided by the University of Luxembourg. A more recent version VeReMi extension [95] addresses shortcomings identified by researchers [96–98] and consists of more attacks. The dataset includes metrics to identify attacks such as DoS, DoS random, data replay, disruptive, traffic congestion Sybil, even-

tual stop, speed anomalies, position falsification, and delayed messages. Another study by [93] simulated a machine learning dataset for connected vehicle malicious attacks. The authors used eclipse MOSAIC software to simulate V2V and V2I communications. eclipse MOSAIC is an open-source software that includes a network simulator OMNET++ and a traffic simulator SUMO. The generated dataset provides metrics to identify bogus information and replay attacks. In this study the authors didn't define the exact map area used for the traffic scenario.

- a) *False traffic information use case scenario 1*: Figure 5 includes lplots of the vehicle latitude against longitude over a period of time. These represent the scatter plots of the position values with regression lines to visualize the changes in latitude and longitude values. According to the scenario, attacker\_CAV sends false information to CAV\_A, CAV\_B, CAV\_C, CAV\_D, and CAV\_E regarding an accident ahead. On receipt of such information, all CAVs are forced to find an alternative longer route, clearing the path for the attacker\_CAV. The lplot in Figure 5(a) indicates a distinct in the scatter plots and regression lines for the attacker\_CAV and the rest of the normal vehicles as opposed to Figure 5(b) with no bogus information. From this scenario, identity, message, and position verification are key metrics for the evaluation of trust in CAVs.
- b) *Replay traffic information attack use case scenario 2*: Figure 6, is a lineplot of the speed of the vehicles over a period of time. CAV\_A, CAV\_B, attacker\_CAV, and CAV\_C join the network first, moving at particular speeds. When the emergency\_CAV joins the network after 30 seconds, all other vehicles are forced to stop to create a clear pathway for the emergency vehicle. From the lineplot, it is observed that after 100 seconds, the attacker\_CAV replays the received message from the emergency\_CAV and acts as another emergency vehicle forcing all other vehicles to lower their speed again. In the end, the attacker\_CAV arrives shortly after the emergency\_CAV. The metrics identified for trust computation in this scenario are message and speed verification.
- c) *Denial of traffic information service use case scenario 3*: Figure 7 includes count plots of the vehicle pseudo (IDs) against the number of messages sent over a specific period of time. According to the simulated scenario 7(a), a vehicle with pseudo ID 10332 transfers messages of high priority and at a higher frequency more repetitively than any other nodes. Such transmissions lead to network delays. Figure 7(b), is a normal count message distribution with no sender taking excessive control over the transmission channel. In summary trust computation models can include channel access and monitoring algorithms that define the rules of access for safety and non-safety messages.

## 4 | TRUST IN CONNECTED VEHICLES

The existing cyber security solutions, such as cryptography, and intrusion detection systems, are very effective for preventing

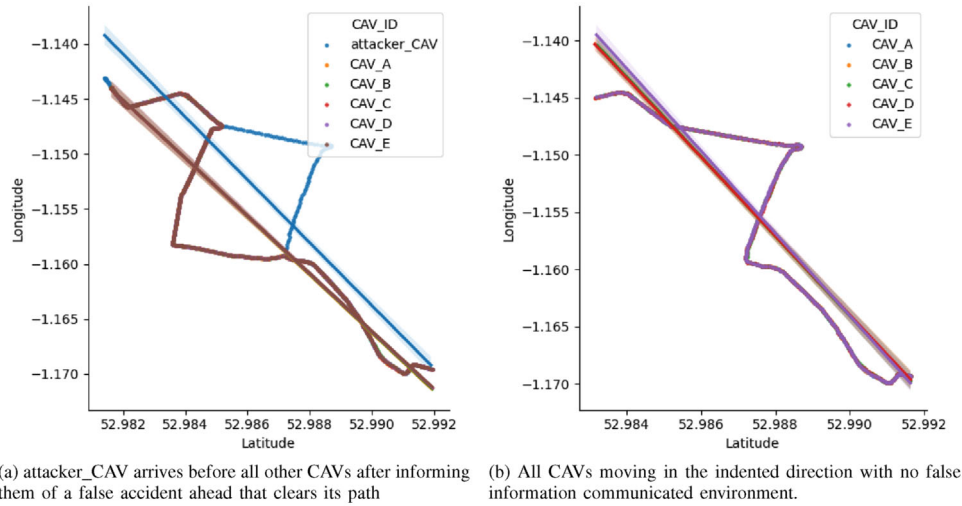


FIGURE 5 False Information in CAVs.

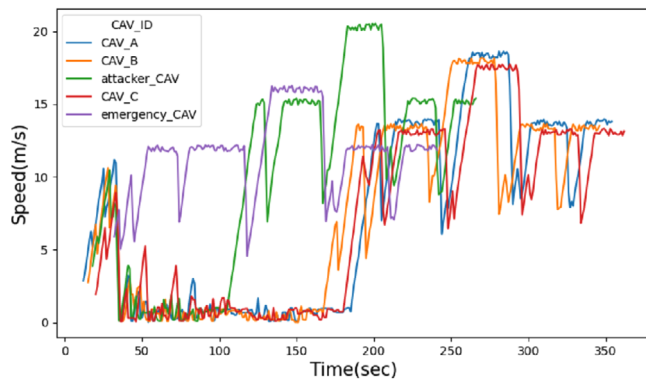


FIGURE 6 attacker\_CAV replays the previous message from the emergency\_CAV.

and detecting external attackers but less effective in internal attack situations. Also, these mechanisms are computationally expensive in the long run and limited to known attacks. To solve such limitations, current research is drawn towards evaluating the sender and message credibility through trust. The below section is a description of the trust taxonomy in CAVs formulated in this research, as illustrated in Figure 8.

#### 4.1 | Trust computation

Trust is a process that establishes confidence between two communicating entities. Generally, trust verifies that the other node is who they claim to be [99]. Trust computation is the calculation of the trustworthiness of the nodes on the network based on entity-centric, data-centric, and hybrid trust-based models. The result of this computation is a trust score that ranges from negative to positive, where 0 indicates no trust. [99].

The entity trust-based model calculates the trust of the nodes which can be direct, indirect, and hybrid.

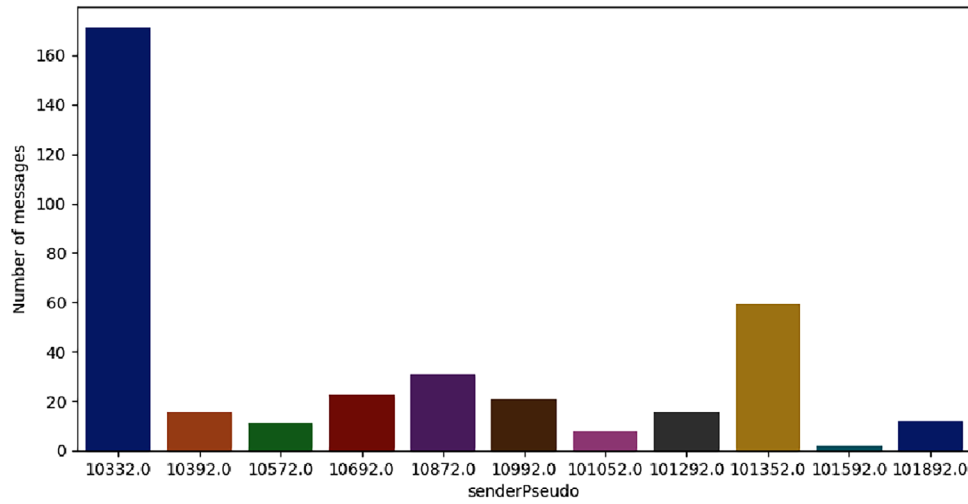
- Direct entity trust is based on the immediate trust computations of node behaviour [42].
- Indirect entity trust is based on recommendations from other neighbouring nodes or third trust parties [99].
- Hybrid trust is a combination of direct and indirect entity trust-based mechanisms.

The data-centric evaluates the trustworthiness of the exchanged message while hybrid trust-based models calculate the trustworthiness of both the node and the exchanged message over the network.

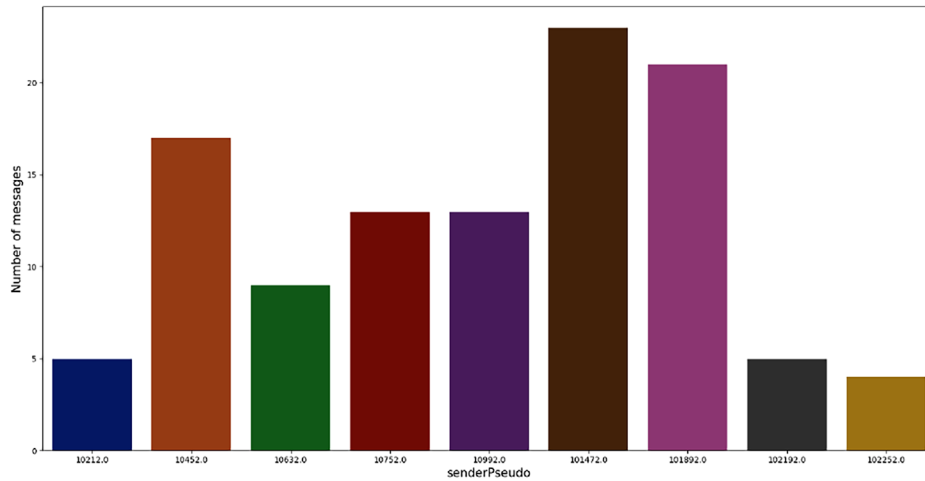
#### 4.2 | Trust management

Trust management includes frameworks that define the structure and coordination of components and activities within the CAV environment. Such activities include update and storage of the computed trust values for current or future use. The trust models explained above can be implemented in different ways, [99] namely: Centralized approach: where a global trust authority calculates and monitors the trust values of the nodes on the network. The centralized nature makes trust computation and monitoring easier; however, this is a single point of failure, and the computation requirements may vary from one node to another. Secondly the Decentralized approach: where the individual nodes fully handle trust computation and monitoring. This fully adapts to the dynamic environment but, requires more computational power in the long run for both trust computation and storage. The models can also be proactive where nodes on the network periodically compute trust values and store them for future use. Since the values are calculated before the need, trust evaluation is faster but requires more computation resources. Reactive: where the model calculates the trust value when needed. This prevents the additional computational resources requirement but may constraint resources if there is a huge amount of data to evaluate, leading to latency.





(a) PseudoID 10332.0 transmitting over 160 messages since it has a higher frequency and priority network.



(b) All psuedoIDs with normal/expected message transfer on the network.

FIGURE 7 A DoS attack scenario.

An effective trust framework ensures effective coordination, availability of resources, and on-time decision-making capabilities at no extra cost. Below is a description of the general trust framework requirements defined by different researchers [99–102].

- 1) *Highly dynamic.* A good trust management mechanism should adopt the highly dynamic nature of CAVs on the network to avoid message delays for safety applications.
- 2) *Distributed/decentralized.* The dynamic and heterogeneous nature of the network environments and topologies makes it possible for a CAV to connect to a network only once and never connect to it again. Therefore, a trust management mechanism must evaluate peer trustworthiness independently other than historical reviews/recommendations, as these may not be available.
- 3) *Scalable.* Scalability is the ability of a mechanism to adapt to the changing resource requirements and components. Such flexibility enables accurate instant decision-making despite the changing resource requirements and different CAV components. For example, in urban or dense areas, the number of communication, requests are higher than in rural or dispersed areas leading to latency if the trustworthiness of each request is calculated individually.
- 4) *Private.* In a quest to validate the identity of the nodes and the exchanged message, privacy should be at the core of the process to guarantee the protection of personal data such as identity and location.
- 5) *Robust.* A trust framework defines the structure and management of trust for all the nodes on the network. Such a framework should have defined strong security measures that protect against and prevent attacks from malicious

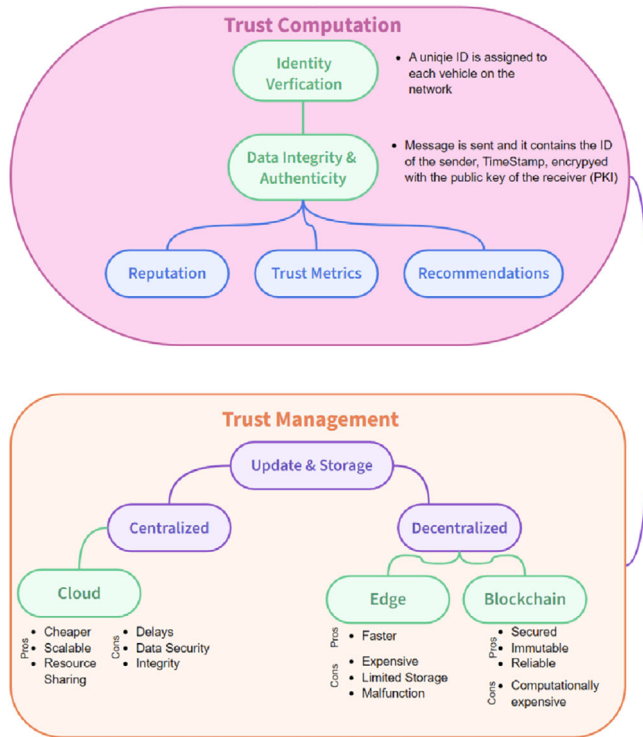


FIGURE 8 A taxonomy of trust in CAVs.

users. It in turn prevents fatal communication errors and failure.

## 5 | RELATED WORK: CURRENT TRUST COMPUTATION MECHANISMS, AND FRAMEWORKS

Numerous efforts have been made to improve the internal security of CAVs using trust-based mechanisms because they require lower computation resources and can be used to prevent or detect internal attacks [103]. Despite these advantages, a couple of drawbacks are identified in the current trust-based security solutions, as detailed in the below section and Tables 2 and 4.

### 5.1 | Fuzzy logic

Fuzzy logic is an artificial intelligence technique used to make decisions about uncertain data based on incomplete, inaccurate, or unreliable knowledge [104]. Fuzzy logic consists of four components: the fuzzifier, knowledge base(rules), intelligence, and defuzzifier. At the start of the fuzzy logic operation, the fuzzifier converts numerical values into linguistic variables in words or sentences. These linguistic variables are then fed into the controller that applies rules from the knowledge base and provides an output value. The value is then fed into the defuzzifier to convert the variables to numerical values. The key advantages of fuzzy logic include the ability to relate uncertain or complex data and increased robustness, but such models require more simu-

lation and review before actual implementation [105]. Research by [106] suggested a direct entity-centric and fuzzy logic trust computation method. First, the model checks the accuracy and integrity of the sender using a unique ID appended to each message. Then a lifetime check is performed to verify the freshness of the message, and once a message is identified as expired, it is discarded. A fuzzy logic model is then used to verify the sender's location. Results from these attributes are used to construct a decision-making model that defines the vehicle's trustworthiness. The model's key advantage is that it stores only the recent trust value however, the performance is low in the presence of many false recommendations. Researchers in [107] suggest a fuzzy logic design to compute virtual trust in self-driving cars. According to the authors, virtual trust is when two vehicles unknown to each other are able to communicate through a common friend(vehicle). The designed Mamdani Fuzzy logic takes three inputs (common car features), information sharing, manufacturer and sensor quality, processes these inputs then outputs a trust value. Given a set of the aforementioned inputs, an output trust value is computed based on membership functions (implemented in MATLAB) and the knowledge base rules. The knowledge base rules that are used to shape the model's trust value are based on the input parameters values expected to be at a maximum of 300. Despite the promising simulation results, there is no comparison with existing fuzzy logic solutions and implementation in the real word self-driving car environment. Previous work by [108] in 2016 suggested a fuzzy logic model that computes the trust of vehicles within the vehicular ad-hoc network to ensure a secure communication path. According to the authors, for vehicle A to communicate with vehicle B, there are relay nodes that are used to form a communication path. The selection of these relay nodes is based on the neighbouring vehicle with the shortest path and highest trust value, known as the relaying trust value. For each relay node, the relay trust value is computed based on three input parameters, distance, network/traffic density, and inconsistencies in trustworthiness. After computing the relay trust value, a coordinating trust value is computed to find the best transmission path from the source to the destination vehicle. This value is based on three parameters, namely the velocity between the sender and neighbouring vehicles, the number of connections, and the connections lost within a particular time frame. The fuzzy logic engine or model (coded in MATLAB and NS-2) then takes the two inputs, coordinating and relaying trust values, calculates the final trust value based on the established knowledge base/rules and outputs trust levels such as perfect, good, acceptable, worst, and bad.

### 5.2 | Game theory

A game is a competitive activity among multiple entities that interact jointly based on rules. Similar to a game, game theory is a mathematical model consisting of entities that make strategic decisions to attain the highest benefits (payoffs). Each entity or player considers other entities' actions before making a decision. A detailed review of game theory terms can be reviewed in [109–111]. The key components of game theory are:

**TABLE 2** A summary of existing trust based models in CAVs.

Reference	Category	Target Attack	Trust Computation	Trust Management	Drawbacks
REPLACE [85]	Roadside units	Platooning Attacks: badmouth, newcomers, and ballot stuffing	Reputation: dirichlet distribution and iterative algorithm for feedback validation.	Centralized and Distributed	1) The server is a potential vulnerability as it stands as the sole point of failure, lacking any specified security measures for its safeguarding.
TMBNST [84]	Roadside units	Malicious vehicles	Timestamps and digital signatures	Distributed	1) RSUs are fully tasked with trust value evaluation, storage, update and deletion, which is challenging in the long run and in remote areas. 2) The performance is highly dependent on stable network connectivity, as a slight drop affects the timestamps leading to faulty confidence computations.
LTT [112]	Roadside units	Repudiation, Man-in-the-Middle and replay attacks	Digital signatures for message authentication and verification.	Centralized and decentralized	1) A constant maximum trust value of 1 is assigned to each RSU, an opportunity for attackers to exploit RSUs. 2) The model's performance depends on stable network connectivity to check message liveness. Therefore, a slight network drop could lead to false negatives.
TACASHI [83]	Roadside units	False location	Recommendation and report history	Distributed	1) Trust management in areas with no RSUs is undefined.
[106]	Fuzzy logic	False information, message alteration, and false location.	Timestamps, location verification, and node behaviour history.	Distributed.	1) Implementing fuzzy logic requires more simulations to eliminate any bias during operation.
T-VNets [113]	Roadside units.	Elimination of malicious nodes and routing attacks.	Vehicle behaviour reports from CAM and DEMNs	Distributed	1) In the long run, more computational resources are required to store the previous trust values on vehicles and RSUs.
[103]	Game theory	False information.	Majority opinion, betweenness centrality, and density compute.	Centralized	1) High-density areas require more defenders and there is a delay in trust computation for nodes that have connected to the network for the first time.
[114]	Game theory	Replay and false data injection.	Bayesian Inference Model: Experience	Distributed	1) No simulations are performed in a real-world environment.
[115]	Game theory	Message falsification.	Reserved price, two round, and m-round bargaining techniques	Centralized	1) More storage space is required in the long run.
[116]	Game theory	Message falsification.	Recommendation and K-means clustering algorithm.	Distributed	1) Highly dependent on the presence of RSUs.
[107]	Mamdani fuzzy logic	Message falsification.	Sensor quality, manufacturer, and information sharing parameters.	Distributed	1) More simulations are required for better model development.
[108]	Fuzzy logic	Routing attacks.	Recommendation and K-means clustering algorithm.	Distributed	1) Highly dependent on the presence of RSUs.

- **Players:** The different participants in the game.
- **Actions:** The moves made by each participant. Throughout the game, each participant aims to make the best move, as detailed in their strategy.
- **Payoff:** This is a return (benefits) of each player for taking specific actions throughout the game.
- **Strategies:** A strategy is a plan of action. For each action made by a participant, there is a detailed plan.

Throughout the game theory, each player makes moves based on their best strategy, which leads to a maximum payoff for all players (win-win situation), known as equilibrium. Nash equilibrium is then used to determine the winner. Furthermore, games in game theory can be classified according to a number of stages, complete information or actions, and perfect information or payoffs [110]. The key drawback is that it requires more simulation to identify the best strategy before implementation. Below is a review of the current trust-based mechanisms implementing the game theory. The authors in [103] proposed a trust model for CAVs based on game theory. The key players in this model are the attacker and defender. Both players aim to find the best strategy before taking any action. The implemented model uses three parameters: majority opinion, betweenness centrality, and density compute to identify the attacker node. The majority opinion calculates the trust level based on experience, such as successful/failed node communication. Betweenness centrality measures the number of times a node acts as a hop or intermediary between two communicating nodes. Density compute identifies and groups nodes travelling with the same speed and direction. The three parameters are calculated for each attacker and defender, and Nash equilibrium is used to define the winning strategy. According to the simulation results, the model performed better compared to one of the existing game theory models; however, this model works best in the presence of many defenders, and new attacker vehicles are not detected instantly as the defender nodes need time to gather opinions about them. A defender is an entity that can monitor (network administrator) and respond to attack actions from the attacker, such as an intrusion detection system.

A study by [115] suggested a theoretical trust approach based on game theory for the secure exchange of data. For each initiated communication between the sender and receiver vehicles, the communication ability of the sender is evaluated by the receiver and stored in the local cache of the sender. Likewise, for each initiated communication with the RSUs, vehicles evaluate the reliability of the information received and the quality of service. Throughout the trust value computation/evaluation process, three concepts are implemented, reserved price, two-round and m-round bargaining game theories. The reserved price is the cost the vehicle has to pay in order to receive information from the RSUs and is based on the trust values of the vehicle and RSU, the load of the RSU, and the shortest distance between the RSU and the vehicle. The lower the trust value, the higher the reserved price (cost) and the standard trust value is 1. Despite the promising simulation results, the model requires more storage space in the long run, as the vehicles and RSUs are responsible for storing the local cache trust values.

Another study by [117] defines a CAV security game model that consists of two players: an attacker and a defender. As the attacker blocks the road based on his/her best attack strategy, the defender will take action based on the best defence strategy. Further research by [114] implements a cooperative game theory model for secure communication on the Internet of Vehicles (IoV). The authors adopted a distributed and direct trust computation using the Bayesian inference model. This model computes the trust level based on experience from direct interactions. For each communication, the message content is evaluated. Using the hedonic coalitional game, the attained trust value is then used to derive cooperation groups with similar trust levels. More research by [116] proposed a model that implements direct and indirect trust models to compute vehicle trust scores. The indirect trust model relies on feedback from neighbouring vehicles and recommendations from RSUs. The weighted K-means algorithm is then used to check the legitimacy of messages. used to identify legitimate messages. Further, a dynamic game theory model is used to support node interaction by awarding cooperative nodes and punishing uncooperative nodes. The implemented dynamic game model consists of clusters, actions, and payoffs. The defined clusters are normal, selfish, and malicious nodes. The actions are information release, forward, receipt, and no action, and the payoffs define the rewards and punishments. The key drawback in the model is the dependence on RSUs to store node reward and punishment history. This implies that the model is ineffective in areas with no RSUs or is expensive to implement on a large scale. Furthermore, like most suggested models, this is not implemented in a real-world environment.

### 5.3 | Based on road side units

Further research has proposed the use of infrastructure such as RSUs. The static nature of RSUs makes them preferable to dynamic nodes because they can maintain stable network connectivity for a long time. Below is a review of trust-based mechanisms that take advantage of the presence of RSUs during trust computation.

Research in [85] suggested a trust-based scheme REPLACE that identifies platoon attacks such as badmouth, on-off attacks, newcomers and ballot stuffing. The trust-based mechanism consists of two algorithms. First is a reputation algorithm based on dirichlet distribution that gathers feedback from surrounding vehicles about a head vehicle. Secondly, the gathered feedback is evaluated using an iterative algorithm to eliminate false feedback from malicious users. At the top of the system model is a trust authority that registers all vehicles, RSUs, and servers on the network. Next are the servers that store and update feedback values. At the bottom are the RSUs stationed along the roads for faster data relay between servers and the trust authority. Throughout the model or communication, feedback gathered is stored in a centralized way using servers. The simulation results indicate the model's great performance; however, the server is a single point of failure, as the researchers didn't consider any security mechanisms to protect the data on it.

Also, the performance of the model in a test bed environment is unknown.

According to [84], some components can stay on the network longer; thus, the emergence of TMBNST, a trust management mechanism based on vehicle stay time. The system model consists of RSUs, evaluators, and normal nodes. At the start of the communication cycle, the RSUs register new vehicles on the network and select the evaluators such as public vehicles (ambulance and police cars) to evaluate the normal vehicle trust. The model evaluates the confidence of the message based on the liveliness of the data and digital signatures (asymmetric key encryption) are used to verify the message broadcast. The simulation results indicate less computation and packet transmission time; however, RSUs are fully tasked with trust value evaluation, storage, update and deletion, which is infeasible in dispersed areas with no RSUs or longer-staying nodes. Furthermore, the model's performance is highly dependent on stable network connectivity as a slight drop affects the timestamps.

A study by [112] suggested a long-term trust model that prevents repetitive bootstrapping and ensures accountability. Bootstrapping defines the trust value of a node when it joins the network for the first time. The system architecture consists of the central authority, RSUs, and vehicles. At the start of communication, the central authority issues a certificate to each RSU and vehicle. For each verified RSU, the CA assigns a permanent trust value of 1 for a lifetime. The RSU then attaches a timestamp and digital signature to each generated message and sends it to the CA for decryption. The trust management model explores three scenarios: when a vehicle connects to the network for the first-time, when a vehicle moves between different RSUs and when a vehicle rejoins the network. This model prevents vehicles from contacting CA repetitively for every connection, which ensures faster trust computation and management. However, its performance is highly dependent on the presence of RSUs and stable network connectivity to ensure correct results for the message liveliness check. Furthermore, the performance of the model in simulation environments is undefined.

Another study by [113], suggested a decentralized and hybrid trust management mechanism T-VNets that identifies malicious nodes and selects the best possible path for message transfer. The system model consists of RSUs and vehicles. It implements the ETSI ITS CAMs and DEMN to support message exchange between the vehicles and RSUs. Throughout the model, RSUs act as trust authorities that gather all delivered-vehicle behaviour reports to form a global vehicle trust view. According to the simulation results, the model has higher detection performance when compared with other models but is infeasible in a highly robust environment. Finally, a study by [83] proposed TACASHI, a trust aware communication architecture for the social Internet of Vehicles. The system model consists of vehicle owners, passengers, RSUs, vehicles, TAs, and online social networks (OSNs). At the start of the communication, the Department of Motor Vehicles verifies an OSN account and issues pseudonyms (IDs). When vehicle A wants to send a message to vehicle B, it encrypts it using the chaotic maps. Before accepting the message sent by A, vehicle B evaluates the

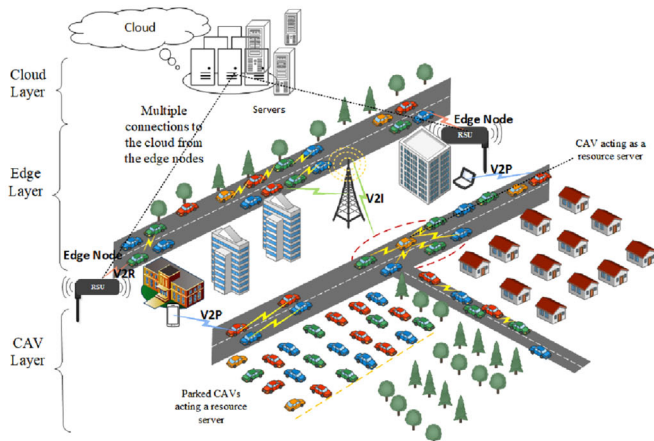
integrity of A by asking its neighbours about A (recommendation). Furthermore, RSUs are used in this model to store the historical values (reports) of neighbouring nodes for each node within the RSU range. The simulation results indicate more than 87% detection rate and high accuracy. Despite the high detection rate, it is unclear whether the RSUs are fully tasked with storing, updating, and managing the trust values in the long run.

## 5.4 | Cloud assisted frameworks

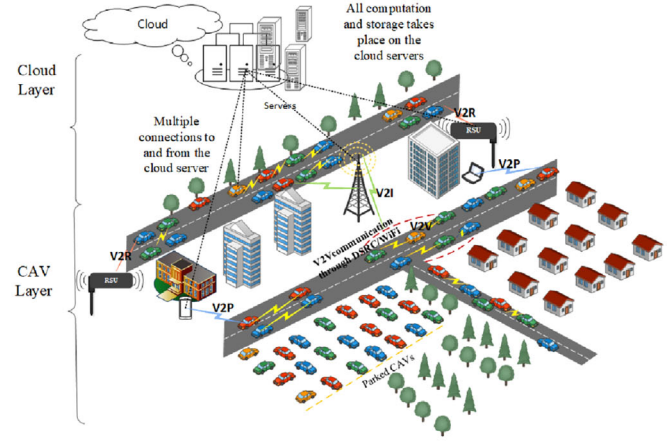
Cloud computing in VANETs is a technology that enables access to and provision of shared system resources on demand over the internet. It is subdivided into vehicular cloud computing (VCC), vehicles using cloud (VuC), and hybrid [122]. Vehicular cloud computing was introduced by [123] to enable resource sharing among vehicles and is further subdivided into static and dynamic vehicular clouds. The former includes a group of vehicles at rest forming a vehicular cloud; for example, CAVs in a parking area can act as a cloud server since they have unused storage and bandwidth and RSUs with more storage and high computational capability as illustrated in Figure 9(b). The latter includes a group of vehicles in motion such as platoon heads with more computational, bandwidth and storage capacity to act as dynamic cloud servers. The vehicular cloud services are categorized into four groups, namely, network-as-a-service (NaaS), sensing-as-a-service (SaaS), computing-as-a-service (CaaS), and storage-as-a-service. (SaaS) explained below:

- Network-as-a-service: The NaaS enables network resource sharing such as internet access. CAVs with higher bandwidth can share the internet with those with lower bandwidth levels to ensure faster connection/transfer speeds.
- Sensing-as-a-service: Vehicles within the VANET are equipped with automotive driving system components that provide surrounding environment status daily. The sensing-as-a-service allows sharing of sensor data with other vehicles when needed.
- Computing-as-a-service: The main limitation of security mechanisms such as cryptography is the limited computational power/speed. For instance, vehicles with less/no computation requests can take up requests from other vehicles with excessive/choking computational requests.
- Storage-as-a-service: Implementing SaaS is a potential solution to the storage constraint issues because CAVs with more storage capacity can share the extra storage space with those with less. Furthermore, storing information required for future use relieves the individual CAVs of the storage responsibility.

The need to ensure resource availability has led to the implementation of CAVs in cloud environments. Previous surveys on vehicular cloud computing that guide the implementation of trust-based schemes in vehicular cloud exist as detailed in [120, 124]. The authors in [120] discuss the architecture for vehicular cloud computing, various components and applications for vehicular cloud computing. The researchers also discuss



(a) Structure of a CAV edge assisted environment



(b) Structure of a cloud-assisted CAV environment [120], [122]

**FIGURE 9** A structure of cloud and edge assisted environments in CAVs.

the security issues that arise due to the implementation of CAVs in cloud environments. Another survey by [124] investigates the impact of cloud computing in CAV environments and suggests a VANET cloud computing architecture. Previous surveys on cloud computing have sparked interest in the security and privacy of these frameworks in vehicular environments. Researchers in [125] proposed a three-layer cloud-based trust management framework for vehicular social networks. The proposed cloud-based network architecture includes the central, Roadside, and vehicular cloud layers. It implements a centralized approach which includes direct and indirect trust computation at the roadside and central cloud layers. The roadside layers use a vehicular virtual machine to process trust computations. Despite the successful model development, its performance in the real-world environment is unknown. Also, trust computations are highly dependent on the presence of RSUs that host the virtual environment and communication with the cloud servers regarding trust history values. Another study by [126] suggested TrustE-VC, a three-level trust evaluation model for CAVs in cloud environments. The framework implements a decision-making algorithm and Fuzzy logic model, to identify and weigh the security vulnerabilities in vehicular cloud. Despite the promising theoretical contribution there is no practical validation of this model in simulation and real-world environments. In [127] the authors suggest an agent-based trust framework for vehicular cloud. The system model consists of mobile and static agents which include trust manager and trust information collection agents. There is an additional component called the knowledge base that stores information such as vehicle status, bandwidth levels, cloud and vehicle IDs. At the start of the communication cycle, the trust manager gathers the trust values of the available service providers using the trust collection agent. These trust values are evaluated and the service provider with the highest value is chosen. This model is a theoretical analysis with no performance evaluation through simulations. Finally, researchers in [128] suggested DBTEC, a trust-based security model for vehicle cooperation in cloud VANET environments.

The authors aim to solve two challenges encountered during collaborative task completion in cloud environments: difficulty selecting trustworthy cooperative vehicles due to the absence of trust information and the secure successful completion of tasks. The system model includes normal vehicles, users, private boards, malicious vehicles, and public boards. Once a vehicle receives a task request and can't fulfil it, it searches the public board for vehicles with good service quality to perform this task. This public board is a global storage of reported vehicle service quality and timestamp. The outcome of the simulation results indicate better performance. In conclusion, the vehicular cloud has enormous benefits in terms of cost and resource usage; however, challenges such as centralized storage of information are a security and privacy risk. Also, critical applications that require instant trust decision-making are highly affected by the back-and-forth communications with the cloud servers making it unsuitable for real-time communication.

## 5.5 | Edge assisted frameworks

In a quest to solve the aforementioned cloud computing disadvantages described in Table 3, researchers have explored the concept of edge computing in VANETs. Edge computing is a technology that implements computation and storage of data at the edge of a network close to the data sources and not far from the vehicles. [119]. The key features differentiating vehicular cloud computing and vehicular edge computing are the real-time local decision-making capability and the presence of resources within the vehicle's proximity. The concept of edge computing is still picking its stand in CAVs. Therefore, less research has taken place in the trust management area.

However, existing studies implement the concept in other areas within VANETs, such as resource sharing. The authors in [119] reviewed edge computing in a vehicular network and suggested a vehicular edge computing architecture which consists of three layers: cloud, edge, and smart vehicular illustrated in

**TABLE 3** A summary of the advantages and disadvantages of the different trust computing frameworks in CAVs.

Analysis	Cloud Computing in CAVs	Edge Computing in CAVs
Advantages	<ol style="list-style-type: none"> <li>1) Resource sharing and efficient utilization. [118]</li> <li>2) Availability</li> <li>3) Cheap: there is no need to buy and install infrastructure as it can be rented.</li> <li>4) Scalable: resource assignment is based on demand due to the pay-as-you-go capabilities.[119]</li> </ol>	<ol style="list-style-type: none"> <li>1) Faster communication: the presence of edge nodes and dynamic vehicles with more resource capabilities eliminates the need for direct and regular communication with the cloud servers. This enables faster decision-making [119].</li> </ol>
Disadvantages	<ol style="list-style-type: none"> <li>1) Delays: The regular communication cycles between CAVs and cloud servers causes delays, yet the connections are instant and dynamic.</li> <li>2) Data security and privacy [120].</li> </ol>	<ol style="list-style-type: none"> <li>1) Highly dependent on the presence of edge nodes and thus a challenge in remote areas</li> <li>2) Instability: the highly dynamic nature of CAVs makes it possible for vehicles acting as cloud servers to disconnect from one network to another while other vehicles utilize its resources [121].</li> <li>3) Limited storage capacity [119].</li> <li>4) Pron to malfunctioning because they are positioned in open environments leading to unreliability.</li> </ol>

Figure 9(a). Researchers in [129] suggested a distributed trust management framework that implements trust computations and evaluations at the network's edge (RSU). The system model consists of the sensing, edge and cloud layers where the edge layer includes RSUs and edge servers that integrate and process trust data from surrounding vehicles. The trust evaluation model implements traffic analysis, vehicle driving behaviour, and evaluation of messages by surrounding vehicles to identify the trust score. The simulation results indicate that the model out-performs other existing models in terms of data delivery (low latency). Further research by edge computing security mechanism for V2V and V2E communications in a 5G network. The system model consists of edge nodes, which are responsible for storing all authenticated and registered vehicles on the network. The model maintains secure V2V and V2E communication using the quotient filter.[130] also suggested an The simulation results indicate a delay in V2E communication with an increase in traffic density Also, the researchers did not define what constitutes the edge nodes. In summary, most stud-

ies refer to edge nodes as RSUs and edge servers; therefore, studies that implement the use of RSUs qualify to be categorized under edge computing environments if they support vehicle-to-edge communication.

## 5.6 | Blockchain frameworks

Recent studies are suggesting the implementation of blockchain technology in CAVs to ensure secure distribution. Below is a brief review of the key concepts in blockchain technology: From a network perspective, a block is a group of records stored on a node, while a chain is a sequence of linked items. Therefore, a blockchain is a group of distributed tamper-proof records stored on different nodes and linked using reference hash values. Each node on the network broadcasts messages encrypted with the sender's private key and decrypted with the sender's public key. Afterwards, minors verify the broadcast messages using a consensus rule before adding the block to the chain. This process is called mining. Blockchain technology ensures the orderly update of records and the addition of blocks through a decision-making process known as consensus The most common consensus algorithms are proof-of-work, proof-of-authority, proof-of-stake, proof-of-activity, byzantine fault tolerance, proof-of-burn, proof-of-stake, proof-of-capacity, proof-of-importance, proof-of-luck, and proof-of-exercise [135]. The key advantages of blockchain technology are decentralization, immutability, security and reliability due to the implementation of asymmetric cryptography with hashes at each block and distributed information storage [136]. Trust mechanisms that use Blockchain technology are detailed below. The authors in [131] suggested a decentralized trust management mechanism that implements blockchain technology. The system model consists of RSUs and vehicles. During communication, the sender vehicle broadcasts a message to the network. The Bayesian inference model is then used to validate the message broadcast and gives a rating which is sent to the nearest RSU and aggregated to generate a trust value. This rating is based on the sender's current trust value and the distance between the sender and receiver. Two consensus algorithms, namely proof-of-work and proof-of-stake, are implemented to ensure an orderly update of these trust values among RSUs. Despite the benefits of using blockchain technology in this model, its operation in areas with no RSUs is infeasible. It is computationally expensive in the long run leading to performance degradation. Research by [132] suggested a reputation trust-based model that implements blockchain techniques. The system model includes ordinary vehicles grouped to form a cluster based on proximity, a TA, a malicious vehicle, and a cluster head. Upon joining the network, a TA registers a vehicle and issues it a certificate. The vehicle is then able to send a broadcast message which is validated and rated by the cluster head (minor). This rating is based on the senders' historical behaviour and is aggregated to form a reputation score that can be uploaded to the trust authority for global storage. Simulation results indicate a drop in message detection accuracy with an increase in the number of malicious vehicles. Additional

**TABLE 4** A summary of surveys on the blockchain, cloud, and edge-assisted trust-based security frameworks in CAVs.

Author	Technology	Summary	Trust Computation Model	Drawbacks
[125]	Cloud assisted	A three-layer cloud trust-based management framework for vehicular social networks	Direct and Indirect Trust computations	Trust computations is highly dependent on the presence of RSUs that host virtual environments and communicate with cloud servers regarding trust history values
TrustE-VC [126]	Cloud assisted	A three-level trust evaluation framework to ensure the security and privacy of CAVs in cloud environments	Mathematical model: Fuzzy Logic	Theoretical contribution with no simulation.
[129]	Edge assisted	Trust management in Vehicular networks using edge computing	Traffic analysis, vehicle driving behaviour and message evaluation.	The assumption that the edge agents are trustworthy is a security risk because they can be compromised.
[130]	Edge assisted	Secure authentication mechanism implemented in an edge computing environment with a 5G network.	Quotient filter is used to ensure secure V2V and V2E communication	Delay in V2E communication with increase in traffic density and edge nodes are not clearly defined.
DBTEC [128]	Cloud assisted	Secure collaborative task completion in cloud environments.	Service quality history and timestamps	Performance of the model is prone to errors for vehicles that have just connected to the network.
[127]	Cloud assisted	Evaluation cloud service provider trustworthiness.	Dumpster Shafer Theory and software agents	Theoretical contribution with no practical validation.
[131]	Blockchain	Decentralized trust-based security model.	Direct data evaluation using Bayesian inference. Proof-of-stake and Proof-of-Work consensus algorithms.	It is computationally expensive in the long run and infeasible in areas without RSUs.
[132]	Blockchain	A decentralized trust-based reputation system.	Indirect trust: History behaviour aggregated to form a reputation score.	Drop in performance with an increase in malicious vehicles.
BTEV [133]	Blockchain	A decentralized trust-based security model that validates traffic events.	Proof-of-Events.	Decline in performance in high-traffic environments.
[134]	Blockchain	A decentralized trust-based security model for clustered IoV environments.	Bayes rule that considers reputation score and message credibility parameters.	Scalability requirements are undefined.

research conducted by [133] proposed a decentralized trust-based model that validates traffic event messages in CAV environments. During the communication, the RSUs receive cooperative awareness messages (CAM) from nearby vehicles that contain the vehicle's speed and location. The RSU then

checks for the validity of the message based on timestamps and discards those that are expired. Valid messages are then broadcasted on the network via a decentralized environment notification message (DENM) stored in a blockchain. When a passing vehicle receives a request about a traffic condition, it will



validate this information against the DENM from the RSUs that contain current road or traffic conditions. Unlike other methods that use proof-of-work, proof-of-stake etc., the researchers suggested a proof-of-events (PoE) consensus algorithm to enable effective information updates and collaboration among the distributed nodes. The simulation results indicate that the PoE consensus algorithm is promising since it demands less computational power. Nevertheless, its effectiveness is affected in environments with high traffic. Finally a recent study by [134] proposed a blockchain trust-based security model for clustered IoV environments. The system architecture includes TA, ordinary vehicles, edge vehicles and RSUs. Upon joining the network, the TA registers and issues certificates to vehicles. These ordinary vehicles are then grouped into clusters based on distance and velocity similarity. For each cluster is a cluster head selected by the TA based on computational capacity, safety distance, and trust value. When a node receives an event notification, it requests the sender's trust score from the cluster head. The cluster head computes the trust score using Bayes rule that takes into account the sender's reputation and message credibility parameters. These trust scores are then aggregated and stored as local blockchains on the edge nodes and globally by the TA. The outcomes of the simulation indicate that the model is feasible in IoV environments. Researchers in [137] proposed a blockchain trust management approach for connected vehicle communication. The multi-layered system model includes RSUs and vehicles grouped into platoons based on speed and proximity. When a vehicle sends a message to the network, its credibility is validated by other vehicles within the same platoon based on recommendations. This credibility is stored in form of trust values at the local (platoon blockchain) and global (RSU blockchain) levels. Despite the analysis, this study is theoretical with no simulations to validate its performance.

## 6 | OPEN ISSUES

Despite the numerous efforts to ensure secure V2X communication through trust computation, the areas below require further research to enhance the deployment and adoption of CAVs in the real world.

### 6.1 | Privacy

Privacy is one of the key security requirements in V2X communication that ensures anonymity, unobservability, unlinkability, and pseudonymity of exchanged data. During trust computation, direct and indirect mechanisms validate vehicle identity and evaluate messages using various techniques detailed in the previous section. This process exposes data to violation of privacy in a quest to ensure secure message exchange. The issue of concern is whether all this information gathered by the trust mechanisms/or models is private. To solve such concerns studies in [42, 80–89] have proposed trust mechanisms that make use of cryptography techniques despite the high computational resource requirement [10]. This raises the issue of whether

privacy solutions in connected vehicles can be implemented without cryptography if not then there is need to minimize resource usage.

### 6.2 | Integration with blockchain

The promising benefits of blockchain, such as immutability, decentralization, security, privacy and anonymity, have attracted its integration into CAVs. [6] Recent studies in [131–134] have integrated blockchain techniques during trust computation as explained in Section 5.6. The outcome of the simulations is promising. However, there are a couple of challenges namely: high computational overhead as the number of blocks increases and the distributed storage of data across the different nodes raises privacy, scalability, and trust concerns. Furthermore, the authors in [138] argue the possibility of legal issues arising from technical errors or system failure. Such issues can be challenging to investigate if no proper data regulatory blockchain measures are in place.

### 6.3 | Integration with artificial intelligence

Recent studies detailed in Sections 5.1 and 5.2 have applied artificial intelligence techniques such as game theory and fuzzy logic to compute trust and detect malicious activities. [139, 140]. The performance of these models is based on the presence of data sets for training and testing purposes. [141]. From the review, these datasets are scenario-based, making model comparison challenging and not fuelling or supporting further research. Furthermore, attackers keep changing the techniques used to strike connected vehicle networks, leading to numerous new attacks that may not be part of the previous datasets. Therefore the implemented artificial intelligence techniques (machine learning) models should also be able to adapt to the changing attack techniques. Researchers in [94, 95, 98, 142] have generated datasets to solve this limitation. However, these are tailored to specific research requirements and, hence, are challenging to use for the evaluation of new machine-learning models. Therefore, there is still a need for a large general real-world dataset that contains various connected vehicle attacks to support integration with artificial intelligence.

### 6.4 | Implementation

From the review, a few of the suggested trust-based security solutions have been simulated and implemented in real-world CAV environments as summarized in Tables 2 and 4. The cost (such as purchasing the CAV and setting up in a suitable environment) that comes with the implementation is a key barrier. There have been recent works where researchers simulate cyber attacks in real-world CAV environments and generate datasets for further research. [93, 142] However, such testing is specific to a particular scenario. Recent research advocates for combined efforts among research organizations, governments and CAV manufacturers to support the set-up of CAV infrastructure [4].

## 6.5 | Scalability

Scalability is the ability of a model to alter its capacity with respect to resource requirement. The analysis of previous literature detailed in the above sections has portrayed how studies ignore the effect of traffic density on model performance. A few researchers have acknowledged the drop in detection levels and message delivery delays with an increase in traffic density [130, 133]. To solve this limitation recent studies have implemented the trust models in cloud [125–127] and edge-assisted environments [119, 129, 130]. However, these are affected by the long communication cycles with cloud servers and the high maintenance and storage for the edge nodes. Therefore there is still a need to implement scalable techniques during trust computation and management to ensure good performance with changing resource requirements.

## 7 | CONCLUSION

This article explores the potential implementation of cybersecurity in connected and autonomous vehicles (CAVs) using trust computation mechanisms. First, we examine the elements that facilitate V2X communication and analyze the vulnerabilities and limitations associated with these components. We then categorize cyberattacks based on security requirements and examine possible mitigation algorithms. By leveraging real traffic data from existing datasets, it provides practical insights that illustrate cases of denial of service (DoS), replay, and false information attacks. For a comprehensive analysis, we critically evaluate existing trust-based cybersecurity solutions and finally suggest future research directions by filling the gaps identified in current studies.

### AUTHOR CONTRIBUTIONS

**Maria Drolence Mwanje:** Conceptualization; data curation; formal analysis; methodology; writing—original draft. **Omprakash Kaiwartya:** Supervision; writing—review and editing. **Mohammad Jaidi:** Writing—review and editing. **Yue Cao:** Writing—review and editing. **Sushil Kumar:** Investigation. **Devki Nandan Jha:** Validation. **Abdallah Naser:** Supervision. **Jaime Lloret:** Supervision; writing—review and editing.

### ACKNOWLEDGEMENTS

The research is funded by the fully funded Ph.D. Scholarship by Nottingham Trent University, UK.

### CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

### DATA AVAILABILITY STATEMENT

Data will be made available via individual request to the corresponding author.

### ORCID

**Omprakash Kaiwartya**  <https://orcid.org/0000-0001-9669-8244>

**Jaime Lloret**  <https://orcid.org/0000-0002-0862-0533>

## REFERENCES

1. Statista Research Department: Forecasted share of new connected vehicles on roads in the united kingdom (uk) from 2018 to 2030. [https://www.statista.com/statistics/993364/new-connected-vehicles-on-roads-uk/#:~:text=This%20statistic%20shows%20a%20forecast,to%20amount%20to%20\(2022\)](https://www.statista.com/statistics/993364/new-connected-vehicles-on-roads-uk/#:~:text=This%20statistic%20shows%20a%20forecast,to%20amount%20to%20(2022))
2. Rebiger, S., Moraes, T., de Vergara, X.L.L.: Connected cars. European Data Protection Supervisor. [https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-3-connected-cars\\_en\(2019\)](https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-3-connected-cars_en(2019))
3. Kumar, S., Singh, K., Kumar, S., Kaiwartya, O., Cao, Y., Zhou, H.: Delimitated anti jammer scheme for internet of vehicle: machine learning based security approach. *IEEE Access* 7, 113 311–113 323 (2019)
4. Rathore, R.S., Hewage, C., Kaiwartya, O., Lloret, J.: In-vehicle communication cyber security: challenges and solutions. *Sensors* 22(17), 6679 (2022)
5. Kim, K., Kim, J.S., Jeong, S., Park, J.-H., Kim, H.K.: Cybersecurity for autonomous vehicles: review of attacks and defense. *Comput. Secur.* 103, 102150 (2021)
6. El-Rewini, Z., Sadatsharan, K., Selvaraj, D.F., Plathottam, S.J., Ranganathan, P.: Cybersecurity challenges in vehicular communications. *Veh. Commun.* 23, 100214 (2020)
7. Sun, X., Yu, F.R., Zhang, P.: A survey on cyber-security of connected and autonomous vehicles (CAVs). *IEEE Trans. Intell. Transp. Syst.* 23(7), 6240–6259 (2021)
8. Ju, Z., Zhang, H., Li, X., Chen, X., Han, J., Yang, M.: A survey on attack detection and resilience for connected and automated vehicles: from vehicle dynamics and control perspective. *IEEE Trans. Intell. Veh.* (2022)
9. Huang, J., Fang, D., Qian, Y., Hu, R.Q.: Recent advances and challenges in security and privacy for V2X communications. *IEEE Open J. Veh. Technol.* 1, 244–266 (2020)
10. Guan, T., Han, Y., Kang, N., Tang, N., Chen, X., Wang, S.: An overview of vehicular cybersecurity for intelligent connected vehicles. *Sustainability* 14(9), 5211 (2022)
11. Yan, C., Xu, W., Liu, J.: Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. *Def. Con.* 24(8), 109 (2016)
12. DiPalma, C., Wang, N., Sato, T., Chen, Q.A.: Security of camera-based perception for autonomous driving under adversarial attack. In: 2021 IEEE Security and Privacy Workshops (SPW), pp. 243–243. IEEE, Piscataway, NJ (2021)
13. Petit, J., Stottelaar, B., Feiri, M., Kargl, F.: Remote attacks on automated vehicles sensors: experiments on camera and LiDAR. *Black Hat Eur.* 11(2015), 995 (2015)
14. Rastogi, N., Rampazzi, S., Clifford, M., Heller, M., Bishop, M., Levitt, K.: Explaining radar features for detecting spoofing attacks in connected autonomous vehicles. *arXiv:2203.00150* (2022)
15. Pham, M., Xiong, K.: A survey on security attacks and defense techniques for connected and autonomous vehicles. *Comput. Secur.* 109, 102269 (2021)
16. Lim, B.S., Keoh, S.L., Thing, V.L.: Autonomous vehicle ultrasonic sensor vulnerability and impact assessment. In: 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), pp. 231–236. IEEE, Piscataway, NJ (2018)
17. Xu, W., Yan, C., Jia, W., Ji, X., Liu, J.: Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles. *IEEE Internet Things J.* 5(6), 5015–5029 (2018)
18. Gluck, T., Kravchik, M., Chocron, S., Elovici, Y., Shabtrai, A.: Spoofing attack on ultrasonic distance sensors using a continuous signal. *Sensors* 20(21), 6157 (2020)
19. Shang, E., An, X., Wu, T., Hu, T., Yuan, Q., He, H.: LiDAR based negative obstacle detection for field autonomous land vehicles. *J. Field Rob.* 33(5), 591–617 (2016)
20. Milaat, F.A., Liu, H.: Decentralized detection of GPS spoofing in vehicular ad hoc networks. *IEEE Commun. Lett.* 22(6), 1256–1259 (2018)
21. Narain, S., Ranganathan, A., Noubir, G.: Security of gps/ins based on-road location tracking systems. In: 2019 IEEE Symposium on Security and Privacy (SP), pp. 587–601. IEEE, Piscataway, NJ (2019)

22. Kamal, M., Barua, A., Vitale, C., Laoudias, C., Ellinas, G.: Gps location spoofing attack detection for enhancing the security of autonomous vehicles. In: 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), pp. 1–7. IEEE, Piscataway, NJ (2021)
23. Sanders, C., Wang, Y.: Localizing spoofing attacks on vehicular GPS using vehicle-to-vehicle communications. *IEEE Trans. Veh. Technol.* 69(12), 15 656–15 667 (2020)
24. Cope, P., Campbell, J., Hayajneh, T.: An investigation of bluetooth security vulnerabilities. In: 2017 IEEE 7th annual computing and communication workshop and conference (CCWC), pp. 1–7. IEEE, Piscataway, NJ (2017)
25. Muhammad, M., Safdar, G.A.: Survey on existing authentication issues for cellular-assisted V2X communication. *Veh. Commun.* 12, 50–65 (2018)
26. Hadded, M., Muhlethaler, P., Laouiti, A., Zagrouba, R., Saidane, L.A.: TDMA-based MAC protocols for vehicular ad hoc networks: a survey, qualitative analysis, and open research issues. *IEEE Commun. Surv. Tutorials* 17(4), 2461–2492 (2015)
27. Abboud, K., Omar, H.A., Zhuang, W.: Interworking of dsrc and cellular network technologies for v2x communications: A survey. *IEEE Trans. Veh. Technol.* 65(12), 9457–9470 (2016)
28. Labib, M., Marojevic, V., Reed, J.H.: Analyzing and enhancing the resilience of LTE/LTE-A systems to RF spoofing. In: 2015 IEEE Conference on Standards for Communications and Networking (CSCN), pp. 315–320. IEEE, Piscataway, NJ (2015)
29. Lu, R., Zhang, L., Ni, J., Fang, Y.: 5G vehicle-to-everything services: Gearing up for security and privacy. *Proc. IEEE* 108(2), 373–389 (2019)
30. Chandavarkar, B., et al.: Mitigation of desynchronization attack during inter-eNodeB handover key management in LTE. In: 2015 Eighth International Conference on Contemporary Computing (IC3), pp. 561–566. IEEE, Piscataway, NJ (2015)
31. Park, S., Kim, B., Yoon, H., Choi, S.: RA-eV2V: relaying systems for LTE-V2V communications. *J. Commun. Networks* 20(4), 396–405 (2018)
32. Miller, C., Valasek, C.: Remote exploitation of an unaltered passenger vehicle. *Black Hat USA 2015(S 91)*, 1–91 (2015)
33. Zeng, K.C., Liu, S., Shu, Y., Wang, D., Li, H., Dou, Y., Wang, G., Yang, Y.: All your GPS are belong to us: towards stealthy manipulation of road navigation systems. In: 27th USENIX security symposium (USENIX security 18), pp. 1527–1544. ACM, New York (2018)
34. Yang, T., Lv, C.: A secure sensor fusion framework for connected and automated vehicles under sensor attacks. *IEEE Internet Things J.* 9(22), 22357–22365 (2021)
35. Yang, Z., Ying, J., Shen, J., Feng, Y., Chen, Q.A., Mao, Z.M., Liu, H.X.: Anomaly detection against GPS spoofing attacks on connected and autonomous vehicles using learning from demonstration. *IEEE Trans. Intell. Transp. Syst.* 24(9), 9462–9475 (2023)
36. Axelrod, C.W.: Cybersecurity in the age of autonomous vehicles, intelligent traffic controls and pervasive transportation networks. In: 2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT), pp. 1–6. IEEE, Piscataway, NJ (2017)
37. Breu, J., Brakemeier, A., Menth, M.: A quantitative study of cooperative awareness messages in production VANETs. *EURASIP J. Wireless Commun. Networking* 2014(1), 1–18 (2014)
38. ETSI, EN 302 637-2 V1.3.1 (2014-09) intelligent transport systems (ITS). Vehicular Communications. Accessed 12 May 2023
39. ETSI, TS 102 637-3, v1. 1.1 (2010), intelligent transport systems (ITS). Vehicular Communications, Basic Set of Applications, Part, vol. 3 (2010). Accessed 27 May 2023
40. Tanuja, K., Sushma, T., Bharathi, M., Arun, K.: A survey on VANET technologies (2015). Accessed 29 May 2023
41. Wang, X., Mao, S., Gong, M.X.: An overview of 3GPP cellular vehicle-to-everything standards. *GetMobile: Mobile Comput. Commun.* 21(3), 19–25 (2017)
42. Kim, S., Shrestha, R.: *Automotive Cyber Security*. Springer, Singapore (2020)
43. Xu, Z., Li, X., Zhao, X., Zhang, M.H., Wang, Z., et al.: DSRC versus 4G-LTE for connected vehicle applications: a study on field experiments of vehicular communication performance. *J. Adv. Transp.* 2017, 2750452 (2017)
44. Kühlmorgen, S., Schmagier, P., Festag, A., Fettweis, G.: Simulation-based evaluation of ETSI ITS-G5 and cellular-VCS in a real-world road traffic scenario. In: 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), pp. 1–6. IEEE, Piscataway, NJ (2018)
45. Cecchini, G., Bazzi, A., Masini, B.M., Zanella, A.: Performance comparison between IEEE 802.11 P and LTE-V2V in-coverage and out-of-coverage for cooperative awareness. In: 2017 IEEE Vehicular Networking Conference (VNC), pp. 109–114. IEEE, Piscataway, NJ (2017)
46. Ansari, K.: Joint use of DSRC and C-V2X for V2X communications in the 5.9 GHz its band. *IET Intell. Transport Syst.* 15(2), 213–224 (2021)
47. Ghafoor, K.Z., Guizani, M., Kong, L., Maghddid, H.S., Jasim, K.F.: Enabling efficient coexistence of DSRC and C-V2X in vehicular networks. *IEEE Wireless Commun.* 27(2), 134–140 (2019)
48. Mir, Z.H., Toutouh, J., Filali, F., Ko, Y.-B.: Enabling DSRC and C-V2X integrated hybrid vehicular networks: architecture and protocol. *IEEE Access* 8, 180909–180927 (2020)
49. Azzaoui, N., Korichi, A., Brik, B., Fekair, M.E.A., Kerrache, C.A.: Wireless communication in internet of vehicles networks: DSRC-based vs cellular-based. In: Proceedings of the 4th International Conference on Smart City Applications, pp. 1–6. ACM, New York (2019)
50. Yu, B., Xu, C.-Z., Xiao, B.: Detecting Sybil attacks in VANETs. *J. Parallel Distrib. Comput.* 73(6), 746–756 (2013)
51. Iwendi, C., Uddin, M., Ansere, J.A., Nkurunziza, P., Anajemba, J.H., Bashir, A.K.: On detection of Sybil attack in large-scale VANETs using spider-monkey technique. *IEEE Access* 6, 47 258–47 267 (2018)
52. Quevedo, C.H., Quevedo, A.M., Campos, G.A., Gomes, R.L., Celestino, J., Serhrouchni, A.: An intelligent mechanism for Sybil attacks detection in VANETs. In: ICC 2020-2020 IEEE International Conference on Communications (ICC), pp. 1–6. IEEE, Piscataway, NJ (2020)
53. Pattanayak, B.K., Pattnaik, O., Pani, S.: Dealing with Sybil attack in VANET. In: Proceedings of ICICC 2019 Intelligent and Cloud Computing, vol. 1, pp. 471–480. Springer, Cham (2021)
54. Hamdan, S., Hudaib, A., Awajan, A.: Detecting Sybil attacks in vehicular ad hoc networks. *Int. J. Parallel Emergent Distrib. Syst.* 36(2), 69–79 (2021)
55. Guttman, B., Roback, E.A.: *An Introduction to Computer Security: the NIST Handbook*. Diane Publishing, Darby, PA (1995)
56. Fan, Q.G., Wang, L., Cai, Y.N., Li, Y.Q., Chen, J.: VANET routing replay attack detection research based on SVM. In: MATEC Web of Conferences, vol. 63, p. 05020. EDP Sciences, Les Ulis (2016)
57. Al-shareeda, M.A., Anbar, M., Hasbullah, I.H., Manickam, S., Abdullah, N., Hamdi, M.M.: Review of prevention schemes for replay attack in vehicular ad hoc networks (VANETs). In: 2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP), pp. 394–398. IEEE, Piscataway, NJ (2020)
58. Kumar, A.: Replay attack detection in VANETs using machine learning algorithm. Ph.D. dissertation, University of Windsor, Windsor (2022)
59. Kumar, A., Shahid, M.A., Jaekel, A., Zhang, N., Kneppers, M.: Machine learning based detection of replay attacks in VANET. In: NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, pp. 1–6. IEEE, Piscataway, NJ (2023)
60. Boyle, R.J., Panko, R.R.: *Corporate Computer Security*. Pearson, London (2015)
61. Liu, J., Zhang, S., Sun, W., Shi, Y.: In-vehicle network attacks and countermeasures: challenges and future directions. *IEEE Network* 31(5), 50–58 (2017)
62. Sheikh, M.S., Liang, J., Wang, W.: A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs). *Sensors* 19(16), 3589 (2019)
63. Gruebler, A., McDonald-Maier, K.D., Alhecti, K.M.A.: An intrusion detection system against black hole attacks on the communication network of self-driving cars. In: 2015 Sixth International Conference on Emerging Security Technologies (EST), pp. 86–91. IEEE, Piscataway, NJ (2015)

64. Quyoom, A., Ali, R., Gouttam, D.N., Sharma, H.: A novel mechanism of detection of denial of service attack (DOS) in VANET using malicious and irrelevant packet detection algorithm (MIPDA). In: International Conference on Computing, Communication & Automation, pp. 414–419. IEEE, Piscataway, NJ (2015)
65. Shabbir, M., Khan, M.A., Khan, U.S., Saqib, N.A.: Detection and prevention of distributed denial of service attacks in VANETs. In: 2016 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 970–974. IEEE, Piscataway, NJ (2016)
66. Kumar, S., Mann, K.S.: Detection of multiple malicious nodes using entropy for mitigating the effect of denial of service attack in VANETs. In: 2018 4th International conference on computing sciences (ICCS), pp. 72–79. IEEE, Piscataway, NJ (2018)
67. Kumar, S., Mann, K.S.: Prevention of DOS attacks by detection of multiple malicious nodes in VANETs. In: 2019 International Conference on Automation, Computational and Technology Management (ICACTM), pp. 89–94. IEEE, Piscataway, NJ (2019)
68. Verma, K., Hasbullah, H.: Bloom-filter based IP-chock detection scheme for denial of service attacks in VANET. *Secur. Commun. Netw.* 8(5), 864–878 (2015)
69. Adhikary, K., Bhushan, S., Kumar, S., Dutta, K.: Hybrid algorithm to detect DDOS attacks in VANETs. *Wireless Pers. Commun.* 114, 3613–3634 (2020)
70. Lahrouni, Y., Pereira, C., Bensaber, B.A., Biskri, I.: Using mathematical methods against denial of service (DOS) attacks in VANET. In: Proceedings of the 15th ACM International Symposium on Mobility Management and Wireless Access, pp. 17–22. ACM, New York (2017)
71. Poongodi, M., Hamdi, M., Sharma, A., Ma, M., Singh, P.K.: DDOS detection mechanism using trust-based evaluation system in VANET. *IEEE Access* 7, 183 532–183 544 (2019)
72. Chen, C.-L., Cheng, K.-W.: Design of a VANET privacy and non-repudiation accident reporting system. *Secur. Commun. Networks* 9(18), 5187–5202 (2016)
73. Choi, J., Jung, S.: A security framework with strong non-repudiation and privacy in VANETs. In: 2009 6th IEEE Consumer Communications and Networking Conference, pp. 1–5. IEEE, Piscataway, NJ (2009)
74. Li, J., Lu, H., Guizani, M.: ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for vanets. *IEEE Trans. Parallel Distrib. Syst.* 26(4), 938–948 (2014)
75. Chen, C.-L., Chiang, M.-L., Peng, C.-C., Chang, C.-H., Sui, Q.-R.: A secure mutual authentication scheme with non-repudiation for vehicular ad hoc networks. *Int. J. Commun. Syst.* 30(6), e3081 (2017)
76. Azees, M., Vijayakumar, P., Jegatha Deborah, L.: Comprehensive survey on security services in vehicular ad-hoc networks. *IET Intell. Transp. Syst.* 10(6), 379–388 (2016)
77. Yao, Y., Zhao, J., Li, Z., Cheng, X., Wu, L., Li, X.: Cognitive risk control for anti-eavesdropping in connected and autonomous vehicles network. In: 2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall), pp. 1–7. IEEE, Piscataway, NJ (2022)
78. Yao, Y., Zhao, J., Li, Z., Cheng, X., Wu, L.: Jamming and eavesdropping defense scheme based on deep reinforcement learning in autonomous vehicle networks. *IEEE Trans. Inf. Forensics Secur.* 18, 1211–1224 (2023)
79. Zhang, L.: Research on security and Privacy in Vehicular ad hoc Networks. Universitat Rovira i Virgili, Catalonia (2010).
80. Qu, F., Wu, Z., Wang, F.-Y., Cho, W.: A security and privacy review of vanets. *IEEE Trans. Intell. Transp. Syst.* 16(6), 2985–2996 (2015)
81. Ali, I., Hassan, A., Li, F.: Authentication and privacy schemes for vehicular ad hoc networks (VANETs): a survey. *Veh. Commun.* 16, 45–61 (2019)
82. Jan, S.A., Amin, N.U., Othman, M., Ali, M., Umar, A.I., Basir, A.: A survey on privacy-preserving authentication schemes in VANETs: attacks, challenges and open issues. *IEEE Access* 9, 153 701–153 726 (2021)
83. Kerrache, C.A., Lagraa, N., Hussain, R., Ahmed, S.H., Benslimane, A., Calafate, C.T., Cano, J.C., Vegni, A.M.: Tacashi: Trust-aware communication architecture for social internet of vehicles. *IEEE Internet Things J.* 6(4), 5870–5877 (2019)
84. Koirala, B., Tangade, S.S., Manvi, S.S.: Trust management based on node stay time in VANET. In: 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 242–248. IEEE, Piscataway, NJ (2018)
85. Hu, H., Lu, R., Zhang, Z., Shao, J.: Replace: a reliable trust-based platoon service recommendation scheme in VANET. *IEEE Trans. Veh. Technol.* 66(2), 1786–1797 (2017)
86. Xiong, J., Bi, R., Zhao, M., Guo, J., Yang, Q.: Edge-assisted privacy-preserving raw data sharing framework for connected autonomous vehicles. *IEEE Wireless Commun.* 27(3), 24–30 (2020)
87. Ren, D., Du, S., Zhu, H.: A novel attack tree based risk assessment approach for location privacy preservation in the VANETs. In: 2011 IEEE International Conference on Communications (ICC), pp. 1–5. IEEE, Piscataway, NJ (2011)
88. Costantino, G., De Vincenzi, M., Martinelli, F., Matteucci, I.: A privacy-preserving solution for intelligent transportation systems: private driver dna. *IEEE Trans. Intell. Transp. Syst.* 24(1), 258–273 (2022)
89. Alshudukhi, J.S., Al-Mekhlafi, Z.G., Mohammed, B.A.: A lightweight authentication with privacy-preserving scheme for vehicular ad hoc networks based on elliptic curve cryptography. *IEEE Access* 9, 15 633–15 642 (2021)
90. Yu, R., Bai, Z., Yang, L., Wang, P., Move, O.A., Liu, Y.: A location cloaking algorithm based on combinatorial optimization for location-based services in 5G networks. *IEEE Access* 4, 6515–6527 (2016)
91. Freudiger, J., Manshaei, M.H., Hubaux, J.-P., Parkes, D.C.: On non-cooperative location privacy: a game-theoretic analysis. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 324–337. ACM, New York (2009)
92. Xu, T., Cai, Y.: Location anonymity in continuous location-based services. In: Proceedings of the 15th annual ACM International Symposium on Advances in Geographic Information Systems, pp. 1–8. ACM, New York (2007)
93. Iqbal, S., Ball, P., Kamarudin, M.H., Bradley, A.: Simulating malicious attacks on vanets for connected and autonomous vehicle cybersecurity: A machine learning dataset. In: 2022 13th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), pp. 332–337. IEEE, Piscataway, NJ (2022)
94. van der Heijden, R.W., Lukaseder, T., Kargl, F.: Veremi: A dataset for comparable evaluation of misbehavior detection in VANETs. In: Security and Privacy in Communication Networks: 14th International Conference, SecureComm 2018, Singapore, Singapore, August 8–10, 2018, Proceedings, Part I, pp. 318–337. Springer, Cham (2018)
95. Kamel, J., Wolf, M., Van Der Hei, R.W., Kaiser, A., Urien, P., Kargl, F.: Veremi extension: a dataset for comparable evaluation of misbehavior detection in VANETs. In: ICC 2020-2020 IEEE International Conference on Communications (ICC), pp. 1–6. IEEE, Piscataway, NJ (2020)
96. So, S., Sharma, P., Petit, J.: Integrating plausibility checks and machine learning for misbehavior detection in VANET. In: 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 564–571. IEEE, Piscataway, NJ (2018)
97. Singh, P.K., Gupta, S., Vashistha, R., Nandi, S.K., Nandi, S.: Machine learning based approach to detect position falsification attack in Vanets. In: Security and Privacy: Second ISEA International Conference, pp. 166–178. Springer, Cham (2019)
98. Amanullah, M.A., Chhetri, M.B., Loke, S.W., Doss, R.: Burst-ADMA: towards an australian dataset for misbehaviour detection in the internet of vehicles. In: 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), pp. 624–629. IEEE, Piscataway, NJ (2022)
99. Grover, J., Gaur, M.S., Laxmi, V.: Trust establishment techniques in VANET. In: *Wireless Networks and Security*, pp. 273–301. Springer, Berlin, Heidelberg (2013)
100. Hussain, R., Lee, J., Zeadally, S.: Trust in VANET: a survey of current solutions and future research opportunities. *IEEE Trans. Intell. Transp. Syst.* 22(5), 2553–2571 (2021)
101. Tangade, S.S., Manvi, S.S.: A survey on attacks, security and trust management solutions in VANETs. In: 2013 Fourth international conference on computing, communications and networking technologies (ICCCNT), pp. 1–6. IEEE, Piscataway, NJ (2013)

102. Zhang, J.: A survey on trust management for VANET. In: 2011 IEEE International Conference on Advanced Information Networking and Applications, pp. 105–112. IEEE, Piscataway, NJ (2011)
103. Mehdi, M.M., Raza, I., Hussain, S.A.: A game theory based trust model for vehicular ad hoc networks (VANETs). *Comput. Networks* 121, 152–172 (2017)
104. Zadeh, L.A.: Fuzzy logic. *Computer* 21(4), 83–93 (1988)
105. McNeill, F.M., Thro, E.: Fuzzy logic: a practical approach. Academic Press, San Diego, CA (2014)
106. Soleymani, S.A., Abdullah, A.H., Zareei, M., Anisi, M.H., Vargas-Rosales, C., Khan, M.K., Goudarzi, S.: A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing. *IEEE Access* 5, 15 619–15 629 (2017)
107. Alroshan, A., Asgher, T., Hussain, M., Shahzad, M., Rasool, F., Abu-Khadrah, A.: Virtual trust on driverless cars using fuzzy logic design. In: 2022 International Conference on Business Analytics for Technology and Security (ICBATS), pp. 1–7. IEEE, Piscataway, NJ (2022)
108. Malhi, A.K., Batra, S.: Fuzzy-based trust prediction for effective coordination in vehicular ad hoc networks. *Int. J. Commun. Syst.* 30(6), e3111 (2017)
109. Osborne, M.J., Rubinstein, A.: A course in game theory. MIT Press, Cambridge, MA (1994)
110. Gibbons, R.S.: Game theory for applied economists. Princeton University Press, Princeton, NJ (1992)
111. Liang, X., Xiao, Y.: Game theory for network security. *IEEE Commun. Surv. Tut.* 15(1), 472–486 (2012)
112. Biswas, T., Sanzgiri, A., Upadhyaya, S.: Building long term trust in vehicular networks. In: 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring), pp. 1–5. IEEE, Piscataway, NJ (2016)
113. Kerrache, C.A., Lagraa, N., Calafate, C.T., Cano, J.-C., Manzoni, P.: T-VNets: a novel trust architecture for vehicular networks using the standardized messaging services of ETSI ITS. *Comput. Commun.* 93, 68–83 (2016)
114. Halabi, T., Zulkernine, M.: Trust-based cooperative game model for secure collaboration in the internet of vehicles. In: ICC 2019-2019 IEEE International Conference on Communications (ICC), pp. 1–6. IEEE, Piscataway, NJ (2019)
115. 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 Trans. Veh. Technol.* 69(3), 3267–3279 (2020)
116. Fan, N., Wu, C.Q.: On trust models for communication security in vehicular ad-hoc networks. *Ad Hoc Networks* 90, 101740 (2019)
117. Alpcan, T., Buchegger, S.: Security games for vehicular networks. *IEEE Trans. Mob. Comput.* 10(2), 280–290 (2010)
118. Aliyu, A., Abdullah, A.H., Kaiwartya, O., Cao, Y., Usman, M.J., Kumar, S., Lobiyal, D., Raw, R.S.: Cloud computing in VANETs: architecture, taxonomy, and challenges. *IETE Tech. Rev.* 35(5), 523–547 (2018)
119. Raza, S., Wang, S., Ahmed, M., Anwar, M.R.: A survey on vehicular edge computing: architecture, applications, technical issues, and future directions. *Wireless Commun. Mobile Comput.* 2019, 3159762 (2019)
120. Whaiduzzaman, M., Sookhak, M., Gani, A., Buyya, R.: A survey on vehicular cloud computing. *J. Network Comput. Appl.* 40, 325–344 (2014)
121. Gu, L., Zeng, D., Guo, S.: Vehicular cloud computing: a survey. In: 2013 IEEE Globecom Workshops (GC Wkshps), pp. 403–407. IEEE, Piscataway, NJ (2013)
122. Hussain, R., Son, J., Eun, H., Kim, S., Oh, H.: Rethinking vehicular communications: Merging VANET with cloud computing. In: 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, pp. 606–609. IEEE, Piscataway, NJ (2012)
123. Olariu, S., Khalil, I., Abuelela, M.: Taking VANET to the clouds. *Int. J. Pervasive Comput. Commun.* 7(1), 7–21 (2011)
124. Bitam, S., Mellouk, A., Zeadally, S.: VANET-cloud: a generic cloud computing model for vehicular ad hoc networks. *IEEE Wireless Commun.* 22(1), 96–102 (2015)
125. Chen, X., Wang, L.: A cloud-based trust management framework for vehicular social networks. *IEEE Access* 5, 2967–2980 (2017)
126. Aladwan, M.N., Awaysheh, F.M., Alawadi, S., Alazab, M., Pena, T.F., Cabaleiro, J.C.: TrustE-VC: trustworthy evaluation framework for industrial connected vehicles in the cloud. *IEEE Trans. Ind. Inf.* 16(9), 6203–6213 (2020)
127. Mudengudi, S.S., Kakkasageri, M.S.: Establishing trust between vehicles in vehicular clouds: an agent based approach. In: 2017 International Conference on Smart Technologies for Smart Nation (SmartTechCon), pp. 529–533. IEEE, Piscataway, NJ (2017)
128. Tang, Z., Liu, A., Li, Z., Choi, Y.-J., Sekiya, H., Li, J.: A trust-based model for security cooperating in vehicular cloud computing. *Mobile Inf. Syst.* 2016, 9083608 (2016)
129. El-Sayed, H., Zeadally, S., Khan, M., Alexander, H.: Edge-centric trust management in vehicular networks. *Microprocess. Microsyst.* 84, 104271 (2021)
130. Garg, S., Singh, A., Kaur, K., Auja, G.S., Batra, S., Kumar, N., Obaidat, M.S.: Edge computing-based security framework for big data analytics in VANETs. *IEEE Network* 33(2), 72–81 (2019)
131. Yang, Z., Yang, K., Lei, L., Zheng, K., Leung, V.C.: Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet Things J.* 6(2), 1495–1505 (2018)
132. Yang, Z., Zheng, K., Yang, K., Leung, V.C.: A blockchain-based reputation system for data credibility assessment in vehicular networks. In: 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1–5. IEEE, Piscataway, NJ (2017)
133. Yang, Y.-T., Chou, L.-D., Tseng, C.-W., Tseng, F.-H., Liu, C.-C.: Blockchain-based traffic event validation and trust verification for VANETs. *IEEE Access* 7, 30 868–30 877 (2019)
134. Ayed, S., Hbaieb, A., Chaari, L.: Blockchain and trust-based clustering scheme for the IoV. *Ad Hoc Networks* 142, 103093 (2023)
135. Álvares, P., Silva, L., Magaia, N.: Blockchain-based solutions for uav-assisted connected vehicle networks in smart cities: a review, open issues, and future perspectives. *Telecom* 2(1), 108–140 (2021)
136. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the Internet of Things. *IEEE Access* 4, 2292–2303 (2016)
137. Kandah, F., Huber, B., Skjellum, A., Altarawneh, A.: A blockchain-based trust management approach for connected autonomous vehicles in smart cities. In: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0544–0549. IEEE, Piscataway, NJ (2019)
138. Dargahi, T., Ahmadvand, H., Alraja, M.N., Yu, C.-M.: Integration of blockchain with connected and autonomous vehicles: vision and challenge. *ACM J. Data Inf. Qual.* 14(1), 1–10 (2021)
139. Sharma, P., Liu, H., Wang, H., Zhang, S.: Securing wireless communications of connected vehicles with artificial intelligence. In: 2017 IEEE international symposium on technologies for homeland security (HST), pp. 1–7. IEEE, Piscataway, NJ (2017)
140. Sharma, P., Austin, D., Liu, H.: Attacks on machine learning: Adversarial examples in connected and autonomous vehicles. In: 2019 IEEE International Symposium on Technologies for Homeland Security (HST), pp. 1–7. IEEE, Piscataway, NJ (2019)
141. Rajapaksha, S., Kalutarage, H., Al-Kadri, M.O., Petrovski, A., Madzudzo, G., Cheah, M.: AI-based intrusion detection systems for in-vehicle networks: a survey. *ACM Comput. Surv.* 55(11), 1–40 (2023)
142. Song, H.M., Woo, J., Kim, H.K.: In-vehicle network intrusion detection using deep convolutional neural network. *Veh. Commun.* 21, 100198 (2020)

**How to cite this article:** Mwanje, M.D., Kaiwartya, O., Aljaidi, M., Cao, Y., Kumar, S., Jha, D.N., Naser, A., Lloret, J.: Cyber security analysis of connected vehicles. *IET Intell. Transp. Syst.* 1–21 (2024).  
<https://doi.org/10.1049/itr2.12504>