World Electric Vehicle Journal

MDPI

Article

Enhancing Intelligent Transport Systems Through Decentralized Security Frameworks in Vehicle-to-Everything Networks

Usman Tariq * and Tariq Ahamed Ahanger

Management Information System Department, College of Business Administration, Prince Sattam Bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia; t.ahanger@psau.edu.sa
* Correspondence: u.tariq@psau.edu.sa; Tel.: +966-11-588-7080

Abstract: Vehicle Ad hoc Networks (VANETs) play an essential role in intelligent transportation systems (ITSs) by improving road safety and traffic management through robust decentralized communication between vehicles and infrastructure. Yet, decentralization introduces security vulnerabilities, including spoofing, tampering, and denial-of-service attacks, which can compromise the reliability and safety of vehicular communications. Traditional centralized security mechanisms are often inadequate in providing the real-time response and scalability required by such dispersed networks. This research promotes a shift toward distributed and real-time technologies, including blockchain and secure multi-party computation, to enhance communication integrity and privacy, ultimately strengthening system resilience by eliminating single points of failure. A core aspect of this study is the novel D-CASBR framework, which integrates three essential components. First, it employs hybrid machine learning methods, such as ElasticNet and Gradient Boosting, to facilitate real-time anomaly detection, identifying unusual activities as they occur. Second, it utilizes a consortium blockchain to provide secure and transparent information exchange among authorized participants. Third, it implements a fog-enabled reputation system that uses distributed fog computing to effectively manage trust within the network. This comprehensive approach addresses latency issues found in conventional systems while significantly improving the reliability and efficacy of threat detection, achieving 95 percent anomaly detection accuracy with minimal false positives. The result is a substantial advancement in securing vehicular networks.

Keywords: vehicular ad hoc networks (VANETs); decentralized intrusion detection systems (D-IDSs); interconnectivity; privacy preserving; hybrid machine learning; fog computing; minority class imbalance; real-time data processing

Academic Editors: Carolina Tripp-Barba, Luis Urquiza and José Alfonso Aguilar Calderón

Received: 20 November 2024
Revised: 29 December 2024
Accepted: 31 December 2024
Published: 3 January 2025

Citation: Tariq, U.; Ahanger, T.A. Enhancing Intelligent Transport Systems Through Decentralized Security Frameworks in Vehicle-to-Everything Networks. *World Electr. Veh. J.* **2025**, *16*, 24. https://doi.org/10.3390/wevj16010024

1. Introduction

As smart cities evolve, the integration of Smart Traffic Management Systems becomes pivotal in shaping the urban transportation landscape, leveraging VANETs to ensure seamless and efficient traffic operations. The rapid advancement of ITSs is closely tied to the effectiveness of VANETs, which are crucial for secure and efficient vehicle-to-infrastructure communications [1]. These networks play a key role in facilitating applications that range from real-time traffic management to cooperative driving to significantly enhance road safety and the overall driving experience. Nonetheless, the open and distributed structure of VANETs exposes them to multiple cyber threats such as spoofing attacks and message manipulation. This research aimed at investigating and applying innovative technologies and methods to enhance the security and dependability of VANETs in the face of these vulnerabilities.

VANETs leverage a decentralized communication paradigm where vehicles directly interact without relying on a central authority. The decentralized structure of VANETs provides benefits like reducing single points of failure and enhancing network resilience, but it also poses unique challenges in security management (such as dynamic network topology, limited computational resources for vehicles, difficulty in key management and distribution, user anonymity, and potential for Sybil attacks) [2]. This drives the necessity for innovative solutions tailored to address these vulnerabilities through enhanced security frameworks that utilize the technology that is eligible to lay the groundwork for improved defensive mechanisms. For a deeper understanding, we thoroughly examined decentralized intrusion detection systems that utilize fog computing and blockchain technology to provide scalable and timely responses, which is crucial for upholding the integrity and security of VANET communications [3]. Herein, addressing the problem of minority class imbalance (i.e., bias towards frequent patterns, reduced attack detection accuracy, difficulty in model generalization, false negatives (undetected attacks), unreliable performance evaluation) in VANET IDS was essential due to the infrequency of malicious events compared to normal traffic activities [4]. Consequently, to augment the accuracy and reliability of IDSs, we investigated various advanced techniques (e.g., SMOTE (Synthetic Minority Over-Sampling Technique), ADASYN (Adaptive Synthetic Minority Over-Sampling Technique), GAN-based Over-sampling (Generative Adversarial Networks), Tomek Links, and Cost-Sensitive Learning) for balancing minority classes in datasets. Balancing minority classes helped to prevent the model from being biased towards frequent normal traffic data.

It is evident that the critical role of real-time anomaly detection is undeniable, as it is fundamental to maintaining continuous network security and operational integrity. By deploying fog nodes at the network edge, the vast amount of data generated by vehicles and infrastructure needs to be processed immediately to reduce latency and ensure the quick identification and mitigation of anomalies and security threats [5]. A thorough investigation of VANET management (e.g., identity management, access control, secure communication, privacy preserving, node reputation verification, and certificate revocation) revealed that software-defined networking (SDN) introduces a transformative approach by decoupling the control layer from the data layer [6]. This separation allows for dynamic network reconfiguration and agile responses to network issues and security challenges. In the described context, our research also focused on SDN applications in VANETs, particularly in terms of isolating compromised network segments, optimizing routing protocols, and enhancing overall security posture with superior attack mitigation strategies. With this, the novel identity-based broadcast encryption (IBBE) was implemented to offer a powerful solution for securing group communications in VANETs. IBBE [7] ensures that only authorized vehicles can decrypt transmitted messages, providing a robust mechanism for protecting privacy and integrity in group communication settings. Our analysis on IBBE demonstrated its effectiveness in preventing unauthorized access to messages and boosting network security. Implementing user privacy in VANETs was undertaken through anonymous vehicle-to-vehicle (V2V) communication, which is crucial for protecting users from potential tracking and profiling.

Thus, the main contributions of this research are as follows:

(a) In consideration with cyber anomalies (such as malicious communication traffic analysis, GPS and node identity spoofing, data forgery, denial of authentication and services, and routing disruption attacks), we investigated D-IDSs using fog computing and consortium blockchain technology to enhance scalability and response times.
(b) We explored real-time anomaly detection using fog computing for immediate data processing to reduce latency and effectively mitigate security threats.

(c) We examined the application of SDN to separate control and data layers to allow for dynamic network reconfiguration and improved security management.
(d) We addressed minority class imbalance in intrusion detection by employing advanced techniques to improve the detection accuracy of rare malicious events.
(e) We implemented and analyzed the novel IBBE to secure group communications to ensure that only authorized vehicles can access transmitted messages.
(f) We developed strategies for anonymous V2V communication to protect user privacy from tracking and profiling without compromising network efficiency.
(g) We conducted a comparative analysis of centralized and decentralized security approaches to evaluate the strengths and weaknesses of each, including their implications for scalability, security, and privacy.
(h) Ultimately, we proposed a novel approach utilizing hybrid machine learning (ML) models for intrusion detection. Our experimental evaluation demonstrates that the proposed method achieves superior accuracy compared to traditional techniques, offering a promising avenue for enhanced security in vehicular communication.

The progression of this research paper unfolds systematically to address the security vulnerabilities in VANETs through innovative decentralized and real-time technologies. As exhibited, the Introduction Section set the stage by emphasizing the importance of security in VANETs for intelligent transportation systems. Following this, a thorough literature review explores existing challenges and highlights the need for improved security frameworks. The core of this paper introduces a novel decentralized intrusion detection system (D-CASBR framework) that leveraged fog computing and consortium blockchain technology to enhance the scalability and response times of security measures. The subsequent sections of this paper dive into the succeeding proposed methodology, system models, and problem definitions. This detailed exploration provides the research community with technical insights into the operations of the novel system and developed framework. Finally, this paper concludes with a comprehensive evaluation of the presented methods, showcasing their effectiveness through simulated/emulated scenarios and highlighting future research directions.

2. Literature Review

VANETs are pivotal in enabling vehicle-to-everything (V2X) communication and managing traffic by allowing vehicles and infrastructure to exchange information in real time, which is crucial for enhancing road safety and optimizing traffic flows. The security of these networks is paramount for their reliable and safe operation as they support safety-critical applications that depend on the accuracy and timeliness of the communicated data. We focused on various cyber anomalies that threaten VANETs including but not limited to malicious communication traffic analysis, GPS and node identity spoofing [8], data forgery, denial of authentication and services [9], and routing disruption attacks [4,6]. We evaluated existing security mechanisms within VANETs and explored how these frameworks can be adapted or improved to mitigate such threats effectively. This analysis is essential for developing robust defense mechanisms that ensure the integrity and availability of communication which supports the sustainable development of ITSs. Figure 1, briefly, and Appendix A comprehensively illustrate the taxonomy of risks, threats, and vulnerabilities that endanger VANETs.

The inherent characteristics of V2X communications heighten their susceptibility to security breaches such as high mobility and dynamic topology which lead to rapidly changing network environments and limited resources that constrain the complexity of security solutions. Traditionally, security threats can be broadly categorized into attacks on confidentiality, integrity, and availability. Confidentiality breaches are exemplified by

eavesdropping attacks where an attacker gains unauthorized access to private communications; integrity threats are highlighted by message tampering and Sybil attacks where false information is injected into the network or multiple fake identities are created to disrupt the network's trust system; and availability is primarily compromised by denial-of-service (DoS) attacks which aim to exhaust network resources, making services unavailable to legitimate nodes. Each of these categories encompasses a broad spectrum of attacks that can severely undermine the functionality and safety of VANETs, which are essential for critical communication and operational efficiency in ITSs, as discussed by [2,5,10] in their comprehensive analyses of V2X security challenges.

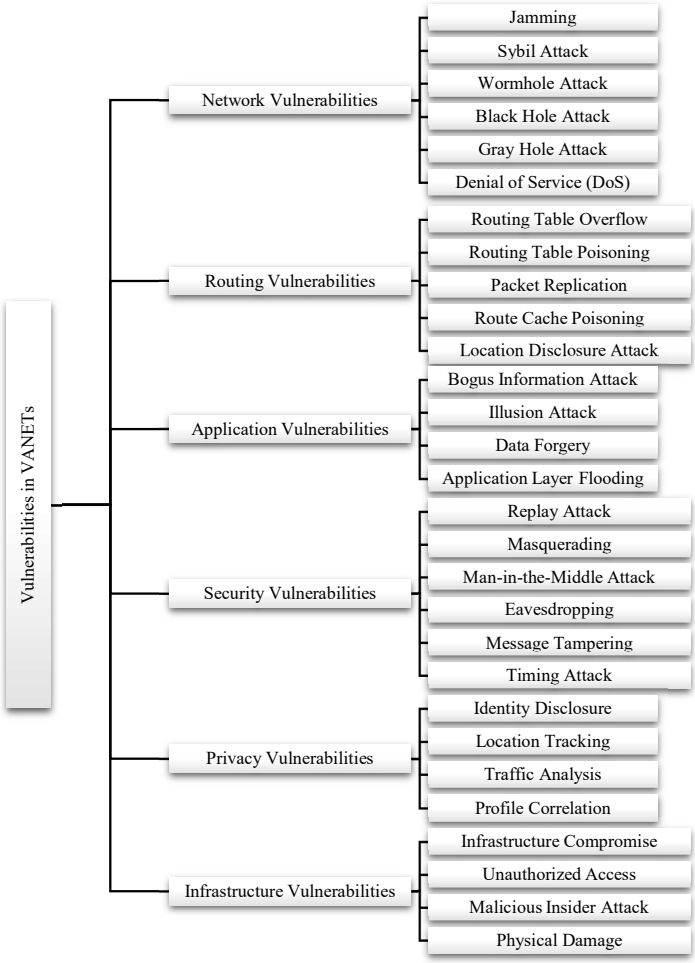


Figure 1. Taxonomy of vulnerabilities in VANETs. (Summarized according to reference [2–8]).

The emergence of cloud-assisted vehicular networks in recent years stems from the significant enhancement in performance that cloud computing can offer these networks through on-demand computing and storage resources [11]. Despite the numerous advantages provided by cloud computing, cloud-assisted vehicular networks continue to encounter substantial challenges related to security, privacy, and trust. These challenges are primarily attributed to the vast, open, and extremely dynamic nature of these networks [12].

Table 1 provides an overview of various characteristics of VANETs. In this context, we could infer the following:

(a) Data dissemination in VANETs can be proactive, reactive, or hybrid, which allows for flexibility in communication strategies.
(b) The latency and bandwidth consumption for these networks are both considered average.
(c) Network overload is not a critical issue, indicating robustness against congestion.

(d) VANETs have limited support for real-time applications and do not support extensive computational tasks.
(e) Geographic distribution is possible within VANETs that can enable coverage over dispersed areas.
(f) Decision-making processes are localized, which suits the decentralized nature of these networks but is restricted by bandwidth limitations.
(g) The computation capacity is medium, which is helpful in balancing between performance and the resources required for vehicular communication systems.
(h) Deployment costs are low, making them economically feasible for widespread implementation.

Table 1. Comparative analysis of fog node-focused VANETs.

Topics					Contributions	Limitations	Year	Ref.
Architecture Design	Mobility	Security	Privacy	Exposure and Hindrance				
✔	✔	✔	✗	✗	• Proposes a data clustering framework to reduce traffic information using fog computing in vehicular networks. • Includes a baseline method for detecting traffic congestion. • Integrates two adapted clustering methods: OPTICS and DBSCAN. • Demonstrates accuracy in highly congested traffic conditions. • Depends on roadside units (RSUs) for data transmission, potentially limiting use in areas without adequate infrastructure.	■ Lacks detailed analysis of communication cost savings. ■ No real-world testing or implementation was mentioned that raised concerns about practical performance.	2021	[13]
✔	✔	✔	✗	✔	• Presents a novel algorithm for diminishing fog computing delay and latency. • Creates a fog computing model for calculating delay and latency through empirical analysis. • Uses 5G SDN for faster communication between vehicles and RSUs.	■ Lack of performance comparison between cloud and fog computing in VANETs. ■ Unanswered questions on handling peak request loads and 5G impact.	2024	[11]
✔	✔	✗	✗	✗	• Proposes a Cloud-based Intelligent Traffic Light Control System (CCITL) to address traffic congestion and reduce wait times at intersections. • Leverages VANETs and cloud computing to gather traffic information and calculate optimal traffic signal formulas. • Offers a global view of the road network through conventional and vehicular clouds. • Enables dynamic traffic signal timing amendments based on real-time traffic requirements.	■ Does not discuss specific strengths or weaknesses of CCITL system identified during simulation.	2023	[14]
✔	✔	✔	✔	✔	• Suggests an active privacy-protective unidentified authentication scheme for condition-matching in fog–cloud-based VANETs. • Uses general ECC to optimize computational efficiency. • Leverages fog computing to boost system vigor and meet the real-time obligations of VANETs. • Utilizes a certificateless approach, eliminating the need for trusted authority (TA)-managed certificates and authorizing cross-domain group session key agreement. • Outperforms similar relevant schemes in terms of computational costs and communication overhead.	■ Security proofs are not provided for all security aspects. ■ Does not consider defiance critical for quantum attacks. ■ Does not explore outsourcing computing to moderate computational constraints for vehicles.	2024	[15]

Herein, reputation management is also integral to the security framework of vehicular networks, as it allows vehicles to assess the trustworthiness of peers and the authenticity of their communications. This system helps mitigate the risks associated with deceptive mes-

sages from adversarial vehicles to enhance the networks' reliability. Central to this function is the role of the TA [16], which is responsible for the periodic updates of reputation scores. This process involves the collection, decryption, and verification of extensive reputation feedback using cryptographic protocols such as RSA or ECC for secure decryption and the Transport Layer Security (TLS) protocol [17] for safeguarding the transmission of data. However, this necessary security measure places substantial computational and communication loads on the TA, often causing delays and serving as a potential bottleneck within the reputation management system.

Trust Management and Privacy Issues

In our research context, trust management (TM) [18] includes assessing the integrity of data and the trustworthiness of message sources, creating models to predict vehicle behavior from past actions, adjusting trust levels according to the current context and environment, distributing the responsibility of trust management to improve system scalability and lessen the reliance on central authorities, and applying machine learning to evaluate trustworthiness in changing network conditions. Our investigation revealed the following complexities that can hinder achieving the optimum trust among ad hoc nodes:

(a) V2V communications constantly experience rapid changes in network topology due to vehicle movement. This makes it challenging to establish and maintain trust relationships between vehicles, as their proximity and interaction patterns are constantly in flux.
(b) On-board units (OBUs) in vehicles have limited processing power, memory, and battery life. Thus, running complex trust management algorithms can be resource-intensive, potentially impacting vehicle performance and battery life. This limitation necessitates the development of an optimized trust management algorithm that tries to be resource-efficient to minimize the impact on vehicle performance and battery life while ensuring robust security measures are maintained. Our investigation was motivated by the Lemma that fog computing can be effectively utilized by offloading heavy computations from OBUs to nearby fog nodes, which are capable of handling more resource-intensive tasks.
(c) Malicious actors exploit the decentralized nature of VANETs to create fake identities (Sybil attacks) and manipulate trust relationships.
(d) TM often involves collecting and storing data on vehicle behavior and interactions. This raises privacy concerns as sensitive information about driving habits and locations could be revealed.
(e) Unlike traditional networks with centralized authorities that manage trust, VANETs lack a central entity responsible for trust verification.
(f) Different VANET applications may have varying trust requirements. For safety-critical applications, a high level of trust is essential. However, for non-critical applications, a more lightweight trust model might be sufficient.

Additionally, privacy concerns [19] involve maintaining anonymity during vehicle-to-vehicle and vehicle-to-infrastructure exchanges, using changing pseudonyms to prevent the tracking of individual vehicles, protecting personal data from unauthorized access and tampering, employing data minimization techniques to reduce the risk of exposure, and safeguarding location privacy against the risks posed by the continuous broadcasting of positional information. Due to the complexities identified in our investigation, achieving optimal privacy for nodes in an ad hoc network remains a significant challenge, and some other challenges are as follows:

(a) Achieving strong privacy guarantees does involve obscuring crucial traffic information (e.g., location, speed) that could be vital for safety applications like collision avoidance.

(b) Even with pseudonymization techniques (e.g., Certificateless Cryptography and Hash-based Pseudonyms), adversaries can attempt to track and profile user movement patterns by correlating pseudonym changes with location data or network behavior. This can potentially reveal sensitive information about driving habits and routines.
(c) Data privacy regulations like GDPR (EU) [20] and CCPA (California) [21] impose restrictions on data collection, storage, and usage in VANETs. Balancing privacy compliance with the need for effective network operation requires careful consideration.

3. Open Challenges and Security Requirements of Projected VANETs

The key open challenges that shaped the landscape of the projected research are as follows:

(a) Identifying scalable security architectures capable of handling high mobility and frequent topology changes.
(b) Developing a robust privacy-preserving mechanism that balances safety and privacy without compromising operational efficiency.
(c) Implementing an efficient real-time communication protocol, ensuring data freshness and timely delivery.
(d) Addressing a spectrum of cybersecurity threats including non-repudiation issues and network layer assaults.
(e) Integrating heterogeneous networks and ensuring interoperability among diverse communication technologies.
(f) Managing and maintaining the integrity of the vast amount of data generated by vehicles and roadside units.
(g) Fostering widespread adoption and compliance with global security standards.

In the context of the security challenges stated above, we confidently pinpointed the security requirements, such as the following:

(a) Ensuring message authenticity and integrity to prevent malicious attacks and misinformation.
(b) Providing end-to-end confidentiality to protect sensitive user data and prevent eavesdropping.
(c) Maintaining availability even under adversarial conditions to ensure continuous and reliable network service.
(d) Enforcing strong entity authentication procedures to verify the identity of communicating entities.
(e) Achieving non-repudiation to ensure that actions or communications by a particular entity can be indisputably proven to other parties.
(f) Implementing efficient key management systems to facilitate secure communication channels.
(g) Guaranteeing privacy to protect users from tracking and profiling while enabling accountability.

4. Proposed Methodology

Our proposed methodology encompasses a comprehensive suite of advanced techniques and technologies designed to strengthen the security infrastructure of VANETs. By integrating decentralized systems, real-time data processing, and innovative cryptographic measures alongside state-of-the-art machine learning algorithms, we aimed to address the inherent multifaceted security challenges.

System Model and Problem definition: The integration of decentralized intrusion detection systems (D-IDSs) utilizing fog computing and consortium blockchain technology within VANETs significantly enhances scalability and response times, effectively mitigating a spectrum of cyber anomalies such as GPS spoofing and data forgery. This robust

configuration, when augmented by a real-time anomaly detection system deployed at the network edge, substantially reduced latency and boosted the detection accuracy of infrequent malicious events. The application of SDN contributed further by enabling the dynamic reconfiguration of network resources, thus enhancing overall security management. Concurrently, the implementation of the novel IBBE ensured that only authenticated vehicles access sensitive group communications, thereby fortifying message confidentiality and integrity. Strategies for anonymous vehicle-to-vehicle communication safeguarded user privacy by preventing potential tracking and profiling, which maintained network efficiency. Our comparative analysis revealed that decentralized approaches, relative to centralized methods, offer improved scalability and resilience against diverse threats in VANETs. Likewise, the adoption of hybrid deep/machine learning models, combining ElasticNet and Gradient Boosting, demonstrates superior anomaly detection capabilities, establishing a more secure and reliable vehicular communication framework.

The core of the projected D-IDS technique utilizes a hybrid approach that combines signature-based and anomaly-based methods. The signature-based method involves the identification of known threats by comparing observed data against a pre-established database of threat signatures:

$$D_{sig}(x) = \begin{cases} 1 \; if \; x \; \epsilon \; Signature \\ 0 \; otherwise \end{cases} \quad (1)$$

where $D_{\text{sig}}(x)$ denotes the detection function for the signature-based method, and x represents incoming network data. Simultaneously, anomaly-based detection focuses on identifying deviations from normal network behaviors. This method relies on a continuous learning process where the system learns the baseline of normal activities and flags deviations as potential threats:

$$D_{ano}(x, \mu, \sigma) = \begin{cases} 1 \; if \; |x-\mu| > k\sigma \\ 0 \; otherwise \end{cases} \quad (2)$$

In Equation (2), x is the observed data point, μ and σ are the mean and standard deviation of the learned normal behavior, and k is a threshold multiplier determining sensitivity.

As identified in Table 2, and Figure 2, our proposed framework deployed a consortium blockchain for the reason that it allowed for controlled access governed by a select group of nodes that enhanced the security and privacy of sensitive vehicular data (e.g., location and speed), which was less exposed to the vulnerabilities typical of open networks. The involvement of fewer nodes in the consensus process led to faster transaction validation and processing, which was a critical requirement for the projected V2V simulated network to rely on real-time data. For data aggregation, we employed a clustering technique that organizes network vehicles into groups based on their geographical proximity and/or communication patterns. This method significantly reduced the data load and enhanced the manageability of information flow to the fog nodes:

$$A_g = \bigcup_{i=1}^{n} D_i(t) \quad (3)$$

where A_g represents the aggregated data for cluster g, and $D_i(t)$ denotes the data collected from vehicle i at time t. Integrating fog computing and a consortium blockchain offered the D-CASBR framework strategic advantages in combating sophisticated cyber threats such as resource-rich node attacks, broadcast tampering, and widespread network breaches. In this context, we applied fog computing distributed data processing tasks closer to the network edge with an aim to enhance real-time response capabilities and reduce latency, which

was crucial for swiftly identifying and mitigating attacks initiated by high-resource nodes and/or during broadcast tampering. Meanwhile, the consortium blockchain provided enhanced data integrity and traceability across vehicles and network nodes. This setup ensured that data transactions and broadcasts were immutably recorded and verifiable across trusted entities, which helped in detecting and isolating tampered transmissions and coordinating defense strategies against attacks distributed across the network. Given the dynamic and decentralized nature of VANETs, our system further incorporated the sophisticated '*Bloom data filtering*' technique to sift through the collected data, ensuring that only relevant information was processed. The Bloom filter was eligible to utilize space-efficient data structures to quickly identify irrelevant data packets based on predefined characteristics. This step was necessary for maintaining system performance and accuracy:

$$F(D) = \{d \in D : f(d) = \text{true}\} \tag{4}$$

where $F(D)$ represents the set of filtered data from the dataset D, and $f(d)$ is a filtering function that returns true for data points that meet specific relevance criteria.

Post 'Bloom filtering', the decision-making module then evaluated these filtered data against predefined parameters to determine the presence of malicious activities. This process involved setting thresholds and weighing the evidence collected to make informed decisions about potential threats:

$$M(x) = \sum_{j=1}^{m} \alpha_j \cdot x_j \tag{5}$$

Table 2. Step-by-step process justifications of proposed novel decentralized intrusion detection system with Collaborative Anomaly Scoring and Consortium Blockchain-based Reputation (D-CASBR).

#	Step	Description	Technique
1	Data Collection and Preprocessing with Compressed Sensing	Each vehicle continuously monitored network traffic at a configurable sampling rate (e.g., adjustable based on network density). Packets were collected that contained the following: • Source and destination IP addresses with Geolocation information (through reverse IP lookup). • Packet size distribution using histograms with variable bin sizes. • Inter-packet arrival times with fractal dimension estimation for traffic characterization. • GPS coordinates with differential privacy.	■ Utilized compressed sensing technique 'Orthogonal Matching Pursuit' [22] for efficient data acquisition, reducing network overhead. ■ Employed Locality-Sensitive Hashing (LSH) [23] for fast similarity search in compressed traffic data for anomaly detection.
2	Local Anomaly Detection with Federated Differential Learning	Vehicles trained a local anomaly detection model collaboratively using Federated Differential Learning. The model analyzed preprocessed traffic data while preserving location privacy. This was achieved by enforcing differential privacy and adding noise to GPS coordinates before transmission.	Utilized deep learning architecture with Generative Adversarial Networks (GANs) [24] to capture complex traffic patterns and identify deviations from learned normal distribution. 'Federated Differential Learning' updated model weights on each vehicle using 'Secure Aggregation of Distributed Learning (SecAgg)' protocol to protect individual training data points. Features of SecAgg included privacy-preserving training to protect individual contributions and enable collaborative model updates.

Table 2. *Cont.*

#	Step	Description	Technique
3	Secure Data Aggregation with Consortium Blockchain and Homomorphic Encryption (HE)	Vehicles periodically generated anomaly reports containing the following: • Encrypted representations of locally detected anomalies using 'HE' [25]. This allowed for computations on encrypted data without decryption. • Signatures by the vehicle using its private key on a zk-SNARK (zero-knowledge succinct non-interactive argument of knowledge) proof [26]. The zk-SNARK proof demonstrated the validity of the anomaly report without revealing its details.	■ Utilized Ring LWE (Learning with Errors)-based HE for efficient encryption of anomaly features while supporting arithmetic operations on encrypted data. ■ Employed consortium blockchain specifically designed for projected VANETs, where pre-selected group of trusted authorities (i.e., for emulation/simulation, we simulated fictious networked nodes) jointly managed blockchain to ensure data security and scalability.
4	Reputation System with Byzantine Fault Tolerance (BFT) and Unsupervised Anomaly Detection	Vehicles verified the received anomaly reports through a gossip protocol with enhanced security measures: • Verified zk-SNARK proofs using public keys that were stored in the consortium blockchain. • Utilized the unsupervised anomaly detection technique 'Isolation Forest' [27] to identify potentially malicious reports deviating from the expected distribution of valid reports.	■ Utilized Byzantine Fault Tolerance (BFT) consensus algorithm 'PBFT' [28] with verifiable random functions (VRFs) to ensure data consistency even in presence of malicious actors attempting to manipulate reports. ■ Assigned reputation scores to vehicles based on combination of factors: ■ Consistency of their reports with majority vote after BFT. ■ Outcome of unsupervised anomaly detection on their reports.
5	Global Anomaly Score Calculation with Secure Multi-Party Computation (SMPC) and Federated Learning	Vehicles collaboratively calculated a global anomaly score for each reported anomaly using a combination of SMPC and federated learning to further enhance privacy and security.	Utilized advanced SMPC protocol '*SecureNN*' [29] to securely perform neural network computations on encrypted anomaly representations obtained through homomorphic encryption in step 3. This allowed for collaborative analysis of anomaly features without decryption. Global score considered the following: ■ Output of secure neural network on encrypted anomaly data, indicating anomaly likelihood. ■ Number of reporting vehicles weighed by their reputation scores.
6	Alert Generation and Secure Dissemination with Group Signatures	If the global anomaly score exceeded a predefined threshold and the *zk-SNARK* proof was valid, an alert was generated.	Alert message included anonymized location of anomaly using secure localization technique 'verifiable multilateration'. Herein, Bloom filter [30] encrypted anomaly features using 'HE' which enabled efficient matching with local traffic data for verification of receiving vehicles.

Table 2. *Cont.*

#	Step	Description	Technique
7	Countermeasure Activation with Blockchain-based Access Control	Based on the alert type and verified anomaly features, vehicles took appropriate actions: • Used smart contract and identity-based blockchain access control mechanisms [31] to isolate suspicious vehicles, thereby blocking their access to safety-critical communication channels. • Report to a trusted authority (i.e., roadside unit—RSU) with a signed message containing the encrypted anomaly data for further investigation.	Smart contracts on consortium blockchain were used to implement access control rules guided by reputation scores and types of anomalies. Our system utilized secure communication channels with trusted RSUs to report critical information.

V2V Security Protocols	Signing Throughput: Messages per Second	Verified Messages Per Second
Wang et al., [11]	858	614
Nazih et al., [12]	357	255
Peixoto et al., [13]	89	47
Gaouar et al., [14]	562	411
Zhan et al., [15]	2579	655
Proposed	40,613	40,613

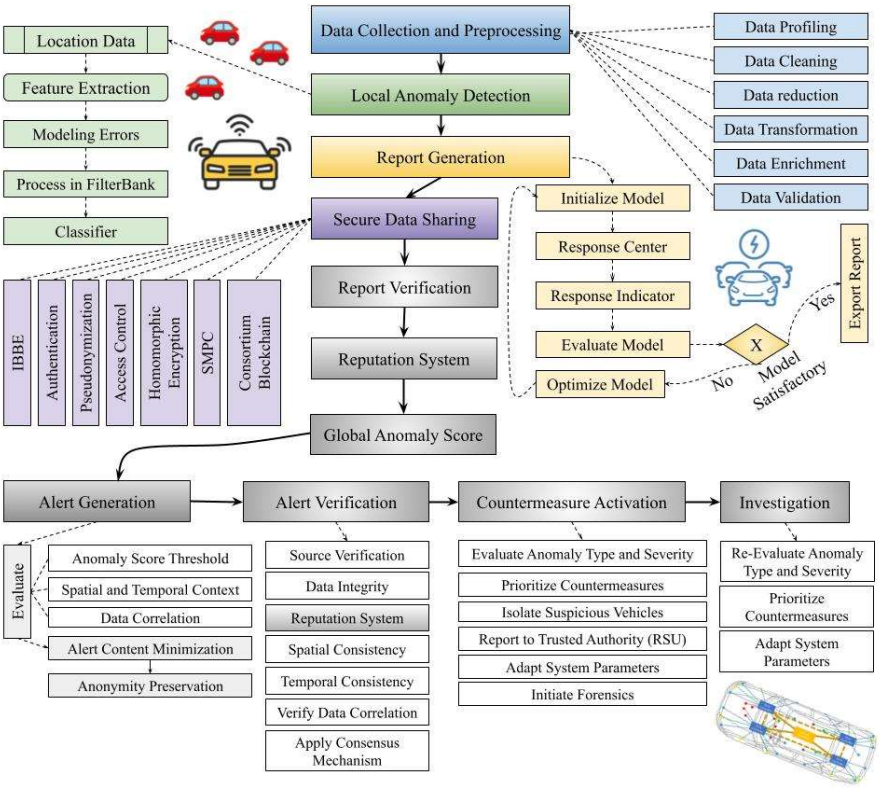


Figure 2. Framework architecture of novel decentralized intrusion detection system with Collaborative Anomaly Scoring and Blockchain-based Reputation (D-CASBR).

In the context of Equation (5), $M(x)$ represents the decision-making function, x_j represents the features derived from the filtered data, and α_j represents the weights assigned to each feature, reflecting their importance in the decision-making process. The response mechanism is then activated upon the detection of a confirmed threat, where the system initiates predefined protocols to mitigate the detected threat. This may include isolating the offending vehicle or alerting the relevant base station:

$$R(c) = \begin{cases} Isolate & if\ c = high \\ Alert & if\ c = medium \\ Monitor\ if c = low \end{cases} \quad (6)$$

Here (i.e., as per Equation (6)), $R(c)$ defines the response actions based on the severity c of the threat. It is worth revealing that to achieve real-time anomaly detection at the network edge, we employed a careful calibration of thresholds and parameters on fog nodes. These strategically positioned nodes perform initial data processing and anomaly identification tasks, filtering out irrelevant information before forwarding potential threats for further investigation.

Consequently, obtaining 'fog computing thresholds' involved establishing sensitivity levels that determine when to report an anomaly. These thresholds were vital because settings that were too sensitive could result in numerous false positives, overwhelming the system with unnecessary alerts. Conversely, if the thresholds were set too high, genuine threats could go undetected. Thus, we applied z-score statistical metrics from moving averages to establish these thresholds, represented as follows:

$$T(x) = \begin{cases} 1\ if\ z(x) > \theta \\ 0\ otherwise \end{cases} \quad (7)$$

Z-scores aided the proposed framework in examining various traffic parameters, such as the following: packet size, transmission frequency, inter-arrival time between packets, speed of nearby vehicles, etc. In Equation (7), $T(x)$ indicates whether an alert should be triggered based on the z-score $z(x)$ of observation x, and θ is the threshold value. Herein, Table 3 exhibits the communication cost for alerts in the D-CASBR scheme and Tamper-Proof Device protocols.

Table 3. Alert communication cost of proposed D-CASBR scheme and Tamper-Proof Device protocols.

V2V Security Protocols	Wang et al., [11]	Nazih et al., [12]	Peixoto et al., [13]	Gaouar et al., [14]	Zhan et al., [15]
Transmission Overhead (Bytes)	154	74	258	96	39

We implemented a multi-path approach [32] for data aggregation in fog computing, aiming to boost data management efficiency by minimizing the volume of data that needs to be transmitted and processed. Data from sensors that measure similar phenomena were aggregated using weighted averages to extract relevant features:

$$A(D) = \sum_{i=1}^{n} w_i \cdot d_i \quad (8)$$

In Equation (8), $A(D)$ represents the aggregated output from data points d_i with corresponding weights w_i, which could reflect the relevance or reliability of the source. Likewise, as stated in Equations (1) and (2), the real-time anomaly detection model (i.e., signature/anomaly) was selected based on its effectiveness in processing large streams of data with minimal delay.

$$D(x) = \text{classify}(x; \alpha) \quad (9)$$

where $D(x)$ represents the decision function, x represents the input data, and α denotes the parameters of the algorithm. Herein, MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol) communication protocols were implemented between vehicles and fog nodes to minimize latency and maximize reliability. The implemented simulation outcome revealed that these (i.e., MQTT and CoAP) protocols ensured timely and reliable data transfer, which is crucial for the immediacy required in VANET environments:

$$P(m) = \text{protocol\_type}(m) \tag{10}$$

As per Equation (10), $P(m)$ specifies the protocol used for message m. We secured the communication by embedding homomorphic encryption [23] (i.e., zero-knowledge proofs) because it protected data without compromising the ability to perform computations on encrypted data:

$$S(d) = \text{encrypt}(d; k) \tag{11}$$

Here, in Equation (11), $S(d)$ denotes the secure transmission of data d, encrypted using key k.

In the exploration of enhancing the projected VANET security and efficiency, the integration of SDN played a pivotal role by decoupling the control and data layers. This separation allowed for dynamic network reconfiguration and heightened security management that presented effectiveness for the inherently dynamic and decentralized nature of V2X communication environments. The SDN controllers were programmed to dynamically adjust network policies and rules, which were then enforced by the SDN-enabled switches and routers within the vehicles and roadside units. Herein, the core operational flow in the dynamic control function is as follows:

$$C(t) = f(S(t), P(t)) \tag{12}$$

In Equation (12), $C(t)$ represents the control decisions at time t; $S(t)$ denotes the current network state, including topology and traffic data; and $P(t)$ encapsulates the predefined network policies and security rules. We programmed the data layer to actively manage independently from the control logic to reliably handle the actual data traffic between vehicles and infrastructure based on the predefined policies that were set by/through the SDN controllers. This separation ensured that the network could scale effectively without bottlenecking at the control layer. We observed that this paramount feature intends to present effectiveness for maintaining high performance in dense vehicular environments:

$$D(t) = g(C(t), T(t)) \tag{13}$$

As indicated in Equation (13), $D(t)$ refers to the data flows managed at time t, and $T(t)$ is the traffic demand. The function g describes how control decisions are applied to manage data flows, ensuring efficient traffic handling and security enforcement. As stated earlier, we applied SDN due to its significant advantage in attaining the capability of dynamic reconfiguration. This feature allowed the V2V network to adapt to frequent changes in topology due to the high mobility of vehicles. For instance, SDN could dynamically update routing paths in response to network congestion and security incident/anomaly detection, rerouting data flows to optimize traffic and minimize risk:

$$R(t) = h(D(t), N(t)) \tag{14}$$

As stated in Equation (14), $R(t)$ represents the routing configurations at time t, and $N(t)$ is the network condition such as node mobility and link stability. The function h effectively recalibrates routing decisions to respond to real-time network dynamics. Conse-

quently, over time, SDN improved security management by centralizing security functions (e.g., threat detection and mitigation strategies). Leveraging the SDN controller, we rapidly implemented consistent security policies across the entire network. This allowed for the swift isolation of compromised segments and dynamic traffic redirection, guaranteeing data confidentiality and integrity.

$$S(t) = j(C(t), V(t)) \tag{15}$$

Here (i.e., Equation (15)), $S(t)$ illustrates the security measures implemented/deployed at time t, and $V(t)$ represents detected vulnerabilities or ongoing attacks. The function j adjusts security postures based on the current threat landscape, optimizing the network's defensive mechanisms.

During emulation/simulation, we observed that the issue of minority class imbalance in D-IDSs was a significant hurdle due to the infrequent occurrence of malicious events compared to normal traffic activities. To tackle this, we employed advanced over-sampling techniques, (a) SMOTE and (b) ADASYN. These methods generated synthetic samples of the minority class (i.e., malicious events) in the dataset to balance the class distribution, thereby enhancing the learning process and detection accuracy of the model.

To secure group communications, we implemented a novel IBBE system that leveraged the broadcast of encrypted messages where decryption is possible only with private keys that correspond to a given set of identities. This approach ensured that only authorized vehicles could access the transmitted messages. The encryption function for a message m using the public parameters PP and a set of identities ID is expressed as follows:

$$E(m, ID, PP) \tag{16}$$

We also developed strategies for anonymous V2V communication to protect user privacy from tracking and profiling. Anonymity was achieved through applied techniques such as group signatures and pseudonyms, which allowed vehicles to communicate without revealing their true identities. Here, the anonymization function A was eligible to take an original message m and a vehicle's identity id and return an anonymized message $m\prime$:

$$m' = A(m, id) \tag{17}$$

During our analysis of scalability, security, and privacy aspects, we observed that the centralized security system was easier to manage, often suffered from single points of failure, and was prone to potential scalability issues (e.g., increased load, delayed processing, limited bandwidth, latency due to geographical dispersion, denial of service, etc.). On the contrary, the decentralized system offered improved resilience and distribution but faced challenges in maintaining consistency and managing complex distributed protocols (i.e., consensus protocol (Byzantine Fault Tolerance (BFT), State machine replication, Anti-Entropy Gossip Protocol, and Distributed Hash Tables (DHTs)).

Ultimately, we matured the proposed novel approach by utilizing hybrid machine learning models that combined the strengths of ElasticNet and Gradient Boosting [33] for intrusion detection. This hybrid model leveraged the regularization capabilities of ElasticNet to prevent overfitting and the sequential correction of Gradient Boosting to enhance prediction accuracy. The intrusion detection function F using these models on a dataset D was modeled as follows:

$$F(D; \alpha, \beta) \tag{18}$$

As described in Equation (18), ElasticNet, parameterized by α, incorporates both $L1$ (Lasso) and $L2$ (Ridge) regularization to balance feature selection and parameter shrinkage

that helped to effectively manage the model's complexity and prevented overfitting. This regularization ensured that the model remains robust even with sparse data, which is a common issue in anomaly detection scenarios where the event frequency is low. β in the model represents the parameters of Gradient Boosting, a powerful ensemble learning technique that builds successive trees where each tree attempts to correct the errors of its predecessor. This approach enhanced the model's ability to adapt to complex patterns in data, significantly improving prediction accuracy. The combination of ElasticNet's regularization with Gradient Boosting's sequential error correction provided a comprehensive modeling strategy that was not only highly predictive but also resilient to variations in data, making it exceptionally suitable for the dynamic and diverse V2X network. We calculated the 'Cost Function' of the underlying parameters and training data (i.e., new or unseen data) of $L1$ and $L2$ as follows:

$$L1 \text{ Cost Function} = \text{Loss} + \lambda \sum_{i=1}^{n} |w_i| \tag{19}$$

$$L2 \text{ Cost Function} = \text{Loss} + \lambda \sum_{i=1}^{n} w_i^2 \tag{20}$$

where w_i represents the coefficients in model, and λ is a regularization parameter. The employment of the $L1$ and $L2$ regularization techniques played a critical role in model optimization and performance. The $L1$ regularization strategically enforced sparsity in the model parameters, effectively reducing the number of features by setting less informative weights to zero, which benefited the feature selection and simplification of the model. This reduction in complexity helped in obtaining faster computations and a clearer interpretation of model behavior. Conversely, $L2$ regularization minimized the risk of overfitting by shrinking the size of the coefficients, thereby maintaining all features but distributing smaller weights. This attribute was crucial for dealing with multicollinearity to enhance the model's stability and predictive accuracy. Together, the $L1$ and $L2$ regularization methods ensured that the proposed anomaly detection framework remained robust and effective with the capability of handling the diverse and dynamic nature of VANET data without succumbing to overfitting or being misled by irrelevant features. This implementation reinforced the security framework against diverse cyber threats to demonstrate the proposed method's capacity to adapt and perform under complex and evolving V2V network conditions.

5. Simulation Setup and Evaluation Outcome

To collect empirical data, the ns-3 network simulator [34] was utilized alongside a VANET infrastructure setup. We used ns-3 for its capability to model the complexities of vehicular networks with high fidelity, ensuring an accurate representation of communication protocols and mobility patterns in VANET scenarios. Its modular architecture and support for detailed physical and MAC layer configurations allowed for a precise evaluation of performance metrics under varying network densities and mobility conditions, which are critical for validating our proposed framework. Testing was conducted within an 8 $\times$ 8 km area over a simulation period of 24 h and 10 iterations. We executed various scenarios (e.g., low/medium/high-density network scenarios; rapid mobility changes with varying vehicle speeds; intermittent connectivity scenarios simulating urban environments; high-speed highway scenarios with continuous vehicle movement; Sybil attack simulation to test the system's resilience against false identity creation; GPS spoofing scenarios to assess the system's ability to detect and mitigate location falsification; Replay attack scenarios to evaluate the effectiveness of the system in identifying and handling repeated old transmissions, etc.) to observe the behavior of the proposed framework under different network densities ranging from 01 to 2000 nodes. We modeled a highway scenario using

the JiST (Java in Simulation Time)/SWANS (Scalable Wireless Ad hoc Network Simulator) Ulm Highway model with three lanes. Vehicles in the simulation could reach a maximum speed of 40 m/s, with an average speed of 25 m/s, and nodes were programmed to follow the mobility patterns that included capabilities such as collision avoidance and lane changing. The physical layer specifies Rayleigh fading and a TwoRay path loss model, with a transmit power of 10.9 dB. The MAC layer was programmed to use the 802.11p standard that is critical for vehicular communications because it supported Dedicated Short-Range Communications (DSRCs) in the 5.9 GHz band. As stated earlier, the network settings are based on the JiST/SWANS implementation that made our framework eligible in supporting a maximum packet size of 4096 bytes. Beacons were transmitted at intervals of 10 Hz, with each beacon having a size of 209 bytes. The beaconing system included various sketch sizes and hash methods (MD5/SHA-128 for probabilistic counting with stochastic averaging (PCSA)) to handle vehicle location and payload data efficiently within the network. The aim of these configurations was to access the communication dynamics and network performance under varying vehicular densities and mobility conditions.

Herein, the subfigures of Figure 3 accomplish the following:

(a) illustrates the number of established communication sessions over a 24 h period which highlights the significant peaks that correspond to periods of high vehicular activity or network load. These fluctuations in session establishment were critical for analyzing the performance of the proposed framework under varying network conditions which demonstrated its ability to handle sudden surges in traffic while maintaining consistent security and reliability.

(b) demonstrates the variability in network activity under different temporal conditions. This analysis highlights the framework's capacity to handle frequent connection requests while ensuring secure communication protocols, which was critical for maintaining system resilience in a real-time evaluation environment.

(c) depicts the number of packet exchanges over the assessment period and showcases the variations in data traffic influenced by network density and communication requirements. This evaluation emphasizes the robustness in managing packet flow efficiently while maintaining secure and reliable data transmission across the infrastructure.

(d) highlights the number of security alerts generated with noticeable peaks during periods of high anomaly detection activity. This demonstrates the efficacy in promptly identifying and flagging potential threats, which ensured continuous monitoring and response to maintain network integrity and security.

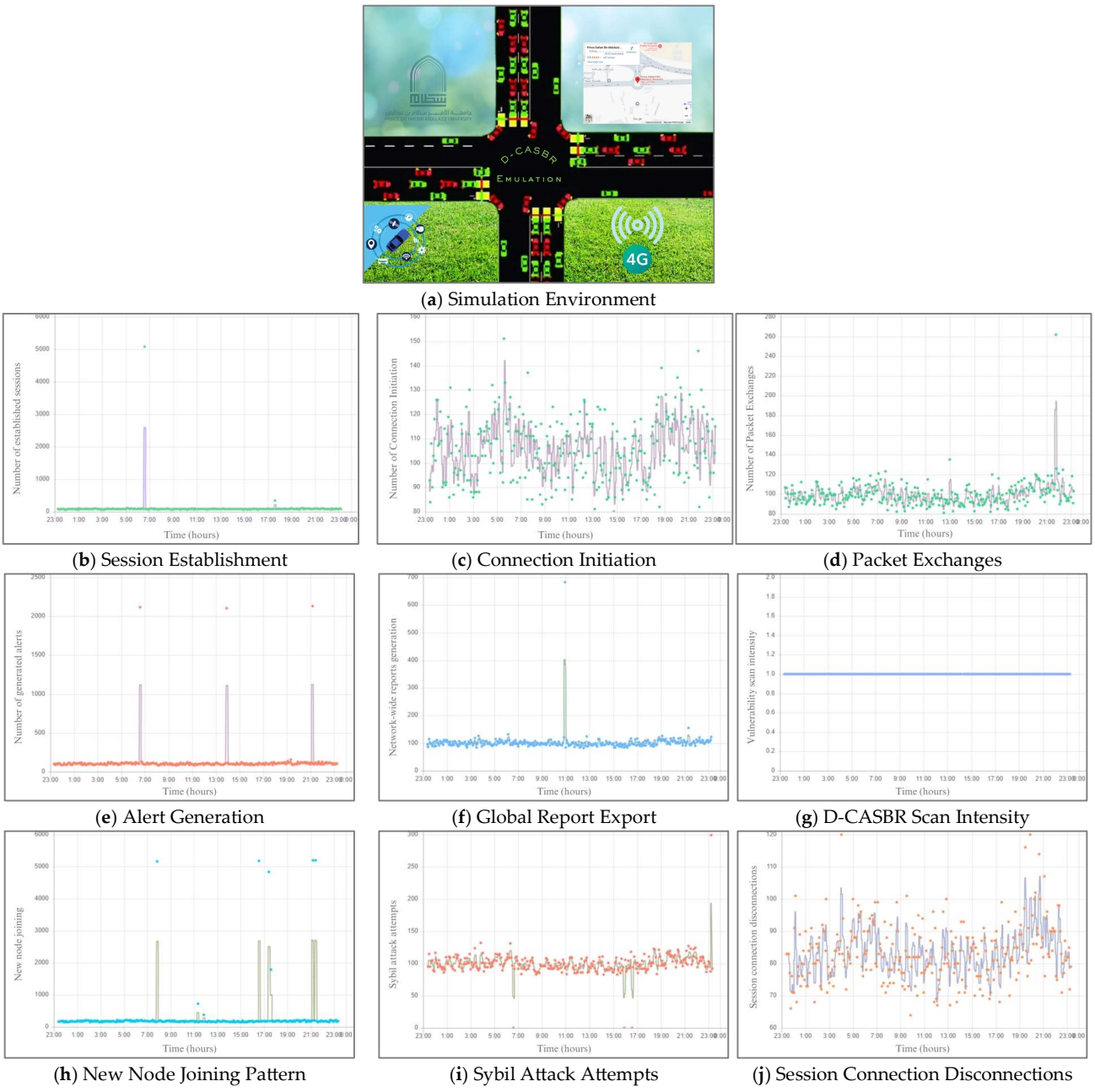
(e) interprets the frequency of network-wide report generation with a significant peak indicating a collective response to heightened anomaly detection during specific intervals, which is indicative of the capability to facilitate collaborative anomaly scoring and coordinated reporting mechanisms to conduct comprehensive threat assessments across the network.

(f) describes a consistent vulnerability scan intensity reflecting the framework's steady operational efficiency in continuous monitoring that confirms persistent and reliable security assessments without fluctuations.

(g) exhibits the pattern of new node joining events within the network with distinct spikes indicating intervals of heightened vehicular participation which reflected that the system was capable of dynamically accommodating the integration of new nodes, and it warranted the seamless expansion of the network without compromising the overall system stability or security protocols.

(h) illustrates the frequency of Sybil attack attempts by showing fluctuations in their occurrence under varying network conditions. This analysis highlights the robustness in detecting and mitigating identity-based attacks.

(i) shows the pattern of session connection disconnections by reflecting variations in network stability due to mobility and environmental factors. This evaluation reflects the ability to manage and recover from frequent disconnections which certified resilience and reliability in maintaining active communication sessions within the setup.



(**a**) Simulation Environment

(**b**) Session Establishment (**c**) Connection Initiation (**d**) Packet Exchanges

(**e**) Alert Generation (**f**) Global Report Export (**g**) D-CASBR Scan Intensity

(**h**) New Node Joining Pattern (**i**) Sybil Attack Attempts (**j**) Session Connection Disconnections

Figure 3. Simulation environment and factors.

Message Loss Rate

To evaluate message loss rates, we focused on analyzing how the length distribution of wireless communication links impacted these rates. Our findings indicated that longer links tend to suffer higher loss rates due to factors such as signal attenuation, multi-path fading, and interference, which become more pronounced with increased link distance. Given the high-speed movement and frequent positional changes in vehicles, the variability in link length significantly influences the reliability and stability of data transmissions. To address these challenges, our experiments utilized advanced modulation and coding

schemes (i.e., Low-Density Parity-Check (LDPC) [35]) with a design aim to enhance signal robustness across varied distances. LDPC utilized a sparse parity-check matrix to decode received messages effectively which significantly reduced the error rate. We also implemented network protocols (i.e., Distance-Aware Rate Adjustment Strategy (DARAS) [36], Density-Aware Transmission Power Control Protocol (DATPCP) [37], and Dynamic Power Adjustment for Vehicular Networks (DPA-VN) [38]) that adaptively managed transmission power and dynamically adjusted the rate of message dissemination based on the prevailing network density and the average vehicular distance. The applied adaptive approach helped the projected V2V setup in mitigating the adverse effects of link length distribution on message loss, thereby fostering more resilient communication strategies and ensuring the reliable exchange of critical safety and operational information among vehicles.

Table 4 and Figure 4 illustrate that as the distance between the sender and receiver increases from 0.5 km to 2.5 km, the message loss rate escalates progressively from 2.5% to 4.5%, peaking at 5.0% at the shortest link when network density is at its maximum. This pattern underscores the challenges posed by signal attenuation, multi-path fading, and interference, which intensify over longer distances and higher network densities. The use of advanced modulation and coding schemes (i.e., LDPC), along with strategically implemented network protocols (i.e., DARAS, DATPCP, and DPA-VN), significantly mitigated these effects. Thorough analysis (i.e., as exhibited in Figure 3) revealed that these adaptations not only enhanced the robustness of signal transmission across varied distances but also ensured the stability and reliability of rapidly evolving V2V communication. The robustness of D-CASBR heavily depends on minimizing message loss rates to maintain the integrity and responsiveness of threat detection. Our analyses revealed that as message loss increased, the latency in anomaly detection also escalated, which could potentially compromise the network's security posture. To tackle this problem, we enhanced our network protocols by employing advanced error-correcting codes and adjustable transmission power controls. The primary parameters for optimization included error correction strength, the coding rate of sophisticated error-correcting codes, transmission range, signal strength, and several environmental factors that influence transmission power controls. These improvements significantly bolstered the reliability of transmitting critical security alerts which greatly diminished the likelihood of missed or delayed threat detections.

Table 4. Message loss rates in simulated VANET setup.

Simulation Iteration	Link Length (km)	Average Vehicular Speed (m/s)	Network Density (Vehicles/km^2)	Message Loss Rate (%)	LDPC Error Rate (%)	Protocol Used
1	0.5	30	100	2.5	0.5	DARAS
2	1.0	35	150	3.0	0.7	DARAS
3	1.5	40	200	3.5	0.9	DATPCP
4	2.0	25	250	4.0	1.1	DATPCP
5	2.5	20	300	4.5	1.3	DPA-VN
6	0.5	30	100	5.0	1.5	DPA-VN
7	1.0	35	150	2.3	0.3	DARAS
8	1.5	40	200	2.8	0.6	DARAS
9	2.0	20	250	3.2	0.8	DATPCP
10	2.5	25	300	3.7	1.0	DATPCP

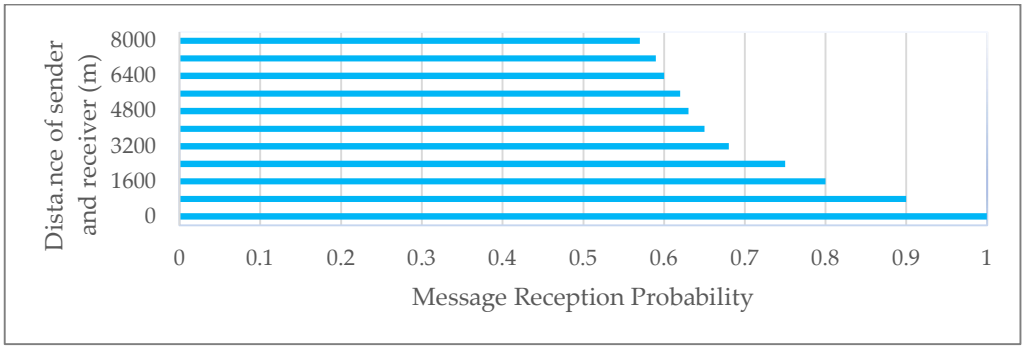


Figure 4. Impact of message loss rate on D-CASBR.

As shown in Figure 5, a higher number of nodes improved spatial coverage, which allowed the proposed framework to enforce more thorough monitoring and data collection. Each node served as a sensor that enhanced the overall detection capabilities. Augmentation in nodes also improved redundancy in data collection and anomaly detection. This reduced the risks linked to single points of failure and made sure no significant blind spots compromised the network's integrity. The addition of more nodes brought diverse observational perspectives and heuristics that enriched the collective detection process. This diversity helped to accurately separate normal network behavior from genuine threats, which reduced false positives and increased the reliability of anomaly detection. Furthermore, the addition of more nodes improved the potential for effective peer-to-peer communication and consensus building. This was crucial in the proposed decentralized system in which validation and response to detected anomalies depended on the agreement of multiple nodes. Likewise, the geographical distribution of nodes contributed to dynamic shifts in network topology, which supported robust intrusion detection across larger areas and sustained effective monitoring, even with the high mobility characteristics of the network.

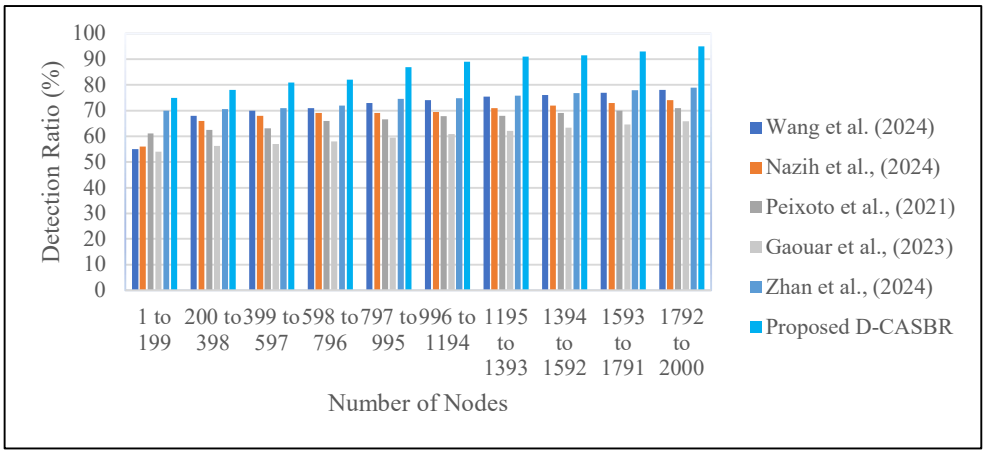


Figure 5. Anomaly detection ratio with number of nodes. [11–15].

6. Conclusions

To address the principal issue of network security within VANETs, our research underscored the imperative need for a robust anomaly detection system that has the capability of thwarting malicious activities and ensuring the integrity of vehicular communications. Our contribution through the novel D-CASBR marked a significant advancement in V2X networks. By harnessing the potential of decentralized technologies alongside hybrid machine learning models, D-CASBR transcended the limitations traditionally associated

with anomaly detection. The proposed framework not only leveraged the decentralization inherent to consortium blockchain technology and the edge-based processing capabilities of fog computing but also employed a sophisticated hybrid ML strategy (i.e., ElasticNet and Gradient Boosting) to enhance detection accuracy. The amalgamation of applied technologies facilitated a reduction in detection latency and improved the scalability of security measures that were capable of effectively accommodating the dynamic nature of VANETs. The proposed framework achieved superior threat detection accuracy by leveraging real-time processing and collaborative anomaly scoring. This significantly strengthened the security framework of the emulated intelligent transportation system.

While the D-CASBR framework represented a substantial leap forward, it did encounter specific limitations (e.g., computational intensity and overhead in real-time processing, struggles with detection of highly sophisticated stealth anomaly types, and resource consumption and latency issues in blockchain operations). The computational intensity required for real-time processing and blockchain operations can impose significant overheads, particularly in highly dynamic environments where rapid decision-making is crucial. Herein, the sophisticated nature of the hybrid ML approach, while beneficial in enhancing detection capabilities, did also struggle with the detection of highly sophisticated stealth anomaly types that do not fit well-defined patterns. Looking ahead, our future research aims to focus on the following:

(a) Optimizing the computational efficiency of the system, possibly through more advanced forms of compression and data simplification techniques that reduce the demands on real-time processing.
(b) Implementing enhancements in blockchain technology with a focus on reducing latency and resource consumption.
(c) Expanding the ML model to include unsupervised and semisupervised learning algorithms to offer a more robust detection mechanism for new and evolving anomaly types.

We reckon that after real-time optimized experimentation, the stated advancements are expected to further enhance a more adaptable and resilient framework that may make D-CASBR a more viable solution for broader ITS deployments and ensure it can keep pace with the rapid evolution of V2X network technologies.

Author Contributions: Conceptualization, U.T. and T.A.A.; methodology, U.T. and T.A.A.; software, U.T.; validation, U.T.; formal analysis, U.T.; investigation, U.T.; resources, U.T.; data curation, U.T. and T.A.A.; writing—original draft preparation, U.T.; writing—review and editing, U.T. and T.A.A.; visualization, U.T.; project administration, U.T.; funding acquisition, U.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Deanship of Scientific Research at Prince Sattam Bin Abdulaziz University under the research project '2024/01/31056'.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

Acknowledgments: We gratefully acknowledge the Deanship of Scientific Research at Prince Sattam Bin Abdulaziz University for their vital resources and support, which were instrumental to the success of this research work through the project number '2024/01/31056'.

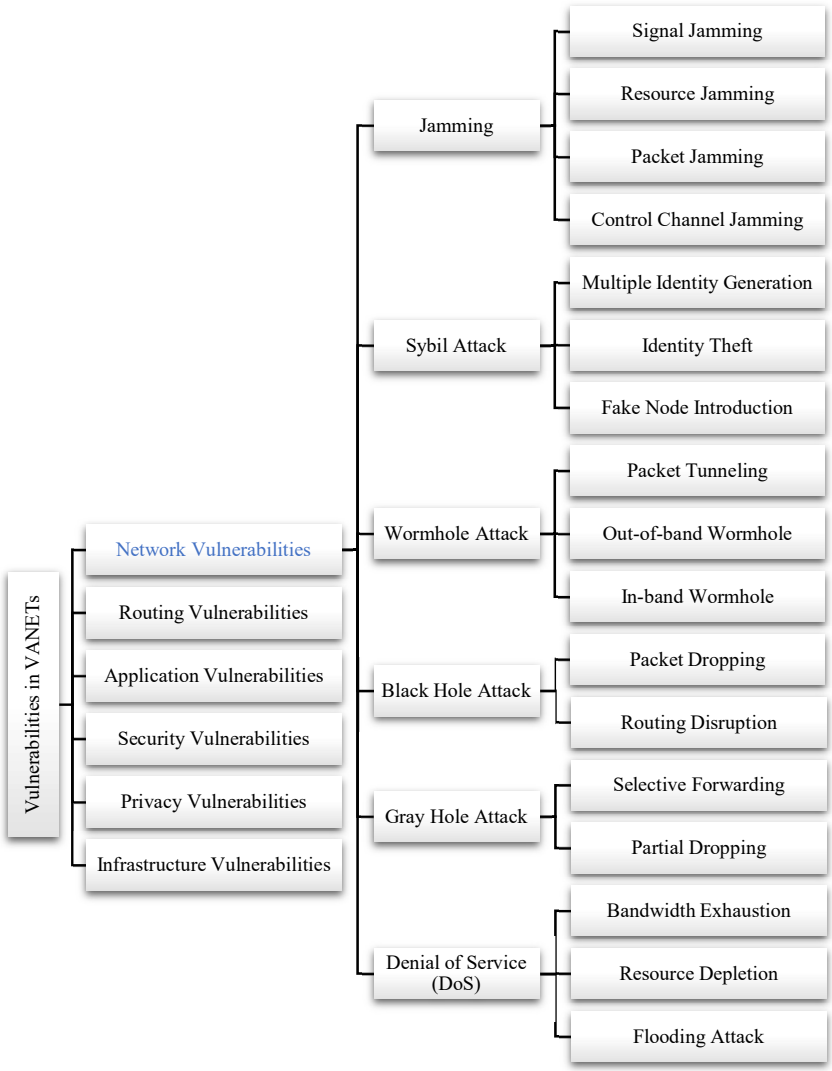
Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

Taxonomy of Vulnerabilities in VANETs

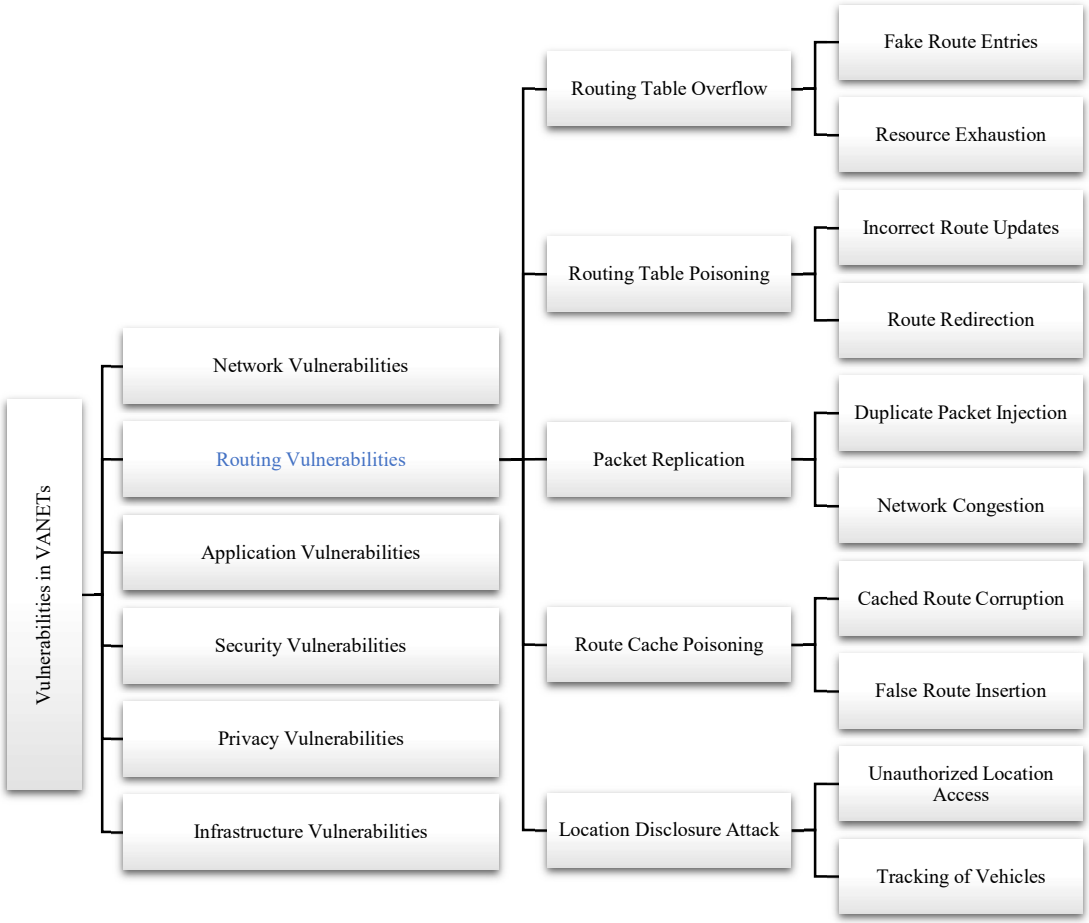
This appendix provides a comprehensive list of vulnerabilities in VANETs categorized into six main groups. Each category contains specific subcategories and their respective

vulnerabilities [2,6,12,18,28]. This detailed taxonomy helped us in understanding and addressing the potential security risks during the experimentation analysis of the D-CASBR framework.

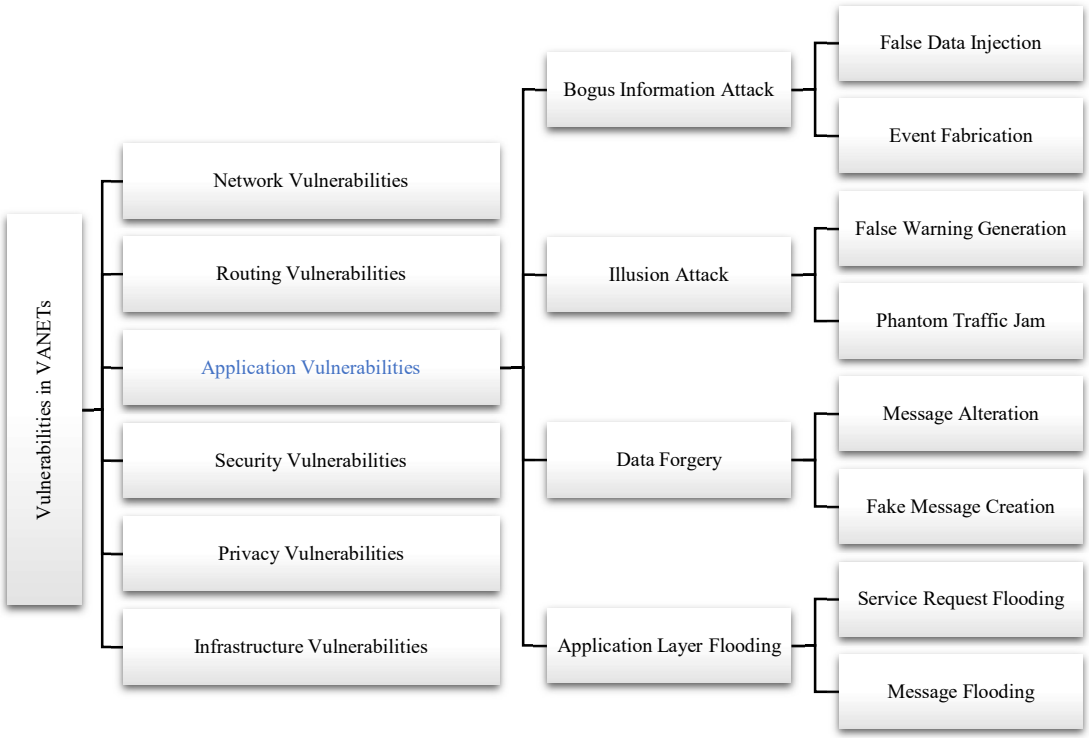


(**a**) Taxonomy of network vulnerabilities in VANETs.

Figure A1. *Cont.*

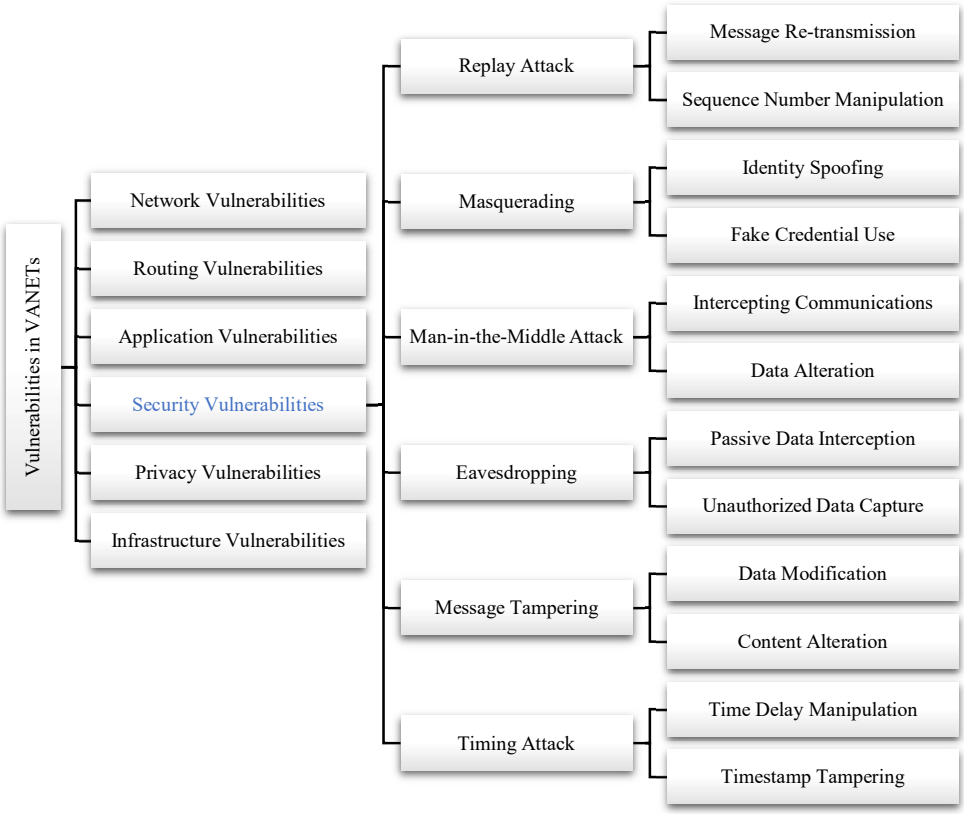


(**b**) Taxonomy of routing vulnerabilities in VANETs.

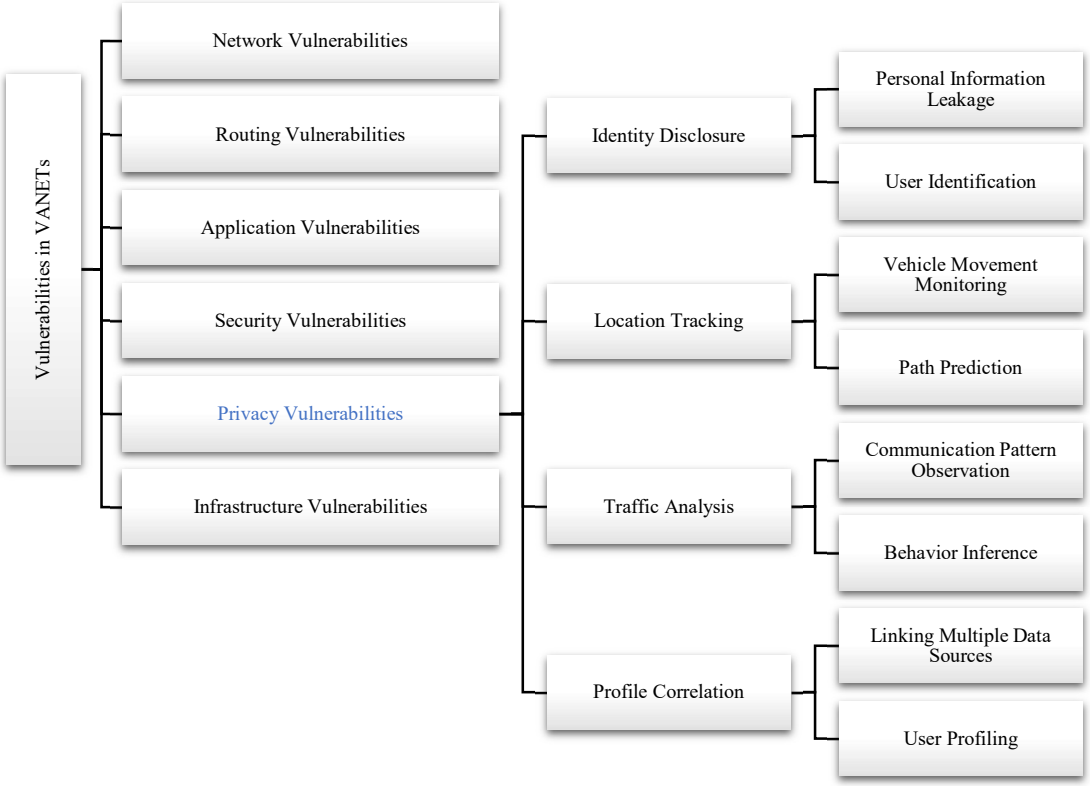


(**c**) Taxonomy of application vulnerabilities in VANETs.

Figure A1. *Cont.*

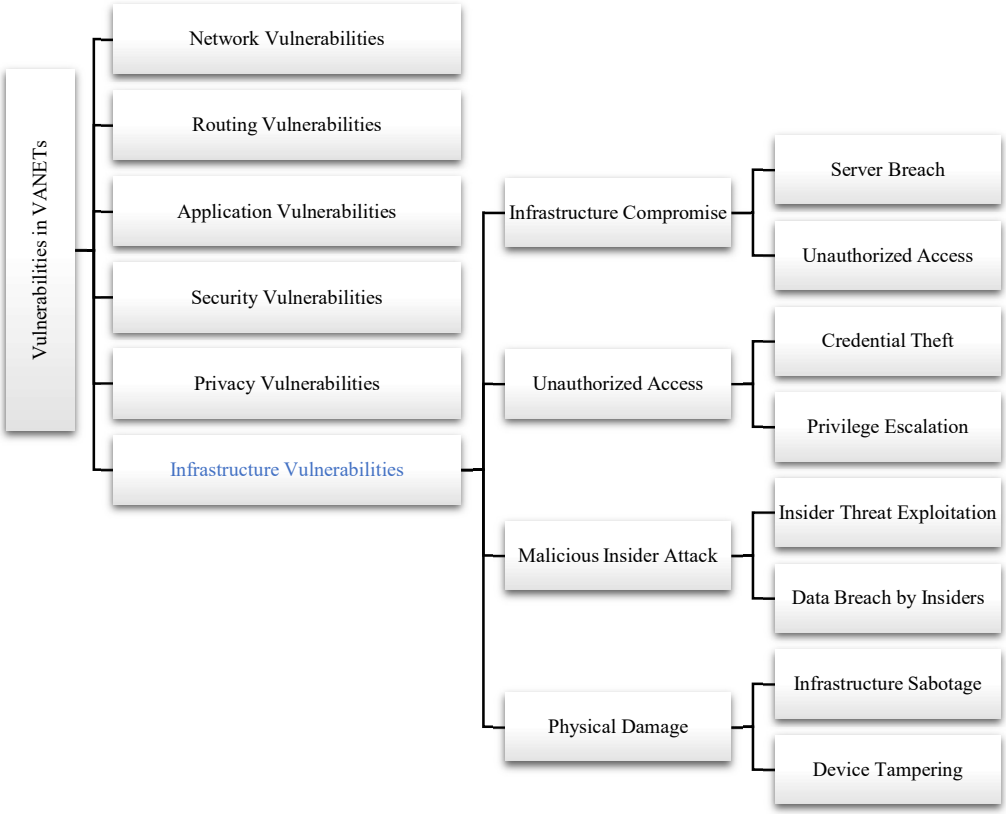


(**d**) Taxonomy of security vulnerabilities in VANETs.



(**e**) Taxonomy of privacy vulnerabilities in VANETs.

Figure A1. *Cont.*



(**f**) Taxonomy of infrastructure vulnerabilities in VANETs.

Figure A1. These taxonomies (**a**–**f**) illustrate the categorically sorted lists of VANET-focused vulnerability-driven listings.

References

1. Yerrathi, S.; Pakala, V. Enhancing network stability in VANETs using nature inspired algorithm for intelligent transportation system. *PLoS ONE* **2024**, *19*, e0296331. [CrossRef]
2. AlMarshoud, M.S.; Kiraz, M.S.; Al-Bayatti, A.H. Security, Privacy, and Decentralized Trust Management in VANETs: A Review of Current Research and Future Directions. *ACM Comput. Surv.* **2024**, *56*, 1–39. [CrossRef]
3. Chen, X.; Qiu, W.; Chen, L.; Ma, Y.; Ma, J. Fast and practical intrusion detection system based on federated learning for VANET. *Comput. Secur.* **2024**, *142*, 103881. [CrossRef]
4. Hassan, M.U.; Al-Awady, A.A.; Ali, A.; Sifatullah; Akram, M.; Iqbal, M.M.; Khan, J.; Ali, Y.A.A. ANN-Based Intelligent Secure Routing Protocol in Vehicular Ad Hoc Networks (VANETs) Using Enhanced AODV. *Sensors* **2024**, *24*, 818. [CrossRef]
5. Awais, S.M.; Yucheng, W.; Mahmood, K.; Badar, H.M.S.; Kharel, R.; Das, A.K. Provably secure fog-based authentication protocol for VANETs. *Comput. Netw.* **2024**, *246*, 110391. [CrossRef]
6. Hussein, N.H.; Koh, S.P.; Yaw, C.T.; Tiong, S.K.; Benedict, F.; Yusaf, T.; Kadirgama, K.; Hong, T.C. SDN-Based VANET Routing: A Comprehensive Survey on Architectures, Protocols, Analysis, and Future Challenges. *IEEE Access* **2024**, 1–59. [CrossRef]
7. Zhang, J.; Su, S.; Zhong, H.; Cui, J.; He, D. Identity-Based Broadcast Proxy Re-Encryption for Flexible Data Sharing in VANETs. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 4830–4842. [CrossRef]
8. Tariq, U. Intelligent algorithmic framework for detection and mitigation of BeiDou spoofing attacks in vehicular ad hoc networks (VANETs). *PeerJ Comput. Sci.* **2024**, *10*, e2419. [CrossRef] [PubMed]
9. Tariq, U. Optimized Feature Selection for DDoS Attack Recognition and Mitigation in SD-VANETs. *World Electr. Veh. J.* **2024**, *15*, 395. [CrossRef]
10. Setitra, M.A.; Fan, M. Detection of DDoS attacks in SDN-based VANET using optimized TabNet. *Comput. Stand. Interfaces* **2024**, *90*, 103845. [CrossRef]
11. Wang, M.; Mao, J.; Zhao, W.; Han, X.; Li, M.; Liao, C.; Sun, H.; Wang, K. Smart City Transportation: A VANET Edge Computing Model to Minimize Latency and Delay Utilizing 5G Network. *J. Grid Comput.* **2024**, *22*, 25. [CrossRef]
12. Nazih, O.; Benamar, N.; Lamaazi, H.; Chaoui, H. Toward Secure and Trustworthy Vehicular Fog Computing: A Survey. *IEEE Access* **2024**, *12*, 35154–35171. [CrossRef]

13. Peixoto, M.; Maia, A.; Mota, E.; Rangel, E.; Costa, D.; Turgut, D.; Villas, L. A traffic data clustering framework based on fog computing for VANETs. *Veh. Commun.* **2021**, *31*, 100370. [CrossRef]
14. Gaouar, N.; Lehsaini, M.; Nebbou, T. CCITL: A cloud-based smart traffic management protocol using intelligent traffic light system in VANETs. *Concurr. Comput. Pract. Exp.* **2023**, *35*, e7686. [CrossRef]
15. Zhan, Y.; Xie, W.; Shi, R.; Huang, Y.; Zheng, X. Dynamic Privacy-Preserving Anonymous Authentication Scheme for Condition-Matching in Fog-Cloud-Based VANETs. *Sensors* **2024**, *24*, 1773. [CrossRef] [PubMed]
16. Su, H.; Dong, S.; Wang, N.; Zhang, T. An efficient privacy-preserving authentication scheme that mitigates TA dependency in VANETs. *Veh. Commun.* **2024**, *45*, 100727. [CrossRef]
17. Kilic, A. TLS-handshake for Plug and Charge in vehicular communications. *Comput. Netw.* **2024**, *243*, 110281. [CrossRef]
18. Amari, H.; El Houda, Z.A.; Khoukhi, L.; Belguith, L.H. Trust Management in Vehicular Ad-Hoc Networks: Extensive Survey. *IEEE Access* **2023**, *11*, 47659–47680. [CrossRef]
19. Mdee, A.P.; Khan, M.T.R.; Seo, J.; Kim, D. Security Compliant and Cooperative Pseudonyms Swapping for Location Privacy Preservation in VANETs. *IEEE Trans. Veh. Technol.* **2023**, *72*, 10710–10723. [CrossRef]
20. Labadie, C.; Legner, C. Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *J. Inf. Technol.* **2023**, *38*, 16–44. [CrossRef]
21. OAG. "California Consumer Privacy Act (CCPA)", State of California-Department of Justice-Office of the Attorney General. 13 March 2024. Available online: https://www.oag.ca.gov/privacy/ccpa (accessed on 3 May 2024).
22. Mehrabani, M.R.; Abolhassani, B.; Haddadi, F.; Tellambura, C. Second-Order Statistics-Aided Channel Estimation for Multipath Massive MIMO-OFDM Systems. *IEEE Access* **2023**, *11*, 21921–21933. [CrossRef]
23. Ma, W.; Peng, Y.; Liu, X.; Cui, J. VeriRange: A Verifiable Range Query Model on Encrypted Geographic Data for IoT Environment. *IEEE Internet Things J.* **2024**, *11*, 3068–3081. [CrossRef]
24. Almehdhar, M.; Albaseer, A.; Khan, M.A.; Abdallah, M.; Menouar, H.; Al-Kuwari, S.; Al-Fuqaha, A. Deep Learning in the Fast Lane: A Survey on Advanced Intrusion Detection Systems for Intelligent Vehicle Networks. *IEEE Open J. Vehicular Technol.* **2024**, *5*, 869–906. [CrossRef]
25. Zhuang, L.; Guo, N.; Chen, Y. TriNymAuth: Triple Pseudonym Authentication Scheme for VANETs Based on Cuckoo Filter and Paillier Homomorphic Encryption. *Sensors* **2023**, *23*, 1164. [CrossRef]
26. Konkin, A.; Zapechnikov, S. Zero knowledge proof and ZK-SNARK for private blockchains. *J. Comput. Virol. Hacking Tech.* **2023**, *19*, 443–449. [CrossRef]
27. Carletti, M.; Terzi, M.; Susto, G.A. Interpretable Anomaly Detection with DIFFI: Depth-based feature importance of Isolation Forest. *Eng. Appl. Artif. Intell.* **2023**, *119*, 105730. [CrossRef]
28. Zhong, W.; Yang, C.; Liang, W.; Cai, J.; Chen, L.; Liao, J.; Xiong, N. Byzantine Fault-Tolerant Consensus Algorithms: A Survey. *Electronics* **2023**, *12*, 3801. [CrossRef]
29. Wang, C.; Xu, J.; Yin, L. A Secure Cloud-Edge Collaborative Logistic Regression Model. In Proceedings of the IEEE/ACM Int'l Conference on & Int'l Conference on Cyber, Physical and Social Computing (CPSCom) Green Computing and Communications (GreenCom), Melbourne, Australia, 6–8 December 2021; pp. 244–253. [CrossRef]
30. Kumar, R.; Kumar, D.; Kumar, D. SMBF: Secure data Transmission using modified Bloom Filter for vehicular ad hoc networks. *Recent Adv. Comput. Sci. Commun.* **2022**, *16*, e310322202909. [CrossRef]
31. Ren, Y.; Chen, C.; Hu, M.; Feng, G.; Zhang, X. BFDAC: A Blockchain-Based and Fog-Computing-Assisted Data Access Control Scheme in Vehicular Social Networks. *IEEE Internet Things J.* **2024**, *11*, 3510–3523. [CrossRef]
32. Hu, H.; Fan, X.; Wang, C. Efficient cluster-based routing protocol for wireless sensor networks by using collaborative-inspired Harris Hawk optimization and fuzzy logic. *PLoS ONE* **2024**, *19*, e0301470. [CrossRef]
33. Tariq, U.; Tariq, B. Proactive ransomware prevention in pervasive IoMT via hybrid machine learning. *Indones. J. Electr. Eng. Comput. Sci.* **2024**, *34*, 970–982. [CrossRef]
34. Nsnam. "Network Simulator", NS-3. 25 February 2024. Available online: https://www.nsnam.org/ (accessed on 10 May 2024).
35. Zou, L.; Yan, H.; Dong, J.; Li, Y.; Chen, P.; Lau, F.C.M. On Construction of Low-Density Parity-Check Codes for Ultra-Reliable and Low Latency Communications. *IEEE Trans. Commun.* **2024**, *72*, 5290–5301. [CrossRef]
36. Wang, Y.; Jia, Y.-H.; Chen, W.-N.; Mei, Y. Distance-aware Attention Reshaping: Enhance Generalization of Neural Solver for Large-scale Vehicle Routing Problems. *arXiv* **2024**, arXiv:2401.06979. [CrossRef]

37. Marydasan, B.P.; Nadarajan, R. An Energy-Conserved Stability and Density-Aware QoS-Enabled Topological Change Adaptable Multipath Routing in MANET. *Int. J. Comput. Netw. Appl.* **2023**, *10*, 964. [CrossRef]
38. Gharibeh, H.F.; Yazdankhah, A.S.; Azizian, M.R. Energy management of fuel cell electric vehicles based on working condition identification of energy storage systems, vehicle driving performance, and dynamic power factor. *J. Energy Storage* **2020**, *31*, 101760. [CrossRef]