IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 2 November 2023, accepted 25 November 2023, date of publication 4 December 2023,
date of current version 11 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3339192

SURVEY

A Survey on Vehicular Cloud Network Security

JUNYI DENG[1], (Member, IEEE), JIKAI DENG[1], PEIHAO LIU[1], HUAN WANG[1], (Member, IEEE), JUNJIE YAN[2], DERU PAN[1], AND JIAHUA LIU[1]

[1]School of Computer Science and Technology, Guangxi University of Science and Technology, Liuzhou 545026, China
[2]School of Electronic Engineering, Guangxi University of Science and Technology, Liuzhou 545026, China

Corresponding author: Peihao Liu (liupeiho@126.com)

This work was supported in part by the Guangxi Science and Technology Planning Project under Grant Gui Ke AD21220161, in part by the Guangxi Natural Science Foundation under Grant 2022GXNSFBA035642, in part by the Basic Ability Improvement Project for Young and Middle-Aged University Teachers of Guangxi under Grant 2021KY0364 and Grant 2022KY0325, in part by the Doctoral Fund Project of Guangxi University of Science and Technology under Grant Xiao Ke Bo 23Z08 and Grant Xiao Ke Bo 21Z22, in part by the National Natural Science Foundation of China under Grant 62106053, in part by 2023 Degree and Graduate Education Reform under Grant JGY2023282, and in part by the Innovation Project of Guangxi University of Science and Technology Graduate Education under Grant GKYC202351.

ABSTRACT The novel Vehicular Cloud Network (VCN) is a close combination of Vehicular Ad hoc Network, Cloud Computing, and Edge Computing. However, VCN is facing the enormous challenge of security and privacy before it is generalized. To address these issues, VCN communication characteristics and security requirements are summarized first. Secondly, the paper conducts an in-depth analysis of the existing security problems and solutions in VCN based on several attack models, including routing, data, identity, DoS, and hostile attacks. And we summarize the security solutions into two categories: security defense measures based on identity authentication and access control, and security protection measures based on traffic detection and anomaly detection. Thirdly, this paper proposes a reliable VCN security architecture consisting of three types of clouds: vehicular, edge, and central clouds. Moreover, the VCN architecture combines a Vehicle Intrusion Detection and Prevention System with a Vehicular Cloud Security Management Platform to ensure the security of VCN. Last but not least, some open issues worth investigating are discussed.

INDEX TERMS Cloud computing, edge computing, security, VANETs, vehicular cloud network.

I. INTRODUCTION

With the rapid development of Vehicular Ad hoc Networks (VANETs) [1], Intelligent Connected Vehicles (ICVs) have become widely used, enabling various types of vehicle applications. The implementation of these applications needs to consume a lot of computational and storage resources. Considering the limitations of vehicle computing and communication capabilities, Cloud Computing (CC) has been applied to VANETs, resulting in the formation of VCC. Vehicular Cloud Computing (VCC) [2] effectively meets various in-vehicle application service requirements through powerful big data analysis and optimization capabilities. However, long-distance transmission between vehicles and the cloud center can lead to high latency and low reliability, while the decommissioning of large amounts of data may lead to congestion of the backbone network. To address these problems, Vehicular Edge Computing (VEC) [3] provides low-latency services by sinking computing capability around the vehicles using infrastructure such as Road Side Units (RSUs) and edge servers. As a result, the Quality of Service(QoS) of ICVs has significantly improved thanks to the cooperation of VANETs, VCC, and VEC, and a Vehicular Cloud Network (VCN) has gradually formed. The origin and evolution of the novel network are shown in Figure 1. And the developments of VANETs, VCC and VEC are described in Section II.

VCN is a comprehensive network architecture based on VANETs, CC, and Edge Computing (EC) technologies that achieves wireless communication and information exchange between vehicles and other entities (roads, pedestrians, and the Internet). Its ultimate goal is to realize the integration

The associate editor coordinating the review of this manuscript and approving it for publication was Tiago Cruz.

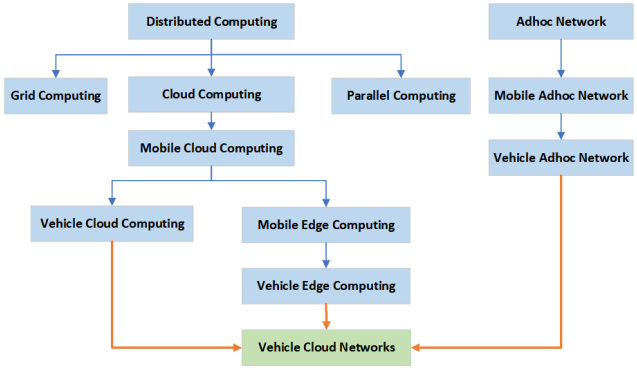

FIGURE 1. The origin and development of vehicular cloud network.

of intelligent traffic management, intelligent dynamic information services, and intelligent vehicle control to enhance the efficiency and safety of transportation systems. However, VCN inherits the discovered and undiscovered security and privacy vulnerabilities related to VANETs, CC, and EC [4], [5]. And it also has many unique attributes that make various security challenges increasingly difficult to handle. For example, the communication mode of VCN has developed from GPSR, 2G/3G/4G, WLAN, and WiMAX to 5G, 6G, C-V2X, and GPS, becoming more complex. Moreover, normal and malicious vehicles have the same authentication method in the security and privacy mechanisms, which puts the security trust problem at risk. Additionally, various attacks (Sybil, DDoS, and Man-in-the-Middle attacks) can also endanger the security of VCN. In the end, these safety challenges will undoubtedly lead to traffic accidents or congestion, and more seriously will affect the operation of the transportation system.

Therefore, the security of VCN is essential to traffic safety. It can not only promote the interoperability of different vehicle networks, but also realize the early warning of accidents, which has a far-reaching implications for the sustained development of Intelligent Transportation Systems (ITS). The purpose of this paper is to summarize and analyze the security of VCN from the perspectives of communication characteristics, security requirements, attack threats, and corresponding solutions. Our contributions are summarized as follows:

- A comprehensive overview of VCN security is provided, where the introduction, communication characteristics, and security requirements of VCN are elaborated in detail. Then, according to the different objects targeted by the attack,the attack types are divided into five types, including routing, identity, data, DoS, and malicious attack. The corresponding solutions and techniques for different attacks are summarized.
- To solve the security of VCN, this paper proposes a secure and reliable VCN security architecture consisting of three types of clouds: vehicular, edge, and central clouds. The architecture combines a Vehicle Intrusion Detection and Prevention System and a Vehicular Cloud Security Management Platform to address security concerns. Finally, several open issues are discussed.

This paper is organized as follows: Section II introduces the concepts of VANETs, VCC, VEC, and VCN. Section III is devoted to concluding the communication characteristics and security requirements of VCN, while the security problems of VCN and corresponding solutions are summarized in Section IV. Section V puts forward a new VCN security architecture. Finally, we discuss the open issues and research challenges in Section VI.

II. BACKGROUND

This section reviews background concepts for four important concepts that appear in the Figure 1, including VANETs, VCC, VEC, and VCN.

A. VEHICULAR AD HOC NETWORKS

VANETs, a subclass of Mobile Ad hoc Networks (MANETs), is a distributed and dynamically changing self-organized communication network that builds network nodes on vehicles and infrastructure [6]. Its basic principle is to use On-Board Units (OBUs), RSUs, and wireless communication technologies such as cellular mobile communications, Dedicated Short-range Communication (DSRC), and Wireless Local Area Network (WLAN) to collect and use vehicle status, performance, location, road conditions, and other information. Therefore, VANETs can effectively improve the efficiency of vehicle communication and enhance driving safety. Currently, VANETs is widely used in traffic management, road monitoring, vehicle tracking, safe driving, intelligent navigation, etc. In the future, it is also expected to be the main carrier of intelligent transportation systems, an important component of smart cities.

B. VEHICULAR CLOUD COMPUTING

VCC is the application of Mobile Cloud Computing (MCC) in VANET, which treats a large number of on-board storage, computing, and sensing capabilities in vehicles as mobile cloud computers. As a cloud member, vehicles integrate resources together to provide cloud services such as environment awareness, path planning, and autonomous driving. VCC can be defined as follows [8]: "A group of largely autonomous vehicles whose corporate computing, sensing, communication, and physical resources can be coordinated and dynamically allocated to authorized users." Compared with MCC, VCC has better computing power and storage capacity.

C. VEHICULAR EDGE COMPUTING

VEC is a novel paradigm for integrating vehicular networks and MEC. It transfers communication, computing, and storage resources to RSUs near the vehicles. RSUs act as edge servers, which are distributed on each road in the city. They have higher computing, processing, and storage power than the OBUs. Therefore, VEC has a shorter transmission

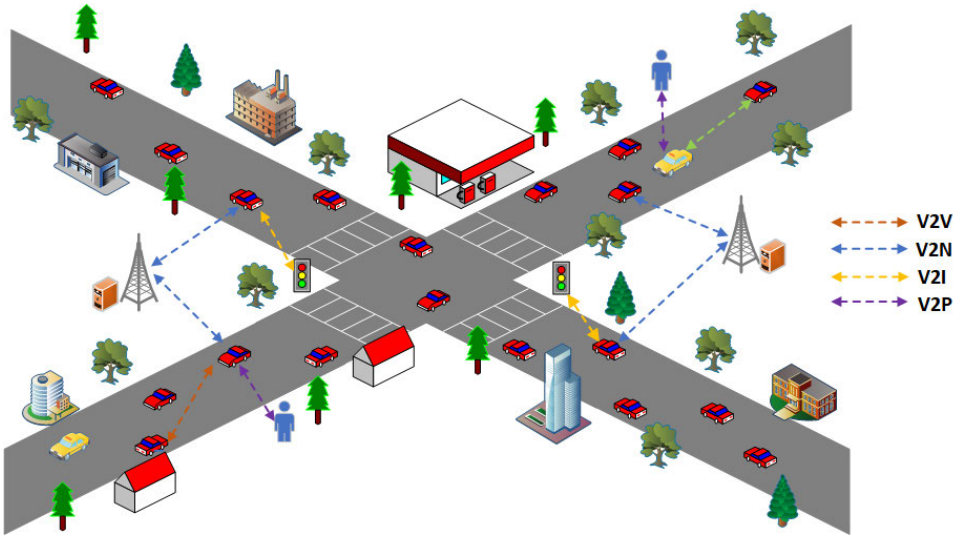

FIGURE 2. The scene diagram of VCN communication characteristics.

distance compared to VCC, which effectively reduces the bandwidth consumption in data transmission. And it also provides more services for vehicles, such as traffic control and path navigation, which significantly improve traffic safety and consistency [5].

D. VEHICULAR CLOUD NETWORK

As demand for intelligent transportation systems increases, vehicles need to be able to communicate not only with other vehicles but also with road infrastructure, pedestrians, and the cloud in the meantime. Secondly, the rapid development of CC and EC technology provides vehicles with near-range computational and storage capabilities, enabling them to process and analyze large amounts of data in real time to improve the driving experience. Furthermore, the fast development of 5G and 6G communications technologies is expected to bring faster, smarter, and wider connectivity to vehicle networks. Therefore, VCN was proposed, which integrates VANETs, CC, and EC. VCN is a solution that aims to provide users with their required resources. It consists in exploiting the underutilized vehicular, edge infrastructure, and cloud services resources optimally.

In recent years, many researchers have focused on this new paradigm and tried to discuss the architecture and security, as shown in Table 1. To begin, Olariu et al. introduced the concept of VCN in the form of autonomous vehicular clouds, in which vehicles dynamically allocate computing and communication resources to authorized users [9]. Hussain et al. presented an architecture consisting of vehicular clouds (VC), vanet-using clouds (VuCs), and hybrid clouds (HCs) [10]. Yu et al. in [11] proposed a scheme to integrate cloud computing into different applications of vehicular networks. Their architecture enables the vehicles to share storage, computation, and bandwidth resources. In [12], a three-tier vehicular cloud networking architecture was introduced by categorizing the clouds into categories of vehicular cloud, infrastructure cloud, and back-end cloud. In addition, the authors proposed use cases in each cloud category and also highlighted security threats. Jabbarpour et al. [13] define a Vehicular Hybrid Cloud, where vehicles act both as service providers (vehicular computing) and as users (vehicular using the cloud). Mekki et al. in [14] focus on the features and architectures of the vehicular cloud and provide an overview of the challenges and design issues in depth. However, their architecture lacks consideration for edge infrastructure. In summary, the architecture of the VCN is still evolving. Security challenges are inevitable in its development process. Therefore, we summarize two security challenges of VCN that are different from VANETs, VCC, and VEC in the following.

1. Security of multi-layer architecture. VCN is a three-layer architecture consisting of vehicle cloud, edge cloud and central cloud. This structure improves the original calculation and storage methods of VCC and VEC, effectively improving system performance, but also increasing security risks. Attackers may attempt to break into one of them and use its control to further attack other layers.As a result, complex interactions between the three levels can have profound security implications for the entire system.

2. Security management complexity. The multi-layer architecture and multifarious communication technologies of VCN make security management more complex. In this context, ensuring the security of each layer and communication link becomes a critical task. Managers must deal with the security requirements between different levels and implement effective security measures such as access control, authentication, encryption, etc.

The related works above alert that the security challenges of VCN are not easy. In the next sections, we aim to emphasize communication characteristics and security requirements in VCN, then introduce the possible attacks and

TABLE 1. Review of the VCN architecture and security surveys.

Work	Year	Vehicle Layer	Edge Layer	Cloud Layer	Security	Solution	Open issues
[9]	2011	✓					✓
[10]	2012	✓		✓			✓
[11]	2013	✓	✓	✓			✓
[12]	2015	✓	✓	✓	✓		
[13]	2017	✓		✓			✓
[14]	2017	✓		✓	✓	✓	✓
Our work	2023	✓	✓	✓	✓	✓	✓

their corresponding countermeasures, and propose a a reliable VCN security architecture.

III. VCN COMMUNICATION CHARACTERISTICS AND SECURITY REQUIREMENTS

VCN facilitates information exchange between the vehicle by On-Board Units (OBUs) and other RSUs, pedestrians, and networks through Vehicle-to-Everything (V2X) communication. V2X can be roughly divided into two types based on the type of communication entities: (1) device-to-device communication, including V2V, V2I, and Vehicle-to-Pedestrian (V2P), and (2) device-to-network communication, namely Vehicle-to-Network (V2N) [15]. The scene diagram of V2N communication characteristics is shown in Figure 2.

- **V2V** enables the exchange and sharing of information among vehicles through OBUs, which gather the basic information of surrounding vehicles to assess driving situations and proactively formulate driving strategies. These strategies include early avoidance of emergency vehicles (fire trucks, ambulances, and police cars), real-time lane change assistance, and adaptive cruise control. In addition, the distance of vehicles is close in V2V, the transmission time is short, and it is difficult to destroy. V2V has low latency and high reliability.
- **V2I** enables communication between vehicles and RSUs. It allows the traffic center to receive pertinent information from roads, including road conditions, traffic volume, and accident information. Additionally, guidance messages can be sent to vehicles to help them plan their travel paths, such as road planning, red light violation warnings, and dynamic lane management. Since the vehicle does not stay in the communication range of a RSU for a long time, V2I is characterized by short life and high data rate connectivity.
- **V2P** enables communication between vehicles and smart devices carried by pedestrians, including smartphones, fitness bands, smartwatches, and so on. It allows vehicles to exchange information with the surrounding pedestrians in real time. By predicting the possibility of a collision and issuing warning messages to alert drivers and pedestrians, potential traffic accidents could be effectively prevented.
- **V2N** refers to the information exchange between vehicles and cloud platforms. It enables vehicles to obtain various vehicle application services from cloud platforms, for example, navigation, monitoring, emergency rescue, and entertainment. These services are processed and calculated by cloud platforms and then sent to vehicles through V2N.

To make it easier to distinguish between these four types of communication, we also summarize the schematic diagram of V2X communication, as shown in Figure 3. The wireless access methods used in the four communication domains include IEEE 802.11p (V2V, V2I, and V2N), cellular networks (3G, 4G, and 5G in V2I), WLAN (802.11 a/g/n/ac in V2I and V2P), Bluetooth (V2P), etc. VCN applications will involve several communication methods. For example, the vehicle device uses LTE, 5G, and other cellular networks to upload the vehicle location and driving status information to the cloud server in real time. At the same time, the server can send real-time traffic information to OBUs through V2N to improve driving safety, road safety, and personal safety. But hackers may obtain sensitive information by intercepting the network packets. It leads to more security challenges for communication technology in VCN. Therefore, the VCN must meet the basic security requirements as follows.

- **Confidentiality**: The data of the sender and the recipient can be correctly encrypted, and only authorized users can access VCN. Therefore, confidentiality can prevent information from being maliciously manipulated or leaked. Its main precaution is cryptography.
- **Integrity**: The information or data is not illegally tampered during transmission and storage. Once this happens, it will be identified immediately. To verify data integrity, digital signatures or message digest technologies are widely utilized [16].
- **Availability**: Authorized users can continue to access VCN. And data information is available at network nodes such as authorized vehicles, edge base stations, and cloud servers. The most common threats include Denial of Service (DoS) attacks, black hole attacks, interference attacks, and spamming attacks [17].
- **Controllability**: The information is always validly owned and controlled by legitimate vehicles or infrastructures. Its transmission range and storage space are also limited. Access control, identity authentication, and audit logging can effectively ensure this security requirement.
- **Reliability**: The network system can quickly recover and maintain normal operation when abnormal situations occur. Fault prevention, error handling, data backup, and recovery can ensure reliability. Reliability also involves other security attributes of VCN, including stability and robustness.

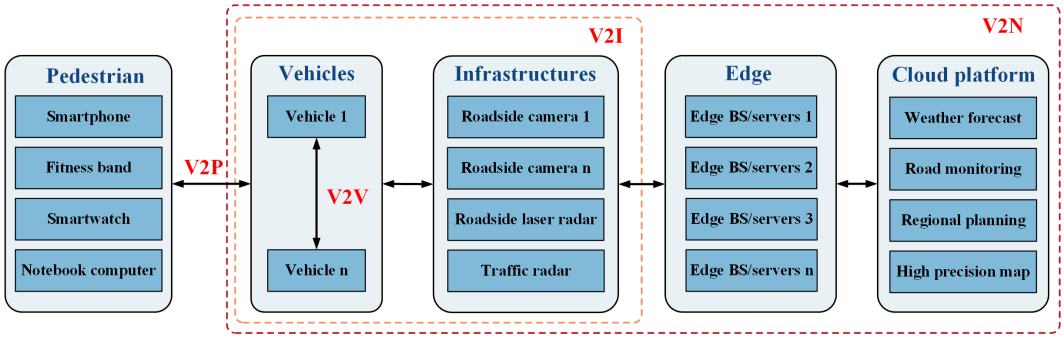

FIGURE 3. The schematic diagram of V2X communication.

To ensure the security of vehicle data transmission, it is necessary to strictly manage five processes and meet basic network security requirements, as shown in Figure 4. Authentication is the first line of defense for network security and the cornerstone of other security mechanisms. Therefore, vehicle users must undergo message and identity authentication before access VCN. Then, the security administrator configures the authorization database according to the needs of vehicle users. Thirdly, the access permissions for resources are determined by the access monitoring equipment. At the same time, the audit system records user activities and requests, and Intrusion Detection System (IDS) monitors abnormal behavior.

- **Authentication**: It includes message and identity authentication. Message authentication detects data integrity and prevents tampering or forgery. Identity authentication is used to ensure that only legitimate users have the right to access VCN.
- **Access Control**: This requirement is responsible for determining network privileges. Some sensitive communications must not be accessed by the other nodes of the network, such as those coming from police cars or other law enforcement authorities. As a result, access control prohibits unauthorized vehicles from accessing services they have no rights to uses [18].
- **Authorization**: As a part of access control, authorization establishes the rights of each network node.
- **Security Auditing**: System vulnerabilities and intrusion behaviors can be examined by recording and analyzing user activity information.
- **Intrusion Detection**: IDS constantly monitors and analyzes network activities according to predefined rules and models. When abnormal behavior is detected, it will provide real-time alerts.

Key protocols and data validation are also very important, which are reflected three processes firstly. Key protocols use encryption algorithms and techniques to ensure information confidentiality and integrity. Data validation involves checking and verifying transmitted data to ensure its authenticity and reliability. In addition, based on the five security attributes, VCN must also meet the following two security requirements.

- **Non-repudiation**: Participants in VCN can neither deny any message sent nor repudiate responses. At the same time, it also needs to be allowed to track the source and destination of information so that some information can be revoked. Therefore, digital signatures, timestamps, and other technologies can be used to ensure the authenticity and legality of information.
- **Accountability**: There must be a clearly designated person to assume responsibility and punishment when a security incident occurs in VCN.

Under the premise of strict execution and implementation of the aforementioned security requirements, the flexibility and efficiency of VCN should also be taken into account. Flexibility means that VCN can quickly adapt the needs of network topologies, protocols, and services. Efficiency involves optimizing resource use, reducing waste, and improving performance. In addition, multiple security policies and mechanisms, for instance access control, firewalls, and intrusion detection, should also be established to ensure integrity and confidentiality. To sum up, the security and reliability of VCN can be effectively achieved by implementing multi-layered and multi-dimensional protection mechanisms.

IV. VCN SECURITY AND SOLUTIONS

A. ATTACKER MODEL

Exploring and analyzing network security requirements is of great significance to improving the security of VCN. However, VCN must suffer various attacks, such as network destruction, data theft, manipulation, deletion, etc. Therefore, this section classifies and analyzes attacks and attackers in VCN.

1) ATTACKS

The security attack layers of VCN include the vehicle terminal layer, V2X communication layer, and cloud network layer. First, we summarize the attacks that every layer may face, as shown in Table 2. It is evident that VCN is subject to a wide range of attacks, and some attacks occur at any layer of the network. According to the different attack objects targeted by the attackers, this paper divides attacks into five categories: routing, data, DoS, identity, and malicious attacks. Their corresponding solutions are summarized in Section IV-B.

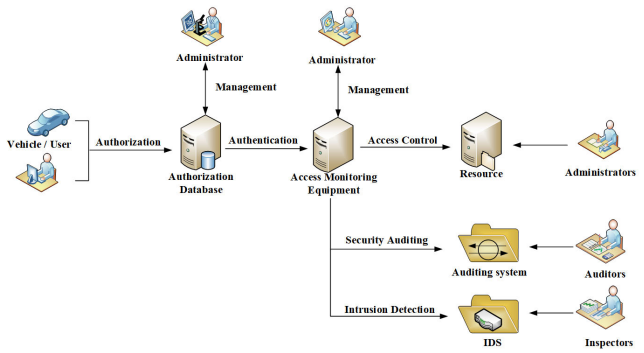

FIGURE 4. Security requirements in V2X data transmission.

a: ROUTING ATTACK

Attackers utilize vulnerabilities in routers and vehicle devices to attack networks.

- **Black Hole Attack**: For luring sending nodes to transfer data through it, a malicious node pretends to have the best path to the target node. Once nodes are attracted, the attacker uses package-dropping technology to intercept or discard packets, resulting in communication failure [22].
- **Gray Hole Attack**: Malicious nodes selectively discard data, or occasionally take in packets, creating the black hole effect. It is more dangerous than black hole attacks.
- **Wormhole Attack**: Two or more malicious nodes create a private tunnel that transmits faster than the original network, attracting neighboring nodes to transmit along the channel. Then, Wormhole nodes can steal or tamper with information between links.

b: DATA ATTACK

Data attacks threaten data transmission in VCN, including interception, tampering, leakage, and so on.

- **Data Interception Attack**: Attackers intercept packets to obtain sensitive information or carry out other data attacks, such as DoS, injection attacks and so on.
- **Data Tampering Attack**: The attacker tampers with, add to, or delete data, causing its integrity to be compromised [23].
- **Data Leakage Attack**: External attackers use software and hardware vulnerabilities to launch attacks, leaking sensitive data from vehicles.
- **Replay Attack**: Attackers re-send previously intercepted communication data to the receiver, which causes the correctness of the identity authentication to be damaged.
- **Data Injection Attack**: Attackers deliberately inject false information, affecting the behavior of other vehicles in VCN.
- **Eavesdropping Attack**: It is a passive attack, also referred to as a sniffing attack. Attackers use network monitoring or intercepting equipment to gain sensitive data during the transmission process.

TABLE 2. Attack classification.

Attacks	Vehicle Terminal Layer	V2X Communication Layer	Cloud Network Layer
Black Hole	✓	✓	✓
Grey Hole	✓	✓	✓
Wormhole	✓	✓	✓
DoS	✓	✓	✓
Jamming	✓	✓	✓
Flooding	✓	✓	✓
Session Hijacking	✓	✓	×
Sybil	✓	×	✓
Impersonation	✓	×	✓
Timing Attack	✓	×	✓
MITM	✓	✓	✓
Authentication	✓	×	✓
Identity Masquerading	✓	×	✓
Malware	✓	×	✓
Spamming	×	×	✓
Botnet	✓	✓	✓
Location Spoofing	✓	✓	×
Data Leakage	✓	✓	✓
Data Injection	✓	×	✓
Data Tampering	✓	×	✓
Data Interception	✓	✓	✓
Replay	✓	✓	✓
Eavesdropping	✓	✓	✓

c: DOS ATTACK

Attackers submit a large number of illegal requests to interfere with the target server to perform vehicle tasks. This causes the server to respond slowly or down, affecting the normal operation of VCN [24].

- **Distributed Denial of Service(DDOS)**: It is a DoS attack from different locations [25].
- **Jamming Attack**: Attackers interfere with communication channels by transmitting high-frequency noise signals, resulting in the transmission process to be interrupted [26].
- **Flooding Attack**: The attacker intentionally injects a huge quantity of fake information into V2X, consuming the communication bandwidth and making communication links inaccessible to legitimate nodes.

d: IDENTITY ATTACK

Attackers destroy the user-identifying information in VCN.

- **Authentication attack**: Attackers utilize the authentication mechanism of network to get access credentials, such as usernames and passwords [27].
- **Identity Masquerading Attack**: The unauthorized attackers disguise as legitimate nodes for getting access to sensitive information. This threat not only bypasses authentication but also impacts the confidentiality, data integrity, usability, and communication efficiency of VCN.
- **Impersonation Attack**: Attackers masquerade as legitimate vehicles in an attempt to gain access to the network.
- **Sybil Attack**: Attackers damage the reputation system of network by creating fake vehicles with identical identities, resulting in less redundant and robust [28].
- **Session Hijacking**: It is an attack that combines sniffing and spoofing techniques. Attackers use the stolen user

TABLE 3. Security requirements attack model.

Security Requirement	Attack Name	Communication Model
Confidentiality	- Black Hole attack - Data Leakage, Interception, Eavesdropping attack - Identity Masquerading, MITM, Session Hijacking, Timing attack - Malware attack	V2V, V2I, V2P, V2N
Integrity	- Black Hole attack - Data Tampering, Leakage, Replay, Eavesdropping - Identity Masquerading, MITM, Session Hijacking, Timing attack - Jamming attack	V2V, V2I, V2P, V2N
Availability	- Routing attack - DoS, Jamming attack, Flooding attack - Spamming, Spamming attack - Identity Masquerading attack	V2V, V2I, V2P, V2N
Controllability	- Black Hole, Wormhole attack - Sybil attack, Session Hijacking - Botnet attack	V2V, V2I, V2P, V2N
Reliability	- Gray Hole attack - Data Tampering, Replay attack - Sybil attack	V2V, V2P, V2N
Non-repudiation	- Data Replay attack - Identity Masquerading attack - Location Spoofing Attack	V2V, V2I, V2P, V2N
Authentication	- Wormhole attack - Data Tampering, Leakage, Replay, Eavesdropping attack - Identity Masquerading, Session Hijacking, MITM, Timing, Sybil attack - Botnet, Location Spoofing attack	V2V, V2I, V2P
Access control	- Data Leakage - Session Hijacking, MITM	V2I, V2N
Authorization	- Data Tampering attack	V2V, V2I, V2P, V2N
Data validation	- Botnet, Location Spoofing attack - Data Tampering, Leakage attack	V2V, V2I, V2P, V2N
Privacy and Anonymity	- Session Hijacking, MITM, Timing attack - Data Leakage, Eavesdropping attack	V2V, V2P, V2N
Traceability and Revocability	- Session Hijacking, MITM attack - Location Spoofing attack	V2V, V2I, V2P, V2N
Flexibility and Efficiency	- Gray Hole attack - Identity Masquerading attack - Jamming attack	V2V, V2I, V2P, V2N
Key Protocols	- Routing attack	V2V, V2I, V2P, V2N

identities to bypass the authentication mechanism and access the data and services [12].

- **Timing attack**: It is a side-channel attack in which attackers analyze the execution time of the encryption algorithm to decrypt the password.
- **Man-in-the-Middle attack (MITM)**: The attacker hijacks the communication nodes, eavesdrops on communication content, and engages in malicious actions.

e: MALICIOUS ATTACK

The paper collectively refers to the other attack types besides those mentioned above. There are four species as following.

- **Malware Attack**: Attackers exploit system weaknesses to inject malicious software or viruses into V2X entities (OBU, RSU), giving them the ability to control and steal sensitive data.
- **Spamming Attack**: Attackers broadcast spam to the V2X channel to increase transmission, latency, and bandwidth consumption.
- **Botnet Attack**: Attackers use malicious software to break into vehicle electronic systems, steal vehicle control information, and transfer it to external servers to enable remote monitoring.
- **Location Spoofing Attack**: Malicious vehicles altering and fabricating their location information make it hard for other network nodes to determine their precise position or even whether they exist.

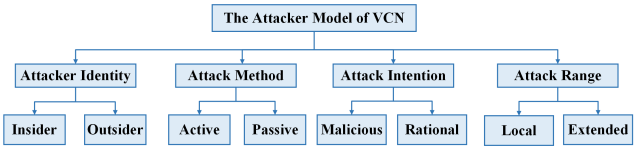

FIGURE 5. The attacker model of VCN.

In conclusion, this paper also summarizes attack types and their communication models in the different security requirements in Table 3.

2) ATTACKERS

Attackers are also an equally important component of VCN and can be classified into four types based on their actions and targets: Insider and Outsider, Active and Passive, Malicious and Rational, Local and Extended, as shown in Figure 5 [29].

a: INSIDER VS. OUTSIDER

Attackers can be distinguished by whether they are members of VCN. Insider attackers are authenticated legitimate nodes who can launch attacks in various ways. But outsider attackers are unauthenticated nodes, and it is relatively difficult for it to carry out an attack. However, it can

eavesdrop on the network to gather information, or design a black hole attack to attract normal nodes passing through it for data transmission.

b: ACTIVE VS. PASSIVE

According to the attack methods, attackers can be divided into active and passive. Active attackers can create new signals or data packets in the network. Passive attackers can only capture sensitive data through packet interception or traffic analysis, and do not make any changes to the data information.

c: MALICIOUS VS. RATIONAL

Attackers can be classified as malicious or rational based on their attack intentions. Malicious attackers use a variety of methods to attack the network without seeking personal benefits. Conversely, rational attackers try to gain benefits by assaulting. As a result, these attacks often have a clear purpose and are easier to be detected.

d: LOCAL VS. EXTENDED

Attackers can be classified based on their attack range. Local attacker has a limited attack scope, it possesses a few vehicles. Extended attackers broaden their scope by controlling several entities that are scattered across the network.

B. SECURITY SOLUTIONS

In order to effectively mitigate attack severity and ensure the security of VCN, this section categorizes and summarizes the corresponding solutions, as shown in Figure 6.

1) THE SOLUTIONS TO ROUTING ATTACKS

Techniques based on thresholds, trust, encryption, and machine learning are frequently used to combat routing attacks [30].

a: FOR BLACK HOLE ATTACK

The threshold-based detection approach identifies the attack behavior by observing the packet drops or sequence number values in a certain time period. Reference [31] proposed an intelligent black hole attack detection scheme for Autonomous Vehicles (AV), IDBA. The method precalculates the threshold for the future behavior of the black hole based on four parameters, namely hop count, end-to-end delay, packet delivery rate, and sequence number. Then, the precalculated threshold is compared with each node to determine whether the malicious node exists. The simulation results show that IDBA outperforms previous approaches. But we find that computing four critical thresholds on each node leads to higher end-to-end latency and processing overhead.

The encryption-based method refers to introducing cryptographic technologies or encryption algorithms into the routing protocol. Reference [33] presented a secure AODV (SAODV) with improvements made in the RREQ and RREP control packets. The method is based on the ruputation of neighboring nodes to detect black hole attack. Results show that the percentage of packets lost with the proposed AODV is much lower as compared to the existing AODV routing protocol. But, the method is quite complex and generates extra overhead. Dhanaraj et al. [34] proposed a secure AODV protocol (SAODV) with a cryptographic approach to identify and eliminate black hole attackers. The method uses a lookup for storing the RREP and RREQ messages and uses RSA for encrypting and decrypting the RREQ message. The method uses a lookup table for storing the RREP and RREQ messages. In VANETs, it achieves a data packet delivery rate of 95%, a throughput of 87%, and a black hole attack detection rate of 98%. But the method is insecure against multiple and collaborative black hole attackers.

b: FOR GRAY HOLE ATTACK

The threshold-based detection approach can also be used for gray hole attack. Krishnan and Kumar [30] put forward SBGM, a novel security method that detects and mitigates black hole and gray-hole nodes in VANETs by performing time series analysis of the dropped packets of each node. The detection rate of SBGM in highway and urban scenarios may reach 99.87% and 99.68%, respectively.

The machine learning-based strategy refers to analyzing and learning from a large amount of data existing in the network in order to identify attacks automatically [36]. Vasapy et al. [35] proposed a neural network method based on radial functions that can detect both black hole and gray hole attacks. And it has good learning and classification abilities for normal nodes and attacker nodes.

The trust-based strategy detects attacks by using the trust value of vehicles, which determines the reputation of each vehicle in the network. Reference [32] designed a blockchain-based decentralized trust score framework that uses the trusted AODV protocol to mitigate insider attacks and improve the throughput of VANETs system. The framework divides the working principle into two phases. The first phase is the collaboration of neighboring nodes to determine the trust score. And the second phase requires RSU to support the blockchain-based accumulation of node trust values. The framework has the characteristics of high efficiency, scalability, and low computational complexity.

2) THE SOLUTIONS TO DATA ATTACKS

a: FOR DATA TAMPERING ATTACK

Using intrusion detection, message authentication, and machine learning methods can verify the reliability of the information. For example, an intrusion detection technique based on an enhanced deep learning generative adversarial network (GAN) model is proposed in [37]. The model effectively verifies data tampering threats by sequentially using Controller Area Network (CAN) message block detection and GAN detectors. But the algorithm cannot achieve frame-by-frame detection. Liao et al. [38] proposed an anonymous

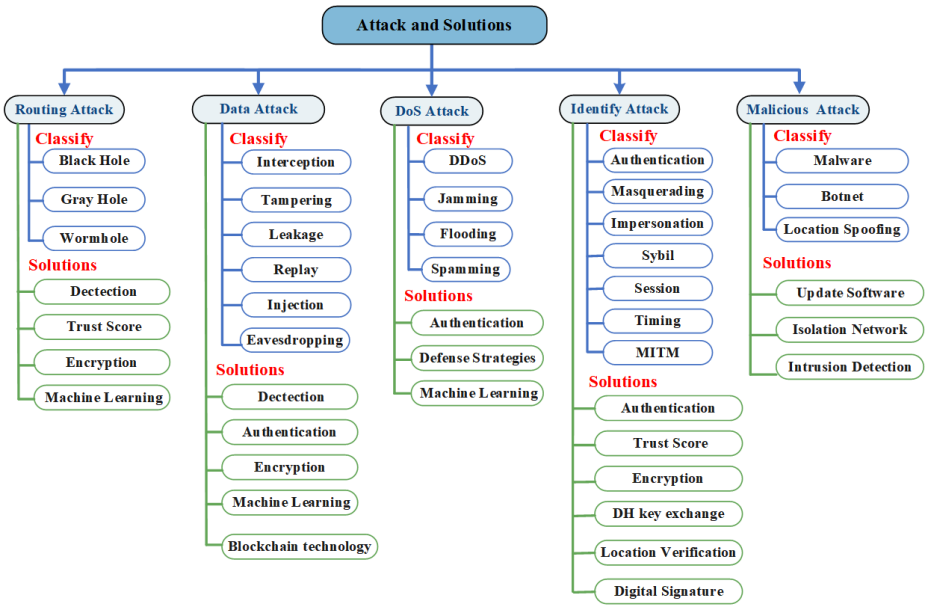

FIGURE 6. Attack classify and corresponding solutions.

and secure message authentication (ASMA) scheme that does not rely on tamper-resistant devices. The scheme can achieve message verification and conditional privacy protection while reducing computational overhead. Furthermore, a proxy-vehicle-assisted batch message verification (PVBA) approach is studied to improve the efficiency of the ASMA scheme, which allows RSUs and proxy vehicles to complete message verification tasks synchronously. Reference [39] used data volume instead of segmentation numbers, applied anomaly scoring for quantifying abnormal degrees, and proposed an intrusion detection method based on an improved MS-iForest algorithm. The approach effectively prevents data tampering attacks on the CAN. Simulation results show that the proposed method is superior to the OCSVM and LOF algorithms.

b: FOR DATA REPLAY ATTACK

Machine learning methods, encryption, and blockchain technology can be utilized to enhance network security and privacy. Reference [40] proposed a vehicle CAN bus detection model based on the Long Short-Term Memory (LSTM) network. The model collects message sequences from the CAN bus, calculates the error between the predicted value and the actual value according to the current ID number, and detects the abnormal message in real time. The results demonstrate that the proposed model can effectively detect replay attacks and frame forgery. A vehicle network security protocol based on dynamic encryption is proposed in [41]. The protocol effectively ensures the confidentiality of communication and the correctness of the message. Reference [42] proposed a secure trust-based blockchain architecture that uses mainly timestamp and hashing techniques to maintain the integrity of transmitted messages and minimize the damage caused by message forgery attacks.

c: FOR EAVESDROPPING ATTACK

Message encryption technology can be used to achieve confidentiality protection for data. Reference [43] adopted two symmetric encryption algorithms (RC6 and Blowfish) to protect the data transmitted on the CAN bus of electric vehicles. Vasudev et al. [44] designed a lightweight mutual authentication protocol using cryptographic operations in IoV scenarios. The scheme can work against various VANETs attacks and reduce the computational and communication costs of onboard devices. However, they did not provide a formal security analysis of the scheme.

d: FOR OTHER DATA ATTACKS

Solving data trust and node trust can significantly improve the credibility of vehicle networks. For example, an attack-resistant trust (ART) management scheme for VANETs is proposed in [45]. The method makes each node have a vector of trust ratings. Then, data trust is evaluated based on the data sensed and collected from multiple vehicles, and node trust is evaluated based on functional trust and recommendation trust. Furthermore, [46] proposed a voting-based trust management system to evaluate vehicle reliability.

3) THE SOLUTIONS TO DOS ATTACKS

a: FOR DOS ATTACK

Authentication-based methods can effectively detect and prevent DoS attacks. Reference [47] proposed an MAuth-CAN authentication method based on assigning shared keys to each Electronic Control Unit (ECU) and authenticator. The protocol consists of four phases. Firstly, each ECU will receive the session key from its communication with the authenticator. Secondly, the ECU will broadcast the message using a MAC derived from the session key. Thirdly, the

authenticator will verify the received message. Finally, the ECU and the verifier will update their session keys and parameters. The method essentially avoids security threats brought by spoofing or DoS attacks on compromised nodes. Gao et al. in [48] designed a method for detecting and defending against DoS attacks. The system takes DoS attack adaptation and daily traffic as feedback, which is mainly divided into two stages. Firstly, Back Propagation (BP) neural network is used to train a large-scale dataset. Secondly, the game theory is used to perform secondary analysis on DoS attacks that could not be identified by the neural network model. Finally, the simulation results show that the detection efficiency of the two stages can reach 99.97% and 99.98%, respectively. In addition, Kolandaisamy et al. proposed a DDoS attack detection method for VANETs by using packet marking based on the Adaptive Watershed Technique [50].The method first produces a neighbor log file and vehicle values based on network density. By comparing this value to a predefined threshold, suspect areas are identified and divided into time windows. Then, the cycle rate is calculated to discover the route for each area window and to calculate the standard deviation value. If it exceeds the normal deviation, then it identifies the node as suspicious. The experiment shows that it outperforms MVSA in terms of drop ratio, delivery ratio, and delay. But the algorithm is performed in V2V communication only.

b: FOR JAMMING ATTACK

Switching transmission channels, using frequency hopping technology, and adjusting wireless technologies are traditional interference defense methods, but they are subject to inherent limitations [51], [52]. Currently, defense strategies based on machine learning are widely applied and researched. In multiple scenarios of sensor edge clouds, a defense scheme based on the Deep Neural Network (DNN) Stackelberg game is proposed for breaking the threat of task offloading in the uplink [53]. And Pourranjbar et al. used Recurrent Neural Network(RNN) to model the interaction between users and jammers and proposed a multi-defense interference strategy [54].

4) THE SOLUTIONS TO IDENTITY ATTACKS

a: FOR SYBIL ATTACK

Trust-based authentication, neighborhood, Received Signal Strength Indication (RSSI), and location verification methods are common approaches to detecting Sybil attacks. Trust-based authentication methods use Public Key Infrastructure (PKI) and strong encryption algorithms to verify the authenticity of nodes. Reference [55] proposed a reliable trust-based platoon service recommendation scheme, which is called REPLACE. This scheme defines the reputation of platoon head (PH) vehicles by collecting and modeling the feedback quality and trust scores of user vehicles. And an iterative filtering algorithm is used to handle unreal feedback from user vehicles. The method effectively helps the user vehicles avoid choosing badly behaved PH.

The neighborhood-based approach uses information from neighboring nodes to identify Sybil nodes. Grover et al. have implemented a distributed and highly robust approach to defend against Sybil attacks in VANETs by using information of neighboring vehicles in [56]. In the approach, each vehicle periodically exchange groups of its neighboring nodes and perform intersection of these groups. If some nodes observe that they have similar neighbors for a significant duration of time, these similar neighbors are identified as Sybil nodes. Reference [57] employed approved infrastructure to provide neighboring vehicles with untampered periodic digital signatures Then, the solution effectively detects and mitigates Sybil attacks in VANETs based on the observed similarity patterns in the movement trajectories of Sybil nodes.

RSSI-based Sybil node detection is an efficient scheme for Sybil attacks.A linear Support Vector Machine (SVM) classifier is used to detect Sybil nodes using anomalous variations in RSSI time series, and a power control-based Sybil attack identification scheme is presented [58]. Yao et al. proposed a widely applicable, lightweight, and fully distributed Sybil attack detection method. It can be applied to VANETs using voiceprint extracted from RSSI time series as an onboard voice and used on the service channel [59]. Simulation results show that the method has good performance.

The location-based verification method utilizes physical measurement values to distinguish between Sybil nodes and legitimate nodes. In [60], a Sybil attack detection scheme is proposed using the Advanced Driving Assistance System (ADAS) sensors of vehicles. The scheme utilizes a deep learning based object detection technique to identify nearby objects. Furthermore, Baza et al. proposed a Sybil attack detection mechanism using Proof of Work (PoW) and Proof of Location (PoL) based on the fact that Sybil attack nodes and vehicles have overlapping trajectories in their physical connections [61]. The scheme has a high detection rate, but it suffers from a high delay and overhead in encrypting and decrypting the vehicle data.

The aforementioned methods mainly focus on detecting Sybil attack nodes, while recognizing Sybil attackers is also an effective solution. A reward-based prediction system is proposed, which uses heuristic algorithms to predict signal strength measurement values, identify vehicle behavior, and expel Sybil attackers in VANETs [62].

b: FOR MITM ATTACK

Authentication and intrusion detection technologies can be used to secure communications. Reference [63] presented a V2I communication protocol with a simplified user revocation and re-registration strategy. The method uses hash algorithms and the Elliptic Curve Discrete Logarithm Problem (ECDLP) to ensure security. Peng et al. [64] proposed an MITM attack detection scheme from the standpoints of signaling and log analysis. The scheme takes advantage of the genetic algorithm in the combination optimization problem, solves the optimal weight combination of weighted Bayesian

TABLE 4. The security solutions.

Attack Types	Solved the Attack Problem	Security Requirements	Solutions
Routing Attack	Black hole	Confidentiality, Integrity, Controllability	[30] [31] [81]
	Grey hole	Confidentiality, Integrity, Reliability, Flexibility and efficiency	[30]
Data Attack	Data Tampering	Integrity, Reliability, Non-repudiation, Authorization	[37] [38] [39]
	Replay	Availability, Non-repudiation, Authentication, Access control, Data validation	[40] [41] [42]
	Eavesdropping	Confidentiality, Traceability and revocability	[43] [44]
Identity Attack	Sybil	Reliability, Authentication, Access control	[55] [56] [57] [58] [59] [60] [61] [62]
	MITM	Confidentiality, Reliability	[63] [64]
	Session Hijacking	Confidentiality, Integrity	[65] [66] [67]
	Timing	Confidentiality, Integrity, Authentication, Controllability	[68]
DoS Attack	DoS	Availability, Non-repudiation	[47] [48] [49] [82]
	DDoS	Availability, Non-repudiation	[50]
	Jamming	Availability, Integrity, Flexibility and efficiency	[51] [52] [53] [54]
Hostile Attack	Botnet	Controllability, Reliability, Authentication, Data validation, Access control	[73] [74]
	Location Spoofing	Confidentiality, Integrity, Non-repudiation	[75] [76] [77]

classifier, and improves the calculation method of weighting parameter. Simulation results have demonstrated that the algorithm has is more stable, simple and accurate.

c: FOR SESSION HIJACKING ATTACK

Integrating RSA-based encryption, RSA digital signature, DH key exchange algorithm, or HMAC-SHA1 integrity validation technology into the TCP protocol is an effective security strategy for resisting TCP session hijacking [65]. Jiang et al. conducted a vulnerability analysis on the SMAKA multi-party identity authentication and key agreement protocol [66], and provided a solution to address the session hijacking vulnerability [67].

d: FOR TIMING ATTACK

[68] proposed an efficient Trust Management System (TMS), which combines timestamp mechanisms and blockchain technology to ensure stable interconnection between vehicles. It also constructed a novel hybrid trust model to calculate trust value between vehicle entities using a credible evaluation method, clustering technique, and threading mechanism. Experimental results show that the trust model has a 92% accuracy in identifying malicious nodes.

e: FOR OTHER IDENTITY ATTACKS

Identity-based attacks mainly use authentication methods to ensure that only authorized users can access the data. Reference [69] proposed a large-scale user password security authentication algorithm under CC technology. It adopts a public key encryption mechanism and combines an attribute-based threshold authentication method with threshold password sharing technology, which effectively reduces the false-negative rate. Furthermore, EC is also widely studied to assist in identification. Yang et al. proposed a decentralized authentication architecture with edge assistance for vehicular networks [70]. The architecture hands over authentication capabilities to edge nodes. In addition, blockchain-based methods effectively verify the authenticity and legitimacy of identities [71], [72].

5) THE SOLUTIONS TO MALICIOUS ATTACKS

a: FOR BOTNET ATTACK

Botnets can be used to carry out a wide range of attack behaviors, including DDoS, spamming, malware injection, and data theft attacks. To avoid vehicle botnet attacks, vehicle software must be updated in a timely manner to address vulnerabilities and use reliable antivirus software to protect the security of vehicle electronic systems. Furthermore, the vehicular network should be isolated in design to ensure the integrity and availability of the vehicle system. Biswas et al. proposed a deep learning method based on the Gated Recurrent Unit (GRU) model to identify malicious botnet activities from legitimate traffic [73]. The model introduces a manually adjusted deep learning models to make the computational complexity low and more accurate than the existing models. Moreover, a standard and very famous NSL-KDD dataset are used to identify attacks. But, the performance evaluation was based on accuracy only. Reference [74] proposed an AntibotV framework based on multi-layer behaviors, which constructs a detection system by collecting network traffic data from legitimate and malicious applications. The decision tree algorithm is used to train vehicle-mounted data and effectively monitor vehicle activities in the network.

b: FOR LOCATION SPOOFING ATTACK

Existing Wireless Sensor Network (WSN), Global Position System (GPS), and collaboration-dependent localization methods are all distance-based. Reference [75] investigated the problem of identifying location spoofing attacks in WSNs under non-line-of-sight conditions, which can prevent single-person and multi-person collaborative attacks. Considering that the Global Navigation Satellite System (GNSS) offers positioning and navigation services for AVs, [77] developed a detection strategy based on predicting distance traveled between two consecutive time stamps and implemented real-time attack detection using an LSTM model. The method can detect simple spoofing attacks, but a complex spoofing attack, such as a turn-by-turn attack or a wrong-turn attack, cannot be detected. Kim et al. proposed

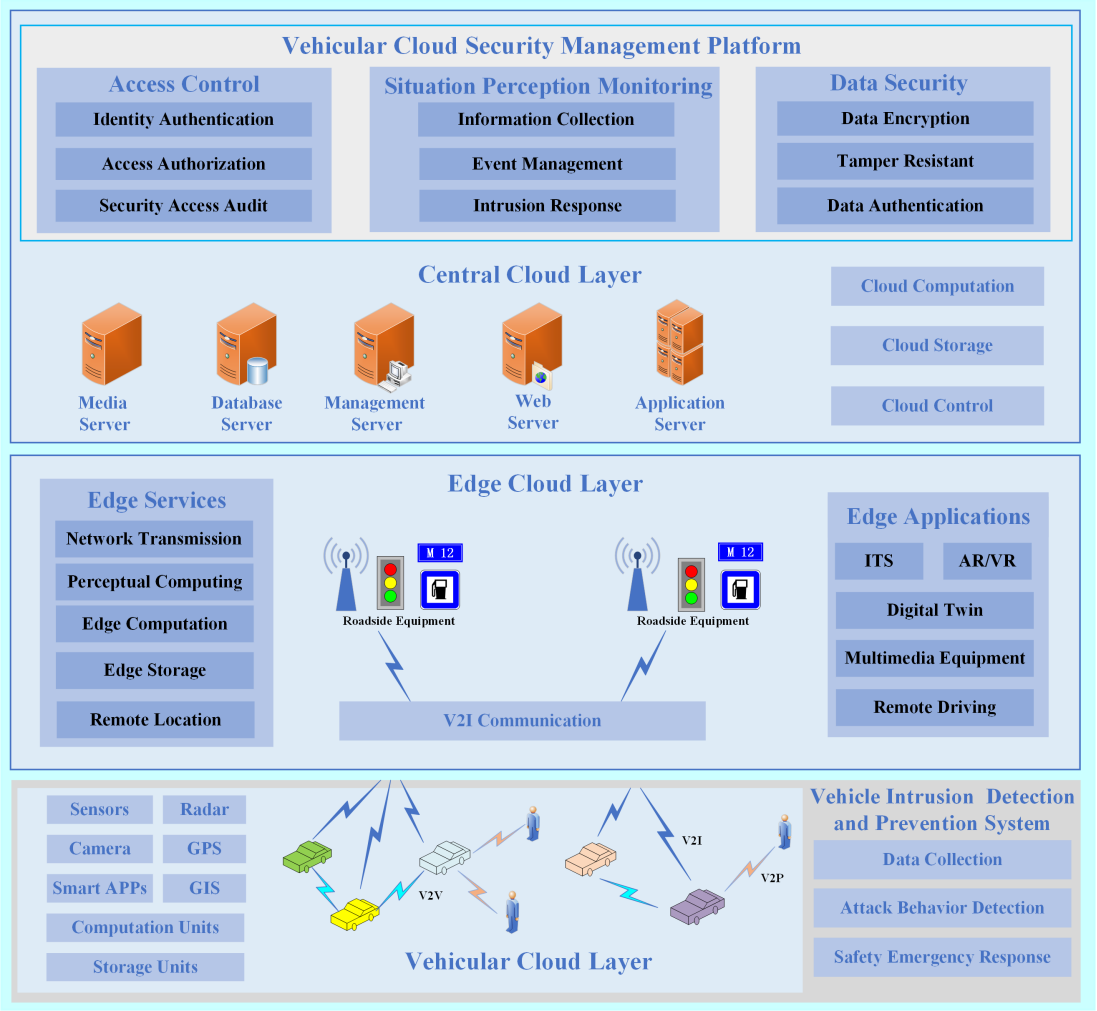

FIGURE 7. The architecture of vehicular cloud network.

a data-driven approach to reliably detect network attacks generated by location spoofing [76].

c: FOR OTHER MALICIOUS ATTACKS

The simplest way is to introduce intrusion detection technology, which is the quickest approach to reducing malicious attacks. Deng et al. proposed a secure and high-integrity YARN framework (SHIYF), which compares the MD5 hashes of the intermediate and final results and achieves a malicious node detection ratio of more than 87% [78]. Reference [79] proposed a vehicular IDS model based on DNN and eXplainable Artificial Intelligence (XAI) technology, and analyzed its advantages from the perspectives of trustworthiness, explainability, and general dependability. Rehman et al. put forward CANintelliIDS, a local area network-based vehicle intrusion detection method based on Convolutional Neural Networks (CNN) and attention-based GRU controllers [80]. The detection model, consisting of three GRU layers and two CNN layers, has significant advantages in detecting single and mixed intrusion attacks on the CAN bus. Furthermore, solutions based on digital signatures and reputation can also ensure that information is only received from trusted sources.

C. SUMMARIZE

We summarize the attacks and their corresponding solutions, as shown in Table 4. According to the characteristics of attack types and defense means, security solutions are classified into two categories.The first is a security defense measure based on authentication and access control, which is an attack solution for vehicle systems. The measures mainly include building an efficient and reliable authentication mechanism for in-vehicle systems and introducing multi-factor authentication technology. Then it adopts technologies such as permission control and data encryption to guarantee access control, authentication, and data security for in-vehicle systems. The second category is security protection measures based on traffic detection and anomaly detection, which is for network detection. The measures need to monitor real-time network traffic, detect abnormal attacks, and make proper solutions to ensure the security of VCN.

V. THE ARCHITECTURE OF VEHICULAR CLOUD NETWORK

In the previous sections, the paper summarized the security requirements, attacks, and corresponding solutions of VCN in detail. These solutions are effective, but VCN still needs a clearer architecture to uniformly monitor and manage security. Therefore, this paper proposes a three-layer VCN security architecture, as shown in Figure 7, which is extended on the basis of existing vehicle cloud security architecture [7], [83]. The architecture is implemented based on the mutual communication and collaborative work of Vehicular Cloud, Edge Cloud, and Centeral Cloud. Their main communication processes are as follows: Vehicles communicate with each other in Vehicular Cloud layer using VANETs technology to exchange real-time road information and vehicle status. Vehicular Cloud layer may process some data locally. Subsequently, the data is sent to the Edge Cloud. Edge Cloud layer mainly acts as coordination and local decision-making. It receives data from Vehicular Cloud layer, coordinates task distribution and data forwarding, and performs some local decisions, for example, real-time road condition assessment and collaborative decision-making. Edge Cloud layer is responsible for interacting with Vehicular Cloud and transmitting data to Centeral Cloud layer when needed. Centeral Cloud layer is at the core of the entire framework. It receives data from Vehicular Cloud and Edge Cloud, and then makes global decisions. The whole communication process is a multi-level collaborative system, which enables the three-layer clouds to effectively complete the task together. Below, we further introduce the three-layer VCN security architecture.

Vehicular Cloud, as the underlying core of the VCN security architecture, is a cloud made up of multiple ICVs. It consists of hardware and software in vehicles, which mainly integrate various internal resources (computation and storage). However, the mobility of vehicles and the topological connectivity between components still pose potential threats to Vehicular Cloud. For example, an attacker can tamper with the navigation instructions in the GPS component, causing the vehicle to travel on the wrong route. To ensure security, a Vehicle Intrusion Detection and Prevention System is introduced into the Vehicular Cloud. Its flow chart is shown in Figure 8. The system first collects and detects potential attacks on the interior network of vehicles and improper behavior on the external network. Secondly, the monitoring results of vehicle status are transmitted to the intrusion detection module. When the abnormality is detected, the intrusion event is reported to the event management module and the intrusion response module in the cloud. Thirdly, the event management module processes the event accordingly and sends the updated defense strategy to the intrusion prevention module. Finally, the intrusion prevention module executes policies to resist the malicious behavior of the attacker.

Edge Cloud plays a key role in data collection and processing in the VCN security architecture and consists of a variety of RSUs. These road facilities receive vehicle

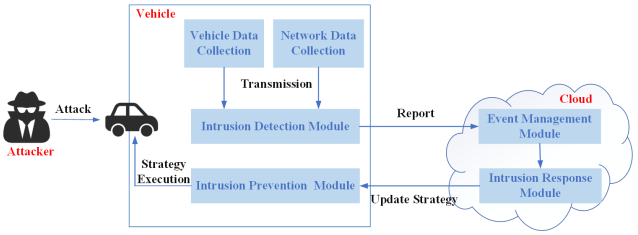

FIGURE 8. The flow chart of vehicle intrusion detection and prevention system.

information through V2I and realize data communication between Vehicular Cloud and Edge Cloud. Therefore, Edge Cloud is used as an intermediate service layer in VCN security architecture, which not only reduces the computational burden on the vehicle,but also reduces the latency of services.

Central Cloud is the traditional cloud in the Internet architecture. It has more resources to achieve rich data storage and computation compared with Edge Cloud. Because of its wide range of communications and high bandwidth requirements, Central Cloud can effectively deploy all-network computing resources to perform complex tasks. And it can get a global view by receiving data from vehicles and enabling centralized network management. As a result, in order to more effectively manage security services in VCN and dynamically coordinate network resources, this paper introduces a Vehicular Cloud Security Management Platform in the VCN security architecture. The platform includes three basic security modules: Access Control, Security Monitoring, and Data Security.

1) ACCESS CONTROL

The module is a core of the Vehicular Cloud Security Management Platform, and its main function is to prevent unauthorized users from attacking VCN. It consists of Identity Authentication, Access Authorization and Security Access Audit. Authentication is used to check the identity of users, ensuring that only authorized users have access to the cloud platform. After the user is authenticated, the access authorization module determines which resources the user can access and which actions to perform based on predefined permission rules. This authorization mechanism prevents unauthorized users from obtaining or modifying sensitive information. Then, the security access audit module tracks and records the user's access and generates a security audit diary. These logs can be used for later breach detection to help identify and resolve potential security issues.

2) SITUATION PERCEPTION MONITORING

The module is responsible for integrating the monitoring information of security equipment, uniformly displaying the state of these information, and timely presenting the network situation. This module contains three sub-modules: Information Collection, Event Management, and Intrusion Response. Information Collection module collects the basic information data of all devices on the network and carries

out identification, classification, and in-depth processing. When a problem is found during the data processing, Event Management receives error information reports and conducts malicious behavior analysis and defense strategy development. Intrusion Response module will also issue real-time early warnings.

3) DATA SECURITY

In order to protect data confidentiality, it needs to be encrypted before transmission, which can keep sensitive information from being stolen by hackers. At the same time, the use of anti-tamper can also effectively prevent data from being destroyed by malicious attackers during transmission. When a message reaches the recipient, authentication is necessary to ensure the source and integrity of the message and avoid security risks such as MITM attack. Therefore, we divide the module into three parts: Data Encryption, Tamper Resistant, and Data Authentication to protect the security of data in VCN.

VI. OPEN ISSUES

The preceding sections summarize potential threats and security solutions in VCN as well as put forward a VCN security architecture. However, the deployment of VCN is still subject to some constraints and needs further exploration. The following briefly discusses the open issues and future development directions regarding VCN.

A. HIGH MOBILITY AND RELIABILITY OF VEHICLES

With the popularity of ICVs, vehicles frequently enter and exit various network environments, including community, public, and company networks. The boundaries of these network environments are fuzzy and constantly changing. In this case, when a vehicle is identified as malicious or suspicious, it is difficult to effectively defend against it in a short period of time. In addition, vehicles from different manufacturers have different types of on-board equipment. There are also differences in topological connectivity and communication quality between these devices, which leads to the unreliability of vehicles. Moreover, the addition of unreliable vehicles to the VCN complicates network management. However, there is still a shortage of vehicle safety management. As a result, future researchers need to investigate dynamic security strategies to adapt to the rapidly changing network environment while requiring a comprehensive analysis and monitoring of on-board equipment to design a powerful vehicle trust model.

B. COMMUNICATION

The continuous development of communication technology plays an important role in the efficiency and security of VCN. First, the construction of roads and infrastructure will have an impact on the performance of the communication system. For example, smart roads can calculate the shortest routes, and sending data over multiple lines helps reduce the communication gap between vehicles. However, obstacles can hinder communication and reduce communication performance. Therefore, we need to fully consider these factors to ensure the security and stability of the network before designing and deploying the VCN. Secondly, with the research and application of the new generation of communication technology, 6G technology is expected to be applied to various intelligent vehicle application scenarios due to its strong bandwidth and low delay communication indicators [84]. However, when 6G technology is applied to vehicle scenarios, it will involve the transmission and processing of more data and information, which will bring greater challenges to the network. Therefore, it is necessary to establish a more perfect security guarantee system and strengthen network security supervision and management. In addition, bidirectional communication authentication and physical isolation of the transport bus can be introduced into the encryption authentication mechanism to ensure communication security.

C. VEHICLE ADAPTIVE SAFETY PROTECTION MECHANISM

Traditional passive safety protection systems, such as seat belts, are no longer able to meet the needs of modern vehicle safety. With the development of VANETs, vehicle adaptive safety protection mechanism is becoming an important tool for addressing security challenges. Therefore, we can consider introducing this mechanism in the area of VCN security to improve the overall safety performance of vehicles on the road, reduce the risk of traffic accidents, and provide more comprehensive support and warning to drivers. In particular, special attention will be paid to the application of technologies such as computer vision, artificial intelligence, and machine learning to vehicle adaptive safety protection mechanisms in future studies.

D. PRIVACY PROTECTION

The provision of personalized privacy protection is an essential requirement in VCN. The existing research typically provides the same privacy protection but does not take into account the different needs for privacy protection of different users, locations, data, and times. For example, when users are at the point of interest, they expect better privacy protection. Conversely, users often require less protection when located in inconsequential areas. Therefore, providing personalized privacy protection by comprehensively considering factors such as user location, data type, time period, and user group can make privacy protection more humane, efficient, and practical.

E. INTEGRATION OF EMERGING TECHNOLOGIES

The integration of emerging technologies into the VCN is crucial to improving data security. For example, traditional encryption algorithms may be effective against known attack vectors, but they demonstrate a decreasing resilience to new, sophisticated threats and attacks. Therefore, it is worth considering adopting more powerful encryption methods,

such as those based on quantum computing or the post-quantum era. These algorithms, using quantum interference and quantum non-clonability, among other unique physical properties, ensure that data is automatically destroyed upon decryption, greatly enhancing data security. Additionally, blockchain technology, serving as a highly secure decentralized distributed database, was applied to the VCN to effectively avoid the risks of single-point failures and data tampering. Furthermore, its combination with smart contract technology enables automated and programmable network security management, providing VCN with greater flexibility to cope with diverse security challenges. Therefore, future research should explore the potential of these emerging technologies in VCN, which will help drive continuous development and innovation in VCN and provide stronger support for data security.

VII. CONCLUSION

VCN is the combination of VANETs, CC, and EC, which provides computing power according to the needs of vehicle users to achieve efficient network services. This paper summarizes the security requirements, problems, and solutions of VCN from five aspects: routing, data, DoS, identity, and malicious attacks. Furthermore, a VCN security architecture is presented, which combines Vehicle Intrusion Detection and Prevention System with Vehicular Cloud Security Management Platform. Finally, the paper lists several unresolved problems in VCN.

In future work, we will first validate the communication validity of our proposed VCN architecture. We plan to use NS-3 or OMNet++ to simulate vehicle communication at the physical, data link, and network layers. And using SUMO to mimic the road network and VeinsLTE to simulate real-world interference when constructing the Edge Cloud layer. Once the architecture has been successfully constructed, we will verify the security of the session layer by simulating the communication of a large number of vehicles. Secondly, we will provide performance analysis for the Vehicular Cloud Security Management Platform regarding proof of concept implementation or simulation. The system design and development for the platform at the Central Cloud layer are carried out using the microservices architecture and Java programming language. It is crucial to note that our research process will strictly adhere to security principles to safeguard the overall security of the system.

REFERENCES

[1] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *J. Netw. Comput. Appl.*, vol. 37, pp. 380–392, Jan. 2014.

[2] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *J. Netw. Comput. Appl.*, vol. 40, pp. 325–344, Apr. 2014.

[3] D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, "A survey on secure data analytics in edge computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4946–4967, Jun. 2019.

[4] A. Masood, D. S. Lakew, and S. Cho, "Security and privacy challenges in connected vehicular cloud computing," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2725–2764, 4th Quart., 2020.

[5] L. Liu, C. Chen, Q. Pei, S. Maharjan, and Y. Zhang, "Vehicular edge computing and networking: A survey," *Mobile Netw. Appl.*, vol. 26, no. 3, pp. 1145–1168, Jun. 2021.

[6] N. Phull and P. Singh, "A review on security issues in VANETs," in *Proc. 6th Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, Mar. 2019, pp. 1084–1088.

[7] S. Zouaidi, A. Belghith, and I. Lengliz, "SVCF: Secure vehicular cloud framework," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, 2020, pp. 412–419.

[8] S. Olariu, T. Hristov, and G. Yan, "The next paradigm shift: From vehicular networks to vehicular clouds," in *Mobile Ad Hoc Networking: Cutting Edge Directions*, 2013, pp. 645–700.

[9] S. Olariu, M. Eltoweissy, and M. Younis, "Towards autonomous vehicular clouds," *ICST Trans. Mobile Commun. Appl.*, vol. 11, no. 7, p. e2, Sep. 2011.

[10] R. Hussain, J. Son, H. Eun, S. Kim, and H. Oh, "Rethinking vehicular communications: Merging VANET with cloud computing," in *Proc. 4th IEEE Int. Conf. Cloud Comput. Technol. Sci. Proc.*, Dec. 2012, pp. 606–609.

[11] R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang, "Toward cloud-based vehicular networks with efficient resource management," *IEEE Netw.*, vol. 27, no. 5, pp. 48–55, Sep. 2013.

[12] F. Ahmad, M. Kazim, A. Adnane, and A. Awad, "Vehicular cloud networks: Architecture, applications and security issues," in *Proc. IEEE/ACM 8th Int. Conf. Utility Cloud Comput. (UCC)*, Dec. 2015, pp. 571–576.

[13] M. R. Jabbarpour, A. Marefat, A. Jalooli, and H. Zarrabi, "Could-based vehicular networks: A taxonomy, survey, and conceptual hybrid architecture," *Wireless Netw.*, vol. 25, no. 1, pp. 335–354, Jan. 2019.

[14] T. Mekki, I. Jabri, A. Rachedi, and M. B. Jemaa, "Vehicular cloud networks: Challenges, architectures, and future directions," *Veh. Commun.*, vol. 9, pp. 268–280, Jul. 2017.

[15] R. Lu, L. Zhang, J. Ni, and Y. Fang, "5G vehicle-to-everything services: Gearing up for security and privacy," *Proc. IEEE*, vol. 108, no. 2, pp. 373–389, Feb. 2020.

[16] V. Hoa La and A. Cavalli, "Security attacks and solutions in vehicular ad hoc networks: A survey," *Int. J. AdHoc Netw. Syst.*, vol. 4, no. 2, pp. 1–20, Apr. 2014.

[17] P. Kohli, S. Sharma, and P. Matta, "Security of cloud-based vehicular ad-hoc communication networks, challenges and solutions," in *Proc. 6th Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Mar. 2021, pp. 283–287.

[18] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.

[19] T. Yeferny and S. Hamad, "Vehicular ad-hoc networks: Architecture, applications and challenges," *Int. J. Comput. Sci. Netw. Secur.*, vol. 20, no. 2, pop. 1–7, 2020.

[20] A. Boukerche and R. E. De Grande, "Vehicular cloud computing: Architectures, applications, and mobility," *Comput. Netw.*, vol. 135, pp. 171–189, Apr. 2018.

[21] B. Hassan and S. Askar, "Survey on edge computing security," *Int. J. Sci. Bus.*, vol. 5, no. 3, pp. 52–60, 2021.

[22] R. Shringar Raw, M. Kumar, and N. Singh, "Security challenges, issues and their solutions for VANET," *Int. J. Netw. Secur. Appl.*, vol. 5, no. 5, pp. 95–105, Sep. 2013.

[23] J. Mahmood, Z. Duan, Y. Yang, Q. Wang, J. Nebhen, and M. N. M. Bhutta, "Security in vehicular ad hoc networks: Challenges and countermeasures," *Secur. Commun. Netw.*, vol. 2021, pp. 1–20, Jun. 2021.

[24] A. M. Alrehan and F. A. Alhaidari, "Machine learning techniques to detect DDoS attacks on VANET system: A survey," in *Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, May 2019, pp. 1–6.

[25] M. Masdari and M. Jalali, "A survey and taxonomy of DoS attacks in cloud computing," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3724–3751, Nov. 2016.

[26] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 767–809, 2nd Quart., 2022.

[27] R. Doshi and V. Kute, "A review paper on security concerns in cloud computing and proposed security models," in *Proc. Int. Conf. Emerg. Trends Inf. Technol. Eng.*, Feb. 2020, pp. 1–4.

[28] M. M. Hamdi, M. Dhafer, A. S. Mustafa, S. A. Rashid, A. J. Ahmed, and A. M. Shantaf, "Effect Sybil attack on security authentication service in VANET," in *Proc. Int. Congr. Hum.-Comput. Interact., Optim. Robot. Appl. (HORA)*, Jun. 2022, pp. 1–6.

[29] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017.
[30] P. R. Krishnan and P. A. R. Kumar, "Detection and mitigation of smart blackhole and gray hole attacks in VANET using dynamic time warping," *Wireless Pers. Commun.*, vol. 124, no. 1, pp. 931–966, May 2022.
[31] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan, and A. Aldegheishem, "Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles," *IEEE Access*, vol. 8, pp. 199618–199628, 2020.
[32] S. Kudva, S. Badsha, S. Sengupta, H. La, I. Khalil, and M. Atiquzzaman, "A scalable blockchain based trust management in VANET routing protocol," *J. Parallel Distrib. Comput.*, vol. 152, pp. 144–156, Jun. 2021.
[33] A. Kumar, V. Varadarajan, A. Kumar, P. Dadheech, S. S. Choudhary, V. D. A. Kumar, B. K. Panigrahi, and K. C. Veluvolu, "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm," *Microprocessors Microsyst.*, vol. 80, Feb. 2021, Art. no. 103352.
[34] R. K. Dhanaraj, S. H. Islam, and V. Rajasekar, "A cryptographic paradigm to detect and mitigate blackhole attack in VANET environments," *Wireless Netw.*, vol. 28, no. 7, pp. 3127–3142, Oct. 2022.
[35] T. D. Ovasapyan, D. A. Moskvin, and M. O. Kalinin, "Using neural networks to detect internal intruders in VANETs," *Autom. Control Comput. Sci.*, vol. 52, no. 8, pp. 954–958, Dec. 2018.
[36] E. V. Malyshev, D. A. Moskvin, and D. P. Zegzhda, "Application of an artificial neural network for detection of attacks in VANETs," *Autom. Control Comput. Sci.*, vol. 53, no. 8, pp. 889–894, Dec. 2019.
[37] G. Xie, L. T. Yang, Y. Yang, H. Luo, R. Li, and M. Alazab, "Threat analysis for automotive CAN networks: A GAN model-based intrusion detection technique," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4467–4477, Jul. 2021.
[38] L. Liao, J. Zhao, H. Hu, and X. Sun, "Secure and efficient message authentication scheme for 6G-enabled VANETs," *Electronics*, vol. 11, no. 15, p. 2385, Jul. 2022.
[39] X. Duan, H. Yan, D. Tian, J. Zhou, J. Su, and W. Hao, "In-vehicle CAN bus tampering attacks detection for connected and autonomous vehicles using an improved isolation forest method," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2122–2134, Feb. 2023.
[40] A. Tongle, W. Chundong, and C. Yang, "Research on vehicle bus anomaly detection based on LSTM," *J. Tianjin Univ. Technol.*, vol. 36, no. 3, p. 5, 2020.
[41] Y. Luo, Y. Wei, D. Ding, and J. Xie, "An in-vehicle network security protocol based on dynamic encryption," in *Proc. 7th Int. Conf. Inf. Sci. Control Eng. (ICISCE)*, Dec. 2020, pp. 286–290.
[42] A. S. Khan, K. Balan, Y. Javed, S. Tarmizi, and J. Abdullah, "Secure trust-based blockchain architecture to prevent attacks in VANET," *Sensors*, vol. 19, no. 22, p. 4954, Nov. 2019.
[43] R. Deeksha. and K. Paramasivam., "Design and validation of CAN protocol with double encryption for electric vehicle applications," in *Proc. Int. Conf. Advancement Electr., Electron., Commun., Comput. Autom. (ICAECA)*, Oct. 2021, pp. 1–6.
[44] H. Vasudev, V. Deshpande, D. Das, and S. K. Das, "A lightweight mutual authentication protocol for V2V communication in Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6709–6717, Jun. 2020.
[45] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, Apr. 2016.
[46] M. Pouryazdan, B. Kantarci, T. Soyata, and H. Song, "Anchor-assisted and vote-based trustworthiness assurance in smart city crowdsensing," *IEEE Access*, vol. 4, pp. 529–541, 2016.
[47] H. J. Jo, J. H. Kim, H.-Y. Choi, W. Choi, D. H. Lee, and I. Lee, "MAuth-CAN: Masquerade-attack-proof authentication for in-vehicle networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 2204–2218, Feb. 2020.
[48] L. Gao, Y. Li, L. Zhang, F. Lin, and M. Ma, "Research on detection and defense mechanisms of DoS attacks based on BP neural network and game theory," *IEEE Access*, vol. 7, pp. 43018–43030, 2019.
[49] J. Xiao, W. J. Li, H. Y. Geng, and Y. B. Zhai, "An anti-DoS attack RFID security authentication protocol in the Internet of Vehicles," *J. Beijing Univ. Posts Telecommun.*, vol. 42, no. 2, pp. 114–119, 2019.
[50] R. Kolandaisamy, R. M. Noor, M. R. Z'Aba, I. Ahmedy, and I. Kolandaisamy, "Adapted stream region for packet marking based on DDoS attack detection in vehicular ad hoc networks," *J. Supercomput.*, vol. 76, no. 8, pp. 5948–5970, Aug. 2020.
[51] R. Engoulou, "Securisation des VANETs par la methode de reputation des noeuds," Ecole Polytechn., Montreal, QC, Canada, 2013.
[52] A. M. Malla and R. K. Sahu, "Security attacks with an effective solution for DoS attacks in VANET," *Int. J. Comput. Appl.*, vol. 66, no. 22, pp. 1–6, 2013.
[53] J. Liu, X. Wang, S. Shen, Z. Fang, S. Yu, G. Yue, and M. Li, "Intelligent jamming defense using DNN Stackelberg game in sensor edge cloud," *IEEE Internet Things J.*, vol. 9, no. 6, pp. 4356–4370, Mar. 2022.
[54] A. Pourranjbar, G. Kaddoum, and W. Saad, "Recurrent-neural-network-based anti-jamming framework for defense against multiple jamming policies," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8799–8811, May 2023.
[55] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A reliable trust-based platoon service recommendation scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1786–1797, Feb. 2017.
[56] J. Grover, M. S. Gaur, V. Laxmi, and N. K. Prajapati, "A Sybil attack detection approach using neighboring vehicles in VANET," in *Proc. 4th Int. Conf. Secur. Inf. Netw.*, Nov. 2011, pp. 1–12.
[57] J. Liang, J. Chen, Y. Zhu, and R. Yu, "A novel intrusion detection system for vehicular ad hoc networks (VANETs) based on differences of traffic flow and position," *Appl. Soft Comput.*, vol. 75, pp. 712–727, Feb. 2019.
[58] Y. Yao, B. Xiao, G. Yang, Y. Hu, L. Wang, and X. Zhou, "Power control identification: A novel Sybil attack detection scheme in VANETs using RSSI," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 11, pp. 2588–2602, Nov. 2019.
[59] Y. Yao, B. Xiao, G. Wu, X. Liu, Z. Yu, K. Zhang, and X. Zhou, "Multi-channel based Sybil attack detection in vehicular ad hoc networks using RSSI," *IEEE Trans. Mobile Comput.*, vol. 18, no. 2, pp. 362–375, Feb. 2019.
[60] K. Lim, T. Islam, H. Kim, and J. Joung, "A Sybil attack detection scheme based on ADAS sensors for vehicular networks," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2020, pp. 1–20.
[61] M. Baza, M. Nabil, M. M. E. A. Mahmoud, N. Bewermeier, K. Fidan, W. Alasmary, and M. Abdallah, "Detecting Sybil attacks using proofs of work and location in VANETs," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 1, pp. 39–53, Jan. 2022.
[62] R. P. Krishnan and A. R. P. Kumar, "A collaborative strategy for detection and eviction of Sybil attacker and Sybil nodes in VANET," *Int. J. Commun. Syst.*, vol. 34, no. 3, pp. 1–10, Feb. 2021.
[63] P. Kumar and H. Om, "An anonymous and authenticated V2I communication with a simplified user revocation and re-registration strategy," *J. Supercomput.*, vol. 79, no. 7, pp. 8070–8096, May 2023.
[64] C. Peng, W. Fan, D. L. Zhu, and F. Yang, "Research on man-in-the-middle attack detection in LTE access network based on weighted Bayesian classifier," *Inf. Netw. Secur.*, vol. 23, no. 2, pp. 1–10, 2023.
[65] M. Chen, F. Dai, B. Yan, and J. Cheng, "Encryption algorithm for TCP session hijacking," in *Proc. Int. Conf. Artif. Intell. Secur.* Cham, Switzerland: Springer, 2020, pp. 191–202.
[66] J. Zhang, H. Zhong, J. Cui, Y. Xu, and L. Liu, "SMAKA: Secure many-to-many authentication and key agreement scheme for vehicular networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1810–1824, 2021.
[67] J. Jiang, W. Susilo, and J. Baek, "Security analysis of 'SMAKA: Secure many-to-many authentication and key agreement scheme for vehicular networks,"' *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 3006-3007, 2022.
[68] H. El-Sayed, H. Alexander, P. Kulkarni, M. A. Khan, R. M. Noor, and Z. Trabelsi, "A novel multifaceted trust management framework for vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 11, pp. 20084–20097, Nov. 2022.
[69] D. Yixing, C. Yi, and W. W. Han, "Large-scale user password security authentication algorithm under cloud computing technology," *Comput. Simul.*, vol. 39, no. 2, pp. 141–144, 2022.
[70] A. Yang, J. Weng, K. Yang, C. Huang, and X. Shen, "Delegating authentication to edge: A decentralized authentication architecture for vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 1284–1298, Feb. 2022.
[71] A. Vangala, B. Bera, S. Saha, A. K. Das, N. Kumar, and Y. Park, "Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems," *IEEE Sensors J.*, vol. 21, no. 14, pp. 15824–15838, Jul. 2021.

[72] Y. Tan, J. Wang, J. Liu, and N. Kato, "Blockchain-assisted distributed and lightweight authentication service for industrial unmanned aerial vehicles," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16928–16940, Sep. 2022.

[73] R. Biswas and S. Roy, "Botnet traffic identification using neural networks," *Multimedia Tools Appl.*, vol. 80, pp. 24147–24171, Apr. 2021.

[74] R. Rahal, A. Amara Korba, N. Ghoualmi-Zine, Y. Challal, and M. Y. Ghamri-Doudane, "AntibotV: A multilevel behaviour-based framework for botnets detection in vehicular networks," *J. Netw. Syst. Manage.*, vol. 30, no. 1, pp. 1–40, Jan. 2022.

[75] D. Liu, Y. Xu, and X. Huang, "Identification of location spoofing in wireless sensor networks in non-line-of-sight conditions," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2375–2384, Jun. 2018.

[76] C. Kim, S.-Y. Chang, D. Lee, J. Kim, K. Park, and J. Kim, "Reliable detection of location spoofing and variation attacks," *IEEE Access*, vol. 11, pp. 10813–10825, 2023.

[77] S. Dasgupta, M. Rahman, M. Islam, and M. Chowdhury, "Prediction-based GNSS spoofing attack detection for autonomous vehicles," 2020, *arXiv:2010.11722*.

[78] J. Y. Deng, "Research on YARN security and its application in vehicular ad hoc networks," Jilin Univ., 2019, doi: 10.27162/d.cnki.gjlin.2019.000155.

[79] H. Lundberg, N. I. Mowla, S. F. Abedin, K. Thar, A. Mahmood, M. Gidlund, and S. Raza, "Experimental analysis of trustworthy in-vehicle intrusion detection system using eXplainable artificial intelligence (XAI)," *IEEE Access*, vol. 10, pp. 102831–102841, 2022.

[80] A. R. Javed, S. U. Rehman, M. U. Khan, and M. Alazab, "CANintelliIDS: Detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1456–1466, Apr. 2021.

[81] S. Lachdhaf, M. Mazouzi, and M. Abid, "Detection and prevention of black hole attack in VANET using secured AODV routing protocol," in *Proc. Comput. Sci. Inf. Technol.*, Nov. 2017.

[82] Q. Hu and Y. Liu, "Secure communication method for in-vehicle network based on CAN-FD bus," *J. Tongji Univ., Natural Sci.*, vol. 47, no. 3, pp. 386–391, 2019.

[83] Y. N. Wu, "Design of cloud security management platform based on cloud computing technology," *Inf. Secur. Commun. Privacy*, vol. 2020, no. S1, pp. 93–97, 2020.

[84] S. Bao, L. X. Li, and H. P. Peng, "An investigation of information security for intelligent vehicle networking," *Inf. Secur. Commun. Privacy*, vol. 2023, no. 3, pp. 10–20, 2023.

JUNYI DENG (Member, IEEE) received the B.E., M.S., and Ph.D. degrees from the College of Computer Science and Technology, Jilin University. He is currently an Assistant Research Fellow with the Guangxi University of Science and Technology, and the Internet of Vehicles Expert with the Guangxi Automotive Group. His research interests include intelligent connected vehicles, cloud-edge collaboration security, and perceptual decision.

JIKAI DENG received the B.E. degree in computer science and technology from Shenyang Shenyang Ligong University, in 2019. She is currently pursuing the master's degree with the Guangxi University of Science and Technology, China. Her research interests include vehicular cloud, edge computing, and intelligent connected vehicles.

PEIHAO LIU received the B.E. degree in computer science and technology from the Huali College, Guangdong University of Technology, China, in 2022. He is currently pursuing the master's degree with the Guangxi University of Science and Technology. His research interests include cloud computing, blockchain, and the Internet of Vehicles.

HUAN WANG (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in computer science and technology from the Changchun University of Science and Technology, Changchun, China. He has been an Associate Researcher with the School of Computer Science and Communications Engineering, Guangxi University of Science and Technology, Liuzhou, China. He is the author of 14 articles. His research interests include network and information security, highreliability software, and the IoT.

JUNJIE YAN received the M.S. and Ph.D. degrees from the Chongqing University of Posts and Telecommunications, Chongqing, China, in 2016 and 2020, respectively. He is currently a Lecturer with the Guangxi University of Science and Technology, Liuzhou, China. His research interests include D2D communication, MEC, and UAV communication.

DERU PAN is currently pursuing the bachelor's degree in software engineering with the Guangxi University of Science and Technology, China. He is a member with the Intelligent Communication and Vehicular Networks Laboratory (ICVN). His research interests include VANET, edge computing, and computation offloading.

JIAHUA LIU received the B.E. degree in computer science and technology from the Tongda College of Nanjing University of Posts and Telecommunications, China, in 2022. He is currently pursuing the master's degree with the Guangxi University of Science and Technology. His research interests include the Internet of Vehicles and routing policy.