VANET Vulnerabilities Classification and Countermeasures: A Review

Vamshi Krishna K[1*], Ganesh Reddy K[2]
1 - VIT-AP University , Amaravati, AP, India.
Email: vamshikrishna.20phd7088@vitap.ac.in (Corresponding author)
2 - VIT- AP University, Amaravati, AP, India.
Email: ganesh.reddy@vitap.ac.in

Received: April 2022 Revised: June 2022 Accepted: July 2022

ABSTRACT:
Information is the driving force in vehicular ad hoc networks (VANET) since vehicles share information (emergency, general, and multimedia). VANET communicates between vehicles using a unique routing protocol, unlike other wireless routing technologies. Many protocols, techniques, and approaches have been developed to secure and protect data. To enhance current security and privacy measures and develop and model new ones, the ideas of machine learning (ML), deep learning (DL), and artificial intelligence are being applied. In this paper, we provide information on the various types of attacks that target VANET communication, VANET layers, the security goals that are affected, and real-time attacks that occur on manufacturing hubs. We compared various VANET attack prevention, detection, and AI techniques proposed, as well as future research work in the field of VANET, for improving accuracy, security, and privacy.

KEYWORDS: V2V, V2I, RSU, AU, OBU, VANET, MANET, Attacks, Layers.

1. INTRODUCTION

Mobile communication technologies have revolutionized the automotive industry over the last decade by allowing communication across diverse systems and from any location. Important data can be transferred among devices while travelling because of this connection's ease of use. A new industry paradigm has arisen around the continuous availability of data. As a result, information technology and communication improvements have made it simple to support the concept of mobile device communication [1]. Among these improvements, the Vehicular Ad-hoc Networks (VANET) concept gained recognition, providing new channels for deploying security features. Different transport automobiles and other linked equipment interact to establish an ad hoc network known as a Vehicular Ad-hoc Network, where they exchange crucial information wirelessly. A tiny web system is created simultaneously, with automobiles and other objects serving as network elements. The nodes share any knowledge they may have with the other nodes. All other nodes receive parallel to how data is distributed by one node. Nodes try to extract valuable knowledge from this data and send it to other devices [2–3]. It is an open platform since nodes are free to enter and exit the network, and connectivity among devices grows.

The market is seeing motor products installing onboard sensors, making it simple for the automobile to connect and integrate into the system and use VANET's advantages. A subtype of Mobile Ad-hoc Network (MANET) is a Vehicular Ad-hoc Network (VANET). The majority of the VANET is made up of cars that connect wirelessly and have network communication. Vehicular Ad-hoc Network, on either side, has developed into a more complex and dependable class or variant of Mobile Ad-hoc Network. This inter-vehicle connection allows information to be passed back and forth, improving traffic efficiency, detecting road conditions, reducing crashes, detecting emergencies, and overall network efficiency. With multi-hops, VANET can transmit messages to remote devices [4]. The following features define VANET.

Dynamical architecture: The continual changes in vehicle speed and direction result in a highly dynamic configuration.

Irregular Connection: The link between devices is always changing. An intersection of two objects that are transferring data, for instance, may break. The high dynamic topology causes recurrent connectivity issues.

Patterns of movement: Traffic signals, speed limits, highways, lanes, and road surfaces all have an impact on how many automobiles move in regular patterns. Vehicular Ad-hoc Network routing algorithms can be created with their help whenever these similarities are

Paper type: Review paper
DOI: https:// 10.30486/mjee.2022.696508
How to cite this paper: V. Krishna K, G. Reddy K, **"VANET Vulnerabilities Classification and Countermeasures: A Review"**, Majlesi Journal of Electrical Engineering, Vol. 16, No. 3, pp. 63-83, 2022.

found.

Unlimited memory and power: The power and memory capabilities of the units in the Vehicular Ad-hoc Network are expected to be limitless. So, the nodes can share data without worrying about how much power they use or how much space they waste.

On-board Sensors: Because of the VANET, nodes frequently have sensors that transmit data to other objects or networks.

The Organization of Paper: The residual portions of the essay are structured as follows: In section 2, we show a graphical presentation of the VANET architecture and the security-related issues it faces. Section 3 provides information related to VANET attacks, layer-wise classification of different VANET attacks, and real-time attacks on the automobile industry. Section 4 contains a survey on VANET attack prevention, detection, and AI technology embedded to improve the accuracy of prevention, detection, and AI. Section 5 deals with further research for encountering security-related issues in VANET and Section 6 is the conclusion.

2. ARCHITECTURE OF A VANET

According to IEEE 1471-2000 [12] and ISO/IEC 42010 [13] standards, VANET's entities can be divided into three categories.

The domain of Mobile: There are two sections to the mobile domain. The first is the domain of automobiles, which includes moving vehicles like buses, vehicles, and lorries. The mobile device domain, which includes all mobile devices, including Personal digital assistants, laptops, GPS, cell phones, etc., is the second domain.

Infrastructure Domain: It is also divided into two portions. The road-side infrastructure component involves stationary road-side elements like traffic signals and poles. On the other hand, the main infrastructure domain contains centralised control hubs for transportation and automobile management.

Basic Domain: Both private and public infrastructures are taken into account. The generic domain, for instance, is home to various nodes, servers, and other computing services that actively or passively support a VANET.

Fig.1 depicts the overall network architecture. Giving vital information to the network's cars and routers is the main objective of the VANET design. The architecture consists of the following components: AU, OBU, and RSU, all of which interact with one another [52].

Road Side Unit (RSU): RSUs are roadside-mounted fixed units. These devices incorporate antennas, CPUs, sensors, charging connectors, and storage systems. The RSU communicates via wired or wireless means [53] [52].

On-Board Unit (OBU): It is a device placed inside the vehicles; it exchanges data with neighbouring RSUs and other vehicles via various communication technologies such as LTE, VoLTE, or 4G and 5G networks (OBUs). The OBU consumes as little power as possible, allowing the vehicle's operations to run smoothly. OBU includes sensors, storage, GPS, a processor, read-write memory, an event data recorder (EDR), and a communication interface [53] [52].

Application Unit (AU): The AU application, which serves as the graphical interface between the user and the On-board Unit (OBU), is obtained by one of two possibilities: the producer of the OBU or purchased from a third party. Remote services are provided by communication units attached to an OBU and the Application Unit (AU) of a car [53] [52] [54].

2.1. VANET Communication Methods

VANET communication can take one of three forms: V2V, V2I, or hybrid (V2X). Unlike V2V, where information is exchanged between two or more vehicles, V2I information is exchanged between a vehicle and its surroundings (RSU). V2X communications, as part of the ITS, play a key role in improving the driving experience by offering highly accurate and genuine knowledge to support traffic safety and efficiency. V2X communication allows information to be sent between V2V and V2I [55]. Many recent efforts have been made to build IEEE 802.11p-based V2X communication systems. 802.11p, on the other hand, the use of a carrier sense multiple access with a conflict prevention medium-access system may provide some difficulties in enforcing strict reliability standards and guaranteeing network scalability as demand increases. Release 14 was the first alternate release from the Third Generation Partnership Project (3GPP) [56]. As of June 2017, a collection of technologies developed by the mobile industry's standard-setting body 3GPP for communication between automobiles and road-side infrastructure had been standardised. This technology is known as cellular vehicle-to-everything (C-V2XA) unified connection architecture is being built to handle V2X communications. [55] [57]. C-V2X can be used in various ways to improve road safety, such as platooning, tag-team driving, avoiding crashes, hazard warnings, and warnings [57]. C-V2X employs two complementary transmission modes: Direct and Network, to provide a wide range of driving safety features.

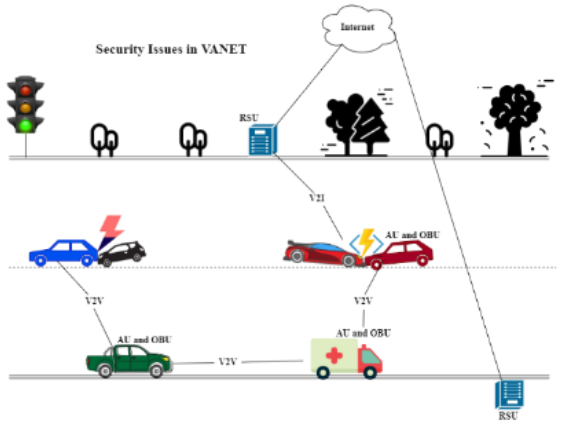

Fig. 1. VANET architecture model displaying communication modes and security concerns.

The most serious concern for VANETs is security. Vehicles communicate with one another via open wireless channels. Intruders can readily alter, interrupt, and erase transmitted data in VANETs due to open wireless communication [5-8] [9]. When an attacker intercepts a traffic-related message, it puts the driver's problems into context. If a hacker alters the data and transmits a wrong signal, it may result in serious traffic problems, including accidents, drivers being sent along the hacker's favoured route, etc. As a result, VANET security has emerged as a hot research topic that has received much attention [10]. End-to-end authentication is required to prevent interruption into VANETs and address security vulnerabilities in VANETs [11]. An intruder is a live node performing malicious operations such as data tampering, data leaking, packet dropping, etc. As a result, specific security procedures should be in place to detect and prevent intruder attacks on normal network behaviour [16]. Sections 4 and 5 will extensively survey existing prevention and detection methods and techniques.

3. VANET ATTACKS

Since the Vehicular Ad-hoc Network has quickly grown, security and privacy concerns must be addressed adequately [52]. The unique characteristics of VANET make it more vulnerable to attacks [58]. The intruder's objective is to obstruct the route from the sender to the receiver [59]. Attackers are divided into the following categories.

Inside the Network vs. Outside the Network: They are the ones who are already authenticated and inside the network, have full access to it, and are well-versed in the network's configuration, making them extremely dangerous to have around.

Outside attackers are not present in the network and launch the attacks from outside the network [52] [60].

Active vs. Passive: An effective attacker modifies the information received by delivering misleading signals, deleting incoming packets, or modifying the data stream. Network data are not injected or altered by a malicious user. To learn more about how data is moved, a passive attacker joins a wireless connection and keeps track of the patterns and rate of data exchanges [52] [60].

Malicious vs. Rational: Malicious attacks provide no personal gain, but rational attackers may be motivated by a desire to make money, which is why they target the network.

3.1. Various Attacks on VANET

3.1.1. Sybil Attack

One of the devastating attacks in VANETs is the Sybil assault [24]. A node (vehicle) may appear to have numerous personalities in a Sybil attack. In other words, the network's other nodes cannot tell if the data originated from a single vehicle or a fleet of vehicles. The attacker aims to shape the networks to satisfy their needs. For instance, an attacker could influence the behaviour of all other automobiles by compelling them to veer off their intended course. In addition to being among the most dangerous types of attack, Sybil assault is also one of the hardest to spot. Because the intruder might give the automobile the appearance of being in numerous places by giving false information about its location, it is particularly riskier on systems that use geographic navigation. Furthermore, it may depict occurrences in locations other than their precise locations.

3.1.2. Denial of Service Attack (DoS)

Denial-of-Service (DoS) effort will be made to declare a system's legitimate operations unavailable. In most cases, the attackers submit significantly more attempts than the system can process. A Vehicular Ad-hoc Network attacker might attempt to disable the system set up by RSUs to stop the vehicle-to-vehicle and RSUs. A DoS assault has major consequences since it prohibits hackers from contacting one another and prevents vehicles from collecting system data such as road conditions. Several nodes could launch attacks simultaneously as part of a Distributed Denial-of-Service (DDoS) attack, making detection more challenging. RSUs, a crucial component of the VANETs architecture, and the network's vehicles could be the target nodes launching a DDoS attack [25].

DoS attacks come in a variety of forms in VANETs. In contrast to many other routing attacks, it follows all routing network protocols. Examples include flooding attacks, jellyfish attacks, and intelligent cheaters. Packets intended to be sent could be interfered with, delayed, or dropped by an attacker. In the end, the network's performance is drastically decreased by end-to-end congestion management protocol flaws. VANETs might easily inherit the jellyfish attack.

The intelligent cheater attack, like the Jellyfish attack, remains undetectable by conforming to routing protocol standards. For the most part, the attacker looks to be acting properly, but in reality, he misbehaves in a scattered manner. Systems of trust might be simply breached by attacks like the intelligent cheater attack and the jellyfish attack. Because of their deception, such attacks are difficult to detect, necessitating end-to-end control methods and long-term monitoring.

Attacks known as flooding create traffic to deplete system resources, including bandwidth, CPU, and power. The two types of flooding attacks are attacks on routing control packets and assaults on data. Each sort of assault has the same effects. Resources on the network are rendered inaccessible to authorised users. In a data flooding assault, an attacker could create useless network packets and broadcast them to every node via their peers. An additional characteristic of a DoS attack is jamming, which involves occupying a network channel by emitting radio frequency signals associated with impairment. The assault could be carried out by an attacker who is not necessarily a network user. The impact and possibility of the assault are regarded quite high, given that anyone with a basic understanding may execute DoS attacks to stop cars from receiving essential traffic information. Furthermore, DoS assaults must be detected as soon as feasible and reaction mechanisms initiated as soon as possible, because once an attack has been successfully carried out, it is very tough for the network to retaliate.

3.1.3. Black hole Attack

The DoS and DDoS attacks focus on bringing the network to a halt; the Blackhole assault, on the other hand, shapes the network. A serious threat to MANETs is a hacker who tricks nearby sites into sending their messages there as frequently as possible. In addition to merely deleting packets, attackers might transfer packets between themselves to form their network [27]. An intruder automobile could exploit routing algorithms in a VANET by pretending to have the best route to the target vehicle/RSU or be in the optimal location to forward messages. Other vehicles will send packets through it since it broadcasts bogus routing information, supposing it is on the correct path.

3.1.4. Wormhole Attack

The attacker must change the network's logical topology to obtain and modify enormous amounts of network traffic. An intruder vehicle delivers a packet that must be forwarded to another vulnerable vehicle to attack VANETs. As a result, identical to the Black hole attack, those two hostile vehicles force routing algorithms to give the connection among them priority over conventional network routes as the optimal path to any location [24]. The vehicles could construct their private network in another variant of this attack.

3.1.5. Bogus Information Attack

In VANETs, vehicles make use of data that is generated or sent by other vehicles or RSUs. The data obtained, though, might not always be correct. An automobile might create false information and autonomously transmit it to the internet. The attacker tries to control other vehicles out of self-interest and malice. It is more effective when there isn't another vehicle available to confirm the data and the attack is hard to spot. [24] l. Furthermore, if there is a fast-moving attacker – sometimes known as a motorway attacker – which broadcasts false information to groups it encounters, the repercussions are more significant.

3.1.6. Tampering Attack

The OBU of a vehicle is likely to be positioned in a region with restricted access. Thus an intruder could try to trick detectors by generating fake circumstances to get predicted results. Because such deception is unlikely to be detected by an intra-vehicle detecting system, this strategy is effective [27]. For instance, a hacker may change safety-related software such that it appears like there is traffic on the road by abruptly braking. Alerts about traffic jams will therefore be shared online. Deception and GPS spoofing are also types of sensor tampering.

3.1.7. Illusion Attack

VANETs are particularly vulnerable to illusion attacks. The attacker mostly changes depending on deep psychological intuition. The hacker must identify or generate an adequate traffic condition before setting up the scene. Consequently, when other drivers receive false information messages, they are more likely to believe them. The intruder must then create a comparable bogus message by tricking the sensor(s) into reporting a true but misleading message rather than altering the output. As an outcome, false information could circulate all over the network. The attack is hard to see, even inside the vehicle [24].

3.1.8. GPS Spoofing

This kind of attack is also known as a tunnel attack. An attacker could provide false location data to another vehicle by using GPS simulators (s). The victim can be awaiting a GPS location [24] after emerging from a real tunnel or a congested area. The GPS simulation may be possible to manufacture signals that are stronger than genuine GPS signals. Therefore, unless a vehicle obtains the genuine satellite signal, it will prefer to believe the attacker's fictitious location data.

3.1.9. Replay Attack

As in MANETs, messages in VANETs could be saved and reused later to deceive other network entities. A replay attack aims to profit from the circumstances when the primary data is delivered. Even if the data is no longer accurate or legitimate, the attacker may gather it, store it, and transmit it to the network [24]. Even the original sender could be responsible for the assault. An attacker might, for instance, save a message they got about a recent tragedy or traffic collision and send it again later.

3.1.10. Passive Eavesdropping Attack

A passive eavesdropping attack analyses the network by employing wireless channel features to follow the motion of the vehicles or listen in on their conversations. Malicious cars could readily receive and study messages sent over the network [28]. Traffic analysis or a stealth assault are other names for this kind of passive attack. There are additional types of attacks, such as route disruption attacks, which take advantage of the cooperativeness and vulnerabilities of routing protocols.

3.1.11. Broadcast Tampering

An attacker can practically feed erroneous messages into the network, causing it to be disrupted [24]. This attack is also similar to false information attacks. Broadcast tampering, on the other hand, typically involves internal attackers.

3.1.12. Remote Firmware

A firmware attack is any malicious malware that gains access to a system thru a backdoor in the processor's software. Backdoors are secret passageways that let selected users get past security and into the system. Due to its tremendous complexity, the backdoor frequently goes undetected, but if hackers use it to their advantage, it can have a big impact [24].

3.1.13. Cryptographic Replication

Attackers could undermine the system in this circumstance by creating many nodes with the same identity. This attack can be performed by replicating key management and certificate [29]. The attacker's purpose is to perplex the authorities and prevent the attacker's identification.

3.1.14. Masquerading

Pretending to be someone else, such as a network identity, is an attempt to get unauthorised access to personal computer files [24]. If an authorization procedure is not properly controlled, a masquerade attack can make it extremely susceptible.

3.1.15. Modification Attack

A modification attack is when someone tries to interfere with one of our resources. These attacks could be categorized as availability attacks, although they could also be characterised as integrity attacks [30]. If we get unauthorised access to a file and change the data it contains, we have compromised the integrity of the information it includes.

3.1.16. ON/OFF Attack

On-Off attacks endanger IoT trust safety by randomly influencing nodes to act in a good or bad way to avoid being classified as a threat. Some countermeasures need past degrees of trust knowledge and time to classify a node's behaviour. A faulty node can sometimes be considered an attacker [26].

3.1.17. Control Override Attack

The control override is the type of attack that springs to mind when someone thinks about their car being "hacked" while driving. It has been demonstrated to be possible in some conditions, as terrifying as it is. The hack takes advantage of CAN networks' vulnerability to denial-of-service assaults. An intruder could routinely deliver urgent notifications to the communication channel [30].

3.1.18. Greedy Drivers

Their goal is to take control of all internet services and use them for their ends. They can create havoc by creating fake traffic congestion data that directs neighbouring nodes away from the intruder's path. To speed up this assault, the attacker smartly adjusted the MAC layer parameters [25].

3.1.19. Remote Access

An internet-based dangerous operation targeted at one or more devices is a remote attack. The remote attack has no impact on the attacker's device. Instead, to get access to a computer or internet, the hacker will look for holes in the security software there [31].

3.1.20. Malware Attack

Malicious code intended to harm Vehicular Ad-hoc Network units or internet connections is called malware. A software exchange or upgrade usually initiated by an insider could contain malware, such as worms or ransomware [24].

3.1.21. Repudiation Attack

Whenever a program or application refuses to consider controls to monitor and log users' activities effectively, permitting harmful modification or creating fake new actions, this is known as a repudiation attack. This exploit can be leveraged to add inaccurate data to log files by changing the authorship data of malicious

user activities. Its application can be broadened to include generic data modification in the identity of others, akin to spoofing mail messages. If this attack is successful, log files' data can be regarded as false or misleading [32].

3.1.22. Impersonation Attack

A user impersonation attack is a scam in which an attacker pretends to be a reliable person to grab money or confidential information from a company. These assaults are typically done by individuals who prey on powerful business leaders.

3.1.23. Poisoning Attack

Poisoning attacks, in which unauthorised users introduce bogus training data to damage the learnt model, are prevalent.

3.1.24. Injection Attack

Data injection attacks come in two varieties: targeted false data injection attacks and random false data injection attacks. Any assault route that can result in inaccurate state variable estimation is sought after by a random false data injection attack. Finding a technique to insert a particular error into particular monitoring variables is the aim of a targeted false data injection attack.

3.1.25. Tunnelling Attack

Fake information is given to a vehicle driving in an area where GPS reception is unavailable, such as a tunnel, where the vehicle may update false information [33].

3.1.26. Ransomware Attack

A ransomware attack poses a significant threat to self-driving automobiles, particularly commercial vehicles. A ransomware attack on self-driving cars might encrypt and use vital in-vehicle information, including a personal media library, communication records, freight tracking logs, crucial control settings, and warehouse locations.

3.1.27. Zombies Attack

Attackers can use zombie attacks to examine weaknesses in a cloud system that have identified vulnerable virtual machines. It's a Clustering-based Classifier Selection Method for Detecting Zombie Attacks and Protection mechanisms.

3.1.28. Gray hole Attack

Messages are deleted as of a result of this attack, also known as a routing misbehaviour attack. The grey hole attack is divided into two stages. Nodes advertise a true path to their destination in the first phase, whereas nodes with a specific probability erase captured packets in the second phase [34].

3.1.29. Sink hole Attack

A sinkhole attack in wireless ad hoc networks is one of the most dangerous. A sinkhole occurrence happens when a compromised or malicious node advertises incorrect routing data to masquerade as a specific node and receives all network traffic. It can either change or discard packet information after receiving the entire network flow, making the network more sophisticated. Ad hoc network protocols, like the DSR protocol, are affected by sinkhole attacks in terms of how well they perform.

3.1.30. Rushing Attack

"Sudden attacks" refers to a new type of DoS attack that directly and negatively affects routing protocols, particularly AODV and Dynamic Source Route. The source car uses VANETs to send the destination car a deluge of road requests (RREQ) during the road discovery phase [27]. At this time, the rushing vehicle receives the RREQ and immediately and without delay transfers the packet to the target automobiles. The destination node will automatically delete the original packet as a copied packet because it has already received the packet from the hasty assault.

3.1.31. Timing Attack

Before advancing a message, malicious vehicles compute some time slots to create a delay. As a result, surrounding vehicles obtain it after they have expressed an interest in receiving it or after the time has passed when they should receive it.

3.1.32. Fabrication Attack

An adversary passes out bogus communications through the network in this assault. For example, a hostile vehicle may transmit a bogus congestion alert or claim to be an emergency vehicle to use the lane alone. Furthermore, this form of attack can cause mishaps [24]. As a result, in V2V communication, checking the freshness and legitimacy of messages is critical to ensure that the messages received are not falsified.

3.1.33. Traffic Analysis

It's a passive attack that gathers data on how many nodes are connected and how much data is processed.

3.1.34. Social Attack

This attack targets all vulnerable attacks. In a Social Attack, the attacker's goal is to indirectly create a problem for the network's users. The attacker delivers random messages to the network's authenticated users, such as "You are stupid," to change the user's behaviour

[30]. When authenticated users read such messages, their conduct shifts from positive to negative and angry.

3.1.35. Distributed Denial of Service Attack (DDOS)

As it is launched from several areas, this attack is dangerous. As a result, the attack's impact is distributed throughout the network.

3.1.36. Spamming Attack

Considering the lack of stable infrastructure and centralised administration in VANET, this assault is extremely difficult to control. Spam messages may cause communication delays to increase, resulting in nodes not receiving messages on time.

3.1.37. Traffic Monitoring

It could be made to find communication parties and capabilities that might be utilized to launch more attacks. Other wireless networks, such as cellular, satellite, and WLAN, are vulnerable to security flaws [31].

3.1.38. Free Riding Attack

In cooperative authentication methods, self-centred vehicles might profit from the verification efforts of others without contributing any of their own. A free-riding assault is a selfish behaviour that poses a major danger to cooperative message authentication.

3.1.39. Dual SYN flood

It's a DoS or DDoS attack that sends many Dual SYN requests to a vehicle to overwhelm and make it unusable. The first employs standard SYN packets, while the second employs large SYN packets [67].

3.1.40. Huge Volumetric Attacks

This attack causes the Saturation of network bandwidth. A DDoS attack tries to eat up bandwidth within the network device or resource and among the rest of the internet. [67].

3.1.41. Hit and Run Attack

These attacks appear when the user has just detected and prevented a DDOS attack. This new type of attack is designed to take advantage of anti-DDoS solutions that are slow to react [67].

3.1.42. Bots Injection Attack

Bot Injection attacks cause damage to OBU, which are used by vehicles to exchange information. These attacks are installed covertly on unsuspecting users' OBU [67].

3.1.43. Spoofing User OBU's

Spoofing OBU means convincing other vehicles that the attacker vehicle is legitimate by providing false data to gain network access. After passing network-level security checks, target servers with catastrophic consequences. [17]

3.1.44. Botnet Zombies Attack

An attack in which a group of compromised vehicles collaborate to attack valid vehicles [67].

3.1.45. Multi Combos Attacks

These attacks are a combination of two or more attacks [17]

3.2. Layer-wise Classification of VANET Attacks

Vehicle networks, like the OSI model, are divided into levels. There is a possibility that an attacker will attempt to compromise one or more of these levels. Attacks like DOS and DDOS can be performed on multi-layer, where some attacks are specific to a particular layer. Throughout this part, we'll talk about several attack patterns and how these assaults affect safety requirements. Table 2 analyses attack specific to particular and attacks that affect multi-layer and impact security goals.

3.3. Layer Wise Attacks Impact on Security Goals

On VANET, an infinite number of attacks are feasible, either shut down the entire network or damage its performance.

Attacks on availability: attack causing a denial of service (DOS) A denial of service attack is the most frequent invasive attack against accessibility. In actuality, it can happen at any networking level. Objectives of the intruder can include jamming communication channels, manipulating vehicle resources, and preventing approved vehicles from accessing the system. Three types of DOS attacks can be distinguished: basic, extended, and distributed denial of service (DDOS) attacks.

Attacks on Authenticity: In Masquerading, an invader must get into the network and have an operational on-board unit to undertake a masquerade attack. The attacker can impersonate a legitimate node and launch any of the assaults. In a network, the easiest assault to launch is a masquerade attack.

Attacks on Integrity: Timing Attack, to trick the user into thinking the message has changed, the hacker adds a delay to the message without altering its substance. As an outcome, clients can encounter traffic jams or, worse, accidents. It's important to remember that consumers should receive information and messages via VANET at the appropriate time. There are two additional levels for timing assault: Basic Level and Extended Level. The basic level concentrates on peer-to-peer (P2P) interaction directly, but the extended level is more severe than the basic level since it concentrates

on a community of participants. Both levels are designed for users in the vehicular network.

Attacks on Confidentiality: Snooping occurs at the network layer and aims to compromise confidentiality in Vehicular Ad - hoc networks. It functions by smelling the communication between two terminals. Consequently, the hackers could eavesdrop on conversations, steal information, and get hold of private information. To get important information, the hacker can pose as one of the nodes or as a fake RSU.

Attacks on Accountability: Non-repudiation is the assertion that no one can repudiate something's authenticity. It prevents scammers from denying their breach since non-repudiation makes it easier to track down targets even if an attack occurs.

Table 1. Correlation of Layer Wise Security Attacks and Security requirements in VANET

Name of the Attack	**Attacker Type**	**Security Requirements**
Sybil Attack	Application layer Transport Layer Network Layer Data Link Layer	Authenticity
DOS	Application layer Transport Layer Network Layer Data Link Layer Physical Layer	Availability
Black hole Attack	Network Layer	Availability
Wormhole Attack	Network Layer	Integrity
Bogus Information Attack	Application layer	Integrity
Tampering Attack	Transport Layer Network Layer Physical Layer	Integrity
Illusion Attack	Application layer Data Link Layer	Integrity
GPS Spoofing	Physical Layer	Authenticity
Replay Attack	Application layer Transport Layer Network Layer Data Link Layer	Integrity
Passive Eavesdropping Attack	Physical Layer	Confidentiality
Broadcast Tampering	Application Layer	Availability
Remote Firmware	Application Layer	Authenticity
Cryptographic Replication	Application Layer	Authenticity
Masquerading	Application Layer Transport Layer	Integrity
Modification Attack	Application Layer	Integrity
ON/OFF Attack	Application Layer	Authenticity
Control Override Attack	Application Layer	Authenticity
Greedy Drivers Attack	Network Layer	Availability
Remote Access	Application Layer	Authenticity
Malware	Application Layer	Availability
Repudiation Attack	Application layer	Non-Repudiation
Impersonation Attack	Application layer Data Link Layer	Authenticity
Poisoning Attack	Network Layer Transport Layer	Integrity
Injection Attack	Transport Layer	Authenticity
Tunnelling Attack	Transport Layer	Availability Authenticity
Ransomware Attack	Network Layer	Confidentiality
Zombies Attack	Network Layer	Integrity
Grey hole Attack	Network Layer	Availability
Sinkhole Attack	Network Layer	Authenticity
Rushing Attack	Network layer	Authenticity Availability Confidentiality Integrity
Timing Attack	Network Layer	Availability
Fabrication Attack	Network Layer Data Link Layer Physical Layer	Authenticity Integrity
Traffic Analysis	Network Layer	Confidentiality
Social Attack	Network Layer	Confidentiality
DDOS	Application layer Transport Layer Network Layer Data Link Layer Physical Layer	Availability
Spamming Attack	Network Layer	Availability
Traffic Monitoring Attack	Network Layer	Confidentiality

Free Riding	Application Layer	Authenticity
Dual SYN flood	Transport Layer Network Layer	Availability
Huge Volumetric attacks	Application Layer	Availability
Hit and Run	Application layer Transport Layer Network Layer Data Link Layer Physical Layer	Availability
Bots Injection	Application Layer	Authenticity
Spoofing user OBU's	Application Layer	Authenticity
Botnet Zombies	Application Layer	Integrity
Multi Combos Attack	Application Layer Network Layer	Authenticity Availability Confidentiality Integrity

3.4. Real-Time Attacks on Manufacturing Hubs

Ransomware threat actors are increasingly targeting businesses. Attacks on all sectors are becoming more daring, frequent, and costly. According to a recent study, the number of ransomware attacks targeting the automobile industry is second only to those targeting the government. The recent KIA Ransomware attack is not the first industrial cyber-attack on a car manufacturer. Some of the best names in the automobile industry have been targeted in recent years. The Ryuk Ransomware attacked both Volkswagen and Peugeot in August 2020. In the same month, one of Tesla's employees was used in a Russian threat actor attack on the company's network.

Billion-dollar failures have been caused by the rise in cyberattacks against the auto sector, and as more automakers enter the autonomous vehicle market, the situation is only getting worse. According to industry analysts, autonomy is the future of the automobile business because driverless cars are safer, more comfortable, and more convenient than ordinary cars. However, this technology has a drawback: it is vulnerable to cyber-attacks. Physical attacks to long-range digital attacks are all possible.

[66] states that an American research team has created a machine learning architecture to enhance vehicle cyber security. Deep reinforcement learning-based allocation of resources and changing target defensive deploying architecture is the name of an in-vehicle network system created by researchers from Virginia Tech, the University of Queensland, and the Gwangju Institute of Science and Technology. Fig. 2 below shows the cyber-attacks on self-driving vehicles and vehicles designed using advanced technology. The recent cyber-attacks done on automobile industries are listed in table 3 below:

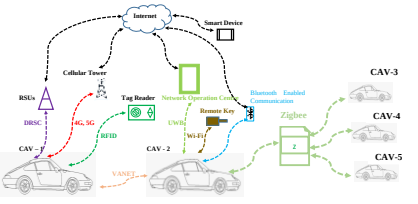

Fig. 2. Cyber-attack vectors in Connected Autonomous Vehicle to Everything (V2X) Communication.

Table 2. Summary of Attacks on vehicle manufacturing plants.

Manufacturing company / Brand	**Type of Attack**	**Hardware / Software Component Hacked**	**Impact**
Tesla	Malware, Social Attack	Software	Information leakage.
Tesla	Sensor impersonation	Hardware	Disclosure of sensitive information
Honda	Remote Firmware	Insecure cryptographic algorithm	Software update unable
Mercedes	Privacy Attack	OBU	Identity revealed
Mitsubishi	Man-in middle attack	Insecure message protocol	Turns lights ON/OFF
BMW, GM, Nissan	Malware Attack	Car-Whisperers, Bluetooth	listening to conversations
All Brands	Jamming Attack	Radio	Modify traffic feed
Honda	Eavesdropping	Remote	All parts can be brought online
BMW	Malware Attack	OBU	Opening and starting the car
Ford, BMW, Vehicles With Push-Button Start	Spoofing Attack	Power Button	Permits a thief to circumvent the

			security system and take the car
BMW, Mercedes, Chrysler & GM	Privacy Attack	digital security	To enable remote management of specific system operations

3.4.1. A review of the literature on attacks on industries hubs

To decrease the amount of HSMs needed, Xie et al. [36] proposed two effective design space exploration (DSE) methods, stepwise decreasing-based heuristic algorithm (SDH) and interference balancing-based heuristic algorithm (IBH). These algorithms look at task allocation, task scheduling, and text schedule. The proposed SDH and IBH outperform the present state-of-the-art method, according to experiments on both synthetic and actual data sets. Their advantage grows as the proportion of security-critical actions rises.

In the proposed supervisory system by Alassery et al. [36], Partial least squares key indicator has been combined with just-in-time neural network (SJITNN)-based CPS monitoring and maintenance to minimise noise and complexity, improve network robustness, predictive maintenance efficiency, RMSE, recall, and accuracy (PLSKI). Huong et al. [38] suggested using anomaly detection to find cyberattacks in industrial control systems. It is suggested to employ one of the most popular networking strategies, the Federated Learning framework, to detect anomalies in time series analysis that are regularly found in industrial systems as part of an anomaly detection architecture for IIoT-based Smart Manufacturing (SM). The architecture delivers superior recognition performance compared to the current finding technique for time series data. Additionally, saving 35% of the bandwidth used in the communication path between the edge and the cloud prove the viability and effectiveness of implementing an IIoT-based SM on top of edge computing hardware.

Sharmila et al. [38] explored the multiple cyber security vulnerabilities and threats in driverless vehicles by creating a graph based on the observed harm propagation of cyber threats and offering a mitigation technique for them. As a result of their connectedness, the networks they are attached to, including the electrical infrastructure, road network sensors, or automobile control functions, suffer security risks. Systems ought to be built to counteract any potential dangers and flaws.

Table 3. Review of Cyber-attacks on Automobile Industries.

Citation	Technique used	Advantages	Disadvantages / Future Research
[35]	Two efficient DSE algorithms	Increases the security	Cost
[36]	Supervisory Just-In-Time Neural Network (SJITNN)	Increases the accuracy and reduces the error	Complex system
[37]	IIoT-based SM	It shows feasibility and efficiency	Memory usage is high
[38]	Self-driving vehicles cybersecurity threats and ANN prevention	dependable and lower safety hazards	The duration of the network is unknown.

4. VANET ATTACKS: PREVENTION AND DETECTION MECHANISMS

4.1. Prevention Schemes in VANET

Authentication is required to accept legitimate VANET users' safety messages. The sender vehicle's signature and the receiver vehicle's signature verification are both required for authentication. The data in the safety message is sent because it is critical for all VANET users. Four risks are associated with broadcasting safety messages: An attacker can change it, an impostor can generate a fake message, message creation denial, and false position information can occur. As a result, the top main security feature in VANET is message authentication. The following authentication requirements must be satisfied for secure communication on the VANET: A re-authentication and revocation mechanism must be available, and authentication must have a minimal computational and transmission cost. (iii) Reliable and long-lasting authentication are required [14].

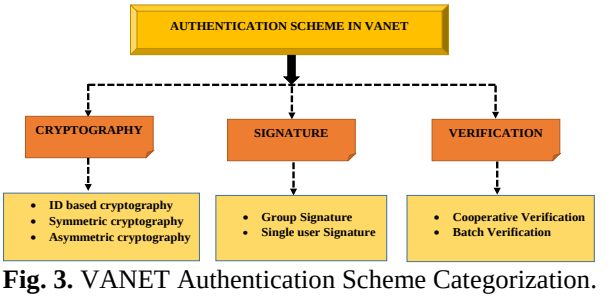

Fig. 3. VANET Authentication Scheme Categorization.

Fig. 3 depicts the classification of authentication techniques in VANETs. In VANET, authentication schemes are classified as cryptography, signature, and verification. Asymmetric cryptography (AC), symmetric cryptography (SC), and identity-based cryptography (IBC) are the three categories of cryptography-based authentication procedures.

4.1.1.A review of the literature on VANET authentication techniques

To produce pseudonyms and signatures and circumvent communication security and privacy issues, Cheng et al. [15] suggested a tamper-proof-based technique that requires storing the program by providing a key in the tamper-proof device (TPD) of cars. It leads to the proposal of an enhanced RSU-based authentication method depending on the Elliptic Curve Cryptosystem (ECC), with the proposed scheme's security significantly enhanced to withstand security issues throughout the pseudonym and private key formation procedures.

Maria et al. [16] proposed a block chain-based anonymous verification method for VANETs to address the vulnerability to security assaults by malicious users. The RSUs may effectively anonymously authenticate the vehicles using the proposed technique and the shared session-id; they can also communicate in the future. It was agreed to provide block chain assisted property transmit command in the future to make it easier for the safe and dispersed transfer of ownership from one vehicle user to another during automobile selling.

A pairing-free certificate less parallel key-insulated signature (CL-PKIS) study was initiated by Yang et al. [17]. It was inspired by the parallel key-insulated mechanism's high stability, ensuring real effectiveness and strong access code security. On the one hand, the research design is constructed using the elliptic curve rather than the laborious pairing procedure. Each vehicle might create or validate, ensuring that is authorised as a result while using less energy. This approach is key-insulated and secure under the discrete logarithm condition in the random oracle model.

For the Vehicular Ad-hoc Networks cross-domain system in IIoT, Khalid et al. [18] suggested an online/offline proposed authentication solution, to make the VANET more secure and effective. The suggested method uses the AES-RSA algorithm to guarantee message integrity and secrecy. Offline joining has been added to prevent remote network invasions and network service disruptions. The suggested work has two major objectives: first, to establish a safe communication on which the information is conveyed, and second, to accomplish effectiveness cryptographically. The Burrows Abdi Needham (BAN logic) logic is utilized to verify that this method is mutually authenticated. The authors want to use the proposed approach in the car industry in the future to provide complete offline authentication functionality.

Jiang et al. [19] proposed SAES, a Self-Checking Authentication Scheme for Vehicular Ad-hoc networks that is more effective and secure, to address the vehicular authentication challenge. The proposed technique replaces formal verification, including the Trusted Authority, with self-checking authentication based on pseudonyms to decrease authentication expenses (TA). Meanwhile, the group signature is utilized to limit the number of times authorized vehicles must be authenticated. Demonstrable privacy and performance analysis of the proposed method's security and reliability results reveal that it not only satisfies the safety requirements for VANETs but also performs noticeably better than the alternatives. The cost of deploying RSUs, on the other hand, is expensive, which makes VANET marketing difficult. Future research must concentrate on reducing the price of deploying RSUs.

A cuckoo filter-based lightweight authentication technique for Vehicular networks was introduced by Moni et al. [20]. It reduces the burden of CRL validation. For ad-hoc vehicle networks (VANETs), pseudonym-based authentication systems aid in maintaining anonymity. Solutions based on the conventional Certificate Revocation List (CRL), on the other hand, incur significant expenses when maintaining a high number of pseudonyms. According to security analysis and verification, our procedure is resistant to man-in-the-middle assaults, replay occurrences, and impersonation attacks. According to our performance evaluation, our approach has a much-reduced authentication overhead than other equivalent schemes.

For cloud-based VANETs, Wang et al. [21] suggested a more practical TPD-based authentication approach with confidentiality features. The offline self-updating technique is often used to review TPD information to fend off side-channel attacks. A fine-grained defect location approach is also created to quickly locate all flawed identities within a problematic collective identity situation. According to our research, the proposed method outperforms existing ones concerning privacy, processing speed, and communication cost, making it more appropriate for a cloud-based VANET.

Cheng et al. [22] presented this study's unique access control technique for block chain-based VANET communication. The authors give thorough information on the network and threat models used to construct our scheme. The network's security analysis shows it can withstand several potential attacks. We also include more smart gadgets into our connection while safe-guarding their security from snoopers. Additionally, we evaluated our performance against that of similar

competing programmes and found it to be superior. Our technique is, therefore, suitable for network access in a VANET with a block chain foundation.

In Al-Shareeda et al. [23], the work's primary goal is to improve the performance of the conditional confidentiality identification service. To secure and boost the effectiveness of VANET connections, it also suggests modifications to the personality conditional confidentiality authentication method. The new framework has been proven secure using the random oracle model and meeting the safety and confidentiality requirements.

Table 4. A Summary of VANET Authentication Schemes.

Citation	Technique used	Advantages	Disadvantages / Future Research
[15]	Elliptic Curve Cryptosystem-improved RSU-based Authentication Scheme (ECC)	Less computation cost and better communication overhead.	It increases error.
[16]	Block chain-Based Anonymous Authentication Scheme (BBAAS)	Efficient in Computational cost, Storage cost, and Communication cost	It has been agreed to build block chain-assisted property transmit command in the future to make it easier for the safe and distributed property transition from one automotive client to the other during car selling.
[17]	Certificate Less Parallel Key Insulated Signature (CL-PKIS)	More Stable and feasible	It takes time to process
[18]	Advanced Encryption Algorithm - Rivest–Shamir–Adleman (AES-RSA)	This algorithm requires less computation, and it gives better efficiency.	The authors want to use the proposed approach in the car industry in the future to provide complete offline authentication functionality.
[19]	Self-checking Authentication Scheme (SAES)	Privacy preservation, Efficient Authentication	Cost is high
[20]	Cuckoo Filter-based Lightweight Authentication Scheme	Robust	Insertion complexity is still presented.
[21]	Tamper Proof Device (TPD)	High security and less computation delay.	Edge Computing and Large Scale batch Authentication
[22]	Block chain-based VANET communication	Capacity to withstand numerous potential attacks.	Scalability issues occur.
[23]	Improving a conditional privacy-preserving confirmation mechanism	Lower computation, reduce the communication cost	-

4.2.Detection Techniques in VANET

Privacy and security are trending topics in almost every industry. When it comes to VANET, it is an important component that is directly related to human life and financial matters. Even minor breaches in VANET privacy and security can result in massive losses. Researchers worldwide devote most of their time to improve security and develop new techniques /methods/ algorithms for detecting various known and unknown VANET attacks. The rest of this section provides a brief overview of detection methods proposed by various authors who have contributed to developing technology that can detect security leaks in VANET at an early stage.

4.2.1. A review of the literature on VANET prevention techniques

J. Liang, M. Ma, and X. Tan [61] proposed an IDS to handle two important issues: 1) Does an IDS's viewpoint on the surroundings transform? 2) Make the IDS flexible for many situations? The authors employed a GaDQN-IDS, a Deep Q-learning Network-based IDS for VANETs based on Bayesian Game theory. The exchanges between an IDS and intruders are seen as a dynamic intrusion detection game. The IDS can choose to either only modify the trade-off between effectiveness and precision or be entirely trained up when its recognition capability has decreased.

By utilising Random Forest and a posterior simulating as many senses on core sets to increase identification efficiency and improve detection

performance, Bangui, H., Ge, and Buhnova [63] suggest a new ML model to increase the accuracy of IDSs. The test findings demonstrate that the suggested model can greatly improve detection performance when contrasted to machine learning models used in traditional applications.

N. Chilamkurti and N. Kumar [16] proposed A unique algorithm that is developed to identify any suspicious attacks in the system and is tuned based on the Collaborative Trust Index (CTI), a new parameter, to cover all potential network attack types. A proposed algorithm for identifying suspicious occurrences using the defined classifier is also made.

To address the aforementioned two problems concurrently, W. Xu, X. Ji, C. Zhang and B. Liu [63] suggest a name/ID hybrid routing (NIHR) system that blends data-name dependent routing and host-ID based routing. We specifically create a bloom filter-based structure for quick content lookup and announce the approach to increase the effectiveness of the in-network storage.

A fog-based DDoS detection approach in 5G-enabled smart cities that employs fuzzy logic to separate malicious traffic from regular traffic is proposed by Gaurav, Akshat, B. B. Gupta, Francisco José Garca Pealvo, Nadia Nedjah, and Konstantinos Psannis [33]. The suggested method successfully distinguishes between DDoS attack traffic with more than 90% accuracy and a real negative rate.

Asim Zeb, Taher M. Ghazal, Taj Rahman, Raed A. Said, Sagheer Abbas, Munir Ahmad, and Muhammad Adnan Khan [45], as well as Bibi, Rozi, Yousaf Saeed, proposed a unique method for the automatic recognition of road irregularities by driverless driving and the provision of road data to approach vehicles. It is based on Edge AI and VANET. The installation of a training sample for road irregularity identification in an automobile and road photos recorded with a camera could assist in lessening the frequency of accidents and dangers on unsafe roads.

Parfenov, D., I. Bolodurina, L. Grishina, and A. Zhigalov [47], demonstrated that the Parzen window approach has an efficiency of 84.15 percent and is approximately 0.3 percent more efficient than the k-nearest neighbour method with lowering values depending on an exponential function with base a <1.

A. A. Aboelfottoh and M. A. Azer [64] suggested Intrusion detection systems that are sharper and more precise using deep learning. On the other hand, it implies additional challenges.

Lu Lihua [65], for connection among currently-operating cars in the IoV, the planned EIDS forecasts secure and energy-efficient end-to-end terminals. The contract administration procedure demonstrates how the cars are linked together to make it safe to communicate data. Regression analysis is used in the prediction phase to assess the proposed EIDS in the IoV environments using the NSLKDD data set. The accuracy and sensitivity components can be effectively improved with 90% and 84.5%, respectively, using the suggested regression-based EIDS technique, according to simulation trials.

Table 5. A Summary of VANET Attacks Detection techniques.

Citation	**Technique used**	**Advantages**	**Disadvantages / Future Research**
[61]	Deep Q-learning Network	Better performance and Higher detection rate	Virtual Simulation, Classifier and father extraction
[62]	Random Forest and a posterior detection	Accuracy and efficiency	Increased the detection efficiency compared to other ML Based IDS
[16]	Collaborative Trust Index (CTI)	includes all potential attack types	Extends the work in the direction of intrusion prevention systems
[63]	The hybrid routing protocol (NIHR)	increases the speed of content lookup and network cache performance	A predefined angle must be carefully set.
[33]	DDOS detection based on fuzzy logic	90% precision and true negative rate	Improves accuracy using other advanced techniques
[45]	Edge AI, Residual Convolutional Neural Network (ResNet-18) and Visual Geometry Group (VGG-11)	Automatic road abnormality identification and data transfer to surrounding vehicles	Future may include brand-new types of irregularities on the road and difficult roads.
[47]	Nearest neighbour and Parzen	Accuracy improved	Use of more ML techniques to

	window method		improve accuracy
[64]	IDS-based deep learning	effectiveness and efficiency	Use of other advanced techniques
[65]	EIDS. NSLKDD data, regression algorithm	Increase the 84 and 90 percent efficiency and precision percentages, respectively.	A new feature selection technique for the machine learning approach's efficient forecasting framework

4.3.Artificial Intelligence in VANET

For more than a decade, Vehicular Ad-hoc Network has been an area of research. Similarly, current advancements in computing skills have increased the implementation of AI approaches in a variety of industries (medical, transportation, engineering, manufacturing, healthcare, and others). Vehicular systems aim to increase the security and productivity of transportation schemes by exchanging information between vehicles, pedestrians, and road-side facilities. The techniques are described below: ML, DL, and SI. AI approaches are now being applied in various real-world contexts due to their superior problem-solving abilities.

Big information availability and advancements in computationally efficient techniques have contributed to AI techniques' current performance. Basic machine learning and deep learning have made considerable strides in recent years, with applications spanning from basic automation to in-depth critical applications and laboratory studies. We highlighted some of the most popular basic Machine Learning (basic ML) techniques, such as reinforcement learning, supervised learning, unsupervised learning, and semi-supervised learning. Some of the machine learning techniques utilised Decision Trees (DT), Support Vector Machine (SVM), Naive Bayes (NB), k-Nearest Neighbour (KNN), Random Forest (RF), Association Rule (AR), Ensemble Learning (EL), K-Means, Principal Component Analysis (PCA), and Reinforcement Learning (RL). Deep learning (DL), a sub-branch of artificial intelligence evolved from machine learning, tries to create knowledge from enormous volumes of data automatically. These strategies have been popular in various practical applications due to their success. The following Fig. 6 summarizes the main deep learning techniques: Deep Auto-Encoders (AEs), Restricted Boltzmann Machines (RBMs), Deep Belief Networks (DBNs), Generative Adversarial Network (GAN), Ensemble of DL Networks (EDLN), and Deep Reinforcement Learning (DRL) [39].

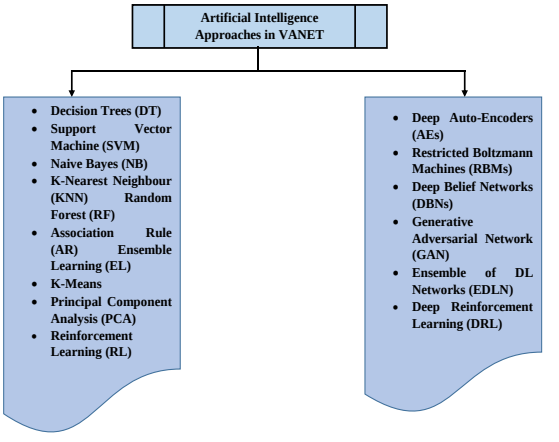

Fig. 4. Artificial Intelligence Approaches in VANET.

4.3.1. A review of the literature on AI in VANET

To enhance IDS performance by raising detection accuracy and productivity, Bangui et al. [40] presented a new machine learning model that uses Random Forest and posterior identification based on core sets. Our proposed method intends to reduce detection time by speeding up the computing process, improving anomaly detection accuracy and reducing false alarms.

Bakkoury et al. [41] presented a clustering technique as an unsupervised machine learning solution with a self-stabilisation approach for delay-sensitive applications in VANET to provide stable and reliable communication between nodes. This project aims to address data sharing delay, provide high data availability, and reduce packet loss in a VANET multi-hop architecture. This method helps us improve cluster stability, reducing dissemination time, packet collision, and data coverage. Our work, however, has several limitations, which can be stated as follows: The cluster head is the fundamental element in the architecture for data sharing applications, which can require additional data fusion time. We share data for vehicles travelling in all directions in this investigation, which means that direction is not considered when creating clusters.

Zang et al. [42] suggested a Machine Learning-based Intrusion Detection System (IDS) to track network traffic and spotted fraudulent activities. This IDS framework provides streaming engines for large data processing, administration, and image processing. A vehicle ad hoc network (VANET) topology with highly interconnected units and mobility capabilities is simulated in the Mininet-Wifi environment. Real-time data is gathered using the sFlow technology and fed into the simulator to create our suggested IDS system. We obtained precise detection performance by employing the Random Forest as the classifier to distinguish the aberrant flows.

Phull et al. [43] presented a method for vehicular ad hoc networks that automates automobile classification and cluster head selection using a game theory approach. Cluster reformation won't be necessary as frequently. The social behaviour of automobiles is grouped using a machine learning technique called the K-means method. The theoretical graph method strengthens and stabilises the cluster head. The simulation findings show that the game theory-based energy-efficient clustering method enhances the sensor network's time responsiveness, increases data transfer, and prolongs the lifetime of the sensor nodes.

Saleem and others [44] suggested that the integrity of primary users can be evaluated via adaptive spectrum sensing. A deep recurrent learning network, also known as long short-term memory, is used to teach the potential of detection under various signal and noise conditions (LSTM). The misleading rate has greatly decreased thanks to the application of LSTM. The proposed methodology is examined using various automotive mobilities on a real-world map of Chengdu, Sichuan Province, southwest China.

Bibi et al. [45]., based on Edge AI and VANET, presented a novel technique enabling autonomous vehicles to automatically detect road irregularities and provide road information to approaching vehicles. Using a trained model for detecting highway abnormalities in an automobile and taking road images with a webcam could help lessen the number of accidents and the danger of threats on poor roads. Residual Convolutional Neural Network (ResNet-18) and Visual Geometry Group (VGG-11) are used to automatically identify and classify simple roads without abnormalities and roads with anomalies like potholes, bumps, and cracks, using a dataset from different internet sources. Future research could include various anomalous roads and roads with multiple issues. Additionally, automatic regulation of automobile movement based on abnormal kind and avoidance can be made in an automated car using less complex deep learning models.

A method for the forecasting network activity that considers the factors that can affect road traffic was presented by Sepasgozar et al. [46]. The proposed model calculates the network flow of traffic based on concurrent road and network traffic using a Random Forest-Gated Recurrent Unit-Network Traffic Prediction algorithm (RF-GRU-NTP). In the third phase, the hybrid proposed model is put into practice. It first applies the deep learning method to improve network traffic flow, with the Gated Recurrent Unit (GRU) method producing the best results, using the Random Forest (RF) machine-learning algorithm to identify major characteristics from the combined dataset (which includes V2V and V2R communications).

Parfenov et al. [47] used metric techniques, including the k-nearest neighbour approach with linearly decreasing values and the Parzen window method, to identify which nonlinear functions to employ for calculating distances between sample items and describing VANET traffic. The effectiveness of the tactics under discussion was assessed using a synthetically generated collection of three different types of network attacks. KNN, on either hand, struggles with large datasets since it takes a long time to calculate the distances between each data point.

Maleknasab et al. [48] described a multi-layer technique and a fuzzy logic-based solution for road-side devices (RSUs). This system uses two fuzzy logic controllers (FLCs), the first of which takes into account variables such as vehicle confidence, RSSI difference, automobiles length, and vehicle angle, and the second of which considers variables such as signal-to-noise ratio, network entry time, number of neighbours, and buffer size. The applied fuzzy sets are tuned using the arithmetic optimisation algorithm (AOA), and the optimal rules are chosen to enhance the performance of the proposed FLCs. As these systems rely on inaccurate information and inputs, their accuracy is affected.

A deep neural network (DNN)-based anomaly detection system for VANETs was presented by Alladi et al. [49]. It employs a sequence reconstruction and thresholding approach. In this system, road-side units (RSUs) that receive broadcast automobile data and carry out outlier detection activities to classify a message sequence as real or abnormal are implemented with DNN architectures. In this experiment, a variety of DNN architectures are created, and the effectiveness of each is evaluated using key evaluation measures.

To address the growing increase in processing capabilities and the need to detect hazardous incidents swiftly, Bangui et al. [50] presented a hybrid ML model to optimise the effectiveness of IDSs. The recommended method largely uses Random Forest's advantages to find known network breaches. Additionally, a post-detection stage is employed to find potential new incursions by utilising the benefits of corsets and clustering algorithms. In the future, we plan to implement our system in virtual environments like the Internet of Vehicles and evaluate how well the suggested approach performs.

Kadam et al. [51] developed a unique Hybrid KSVM method founded on KNN and SVM algorithms to form a safe structure to identify Distributed Daniel of Service attacks, increase performance, and fit the VANET scenario. The work's future scope is that we can use the same technology to detect multiple types of assaults, such as Dos and Sybil. By evaluating various network security methods, a more secure framework for communication can be developed that ensures message integrity and confidentiality while in transmission.

Thilak et al. [52]., proposed a Variant Artificial Bee Colony Algorithm (VABCA) to improve the choice of an automobile network to replace the damaged DDoS automobile network. In the spectator bee, differentiated development and combined Chaotic and opposition learning are used as search techniques. In the scout bee, an incorporated Chaotic and opposition learning is used. VABCA is an enhanced form of ABCA. The primary goals of VABCA are to enhance the worldwide optimal detection point for DDoS attacks and achieve high levels of convergence rate and effectiveness to find the most workable solutions. It is proposed that this Artificial Bee Colony Optimization be enhanced in the future by using tent map-based chaotic systems to clarify the degree of population variance that causes a scalability rise in any optimal solution.

Table 6. Review of Artificial Intelligence in VANET.

Citation	Technique used	Dataset	Advantages	Disadvantages / Future Research
[40]	The hybrid machine learning model for IDS	CICIDS2017	Decreases the computational time	High error susceptibility
[41]	Clustering for delay-sensitive application in VANET	Real-time data	Reduces the time and data collision	The authors share data for vehicles travelling in all directions in this investigation, which means that direction is not considered when creating clusters.
[42]	Machine learning-based IDS framework	CICIDS2017	quick detection and training times	A lightweight approach slightly burdens the system.
[43]	Game theory-based energy-efficient clustering approach	Real-time data collection	More reliable and stable network	Large data requires more time to process.
[44]	LSTM	Real-time dataset	The cluster head is selected accurately	LSTM requires more memory to train.
[45]	ResNet-18 and VGG-11	Kaggle dataset	Getting protection and reliability in the flow of traffic	The research can be expanded in the future by including other sorts of irregular road conditions and roads with several issues
[46]	RF-GRU-NTP	Vehicular Network dataset	Good results in traffic flow prediction	Nevertheless, when the quantity of automobiles rises, the volume of data produced by them increases, resulting in big data, which we will implement in our future work.
[47]	Real-time data	K-Nearest Neighbour (KNN)	Classification accuracy is higher	It does not function well with large datasets since calculating distances between data instances is quite time-consuming.
[48]	Real-time data	Fuzzy Logic Controllers (FLC)	Packet loss is less	Inaccurate information and input accuracy are affected.
[49]	Real-time data	Anomaly detection using Deep Neural Network (DNN)	Highest accuracy in anomaly detection.	To perform better than other strategies, requires a large amount of data.
[50]	IDS Dataset	hybrid machine learning-based detection model driven by data	Computational time consumption	In the future, we plan to implement our system in virtual environments like the Vehicular networks and evaluate how well the proposed approach performs.
[51]	Kaggle dataset	KSVM	It gives a better result in accuracy, recall,	A more secure framework for communication can be developed that ensures the confidentiality and

			and precision.	reliability of the communication in transfer.
[52]	Real-time data	VABCA	Reduction in prediction variance and mean prediction variance.	This Artificial Bee Colony Optimizer is proposed to be enhanced in the future by using tent map-based chaotic systems to explain the amount of population fluctuation that results in a scalable rise in any optimal solution.

4.4.Summary

The management of vehicular networks because of reduced transmission latency and decreased message latency among vehicular nodes is the most crucial component of VANETs. All fundamental security needs must be addressed, and reliable vehicular communication is a prerequisite of the vehicular communication system. Security is the primary factor to be taken into account for VANET installation. When addressing these security vulnerabilities, several open questions need to be addressed. These issues demand special consideration from academics and will likely remain an open area of study. We have outlined a few unresolved problems that may develop into frequently studied areas in the upcoming years.

Authentication has been a key security need and a fundamental step in providing security in VANETs. The sorts of cryptographic methods, signatures, and verification are used in authentication techniques to assure security are protected. Asymmetric Cryptography Based Authentication Method (ASC-BAS) is a centralised cryptography-based authentication technique, whereas Symmetric Cryptography Based Authentication Scheme (SC-BAS) is a decentralised scheme. Non-repudiation, a major safety need, is not mentioned in SC-BAS. Although several authentication methods have been given, several safety issues need to be solved before VANET can be put into practice.

The goal of VANET is to ensure that driving is both safe and cooperative. Giving the critical data to the operator or automobile achieves this. It is crucial to validate and double-check the data sent across VANET. Further research is required for Data-centric trust and validation of the tamper-resistance hardware used in automobiles to identify unnecessary accident warnings. By correlating incoming details concerning conditions and surroundings with its data for context verification, a vehicle must be able to function as an intrusion detection system. Furthermore, the reactive security concept must be improved.

5. FUTURE RESEARCH

Apart from the benefits that can be gained from VANET adoption, VANET challenges several obstacles. These challenges could be viewed as potential future study paths or unresolved study objectives that still need to be advanced and resolved. Some of the challenges that consumers might use as a study topic include the following:

Data Administration and Storage: Vehicles must communicate to exchange information. The attacker takes advantage of vehicle storage capabilities and opportunistic communications that can occur when one vehicle enters the communication range of another. To steal the information shared, attackers, employ various methods, including DOS, DDOS, Black hole, Rushing, and others. Analysing, managing, and preserving such vast information remain challenging for researchers. Future research is still needed to fully understand the fusion of two concepts, even though techniques like Big Data can address this issue.

Security and Privacy: Vehicular Network is an open network that allows any vehicle to connect. A few mechanisms are essential for ensuring that the vehicles entering and exiting the network are trustworthy. As a result, security experts are worried since wireless connections are used for vehicular communications, making it possible for any vehicle to transmit harmful data and seriously injure other vehicles. Furthermore, it is challenging to identify such a vehicle, necessitating the creation of better privacy algorithms to guarantee Ad - hoc network security. Additionally, by using the VANET, unreliable cars can learn about other users' behaviours, routines, and patterns, posing a serious threat to personal privacy.

Delivery of Quality Services: The networks that make up a VANET are adaptable and dynamic. Numerous variables, including node position, architecture, length among nodes, connectivity, and others, make routing algorithms and protocols inadequate for delivering a satisfactory level of service.

Various attacks in VANET, such as jamming attacks, black hole attacks, and others, can affect the quality of service (QoS). VANET requires designing, modelling, and implementing mechanisms that provide real-time message propagation that can deliver data in a timely and accurate manner to ensure that emergency and safety-related information is safe-guarded against such attacks and maintains a high level of service quality across the network.

The usage of AI is one of the popular tactics being used to improve the new V2X mode of communication.

AI strategies can be supplied, such as incorporating road and temperature variations for work scheduling, modelling techniques, and allocation of resources. However, at this high level of standardisation, AI must be used with caution, and this will continue to be difficult for future research initiatives focusing on AI approaches and VANET integration.

Routing Techniques: Because the involved automobiles are so movable and can change the routing protocols in a matter of seconds, conventional routing protocols are useless in a VANET. Additionally, to give better bandwidth, better customer service, and a higher packet delivery ratio, it is necessary to connect vehicles, share data among input and output vehicles, and propagate data to other vehicles.

6. CONCLUSION

VANETs are critical in protecting vehicles from meeting potential obstacles in intelligent transportation systems. VANETs, on the other hand, employ routing protocols to communicate via open wireless channels, which pose significant security concerns. In this essay, we thoroughly examine numerous VANET attacks; we have mapped the various attacks that affect the VANET communication layers (specific layer and multi layers) and the impact it causes on security goals that can provide useful information to other researchers working on VANET attacks. In addition, we presented a survey of various authentications and prevention mechanisms used in the VANET area to mitigate attacks. We also comprehensively assessed important AI systems that can be applied to VANETs. Finally, we explored some of the unresolved issues in the VANETs domain that pose a significant effect in the future.

ACRONYMS

AU	Application Unit
C-V2X	Cellular Vehicle to Everything
CR	Cognitive Radio
DOS	Denial of Service
DDOS	Distributed Denial of Service
GPS	Global Positioning System
GNNS	Global Navigation Satellite System
INTS	Intelligent Transportation System
ITS	Intelligent Traffic System
MANET	Mobile Ad hoc Network
OBU	On – Board Unit
OSI	Open System Interconnection
RSU	Road Side Unit
V2X	Vehicle to Everything
3GPP	Third Generation Partnership project
WAVE	Wireless Vehicular communications

REFERENCES

[1] B. Bako, & M. Weber, **"Efficient information dissemination in VANETs,"** *INTECH Open Access Publisher*, 2011.

[2] P. Ranjan, & K. K. Ahirwar, **"Comparative study of vanet and manet routing protocols,"** *In Proc. of the international conference on advanced computing and communication technologies (acct 2011)* No. Acct, pp. 978-981, 2011, January.

[3] R. Kumar, & M. Dave, **"A review of various vanet data dissemination protocols,"** *International Journal of u-and e-Service, Science and Technology*, Vol. 5, No. 3, pp. 27-44, 2012.

[4] H. Hartenstein, & K. P. Laberteaux, **"A tutorial survey on vehicular ad hoc networks,"** *Communications Magazine, IEEE*, Vol. 46, No. 6, pp. 164-171, 2008.

[5] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin, and A. Hassan, **"Vehicular ad hoc networks (VANETs): Status, results, and challenges,"** *Telecommun. Syst.*, Vol. 50, No. 4, pp. 217–241, 2012.

[6] S. S. Manvi, and S. Tangade, **"A survey on authentication schemes in VANETs for secured communication,"** *Veh. Commun.*, Vol. 9, pp. 19–30, 2017 Jul.

[7] R. Mishra, A. Singh, and R. Kumar, **"VANET security: Issues, challenges and solutions,"** *In Proc. Int. Conf. Electr., Electron., Optim. Techn. (ICEEOT)*, pp. 1050–1055, 2016, Mar.

[8] J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, **"An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks,"** *IEEE Trans. Intell. Transp. Syst.*, Vol. 20, No. 5, pp. 1621–1632, 2018 May.

[9] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, **"Survey of authentication and privacy schemes in vehicular ad hoc networks,"** *IEEE Sensors J.*, Vol. 21, No. 2, pp. 2422–2433, 2020 Jan.

[10] L. Xie, Y. Ding, H. Yang, and X. Wang, **"Block chain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs,"** *IEEE Access*, Vol. 7, pp. 56656–56666, 2019.

[11] G. Kumar, R. Saha, M. K. Rai, and T. H. Kim, **"Multidimensional security provision for secure communication in vehicular ad hoc networks using the hierarchical structure and end-to-end authentication,"** *IEEE Access*, Vol. 6, pp. 46558–46567, 2018.

[12] N. Kumar, and N. Chilamkurti, **"Collaborative trust aware intelligent intrusion detection in VANETs,"** *Comput. Elect. Eng.*, Vol. 40, No. 6, pp. 1981–1996, 2014.

[13] M. W. Maier, D. Emery, & R. Hilliard, **"Software architecture: introducing IEEE Standard 1471,"** *Computer*, Vol. 34, No. 4, pp. 107-109, 2001.

[14] R. Tomar, M. Prateek, & G. H. Sastry, **"Vehicular Adhoc network (vanet)-an introduction,"** *International Journal of Control Theory and Applications*, Vol. 9, No. 18, pp. 8883-8888, 2016.

[15] F. Azam, S. K. Yadav, N. Priyadarshi, S. Padmanaban, & R. C. Bansal, **"A comprehensive**

review of authentication schemes in a vehicular ad-hoc network," *IEEE Access*, Vol. 9, pp. 31309-31321, 2021.

[16] H. Cheng, & Y. Liu, **"An improved RSU-based authentication scheme for VANET,"** *Journal of Internet Technology*, Vol. 21, No. 4, pp. 1137-1150, 2020.

[17] A. Maria, V. Pandi, J. D. Lazarus, M. Karuppiah, & M. S. Christo, **"BBAAS: Block chain-based anonymous authentication scheme for providing secure communication in VANET,"** *Security and Communication Networks*, Vol. 2021, 2021.

[18] M. Yang, J. Chen, Y. Chen, R. Ma, & S. Kumar, **"Strong key-insulated secure and energy-aware certificateless authentication scheme for VANETs,"** *Computers & Electrical Engineering*, Vol. 95, pp. 107417, 2021.

[19] H. Khalid, S. J. Hashim, S. M. S. Ahmad, F. Hashim, & M. A. Chaudhary, **"A lightweight and secure online/offline cross-domain authentication scheme for VANET systems in Industrial IoT,"** *PeerJ Computer Science*, Vol. 7, pp. e714, 2021.

[20] H. Jiang, L. Hua, & L. Wahab, **"SAES: a self-checking authentication scheme with higher efficiency and security for VANET,"** *Peer-to-Peer Networking and Applications*, Vol. 14, No. 2, pp. 528-540, 2021.

[21] S. S. Moni, & D. Manivannan, **"A lightweight Privacy-Preserving V2I Mutual Authentication Scheme using Cuckoo Filter in VANETs,"** *In 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC) IEEE*, pp. 815-820, 2022.

[22] Y. Wang, W. Zhang, X. Wang, M. K. Khan, & P. Fan, **"Efficient Privacy-Preserving Authentication Scheme with Fine-Grained Error Location for Cloud-Based VANET,"** *IEEE Transactions on Vehicular Technology*, Vol. 70, No. 10, pp. 10436-10449, 2021.

[23] Y. Cheng, S. Xu, M. Zang, S. Jiang, & Y. Zhang, **"Secure Authentication Scheme for VANET Based on Blockchain,"** *In 2021 7th International Conference on Computer and Communications (ICCC), IEEE*, pp. 1526-1531, 2021.

[24] M. A. Al-Shareeda, M. Anbar, S. Manickam, & I. H. Hasbullah, **"Towards identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks,"** *IEEE Access*, 2021.

[25] S. Ercan, M. Ayaida, & N. Messai, **"Misbehavior Detection for Position Falsification Attacks in VANETs Using Machine Learning,"** *IEEE Access*, Vol. 10, pp. 1893-1904, 2021.

[26] M. Al-Mehdhara, & N. Ruan, **"MSOM: Efficient Mechanism for Defense against DDoS Attacks in VANET,"** *Wireless Communications and Mobile Computing*, Vol. 2021, 2021.

[27] A. Alharthi, Q. Ni, & R. Jiang, **"A privacy-preservation framework based on biometrics blockchain (BBC) to prevent attacks in VANET,"** *IEEE Access*, Vol. 9, pp. 87299-87309, 2021.

[28] O. N. U. R. Polat, C. E. M. A. L. Koçak, & H. Ü. S. E. Y. İ. N. Polat, **"Recognition of DDoS Attacks on SD-VANET Based on Combination of Hyperparameter Optimization and Feature Selection,"** *Expert Systems with Applications*, Vol. 117500, 2022.

[29] D. Parfenov, I. Bolodurina, L. Grishina, and A. Zhigalov, **"Investigation of the effectiveness of metric classification methods in identifying attacks in VANET,"** *In Journal of Physics: Conference Series IOP Publishing*, Vol. 2094, No. 3, pp. 032066, 2021.

[30] M. Maleknasab Ardakani, M. A. Tabarzad, & M. A. Shayegan, **"Detecting Sybil attacks in vehicular ad hoc networks using fuzzy logic and arithmetic optimisation algorithm,"** *The Journal of Supercomputing*, pp. 1-33, 2022.

[31] B. K. Pattanayak, O. Pattnaik, & S. Pani, **"Dealing with Sybil attack in VANET,"** *In Intelligent and Cloud Computing, Springer, Singapore*, pp. 471-480, 2021.

[32] T. Alladi, B. Gera, A. Agrawal, V. Chamola, & F. R. Yu, **"Deep ADV: A Deep Neural Network Framework for Anomaly Detection in VANETs,"** *IEEE Transactions on Vehicular Technology*, Vol. 70, No. 11, pp. 12013-12023, 2021.

[33] A. A. Sabbagh, & M. V. Shcherbakov, **"A Secure and Stable Routing Protocol for VANET Under Malicious Attacks,"** *In Conference on Creativity in Intelligent Technologies and Data Science, Springer, Cham*, pp. 421-435, 2021.

[34] H. Bangui, M. Ge, & B. Buhnova, **"A Hybrid Data-driven Model for Intrusion Detection in VANET,"** *Procedia Computer Science*, Vol. 184, pp. 516-523, 2021.

[35] R. Kolandaisamy, R. M. Noor, I. Kolandaisamy, I. Ahmedy, M. L. M. Kiah, M. E. M. Tamil, & T. Nandy, **"A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET,"** *Journal of Ambient Intelligence and Humanized Computing*, Vol. 12, No. 6, pp. 6599-6612, 2021.

[36] Alhaidari, A. Fahd, and Alia Mohammed Alrehan, **"A simulation work for generating a novel dataset to detect distributed denial of service attacks on Vehicular Ad hoc NETwork systems,"** *International Journal of Distributed Sensor Networks*, Vol. 17, No. 3, pp. 15501477211000287, 2021.

[37] N. Kadam, & R. S. Krovi, **"Machine Learning Approach of Hybrid KSVN Algorithm to Detect DDoS Attack in VANET,"** *Machine Learning*, Vol. 12, No. 7, 2021.

[38] K. Thilak, A. Deepa, Amuthan, and S. Rajkamal, **"Mitigating DDoS attacks in VANETs using a Variant Artificial Bee Colony Algorithm based on cellular automata,"** *Soft Computing*, Vol. 25, No. 18, pp. 12191-12201, 2021.

[39] A. Gaurav, B. B. Gupta, F. J. G. Peñalvo, N. Nedjah, & K. Psannis, **"DDoS Attack Detection in Vehicular Ad-Hoc Network (VANET) for 5G Networks,"** *In Security and Privacy-Preserving for IoT and 5G Networks, Springer, Cham.*, pp. 263-278, 2022.

[40] F. Bensalah, N. Elkamoun, & Y. Baddi, **"SDNStat-Sec: a statistical defence mechanism against DDoS attacks in SDN-based VANET,"** *In Advances on smart and soft computing, Springer, Singapore*, pp. 527-540, 2021.

[41] Y. Xie Y. Guo, S. Yang, J. Zhou, & X. Chen, **"Security-Related Hardware Cost Optimization for CAN FD-Based Automotive Cyber-Physical Systems,"** *Sensors*, Vol. 21, No. 20, pp. 6807, 2021.

[42] F. Alassery, **"Predictive maintenance for cyber-physical systems using neural network based on deep soft sensor and industrial internet of things,"** *Computers and Electrical Engineering*, Vol. 101, pp. 108062, 2022.

[43] T. T. Huong, T. P. Bac, D. M. Long, T. D. Luong, N. M. Dan, B. D. Thang, & K. P. Tran, **"Detecting cyber-attacks using anomaly detection in industrial control systems: A Federated Learning approach,"** *Computers in Industry*, Vol. 132, pp. 103509, 2021.

[44] V. C. Sharmila, H. M. Aslam, M. M. & Riswan, **"Analysing and Identifying Harm Propagation of Cyber Threats in Autonomous Vehicles and Mitigation Through ANN,"** *In Smart Trends in Computing and Communications, Springer, Singapore*, pp. 405-417, 2022.

[45] A. Mchergui, T. Moulahi, & S. Zeadally, **"Survey on Artificial Intelligence (AI) techniques for Vehicular Ad-hoc Networks (VANETs),"** *Vehicular Communications*, pp. 100403, 2021.

[46] H. Bangui, M. Ge, & B. Buhnova, **"A hybrid machine learning model for intrusion detection in VANET,"** *Computing*, Vol. 104, No. 3, pp. 503-531, 2022.

[47] S. Bakkoury, S. Ouahou, Z. Bah, **"New machine learning solution based on clustering for delay-sensitive application in Vanet."**

[48] M. Zang, & Y. Yan, **"Machine learning-based intrusion detection system for big data analytics in VANET,"** *In 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), IEEE*, pp. 1-5, 2021.

[49] N. Phull, P. Singh, M. Shabaz, & F. Sammy, **"Enhancing Vehicular Ad Hoc Networks' Dynamic Behavior by Integrating Game Theory and Machine Learning Techniques for Reliable and Stable Routing,"** *Security and Communication Networks*, Vol. 2022, 2022.

[50] M. A. Saleem, Z. Shijie, M. U. Sarwar, T. Ahmad, A. Maqbool, C. S. Shivachi, & M. Tariq, **"Deep learning-based dynamic stable cluster head selection in VANET,"** *Journal of Advanced Transportation*, Vol. 2021, 2021.

[51] R. Bibi, Y. Saeed, A. Zeb, T. M. Ghazal, T. Rahman, R. A. Said, ... & M. A. Khan, **"Edge AI-based automated detection and classification of road anomalies in VANET using deep learning,"** *Computational intelligence and neuroscience*, Vol. 2021, 2021.

[52] S. S. Sepasgozar, & S. Pierre, "**An Intelligent Network Traffic Prediction Model Considering Road Traffic Parameters Using Artificial Intelligence Methods in VANET,"** *IEEE Access*, 2022.

[53] A. K. Goyal, A. Kumar Tripathi, and G. Agarwal, **"Security Attacks, Requirements and Authentication Schemes in VANET,"** *International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, pp. 1-5, 2019, doi: 10.1109/ICICT46931.2019.8977656.

[54] A. Verma, R. Saha, G. Kumar, & T. H. Kim, **"The Security Perspectives of Vehicular Networks: A Taxonomical Analysis of Attacks and Solutions,"** *Applied Sciences*, Vol. 11, No. 10, pp. 4682, 2021. https://doi.org/10.3390/app11104682

[55] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, and R. Das, **"Attacks on Self-Driving Cars and Their Countermeasures: A Survey,"** *In IEEE Access*, Vol. 8, pp. 207308-207342, 2020. doi: 10.1109/ACCESS.2020.3037705

[56] M. S. Sheikh, J. Liang, & W. Wang, **"A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs),"** *Sensors*, Vol. 19, No. 16, pp. 3589, 2019. https://doi.org/10.3390/s19163589

[57] R. Molina-Masegosa, and J. Gozalvez, **"LTE-V for Sidelink 5G V2X Vehicular Communications: A New 5G Technology for Short-Range Vehicle-to-Everything Communications,"** *In IEEE Vehicular Technology Magazine*, Vol. 12, No. 4, pp. 30-39, Dec. 2017. doi: 10.1109/MVT.2017.2752798.

[58] Cellular-Vehicle-to-Everything-C-V2X. Available online: https://internetofthingsagenda.techtarget.com/definition/Cellular-Vehicle-to-Everything-C-V2X

[59] M. M. Hamdi, L. Audah, M. S. Abood, S. A. Rashid, A. S. Mustafa, H. Mahdi, & A. S. Al-Hiti, **"A review on various security attacks in vehicular adhoc networks,"** *Bulletin of Electrical Engineering and Informatics*, Vol. 10, No. 5, pp. 2627~2635, October 2021. ISSN: 2302-9285, DOI: 10.11591/eei.v10i5.3127

[60] K. Vamshi Krishna, and G. Reddy, **"A Delay Sensitive Multi-Path Selection to Prevent the Rushing Attack in VANET,"** *2021 5th International Conference on Information Systems and Computer Networks (ISCON)*, pp. 1-7, 2021. doi: 10.1109/ISCON52037.2021.9702331.

[61] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, **"Survey of Authentication and Privacy Schemes in Vehicular Ad hoc Networks,"** *In IEEE Sensors Journal*, Vol. 21, No. 2, pp. 2422-2433, Jan.15, 2021. doi: 10.1109/JSEN.2020.3021731.

[62] J. Liang, M. Ma, and X. Tan, **"GaDQN-IDS: A Novel Self-Adaptive IDS for VANETs Based on**

Bayesian Game Theory and Deep Reinforcement Learning," *In IEEE Transactions on Intelligent Transportation Systems.* doi: 10.1109/TITS.2021.3117028.

[63] H. Bangui, M. Ge, & B. Buhnova, **"A hybrid machine learning model for intrusion detection in VANET,"** *Computing*, pp. 1-29, 2021. https://doi.org/10.1007/s00607-021-01001-0

[64] W. Xu, X. Ji, C. Zhang, and B. Liu, **"NIHR: Name/ID Hybrid Routing in Information-centric VANET,"** *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1-7, 2020. doi: 10.1109/WCNC45663.2020.9120459.

[65] A. A. Aboelfottoh, and M. A. Azer, **"Intrusion Detection in VANETs and ACVs using Deep Learning,"** *2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC)*, pp. 241-245, 2022. doi: 10.1109/MIUCC55081.2022.9781691

[66] L. Lihua, **"Energy-Aware Intrusion Detection Model for Internet of Vehicles Using Machine Learning Methods,"** *Wireless Communications and Mobile Computing*, *Hindawi*, 2022. 2022/05/26. https://doi.org/10.1155/2022/9865549.

[67] J. Mahmood, Z. Duan, Y. Yang, Q. Wang, J. Nebhen, & M. N. M. Bhutta, **"Security in Vehicular Ad Hoc Networks: Challenges and Countermeasures,"** *Security and Communication Networks*, Vol. 2021, Article ID 9997771, pp. 20, 2021. https://doi.org/10.1155/2021/9997771