Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606

Volume 08 Issue 01
2024

Research Article
https://doi.org/10.56979/801/2024

Enhancing Security of Autonomous Vehicles using Layered Strategy with Defensive Techniques-A Survey

Saadia Bano[1*], M. Ismail Kashif[1], and Qudsia Zafar[1]

[1]National College of Business and Economics, Lahore (Multan Campus), 66000, Pakistan
[*]Corresponding Author: Sadia Bano. Email: saadiabano16@gmail.com

Received: August 02, 2024 **Accepted:** September 29, 2024

Abstract: Autonomous vehicles (AV) are a revolutionary advancement in transportation technology defined as independent of humans for their performance. Autonomous vehicles are user and environment-friendly as they are easy to operate and help in traffic flow optimization with other benefits. Autonomous vehicles work with an array of modern technologies like sensors, light imaging detection and ranging (Lidar), cameras, GPS, and advanced computing systems that help the autonomous vehicle to predict its surroundings to make optimal decisions in real time. AV is highly dependent on communication, the base of AV relies on communication like inter-vehicle communication, infrastructure communication, and vehicle-to-everything communication. The high dependency on communication channels attracts adversaries with the possibility of information theft, GPS spoofing, and deployment of malicious software for different fraudulent activities. In this research, we have explored the potential security threats of AV with layered-based model approach. This paper have surveyed the recent research trends with countermeasure strategies. This discussion will not only provide an overview of security challenges of AV but also present the open challenges for further research.

Keywords: Autonomous Vehicles; Cyber Security; Autonomous Vehicle Attacks; LIDAR; Sensor; GPS; Data Privacy.

1. Introduction

The Industrial Revolution eliminated the need for human factors day by day. One key field in the Industrial Revolution was transportation. The concept of autonomous vehicles has changed the transport concept drastically, the world is moving towards automation of vehicles. Autonomous vehicles have changed the concept of how people and things move. Smart vehicles with the help of smart sensory devices minimize the risk of accidents without human assistance. The automation in vehicles is based on sensors and communication models. These vehicles are connected, with pedestrians and with service providers, it provides more flexibility by allowing users to share data via Bluetooth, AUX cable, USB, etc[1]. To monitor surroundings autonomous vehicles, take the help of cameras and Lidar, to predict route navigation systems is helpful, with the help of these devices the vehicles can predict the route, fellow vehicles, and pedestrians to make real-time decisions without human help.[2] Vehicle automation is categorized into five levels. There are five levels of automation of vehicles as shown in figure 1.

Level 0
Level 1
Level 2
Level 3
Level 4
Level 5

Figure 1. Level of automation

Level 0-2 is categorized as driver-assisted, levels 3-4 are semi-automatic and level 5 is fully autonomous. Currently, level 4 of automation is achieved and implemented. With the help of machine learning and artificial intelligence level 5 automation is in progress. [3]

Due to its smart approach and safe ride marketing trends of autonomous vehicles seem to be increasing. In Fig 2 growing industry trends are shown that are supposed to be on their peak by 2040[4]. In 2050 the investment will be in trillions. With the growing industry gaining public trust is important and depends on safeguarding passengers by improving security standards.

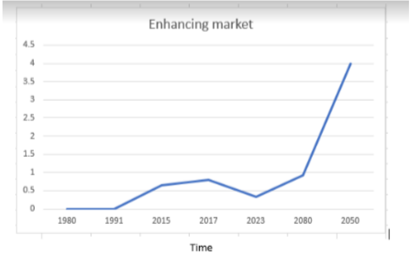

Figure 2. Graph on growing AV industry

More connectivity makes it more vulnerable to the intruders. Despite of all the research and adding new features, 300 vulnerabilities were found in the vehicles of Tier 1 companies in 2020[4]. Many aspects of smart vehicles still need to be addressed.

The underlying structure that helps the vehicle to operate autonomously is connected and autonomous vehicle architecture (CAV). CAV is a combination of hardware, software, and connectivity features. CAV typically consist of sensors, GPS, control systems, cameras, communication models, security systems, CPU, and onboard computers. The features may vary a bit due to vendor but the main functionality depends on the above[5]. The working of autonomous vehicles depends on real-time data collection and processing. The data is mainly collected with the help of Lidar, cameras, and sensors, the amount of data collected is in terabytes per hour. This huge data causes security breaches. Connectivity is the key to successful automation. It increases the likelihood of security gaps and vulnerabilities[6]. The type of communication that an autonomous vehicle carries are discussed next.

1. Vehicle-to-infrastructure communication: This refers to the communication with infrastructure like roads, traffic signals, and street lights with the help of sensors.
2. Vehicle-to-vehicle communication: It helps the vehicle to capture and exchange data. Each vehicle acts like a node that connects to other nodes.
3. Vehicle to cloud: Due to the immense generation of data the autonomous vehicle uses a network like 5G to store data in the cloud. It helps the vehicle to get over-the-air updates.
4. Vehicle to devices: The general example of the vehicle to the device is Bluetooth which helps to connect the vehicle with mobile or any small device.
5. Vehicle to pedestrian: Unlike its name, it’s not connected to the pedestrian it is just a sensor that gives a 3D view of the pedestrian to avoid the collision.
6. Vehicle to network: An autonomous vehicle can be connected to the nearest tower, WIFI, or 5G.
7. Satellite communication: It helps an automated vehicle to locate its location using GPS.

Within the CAV architecture data is transmitted between in-vehicle, vehicle-to-vehicle, and vehicle to everything, to improve overall security and traffic efficiency. This approach relies on modern protocols and communication models to perform seamless communication. However, the CAV model is dynamic, with the new trends and research it changes. Another obstacle in autonomous vehicles is the lack of industry-wide safety standards. The security measures are not uniform on the industry level due to multiple manufacturers. Some manufacturers like Tesla and Ford have introduced new features like auto parking, track control systems, adaptive cruise control, lane departure warning systems, etc, despite all these still vulnerabilities are there. There is a need for uniform security standards on the industrial level to reduce the risks. Cyber security measures must be funded and research must be continued.

The focus of this paper is to highlight the security challenges of communication models layer by layer. In Fig 3, a layers approach of autonomous vehicles (AV) is shown. This paper will focus on four layers without discussing its hardware and software faults. The dependency of AV on its communication model make it more sensitive for attacks so we focus on vulnerable openings within these layers and possible attacks that could be done via wired or wireless communication.

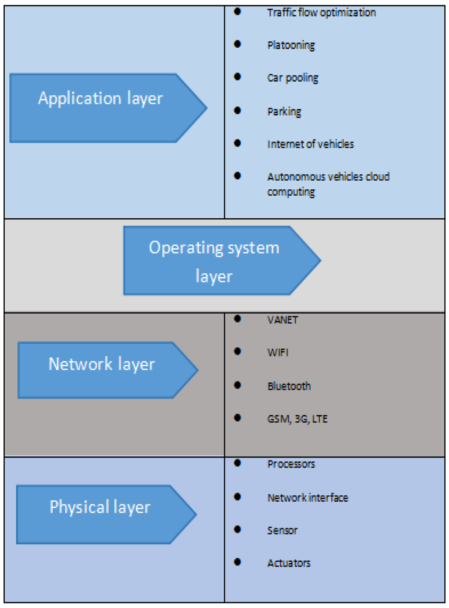

Figure 3. AV Layers

2. Literature Review

2.1. Related Survey

The advancement of automotive technology leads to the rapid manufacturing of autonomous vehicles. This approach have enhanced the need of security framework to encounter security threats. In the last five years of research, immense work can be seen on autonomous vehicles. Most of the surveys revolves around cyber-attack, environmental facts and its defensive techniques. In [7], M.Hataba et al, have Surveyed security challenges and privacy concerns in autonomous vehicles. They used Layer-based approach to examine security challenges and Survey of security and privacy attacks with countermeasures. Tanvi Garg et al. [8] have mentioned Security and privacy issues in IOV architecture comprehensively. Layered security model implemented for secure communication in IOV. Security and privacy challenges addressed in VANET through layer-based survey. This Survey covers message, vehicle, and network security and privacy. [9] Multiple surveys with different aspects have conducted like survey on 5G vehicles [10], on adhoc networks [11], security issues in sustainable cities [12]. Thai Hung Nguyen et al, [13] surveyed Privacy and data protection challenges in autonomous vehicle systems. Lack of knowledge on data usage and potential privacy risks. M Sameer sheikh et al, [14] have surveyed the security challenges on vehicular cloud computing .

2.2. Security Issues in Vehicular Network

Azeem Hafeez [15] highlighted the importance of securing vehicles against cyber-attacks and unauthorized access, proposing a solution that combines hardware and software components for enhanced security. In another paper Azeem hafeez et al, [16] suggests using the unique frequency response of engine control units (ECUs) to authenticate CAN nodes, enhancing in-vehicle communication security.

In [4], Takahito yoshizawa et al, have conducted a survey that addresses privacy and security of Vehicle to everything (V2X) communication systems. Recommendations provided for improving safety and security in vehicular communication. Another survey have focused on security, privacy challenges in autonomous vehicles, discussed attack detection, prevention systems and research gaps in ADPS [17]. CAN bus lacks authentication and encryption, making CAVs vulnerable and Attackers can remotely access ECUs to broadcast forged messages. B Veera Jyothi et al, in [18] have discussed security concerns of VANET of driver and passengers. They have included the challenges like availability, authentication, privacy, data verification and key management. Another relevant survey was conducted by DA Alex et al, [19] in which they have discussed the compromised security aspects of VANET.

2.3. Security Solutions Based on Cryptographic Approach

Cryptographic approach plays an important role in protecting and securing data. Cryptographic solutions are being presented in some research papers. Kurunandan Jain [20] covered RC6, AES, and DES used in blockchain for data security. He proposed that Cryptographic algorithms enhance data privacy in blockchain storage systems [21-23].

Table 1. An Overview OF PREVIOUS research Approach

Focus area	year	Ref	Strength
Layered based approach of AV	2022	[1]	Discussed the security challenges on each layer.
Security and privacy issues in IOV	2020	[2]	Layered security model implemented for secure communication in IOV
VANET	2021	[3]	Security and privacy challenges in VANET
5G vehicles	2019	[4]	Elaborate issues of the 5G vehicles
Adhoc networks	2013	[5]	Security aspects of adhoc network
Security issues in sustainable cities	2022	[6]	AV security issues in sustainable cities.
Data protection in AV	2022	[7]	Data protection and privacy issues in autonomous vehicles
vehicular cloud computing	2020	[8]	Security challenges in vehicular cloud computing
In- vehicular security	2020,2018	[9][10]	Importance of securing vehicles, suggests the unique frequency response of engine control units (ECUs) to authenticate CAN nodes
V2X communication	2023	[11]	Recommendations provided for improving safety and security in vehicular communication.
VANET	2023	[13]	Challenges like availability, authentication, privacy, data verification and key management
VANET	2023	[14]	Discussed the compromised security aspects of VANET.
Cryptographic solutions	2022	[15]	Proposed that Cryptographic algorithms enhance data privacy in blockchain storage systems
Cryptographic solutions	2021,2012	[16][17]	proposed cyprographic approach as a security solution
Cryptographic solutions	2021	[18]	Presented symmetric key cryptographic technique
Machine learning	2023	[19]	Discussed the reasons of spoofing attack with ML solution.
Machine learning	2022	[20]	Proposed machine learning solution for IDS
Machine learning	2020	[21]	Presented the idea of nearest-neighbor machine translation, which enhances translation models by predicting tokens using a nearest neighbor classifier over a large data

			store of cached examples, without requiring additional training.
Importance of Forensical aspect in AV	2022	[22]	Focused on the forensics data analysis of CAV

2.4. Security Solutions Based on Machine Learning Approach

Farzan Majeed Noori et al, [24] elaborate the vulnerability of CAN protocol that make it prone to spoofing attack. They proposed method using DAC errors for ECU identification enhances security. Likewise RUD Refat et al, [25] proposed machine learning solution for IDS. Urvashi Khandelwal et al, [26] presented the idea of nearest-neighbor machine translation, which enhances translation models by predicting tokens using a nearest neighbor classifier over a large data store of cached examples, without requiring additional training.

2.5. Forensical Data Analysis on Autonomous Vehicles

Some research papers have covered the importance of Forensical data analysis using different techniques to inquire the reason of accidents, fraudulent activities and data alterations. M Girdhar et al, have focused on the forensics data analysis of CAV[27]. J Repas et al, [20] focuses on data acquisition, analysis, and reporting. They emphasis the need of new tools, techniques, approached to collect and process data.

2.6. Need of layered based approach

The modern vehicles have more advanced and sophisticated architecture. To protect that sophisticated architecture a coordinated and systematic framework is needed to be designed. In literature we found the lack of layered security framework. The contribution of this paper is to cover all the aspects of security with layered approach. Layer by layer the challenges and security solutions will be highlighted. We hope a big picture of challenges and solution will develop for the ease of understanding the AV technologies, its security risks and possible solutions. Interventionary studies involving animals or humans, and other studies that require ethical approval, must list the authority that provided approval and the corresponding ethical approval code.

3. Security aspects of AV in Multi layers

Vehicle to vehicle communication, vehicle to infrastructure communication, vehicle to everything communication is the backbone of driver-less cars. This high dependency of communication make it vulnerable of cyber-attacks. Day by day the vehicles are updating and becoming more sophisticated. This approach leads to discussion of layered model to discuss the possible attacks of each layer and how to encounter those attacks specifically. In fig 1, we have already given an overview of layered approach of autonomous vehicles. According to figure the communication layers of autonomous vehicles are divided into four layers. Application layer, operating system layer, network layer and physical layer. Each layer have specific functionalities that needs to be protected for the normal performance of autonomous vehicles.

3.1. Application layer

Research have revolutionized the new application to make the working of AV better. Some applications have existed before, some have added new features to the automation. With the new development new possibilities of security risks have come. Some of the major task of application layer include parking, automated charging, IOV (internet of vehicles), sensor data gathering, crash prevention, entertainment, carpooling, forensics, platooning, navigation, efficient routing and traffic management. Here we have highlighted the primary working areas of application layers, security threats to them and an overview of the work to secure them.

3.1.1. Parking

Parking is a global issue in major cities worldwide. Due to increase in vehicular density it’s not easy to find feasible parking spot especially during public events and holidays. To find a suitable parking spot may take lots of time, extra fuel consumption, efforts, more it can put a burden on already crowded streets. There are some big tech giants like IBM, that are not directly involved in car manufacturing but they provide some solutions that helps to park automatically. These tech giants provides an algorithm that deals with steering, breaks and transmission control whereas autonomous vehicle companies are still developing the ways to deal with physical control issues of parking.

Automatic parking seems an excellent idea where you can command your vehicle to park itself by finding a suitable spot, after you are done with your work it picks you up. To implement this ideal situation the parking lots and cars should be synced. An efficient system is required to tell your vehicle where to find a suitable parking spot.

But now, how can you trust that your car will not be stolen during this process? An attacker may remotely access your vehicle by launching man-in-the-middle attack. The attacker can gain access by compromising the authentication between your smart phone and AV. He can start your vehicle by gaining access. The next problem is how can you trust that your location privacy is secure? The attacker may try to find a person's location by penetrating its cars system. It may involve other adversaries that follow a specific person, intercept its messages and gain access of its vehicle. Another concern is what if an attacker pretends to be honest and legitimate person, that get connects to your system, to steal your location and vehicle? After gaining access He may pretends to be you by commanding your vehicle to reach a specific spot, with this act he could even defame parking lot. Due to all these reasons researchers have proposed authentication protocols to address the security concerns of parking problems.

D Wang et al, [28] addresses the long range autonomous valet parking by proposed three way authentication and key agreement protocol named as secLAVP. The protocol helps to mitigate the risk like dictionary attacks, drop off/ pickups points and parking insecurities. C Huang et al, [29] addresses the problem of double reservation attacks in parking of AV. They discussed the privacy of identity challenges when a vehicle sends repetitive parking requests, it may reveal the information of person or vehicle. To counter this challenge they proposed privacy preserving preservation scheme that ensure that one user have one reservation token at a time. A Aggarwal et al, [30] addresses the attacks like spoofing GPS signal, DOS attack, sniffing by proposing block chain and decentralized system. Another block chain model using artificial intelligence is proposed by SK Kim et al, [30] that helps to encounter potential hacking threats. Y Koh et al, [31] proposed IPS and IDS using ML and deep learning.

Yan Zhang et al, [21] have proposed a secure parking protocols for VANET using block chain. Their proposed protocol claims to tackle parking vulnerabilities by ensuring authentication, message confidentiality and privacy preservation. The protocol secure vehicle from false parking spots and multi reservation attacks. Kale Poorna et al, [32] presents vehicle security operations during parking, they proposed uses camera, sensor and artificial neural network to detect the object in the surrounding of vehicle for efficient parking. GA Francia highlighted the importance of developing security matrices of connected vehicles through qualitative and quantitative measures. The paper illustrated the applicable security metrics with multiple aspects including parking security[33]. H Alfehaid et al, [34] discussed the cyber-attacks that targets the security of the location and identity of vehicle. They emphasis the importance of detecting and preventing those attacks for the safety of human and vehicle.

3.1.2. *Automated charging*

Electric vehicles are picking up the market shares and capturing the attention. The vision to deploy hybrid cars is to save fuel consumption and environment friendly vehicles. Now the need of fuel is shifted towards the charging of automated cars. So far the electric vehicles relies on plugged charging. But now wireless charging are appealing drivers due to its more convenient approach. The charging of vehicle needs two basic units, one unit in the body of vehicle, second external unit may be deployed in garage or anywhere else. As soon as you park your car the smart charging system will get connected to the car.

Open charge point protocol (OCPP) is a communication protocol that is used in electric vehicles for smart charging. The latest version of this protocol was released in 2020 which is OCPP 2.0.1.

It creates open platform for communicate between electric vehicle charging station and charging station management system as illustrated in figure 2. It is a cloud based service managed by the charging station company. With electric vehicle owner perspective it locate charging station schedule slot, easy payment, invoice and reimbursement. From charging station owner perspective it monitors entire charging network with the help of web based applications, real time charging data access, manage authorization of users, runs diagnostic checks, helps to manage power, firmware updates and charging cost management. Despite of its lots of benefits the OCPP is found with some vulnerabilities that opens the door for attackers to penetrate in the car system. The OCPP is more susceptible of man in the middle attack in which attacker can interrupt the connection between charging vehicle and central server, leads to the theft of vehicle credentials and transaction details. W Terrance et al, [35] discussed the potential vulnerabilities of OCPP including man in the middle attack. K Gandhi et al, [36] highlighted how the hacker can use charging station points and OCPP to conduct attacks on micro grids. The vulnerabilities and security challenges of OCPP are mentioned by Z Garoflaki et al, [37] they identify lack of security features in smart charging. They have suggested some solutions to those threats with some future direction to work on those open challenges. B Vaidya et al, [38] have proposed digital signature to secure communication between charging point and protocol. They haven't specified the protocol they just focused on the importance of security measures during charging. K Kirihara et al, [39] emphasis that the architecture of protocol cannot provide quick response, they also mentioned the lack of sufficient control for large and small disturbance. They proposed a model in paper that predict control and provide integrity protection in the architecture. SY Mattepu et al, [40] have mentioned the importance of simulator like OCSS that can help managing the charging station infrastructure effectively, it will also highlight the limitation of the infrastructure management. S Deniz mentioned the need of formal standards development for OCPP so that across the world those standards of security and development should be followed [41].

PROTOCOL
FOR
COMMUNICATION
OCPP
Electric vehicle charging stations
Charging Station Management System

Figure 4. Working of OCPP

3.1.3. Sensor data gathering

Self-driving vehicles uses sensor to navigate without human intentions. Sensors plays an important role in the working of autonomous vehicles. The real time decisions are made on the basis of data gathered by the sensors. Sensors helps to handle vehicles on the weather or conditions that are out of the bound of human capability like driving in a sunny day is easy but to drive in rain or dense fog is challenging and risky in case of zero automation. The sensors that helps the AV are Lidar, camera, and radar. Lidar is a laser sensor used to measure the distance of other vehicle, camera is a well-known passive sensor that can be extended into infrared or night vision, and the radar is an active sensor use waveform to detect moving objects in the surrounding of vehicle. These all sensors collect data of huge amount, in Terabytes per hour to make real time decisions. Every sensor have its limitation, depends on the weather or environment conditions. So the concept of sensor fusion is used to optimize the performance. Like shown in fig 5.

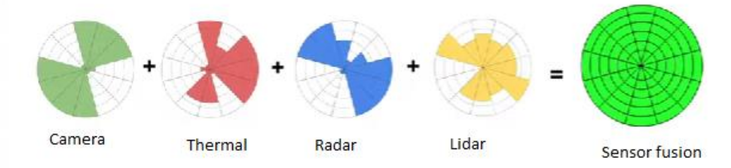

Figure 5. Sensor fusion

The high dependency of AV on sensors makes it more crucial for security aspect. A bit of change in gathered data can leads to serious consequences. These sensors are prone to spoofing attack, jamming attack, blinding attack and relay attack. Jamming attack aims to generate ultrasonic noise that make the sensor fail to detect object and it may collapse. Spoofing attack is carefully crafted to deceive vehicle, in which attacker will change the data gathered by the sensor like distance measurement. Blinding attack aims to put unnecessary optical inputs to produce unrecognizable images.

Lidar plays an important role to detect obstacles, the change in the information can change the prediction of Lidar to misguide the vehicle. Lidar is known as an expensive yet not safe feature of AV, like in case of intense weather like snow, heavy rain the working of Lidar can be effected. SHV Bhupathiraju et al, [42] exposed the vulnerabilities of Lidar, they focused on electromagnetic interference attacks. The research illustrates that these vulnerabilities may lead to the misclassification of objects and the false perception of obstacles, consequently reducing the classification accuracy to less than 50% across different autonomous vehicle perception components. Furthermore, the article assesses the influence of IEMI injection on fusion algorithms and suggests methods for identifying signal injection as possible preventive actions. X Jin et al, [43] authors recognize the emphasis placed in the paper on the resilience and dependability of the recognition framework. Nevertheless, they underscore the necessity for forthcoming research aimed at enhancing the real-time efficiency and precision of the framework in practical vehicular applications. This suggests that, although the existing framework exhibits potential, additional refinement and experimentation in realistic scenarios are warranty. T Liu et al, [44] have mentioned the limitation of Lidar in his paper, they mentioned the lack of description of feature points and the assumption of uniform motion. Another limitation mentioned in the paper is the need of ego motion estimation. They emphasis the importance of developing more smart solutions like deep learning to improve accuracy and reduce mismatch ratio over long distance predictions. J Taher et al, [45] discussed the single wavelength Lidar sensor vulnerabilities based on material spectral properties due to their monochromatic operation. This limitation can lead to challenges in proper classification of objects in varying road environment. They proposed the usage of hyperspectral signal to enhance the accuracy during low photon flux. By using hyperspectral signal the ability of robotics perception can be improved that will make it less vulnerable than traditional Lidar. Research of DJ Zea et al, [3] based on evaluation of reliability of Lidar with the help of geometric model, they focused on the angel and distance accuracy of Lidar detection. The paper have mentioned the importance of Lidar accuracy for that purpose they have proposed sensor integration and geometric modelling approach. Y Cao et al, [46] highlighted the physical removal attack. The misidentification of obstacle by Lidar involves the removal of Lidar cloud data of actual obstacle. The failure of detection can be dangerous. The study emphasis the effectiveness of PRA to achieve high accuracy rate via fusion model. X Sun et al, [47] writes that the compression techniques of Lidar data results in rate distortion optimization and some task requirements of autonomous robots. Another limitation is bandwidth intense nature of transmitting large scale Lidar point clouds. There is need of more efficient coding framework that consider both task driven and semantic information for AV. C Vishnu et al, [48] have mentioned the vanishing adversarial attack, that deceive lidar by adding noise. They demonstrate that semantic segmentation of point clouds are not reliable always, they proposed EVAA which has high success rate to encounter this attack.

A significant security challenge is attack on camera system of AV as it helps to preceive to make run time decision. The combination of camera and lidar helps the vehicle to generate 3D object detection with multi sensor fusion (MSF), however this model is not immune to attack. The attack can reduce the detection performance of perception. [49] A computationally expensive approach is the use of deep neural network model with camera images. A multi-level framework is proposed to monitor attacker's capability, the framework introduced a binary decision attack strategy to enhance effectiveness. [50]

Y Man et al, [51] discussed the remote perception attack on object detection and recognition systems. The attackers can add adversarial patterns to create false image of object, this attack leads to the false recognition or no recognition of object that can make vehicle to take wrong decision. Their study have demonstrated such sorts of attacks using cameras and also have proposed countermeasures. O Adeboye et al, [52] have introduced the concept of LIFT (location inference attack),it exploits the location privacy. The research assesses the effectiveness of LIFT on Google Street-view data and altered images, revealing a 20% enhancement in localization precision in comparison to standard methods.

3.1.4. Infotainment system

Now the cars have lots more than just entertainment from AM radio to AI infotainment system is the evolution. We cannot imagine to travel anywhere without GPS, WiFi, videos and music. It all started with AM radios, in 1981 on board navigation system was introduced in Japan by Toyota. In 1990 Mazda introduces the first GPS system for automotive navigation, by the 90's digital data made its way into cars on compact disks. Bluetooth came into demand by 2006, and USB ports made their appearance to store and play mp3. The first infotainment system was emerged into 2000s with touch screen to play music or to get GPS assistance. Today we have advanced infotainment systems to enjoy traveling experience with lots of options. The mass adoption of smart phones and connected vehicles that leverage IOT and AI technology have paved the ways for android based infotainment systems. The next level of disruption is infotainment system technology. Manufacturers have brought whole new level of connectivity and intelligence system with the power of android. Lots of security threats are there that can breach infotainment system cause misleading to vehicle and humans. To ensure safety and reliability there are some unique vulnerabilities in infotainment systems that need to be addressed. Commonly used protocol like control area network lack authentication and encryption that make it susceptible to remote control attacks. G Aravind et al, [53] have mentioned in their research paper about the CAN protocol vulnerabilities. C Wienrich et al, [5] highlighted the need of further research and evaluation of VR entertainment systems, previously VR systems have showed good results in terms of user experience but there are challenges when this system integrated with autonomous vehicles.

3.1.5. Traffic flow management

To ensure maximum road utilization traffic is directed towards the road with network to minimize traffic congestion and travel time, the focus is on the traffic message communicated by the car on network. It can have multiple vulnerabilities on network level. The threats to the security and privacy of traffic flow management system are sybil attacks, data integrity concern and privacy of route. The data integrity is more susceptible to sybil attack, man in the middle attack and repudiations attack.

A Afdhal et al, [54] addresses the causes of sybil attacks in which the attacker can disrupt communication by creating fake nodes. This paper have proposed the realistic approach on traffic model that implement detection based approach and mitigate sybil attack in traffic flow system.

In a research DD Dun et al, [55] have mentioned that how semi-automated vehicles can be destabilized by the attackers to cause traffic flow instability. The attacker can use the errors to cause traffic jam, delay, and discomfort and increase accidental risks.

I Gokasar et al, [56] have proposed the utilization of V2V, V2X technologies to manage traffic, this alternative approach is named as SWSCAV. This approach will help to reduce congestion as compared to lane control system and variable speed limits. J Ivanchev et al, [57] have discussed the mixed traffic challenge approach in which human and vehicles are involved. They proposed agent based simulation to design a scenario, they adopt multi objective optimization approach to analyze comfort, speed, safety and efficiency to maximize objective function. P Galantai et al, [58] have discussed the dangerous situations of traffic in AV focusing on the vulnerabilities of adaptive cruise control systems. The ACC system may face problems while dealing with static object, driving in curves, lane change. The tracking perception of vehicle will decrease by 50%. They emphasis the usage of camera and radars to enhance accuracy.

3.1.6. Platooning

Platooning of autonomous vehicles is defined as a group of cars in cluster that are closely connected in close range to maintain traffic flow. Platooning eliminate the human involvement during heavy traffic flow on road that improves fuel consumption, better road space utilization, and traffic flow management. The vehicle RF technology is IEEE 802.11p, platoon members communicate via this protocol. The malicious activities that can alter the normal operation of platooning is the integrity of traffic flow message and communication interruption of platoon application.

T Yang et al, [59] highlighted platooning attacks in AV that are closely coupled. With the manipulation of cooperative adaptive cruise control the entire platoon propagation data can be corrupted leading to collusion and traffic delays. The paper proposed a a co-design methodology for the synthesis of distributed attack monitors and controllers, with the objective of reducing the effects of stealthy False Data Injection (FDI) attacks and system disturbances on platoon dynamics, while also guaranteeing the specified performance levels. This strategy is geared towards fortifying the resilience of Connected and Automated Vehicles (CAVs) against attacks targeted at platooning systems. X Ge et al, [60] addresses the issue of denial of service against safe platooning and resilient in vehicle to vehicle communication. They present distr5ibuted longitudinal platooning control law to ensure platoon safety, scalability, attack resilience and stability. The focus of the research is on a method development to encounter DOS attack while maintaining safety, scalability requirements. Another similar research is done by X Zang et al, [61] in which they proposed solution against DOS attack of wireless network connection of AV. The proposed solution include the detection of communication disrupts, to mitigate the impact of DOS attacks on platooning. F Li et al, [62] addresses the platooning attack by proposing human robot interaction framework to enhance security. During emergencies they introduced and observer based control strategy that helps in human supervision to encounter vehicle to vehicle cyber-attack. This system has an anomaly reporting system, trust based information management system and GUI. By conducting simulations and experiments involving human participation, the framework showcases a notable decrease in platoon susceptibility and the cognitive load on individuals in contrast to conventional surveillance techniques. The study of S Xiao et al, [63] investigated the secure distributed adaptive platooning control through ad-hoc networks to encounter DOS attacks on AV. They presented a validate data packet with time stamp to identify DOS attack. They also suggested neural network based approach to achieve secure platooning. M Maleki et al, [64] investigated the impact of jamming, the study shows that the usage of ComFASE and veins, three forms of jamming barrage jamming, destructive interfaces and deceptive jamming were replicated on IEEE 802.11p protocol. The findings suggest that these attacks have the potential to compromise the safety of vehicles, resulting in events of sudden braking and collisions. The research underscores the importance of taking into account a variety of attack parameters, including the initiation time,intensity and duration, when evaluating the repercussions on the behavior of vehicles within platoons. S Ucar et al, [65] demonstrate that platooning attacks in AV involve security vulnerabilities such as channel overhearing, data packet injection, jamming, and fake packet transmission by malicious entities.in research paper they suggested A hybrid security protocol named SP-VLC, which enhance the security of platoon communication with IEEE 802.11p and Visible Light Communication (VLC).SP-VLC aims to establish secret keys, identify jamming, authenticate messages and ensure platooning scheme.

The study demonstrates through simulations that SP-VLC effectively reduces speed and distance disruptions among platoon members in the event of security attacks when compared to previously suggested protocols, ultimately guaranteeing a stable and secure autonomous platooning environment.

3.1.7. Carpooling

In the last decade ride sharing system also known as carpooling have introduced in which multiple individual share ride to reach a common destination. Carpooling concept is environment friendly as it lessened the burden on roads. C Vitale et al, [66] employs Multi-Radio Access Technology (Multi-RAT) for facilitating Vehicle-to-Everything (V2X) communication infrastructure, thereby augmenting security and privacy via innovative Machine Learning algorithms integrated within the On-Board Unit (OBU) and the Multi-access Edge Computing (MEC) platform. A cryptographic system known as Public Key Infrastructure (PKI) is utilized for the registration and authorization of all vehicles' data transmissions, intervening in instances where anomalies are identified by updating or modifying the various elements of the CARAMEL framework.

F Zafar et al, [2] highlighted the challenges of carpooling like security, privacy, communication, time scheduling and business model. They also mentioned the lack of research and future directions in this specific area. J Yang et al, [6] focuses on the limitations that causes GPS spoofing attacks on AV fleet, error in perceived location of vehicles can cause incomplete trips, trust issues, and time delays. The study also present an awareness of the impact of GPS spoofing attacks with different spoofing capabilities. M Kamal et al, [67] found the susceptibilities in AV that can be exploited by adversaries. They include the GPS positioning, message transmission and vehicle on board unit. The article represents how to mitigate these vulnerabilities using CARAMEL with security algorithms.

3.1.8. Internet of vehicles

Another aspect of autonomous vehicles that is of worth discussion here is internet of things, commonly known as internet of vehicles. This application is equipped with all sort of sensors that gather all sort of data from the surrounding and environment. These sensors include internal sensors of vehicle like seat position, temperature maintenance, voice capture and recognize, breaks organizer, accelerator and steering control, external sensors like Lidar, camera, GPS etc. The difference in IOT and IOV is that IOV is mobile network. IOV doesn't shift all of its data on network. Mostly decisions are to be made on the basis of collected data on runtime. This continuous information flow creates privacy and security threats to the moving vehicle. The major security threats to IOV are the user’s privacy may be compromised, location spoofing, identity theft and replay attack.

H Taslimasa et al, [68] Discussed the vulnerabilities of Internet of Vehicles (IoV) encompass security risks within both Intra-Vehicle and Inter-Vehicle communications. Intra-Vehicle communication vulnerabilities manifest due to the utilization of diverse network protocols that link sensors and Electronic Control Units (ECUs), potentially enabling malevolent actors to disrupt their operations. Inter-Vehicle communication vulnerabilities arise from active communication among vehicles and infrastructure, thereby creating avenues for unauthorized access. These vulnerabilities present risks to the confidentiality, integrity, availability, and authenticity of IoV systems, underscoring the necessity for the development of

Intrusion Detection Systems (IDS) to identify and address malicious behaviors. Z Cui et al, [69] noted that the vulnerabilities IOV (inherent in the Internet of Vehicles) encompass cyber security risks that nodes may encounter within the realm of Intelligent Transportation System (ITS),it may include cyber security risks associated with Connected and Automated Vehicles (CAVs) and risks related to IoV communications. The spread of malicious information resulting from cyber-attacks has the potential to security risks across IoV communication networks, it gave rise to significant security challenges within the transportation infrastructure. The research explores the propagation and regulation of malicious information within IoV communication networks, emphasis on the importance of mitigating these vulnerabilities to safeguard the security of IoV environments. W Wei et al, [70] explores the vulnerabilities inherent in the networks of Internet of Vehicles (IoV) starts from the potential harm that can be caused to nodes and channels as a result of dynamic environmental conditions and malfunctions. To encounter this problem the study suggests the utilization of Fractional Critical Deleted Graph (FCDG) as a Fractional Factor (FF) within IoV networks for stability and dependable connectivity in scenarios where segments of the network are damaged. Recognizing the correlation between toughness and FCDG is essential in preserving the robustness of the network. This feasibility analysis aids in the repairing of broken links, which are essential for continuous connectivity in the upcoming era of advanced transportation systems.

J Wang et al, [71] explores the vulnerabilities of Internet of Vehicles (IoV) such as hardware tampering, message manipulation, illegal data access and the tracking of vehicle locations. The authentication protocols currently utilized in IoV networks often demonstrate weaknesses such as link-ability, server impersonation, and replay attacks, consequently compromising the security requirements. The study proposed a multi-server-based authentication and key agreement protocol (SeMAV) for IoV, incorporating passwords and smart cards to secure private keys. This protocol is designed to address these vulnerabilities and has shown results against common attacks through both formal and informal security validations, thereby enhancing the security of IoV networks.the security vulnerabilities of IOV are highlighted by T Christensen et al, [72],he concentrated on security risks, particularly Distributed Denial of Service (DDoS) attacks carried out via botnets.As vehicles becoming more interconnected his research emphasizes the importance of addressing these security barriers . Despite the progress made in IoV technologies like collaborative schemes and online learning algorithms the insufficient attention is given to botnet and DDoS attack, study presents a notable threat to IoV users on a global scale. If these vulnerabilities are not addressed, the Internet of Things environment may suffer grave safety consequences.

R Sedar et al, [72] mentions the vulnerabilities inherent in Internet-of-Vehicles (IoV) systems are primarily rooted in their openness to multi-domain denial-of-service (DoS) attacks. These malicious activities have the capability to disturb regular operations by inducing network unavailability, thereby preventing legitimate vehicles' access to essential services. The research carries out a comprehensive evaluation of the vulnerabilities present in 5G-enabled IoV systems in the face of various DoS attack forms. Furthermore, it evaluates how well an authentication method designed for the IOT (Internet of Things) can mitigate these kinds of attacks and presents a data centric detection approach to prevent DOS threats in the radio access network. In conclusion, the study emphasizes how urgently these vulnerabilities must be fixed in order to protect the security and dependability of IoV systems.

B Asher et al, [73] stated that security issues resulting from Vehicle Ad Hoc Networks (VANETs) open-access features are the main reason of the Internet of Vehicles (IoV) vulnerabilities. Due to its susceptibility to security and confidentiality issues, VANETs may have an effect on how vehicles distribute messages. To address these weaknesses, research has focused on improving the communication security of VANET by investigating well-established methods. It further explores the components of VANET and evaluates earlier research attempts to address these issues. Therefore, the primary weaknesses of IoV stem from the security and confidentiality risks brought about by VANETs open-access design. S Liu et al, [74] investigated the problems related to high connectivity and the integrity of critical areas, that are the foundation of the Internet of Vehicles (IoV) vulnerabilities. The critical sections of the framework are often overlooked by current approaches, which could lead to potential failures that have a significant influence on the system's operational efficiency and connection. To address this issue, this research paper presents an advanced vulnerability assessment method that focuses on the integrity and dynamic connection of key locations. This technique uses spectral partitioning to identify the most economically reliable set of components whose failure could seriously impair the system's essential areas and connectivity. Within the IoV architecture, this tactic successfully reduces significant losses in system performance and connection.

S Arthi et al, [75] explains the Vulnerabilities of the Internet of Vehicles (IoV) including the transfer of unknown or compromised data, which may result in security breaches. These vulnerabilities results in problems like data integrity compromise, collisions, and improper traffic management. This paper recommends the use of trust-based solutions to address these issues by attempting to provide secure communication between the nodes in the vehicular network. The Internet of Vehicles (IoV) can provide a more reliable environment for data sharing by using trust administration models, which can reduce end-to-end delays and false positive rates. Building trust between the many parties in the network is crucial to successfully reducing the risks in the Internet of Vehicles. A major concern is the reliability on wireless networks to access cloud resources, which are often considered unreliable for the applications that need to operate in real time, endangering the timely completion of critical calculations that are necessary to guarantee the security of autonomous vehicles.[76]. A Masood et al, [77] cloud computing in AV (autonomous vehicles) is vulnerable because of irregular wireless communications, high mobility of vehicles, rapid resource scalability combined with decentralized operations and security and privacy issues brought on by multi-tenancy cloud environments. These vulnerabilities could lead to security threats at many layers, including as the vehicular cloud layer, the vehicle-to-everything (V2X) network layer, and the physical resource layer, which can influence the system's overall security. Effectively addressing these vulnerabilities are essential to ensure the safe and secure operation of cloud-computing enabled autonomous cars.

3.1.9. Autonomous vehicles cloud computing

Cloud computing make the computation more easy and powerful. New features demands more computation power with more memory, powerful processor and storage capacity. The aim of autonomous vehicle cloud computing (AVCC) is to provide computing services as a utility. Cloud computing facilitate the user to avail already designed services like Software as a service, platform as a service, infrastructure as a service etc. without deploying setups of their own. These services provides users with the facilities that are physically out of reach. It operates remotely with different scenarios. All the scenarios share common security threats. The data passing through the network is supposed to be integral, confidential and available. The security demands make the AVCC more challenging as the vehicle is not stationary, it will change its position continuously and will interact with multiple network devices and servers. The data moving on cloud is encrypted and decrypted continuously. For security aspect rely on cloud server is not sufficient as it can open new surface of attack. J Kang et al, [77] the article examines the difficulties related to managing, safeguarding, and ensuring reliability in vehicular cloud (v-cloud) systems for autonomous vehicles. Vulnerabilities in cloud computing for autonomous vehicles arise from the dynamic and diverse nature of the vehicles, which can result in challenges when designing v-cloud structures, establishing efficient routing protocols, safeguarding v-cloud environments, and improving v-cloud dependability. These vulnerabilities emerge from the intricate interactions and communication among autonomous vehicles within the v-cloud system, necessitating strong security measures and reliable protocols to address potential risks.

M Hataba et al, [78] examines the improvement of software protection within Autonomous Vehicular Cloud Computing (AVCC) platforms, with a specific focus on addressing security issues like timing side-channel attacks that aim to disclose information on the execution of code. The proposed method involves the introducing encrypted compilation at the compiler level. While the article does not specifically address cloud computing vulnerabilities in autonomous vehicles, it more emphasizes how important it is to secure programs running on AVCC in order to lessen security risks, such as timing side-channel attacks. In another research M Hataba et al, [79] proposed a technique to address security concerns with software used in Autonomous Vehicular Cloud Computing (AVCC). The goal is to secure AVCC software by using dynamic encrypted compilation to obstruct program execution paths and stop side-channel assaults from leaking confidential information. By adding time differences in code execution this method aims to solve weaknesses in cloud computing for autonomous vehicles and maybe prevent side-channel attacks. Thus by safeguarding software through dynamic encrypted compilation, the study's suggested software protection method seeks to improve the security of cloud computing in autonomous vehicles.

4. Operating system layer

Unlike of traditional operating system the operating system of autonomous vehicles is very challenging to design. It is like a data center that is connected with multiple entities via network to perform different tasks. In autonomous vehicles ECU's (electronic control units) are the brain, they are in multiple numbers that differ in size, tasks they handle and OS of their own. Tasks ECU handle are control steering wheel, tracking system, radio navigation system, advanced front light system, automatic gear level indicator, safe sunroof shade, intelligent LED back light, dual battery management control etc.

QNX neutrino is the master OS for AV. It runs all the processes in time frame needs for the safe execution of automation. This OS platform is owned by blueberry. QNX is already in partnership with 40 AV manufacturers like Ford, BMW, Acura and Audi.

Linus is also a popular OS in autonomous vehicles, car manufacturers like BMW, Tesla, Mercedes, Honda use Linux as an OS for their vehicles. The Linux foundation based on automotive grade Linux that helps to secure the OS. Likewise android automotive OS, apple car play, ROS (robotic OS), Microsoft are also providing services for the AV. Due to continuous progress the OS have secured remarkable advancement in AV. In recent X86 based software are contributing significantly in performing functions of AV. However the vulnerability like malware attack, interruption in cloud based protection, alteration of Machine learning protocols of OS can lead to the disability of AV components that can impair vehicle performance.

Out of the various standards X86 based software contributes significantly in driving safely. However the security risks of these software's can impair the AV performance. The safety and operation of autonomous vehicles (AVs) are seriously threatened by malware assaults on X86-based autonomous systems. These systems are especially susceptible to cyberattacks since they mostly rely on networked electronic control units and complex software. Because of the real-time demands and resource limitations of antivirus programs, traditional malware detection techniques like static and dynamic analysis encounter difficulties in this field.

S Aurangzeb et al, [80] studied malicious software assaults pose a serious risk to autonomous systems, particularly autonomous cars in smart cities, as they can cause power outages and communication delays. To guarantee safe transportation the research paper explores the need of real-time detection in Intelligent Transport Systems (ITS). By combining static and dynamic analysis it offers a hybrid approach that successfully detects malicious software in smart city settings. This method addresses zero-day attack challenges and resource consumption. The suggested methodology focuses on real-time malware identification with the goal of strengthening autonomous vehicle cyber security against threats in smart city environments. The study offers an autonomous vehicle cloud computing (AVCC) safeguarding software approach in order to combat security vulnerabilities. This strategy reduced vulnerabilities in cloud computing for AV (autonomous vehicles) by introducing timing variations in code execution to prevent potential side-channel attacks. The proposed mechanism in this paper seeks to enhance the security of cloud computing for autonomous vehicles by safeguarding software via dynamic blur compilation. S Jha et al, [81] in their paper revolves around machine learning-based malicious software that targets the safety of antivirus systems, presenting a sophisticated malware named RoboTack that strategically disrupts normal working in self-driving vehicles. This malicious software is designed to deceive the decision-making process of autonomous vehicles by inducing safety risks like collisions by tampering with sensor information. The research highlighted the significance of addressing vulnerabilities in automated systems to prevent disastrous incidents triggered by cyber-attacks. The investigation's overall highlights how important it is to strengthen the security standards of systems for self-driving cars in order to reduce the risks associated with sophisticated malware that targets these vehicles. PJ Bonczek et al, [82] investigates cyberattacks that aim against self-governing systems that focus on virus assaults that alter controller configurations or generate unique responses.

Dangerous circumstances like losing control and being hijacked could be the result of these attacks. The suggested action is real-time monitoring that compares anticipated and actual readings to identify discrepancies. To mitigate these effects of malicious activity a recovery strategy that modifies the status vector and reference signal is also proposed. The goal of this approach is to ensure that autonomous systems will function dependably even in the case of cyberattacks against the onboard controller. M EI Mouhib et al, [83] uses stochastic modeling in their study to simulate the behavior of connected and autonomous cars when they are infected with malware which is influenced by epidemiology. It aims to fix security problems that arise with larger systems. The study uses modified processes to simulate the autonomous vehicle network and investigate the dynamics of malware propagation inside it. The paper offers insights into the consequences of malware attacks on autonomous systems, highlighting the critical need to address security concerns in the development and application of connected and autonomous car technologies. Malware attacks on QNX is a major threat to the integrity and functionality of neutrino autonomous systems that are crucial for many applications such as intelligent transportation and cities.

Autonomous systems, including cars, employ the QNX operating system, which is renowned for its resilience and real-time capabilities. It controls subsystem communication and guarantees smooth job execution. But these systems are becoming more and more connected, which makes them open to sophisticated virus attacks. For example, malware can degrade vehicle autonomy, increase communication latency, and drain power in smart autonomous vehicles, which rely on cyber-physical systems (CPS) for communication and operation. This can result in traffic congestion and safety risks.

CP Goncalves the constraints of automated gate specification for quantum communications and quantum networked computation are discussed in the study, with particular attention paid to the vulnerability of the automation software to malware that aims to damage it and alter its protocols and algorithms. He also highlights the difficulty in differentiating between a unitary scrambling attack and hardware failure or background noise because of the strategic disruption brought about by altering the automated gate specification, which makes it challenging to determine which node in a quantum communications network was attacked.[84]

M Shapna akter et al, [85] The study shows that adversarial attacks can affect both machine learning (ML) and quantum machine learning (QML) models. Quantum neural networks (QNN) demonstrate a greater decline in accuracy than conventional neural networks (NN). When these models are used in applications where security is a top priority, their resilience is called into question by this problem.The study also shows that adversarial samples created for one model type can have a negative effect on the performance of the other model type, underscoring the need for robust defense mechanisms to protect ML and QML models against adversarial attacks. This result emphasizes how crucial it is to create plans to improve the security and robustness of these models—especially QNN, considering its recent improvements.

The safety, security, and operation of autonomous vehicles (AVs) are seriously threatened by malware attacks on their Android operating systems. Because autonomous vehicles (AVs) depend more and more on wireless connection with other vehicles and infrastructure as well as interconnected electronic control systems, they are vulnerable to sophisticated cyberattacks, such as malware that can corrupt vehicle control units and cause operational disruptions.[86] Such attacks could have serious repercussions, from increased communication latency and power depletion to traffic jams and financial loss, endangering both public confidence in AV technology and passenger safety. According to research, clever malware can intentionally time attacks to maximum disruption and result in serious safety risks such forced emergency braking and crashes. Malware in AVs spreads like an infectious disease, and self-propagating viruses like Stuxnet are a quick and potent danger to both the AV system and the transportation infrastructure.[87] Different defensive and detection systems are being developed to counter these threats. In order to detect Android malware in auto-driving cars, for example, a machine learning-based detection approach utilizing hybrid analysis-based particle swarm optimization (PSO) and an adaptive genetic algorithm (AGA) has demonstrated high accuracy, reaching up to 99.82% accuracy with the XGBoost classifier. Furthermore, integrating resource file and permission features for Android malware detection has shown to be successful in enhancing accuracy and getting around the drawbacks of conventional detection techniques. [88] For AVs to be protected from malware assaults, sophisticated intra vehicle and inter-vehicle communication networks must be integrated, and strong security mechanisms including network security, software vulnerability detection, and cryptography must be put in place [89, 90].

5. Network layer

Vehicular communication gain attention of both industry and academic sector in recent decade. It provides huge platform to researchers. In Vehicular communication refers to the exchange of data within the components of vehicles, vehicle to everything communication (V2X) refers to the communication of vehicle with other vehicle, with pedestrian and infrastructure. With V2X vehicle collects data that helps it to remain safe and perform functions autonomously like traffic management, infotainment system and road safety. The security concerns of network layer are availability, confidentiality, authentication, data integrity and non-repudiation. The threats to these services are given in details as follows.

Availability: threats to the network availability of AV are malware, spamming, black and Grey hole, broadcast tempering, jamming and DOS.

Confidentiality: the threats to confidentiality are Man in the middle attack, traffic analysis interruption, social engineering and eavesdropping.

Authentication: Sybil attack, tunneling, GPS spoofing, key replication, etc can affect the authentication of data on a network.

Data integrity: the threats to data integrity is masquerading, replay attack,illusion and message tempering.

K Lakshmi et al, [91] draws attention to how difficult it is to maintain the source cars' identities in a dynamic setting, even with the advent of numerous algorithms that employ pseudonym techniques. This constraint suggests that the issue of effectively safeguarding the privacy of vehicle locations has not been entirely solved by current methods. The considerable risk of tampering with the identities of vehicles' locations in Vehicular Ad-hoc Networks (VANET), a crucial field of research in intelligent transport systems, is another constraint noted in the paper. This restriction highlights the continued worry about security lapses and the requirement for improved privacy protection mechanisms in VANET. C Shekhar et al, [92] highlighted context of networked autonomous vehicles, the study presents a lightweight IoT based framework for vehicular ad-hoc networks, or VANETs.It highlights how vital VANETs are to the advancement of networked autonomous vehicles, intelligent transportation systems, and smart city planning. This paper primarily proposes a Synchronous-Transmission (ST) based technique to address issues related to security, efficiency, and scalability in VANETs.

The framework intends to create considerably efficient, dispersed, and attack-resilient communication within VANETs by switching from conventional Asynchronous-Transmission (AT) methods to ST, hence improving the application of VANETs in autonomous cars.

X Chen et al, [93] In the paper, it is discussed how conventional vehicular ad hoc networks (VANETs) are being replaced by a new paradigm known as vehicle as a service (VaaS), in which intelligently driven autonomous vehicles operate as a service network within smart cities. It draws attention to how useful it might be to use cars equipped with sophisticated sensing, communication, processing, storage, and intelligence to offer services like smart living and public safety. The report highlights the shift toward using cars as mobile servers and communicators to improve service capabilities in future smart cities, even though it does not expressly address VANETs.

M Haris et al, [94] present the idea of intelligent volunteer computing-based vehicle area networks (VANETs) is covered in the article. It focuses on using volunteer computing in opportunistic networks to leverage the collective computational resources of vehicles. The study recommends predicting volunteer cars ability to handle complex computing tasks using machine learning. The goal of the research is to choose volunteer cars wisely by considering their expected capabilities. In order to identify appropriate volunteer cars for effectively carrying out tasks, the study proposes a predictive modeling approach. This paper thus tackles the utilization of VANETs in the context of autonomous vehicles.Amit Kumar et al,[95]The development of autonomous vehicles is greatly aided by vehicular ad-hoc networks, or VANETs, which facilitate communication and connection between vehicles while they are on the road. Intelligent transport systems rely heavily on VANETs, which establish a wireless network among mobile vehicles to enable inter-vehicle communication. In the context of autonomous road cars, the study highlights the importance of VANETs and their role in improving technology, safety, energy efficiency, and practical applications. As a result, VANETs are crucial for the development of autonomous vehicles on roads by facilitating effective coordination and communication among them. V Kharchenko et al, [96] present shortcomings include its emphasis on modeling the most basic wireless communication channel in VANET, which might not accurately capture the complexities of actual VANET communication scenarios. The use of theoretical modeling and simulation using NetCracker, which might not fully reflect all the subtleties and uncertainties inherent in real VANET communication, is another drawback. GA Issac et al, [97] draws attention to the security flaw in VANET that allows for Denial of Service (DoS) attacks because of decreased message throughput, which may result in packet loss from moving vehicles.

In order to counter the denial-of-service attack in VANET, a modified prediction-based authentication scheme (PBA) is implemented with the goal of minimizing validation delays for emergency vehicles such as ambulances and fire services.

6. Physical layer

The autonomous vehicles are fully equipped with sensors and highly depends on it. These sensors helps the vehicle to monitor surrounding and move safely. The attack on these sensors can disrupt the vehicle drive. Attacker may produce false message or cause physical damage to these sensors. The possible security attacks on physical layer are sensor attack, system level attack, and adversarial attack.

In sensor attack jamming and spoofing is done. The sensor will either send false data or no data in case of attack. The attacker can use sensing system, tracking system and transmitter to conduct this sort of attack. J Zheng et al, [1] proposed the 3D Depth Fool (3D Fool) attack is introduced in this study, which discusses physical 3D adversarial assaults on monocular depth estimation (MDE) in autonomous driving. This approach is more effective and resilient to different weather conditions and views since it employs 3D textures to fool MDE models over a larger area. Although MDE models are the main focus, there is also discussion of physical layer attacks against autonomous cars, such as tampering with sensor inputs using 3D textures. Therefore, using MDE vulnerability as a lens, the study subtly discusses the possibility of physical layer attacks against autonomous vehicles. ZU Abideen et al, [98] study how to tackles physical adversarial threats, such as painting black lines on roadways, on the visual perception modules of autonomous vehicles. These attacks specifically target deep neural networks, which are essential for controlling autonomous vehicles. According to the study, such assaults can drastically lower state-of-the-art networks' accuracy by up to 30% and are surprisingly simple to carry out. Hence, the study exposes flaws in deep learning models used in self-driving cars and shows the viability and effect of physical layer attacks on autonomous vehicles' sensory systems.

Y Cao et al, [46] study presents Physical Removal Attacks (PRA), which cause AV obstacle detectors to malfunction by selectively removing LiDAR point cloud data of real impediments using laser-based spoofing techniques. By physically altering sensor data, these attackers trick autonomous cars into making risky driving decisions. The study shows that PRA has a high success rate in concealing barriers from perception systems when compared to popular AV obstacle detectors and fusion models.

MS Alam et al, [99] In response to assaults on connected and autonomous vehicles (CAVs), a unique secure physical layer key generation technique is proposed in this paper. A unique pre-shared key (PSK) is formed by appending a random sequence key to the demodulated sequence, strengthening security against adversaries. Comprehensive simulations show that attackers cannot recover the valid PSK emitted by the receiving vehicle, even with identical fading and Additive White Gaussian Noise (AWGN) characteristics. Therefore, by guaranteeing secure key generation in the presence of possible attackers, the suggested solution successfully mitigates physical layer assaults on autonomous vehicles.

Z Chen et al, [100] indicates a gap in our current understanding of potential threats to autonomous driving systems, as the paper points out that while security risks associated with camera-based sensors have been thoroughly investigated, research on the vulnerability of deep learning models for Lidar-based sensors is still in its early stages. Physical Point Attack (PPA), a suggested attack technique, seeks to create 3D hostile objects that can deceive Lidar scanners in a real-world setting. The lack of discussion of potential defenses or counters against these types of assaults, however, suggests that this work is limited in its ability to address the defensive components of this security issue. R Muller et al, [101] presents AttrackZone, a physically-realizable tracker hijacking attack against Siamese trackers that takes control of an object's bounding box by taking advantage of the heat map generating process. This can result in physical consequences such as uninvited pedestrian encroachment and vehicle collisions. With an average execution time of 0.3–3 seconds, AttrackZone meets its assault objectives 92% of the time, demonstrating its efficacy in both the digital and physical worlds.

X Han et al, [102] focuses on physical backdoor attacks that aim to undermine DNN models through tainted training data, endangering the safety of the vehicle and its occupants. These attacks target lane detection systems in autonomous driving. In order to create poisoned samples that infect the trained lane detection model and cause incorrect detection when triggered by common objects, the authors introduce two attack methodologies (poison-annotation and clean-annotation). This could result in the vehicle driving off the road or into the opposite lane. AZ Mohammad et al, [103] mentions a physical-layer data manipulation attack on the Controller Area Network (CAN) bus is discussed in the paper, with an emphasis on bit-flips caused by compromised Electronic Control Units (ECUs) working together to flip dominant bits to recessive ones. By creating transient voltages in the CAN bus and taking use of the non-ideal characteristics of the line drivers and the parasitic reactance of the bus, the attack allows for random bit-flips in sent messages' Lou et al, [104] describe the susceptibility of ultrasonic sensors in cars to signal injection attacks—a tactic in which malevolent acoustic sounds are used to spoof obstacles and deceive autonomous vehicles—is covered in this research.

The authors present SoundFence, a physical-layer security system that can accurately detect anomalous sensor readings and identify signal injection attacks by analyzing physical-layer signatures of ultrasonic waves and sensor readings. W Jia et al, [105] focuses on creating strong physical adversarial examples (AEs) that target real-world object detectors, with a particular focus on autonomous vehicle Traffic Sign Recognition (TSR) systems. In order to fool the YOLO v5 based TSR system in a variety of ways, the suggested pipeline simulates in-car cameras, creates bounding box filters, and takes into account a number of attack vectors. Successful attacks are shown on a 2021 model vehicle. Z Sun et al, [106] proposed to increase the security and dependability of mm Wave-based sensing systems in autonomous vehicles (AVs), this research focuses on their security flaws. Using an AV test bed and a cutting-edge mm Wave test bed, the study demonstrates how to undermine the security and safety of the target AV by spoofing it and designing and implementing realistic physical layer attack and defense tactics in real-world scenarios. P Dash et al, [107] introduces PID-Piper, a system that uses an attack-resistant Feedforward Controller (FFC) based on machine learning to automatically recover Robotic Vehicles (RVs) from physical attacks. The FFC functions in conjunction with the RV's primary controller. PID-Piper has been proved to enable RVs to successfully perform their objectives in 83% of the cases through studies on 6 RV systems, including 3 real RVs.

7. Future Research Directions

The field of autonomous vehicles (AVs) is still progressing, with a lots of sensitive data and new technological challenges. The topic is multifarious due to its vast range and complexity. This is made worse by the lack of thorough international standards that direct AV development, safety, and security protocols. Because of this, looking into and dealing with problems related to the security and safety of AVs is not only extremely complex but also crucial.

Technological advancements of autonomous vehicles (AVs) are anticipated to expand their ecosystem to encompass an increased quantity of standalone devices and additional infrastructure.

This expansion will probably improve connection, but it may also make AVs more susceptible to a variety of security threats. This breakthrough raises important issues and problems that need to be researched right away.

Safeguarding V2X communication: Vehicle-to-everything (V2X) communication security must be guaranteed, compromised AVs may have a huge impact on linked smart infrastructure. An attack on an electric car might affect networks, charging stations, and the electrical grid.The creation of safe communication channels and the development of robust preventative measures need to be the top priorities for future study.

Synchronized safety and security protocols: Generally, evaluations of vehicle security and safety are carried out independently, resulting in the development of inconsistent preventative measures. But it's crucial to promote a smooth collaboration between security and safety procedures in antivirus software.To determine the coordinated efficiency of safety and security measures, future study should focus on assessing their interrelationships

Interaction with non-automated vehicles: In case of mixed traffic, autonomous vehicles (AVs) must collaborate and communicate efficiently with both automated and non-automated road users, including bicycles, pedestrians, and conventional cars.It can be challenging to understand and forecast human behavior in this scenario involving mixed traffic,it is essential to maintaining safety. Research at interaction of human and AV in these situation is desperately needed.

Protecting CAN bus communications: Potential threats can target the Controller area network (CAN) bus that manages the transfer of sensor data. Without security precautions like encryption, sensitive mission-planning, data may be revealed. Subsequent research should be conducted that efficiently protect CAN bus communications in order to preserve data authenticity and integrity.

Adapting to new attack techniques: Cyber-attack techniques also evolve along with technology. In order to stay ahead future research must aim to anticipate new ways that attackers might try to compromise security and must develop countermeasures before these attacks can occur.

Developing comprehensive guidelines and regulations: One major challenge is the lack of global guidelines for the security and safety of autonomous vehicles. International standards would provide a consistent framework to direct the development of safe and dependable AV systems.

Taking care of machine learning flaws: Al and machine learning particularly deep learning are the foundation of antivirus technology. Future research need to focus on creating strong defenses against these possible intrusions for machine-learning systems inside of autonomous vehicles.

8. Challenges

The advancement of self-driving cars brings revolution in the of public and private transportation networks. However the achievement of this future depends on the resolution of several challenges, mostly related to security. As research in this area continues, it becomes more and more obvious how difficult it is to guarantee the safe and dependable operation of AVs. AVs' essential components are sensor systems and communication channels that are vulnerable to a variety of cyberattacks. Significant advancements in the fields of visual analysis and processing capacity are required in order to consistently and accurately make the best judgments in real time. Apart from the technical constrains, there exist noteworthy legal, sociological and ethical barriers that demands further investigation. Public trust in AVs' dependability and safety is essential to their social acceptance thorough safety evaluation. Moreover different countries having different requirements so the surrounding environment of autonomous vehicles is always changing and poses a substantial obstacle. Lastly there are ethical dilemmas about the decision-making capabilities of autonomous vehicles in critical circumstances that require resolution. It will be essential to solve these complex issues if driver less vehicles are to become widely used in the future.

Ultimately considering the enormous changes in the transportation sector there is a great deal of interest in how autonomous vehicles (AVs) can fundamentally transform the way we travel. A number of challenges appear as these vehicles develop further especially with regard to their ability to identify and react to human behavior. Based on our in-depth analysis, we have identified the following crucial areas that need attention and more study.

Risk mitigation: The risk involves when we switch from manual to automated driving. The object detection dimensions, cyber security, and privacy in V2X interactions are important themes in the discussion of risk mitigation requirements of these issues.

Real-time decision making: An autonomous vehicle needs to be able to make decisions in real time to surpass the abilities of a human driver in order to be more reliable. For such accomplishments to be feasible, technology must continue to progress, particularly in the fields of high-speed computing and decision making algorithms.

Gaining public trust: To determine whether autonomous cars are ultimately successful and widely integrate the level of public trust is a significant factor, this necessitates a level of technical precision ensuring the autonomous vehicle's overall safety and developing confidence in its capacity to resolve problems.

Precision positioning technologies: The development of technology is essential that can accurately locate automobiles to create reliable and secure intelligent transportation networks. A vast array of unknown variables, including irregular pedestrian behavior, scattered objects, and different road conditions, must be taken into consideration by these algorithms.

Environmental detection: The ability of an autonomous vehicle to accurately perceive its surroundings is essential for efficient navigation. Thus, AV safety depends on the development of technologies that can identify and react to a variety of situations.

Pedestrian detection: The safety of pedestrians must come first when designing autonomous cars. This demands the use of accurate and reliable detection technologies.

Path planning: Mapping its own route is a critical component in assessing an autonomous vehicle's effectiveness and safety. Developing systems that allow for precise route planning and prediction is essential.

Motion control: Effective motion control is necessary for autonomous vehicles (AVs) to navigate safely.The primary objective is to develop technologies that can precisely regulate a vehicle's mobility under unexpected circumstances.

Vehicular communication technologies: For the field of V2X communications to progress and ensure trouble-free connectivity between autonomous cars and infrastructure, trustworthy vehicular communication solutions must be developed.

Traffic management: The increasing number of autonomous cars can lead to traffic congestion if insufficient and unstable traffic control techniques are implemented. Modern methods include policy-based deep reinforcement learning and intelligent routing, which lessen traffic, can optimize traffic flow management.

Even if these challenges appear unresolved they serve as a reminder of the immense scope for additional research and development on autonomous vehicles in general. By addressing these issues we can ensure the safe and efficient integration of autonomous vehicles into our transportation networks, bringing in a new era of mobility. Researchers can ensure the safe and effective integration of autonomous vehicles into our transportation networks in the coming era of mobility by tackling these problems.

9. Open Challenges with solutions for Autonomous Vehicle Security

In the context of autonomous vehicles understanding how dynamic security is when debating specific issues and potential solutions. The combination of technologies like blockchain, AI, and IoT not only adds complex security challenges that require detailed and innovative solutions, but also enables previously unattainable levels of automation. Because of the complexity of these problems, autonomous vehicles operate in dynamic, real-time environments, necessitating the use of robust, adaptable security solutions. Therefore, it is crucial to understand the potential roadblocks to implementing additional features and fundamental security principles as well as to find practical solutions for these issues. Let's look at a few of these problems and their solutions.

System complexity: Self-driving cars provide a complex web of sensors, sophisticated algorithms, and interconnected systems that make applying security principles much more difficult.

Proposed solution: Adopting a "security by design" approach is crucial, whereby security measures are included into the system's architecture from the start. System compartmentalization ensures that each component operates independently and is maintained isolated from the others, which could further lower the chance of security lapses.

Real-time operation requirements: Because autonomous vehicles make operational decisions in real-time, many security activities—particularly those using sophisticated encryption techniques—can induce latency with smooth functioning.

Proposed solution: It is possible to meet real-time requirements while maintaining security by utilizing lightweight encryption techniques and hardware-accelerated security procedures.

Scalability issues: The volume of data being exchanged and maintained may increase as autonomous vehicles become more prevalent, adding to the system's workload and making incident response and security maintenance more challenging.

Proposed solution: Implementing Scalable security solutions is necessary. Security and anonymity can be ensured by decentralized and Scalable distributed ledger systems, such as blockchain.

Long vehicle lifespan: One specific issue is that, compared to the rapid evolution of cyber threats, the average vehicle life cycle is significantly shorter.

Proposed solution: Autonomous vehicles may undergo periodic security system upgrades to fight emerging threats, partly due to over-the-air (OTA) updates. Ensuring backward compatibility of improvements is an essential part of this approach.

Legislation and standards: Autonomous car technology is often developing faster than existing regulations and security standards.

Proposed solution: Automakers, cyber security experts, and politicians must work together to create and uphold regulations and standards specifically tailored for autonomous vehicles.

As long as research, innovation, and concerted efforts from all the various companies involved in the development and implementation of autonomous vehicles are maintained, despite their magnitude these issues can be resolved.

10. Conclusion

This article examines the security challenges of autonomous vehicle that is developing quickly and changing the face of transportation as a result of recent advancements. These inventions have a lot of potential, but there are significant obstacles in the way of their general implementation. The twin issues of safety and cyber security that are critical components that demand an in-depth analysis and preventative actions. Our study illustrates information security dynamics that enable the safe operation of AV. We gave a thorough rundown of various cyber security threats in a layered model approach.

The autonomous vehicle (AV) research sector, which is expanding and has garnered significant scholarly attention, poses the greatest threat under numerous cyber threats. One major weakness in our defense mechanisms against the constantly changing cyber security threats. Without a doubt, AVs' ability to withstand such incursions and remain impenetrable will be a key factor in deciding their future development and level of society acceptance. Determining, classifying, and understanding these potential attacks is another critical component of our work. We have provided a thorough study of the dangers currently facing the AV sector by classifying these threats according to the principles of data availability, authenticity, integrity, and secrecy.

This classification not only shows how the threat landscape is currently evolving, but it also highlights areas that require further research and mitigation by exposing the weaknesses in present defense techniques. We classified the threat as fully mitigated for attacks that have been totally neutralized by countermeasures, partially mitigated for threats that are still present in specific situations, and uncovered for threats that need more investigation or for which current defenses have not been adequate. The results presented above show how urgently the AV technology sector needs to implement stronger security measures. The potentially disastrous effects of security failures make sure the safety of these systems not simply suggested but absolutely imperative.

Future research must therefore concentrate on developing and putting into practice strong encryption methods, addressing fundamental vulnerabilities and coming up with innovative remedies that can adapt to a continuously changing threat environment. It is crucial that we keep up our proactive efforts to mitigate the cyber security dangers that come with this technological shift as we enter a new era where driver less cars have the ability to drastically alter our transportation infrastructure. By establishing a robust and secure operating environment we can ensure the operational efficacy of unmanned autonomous vehicles and promote public confidence in their deployment. But it's crucial to remember that this project is a journey rather than a destination

Our defense plans need to change to keep up with the ever-evolving threat landscape. By remaining attentive we can successfully navigate this complex environment and safeguard the bright future of autonomous vehicles from the threats posed by cyber security by carrying out ongoing research, and working across disciplines.

References

1. J. Zheng, C. Lin, J. Sun, Z. Zhao, Q. Li, and C. Shen, "Physical 3D adversarial attacks against monocular depth estimation in autonomous driving," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2024, pp. 24452-24461.
2. F. Zafar, H. A. Khattak, M. Aloqaily, and R. Hussain, "Carpooling in connected and autonomous vehicles: current solutions and future directions," ACM Computing Surveys (CSUR), vol. 54, no. 10s, pp. 1-36, 2022.
3. D. J. Zea, A. P. Toapanta, C. A. Minaya, C. A. Paspuel, and I. E. Moreno, "Evaluation of the Reliability of a LiDAR Sensor Through a Geometric Model in Applications to Autonomous Driving," in The International Conference on Advances in Emerging Trends and Technologies, 2022: Springer, pp. 688-705.
4. T. Yoshizawa et al., "A survey of security and privacy issues in v2x communication systems," ACM Computing Surveys, vol. 55, no. 9, pp. 1-36, 2023.
5. C. Wienrich and K. Schindler, "Challenges and requirements of immersive media in autonomous car: exploring the feasibility of virtual entertainment applications. i-com 18 (2), 105–125 (2019)," ed.
6. J. Yang, A. Estornell, and Y. Vorobeychik, "Location Spoofing Attacks on Autonomous Fleets," in Symposium on Vehicles Security and Privacy, 2023: Internet Society.
7. M. Hataba, A. Sherif, M. Mahmoud, M. Abdallah, and W. Alasmary, "Security and privacy issues in autonomous vehicles: A layer-based survey," IEEE Open Journal of the Communications Society, vol. 3, pp. 811-829, 2022.
8. T. Garg, N. Kagalwalla, P. Churi, A. Pawar, and S. Deshmukh, "A survey on security and privacy issues in IoV," International Journal of Electrical & Computer Engineering (2088-8708), vol. 10, no. 5, 2020.
9. B. P. Nayak, L. Hota, A. Kumar, A. K. Turuk, and P. H. Chong, "Autonomous vehicles: Resource allocation, security, and data privacy," IEEE Transactions on Green Communications and Networking, vol. 6, no. 1, pp. 117-131, 2021.
10. E. T. Sağlam and Ş. Bahtiyar, "A survey: Security and privacy in 5G vehicular networks," in 2019 4th International Conference on Computer Science and Engineering (UBMK), 2019: IEEE, pp. 108-112.
11. M. A. Razzaque, A. S. S, and S. M. Cheraghi, "Security and privacy in vehicular ad-hoc networks: survey and the road ahead," Wireless Networks and Security: Issues, Challenges and Research Trends, pp. 107-132, 2013.
12. Z. Wang, H. Wei, J. Wang, X. Zeng, and Y. Chang, "Security issues and solutions for connected and autonomous vehicles in a sustainable city: A survey," Sustainability, vol. 14, no. 19, p. 12409, 2022.
13. T.-H. Nguyen, T. G. Vu, H.-L. Tran, and K.-S. Wong, "Emerging privacy and trust issues for autonomous vehicle systems," in 2022 International Conference on Information Networking (ICOIN), 2022: IEEE, pp. 52-57.
14. M. S. Sheikh, J. Liang, and W. Wang, "Security and privacy in vehicular ad hoc network and vehicle cloud computing: a survey," Wireless Communications and Mobile Computing, vol. 2020, pp. 1-25, 2020.
15. A. Hafeez, "A robust, reliable and deployable framework for in-vehicle security," 2020.
16. A. Hafeez, M. Tayyab, C. Zolo, and S. Awad, "Finger printing of engine control units by using frequency response for secure in-vehicle communication," in 2018 14th International Computer Engineering Conference (ICENCO), 2018: IEEE, pp. 79-83.
17. T. Limbasiya, K. Z. Teng, S. Chattopadhyay, and J. Zhou, "A systematic survey of attack detection and prevention in connected and autonomous vehicles," Vehicular Communications, vol. 37, p. 100515, 2022.
18. B. Veera Jyothi, L. Suresh Kumar, and B. Surya Samantha, "Security Issues in Vehicular Ad Hoc Networks and Quantum Computing," Evolution and Applications of Quantum Computing, pp. 249-264, 2023.
19. D. A. Alex, D. B. Desmond, and B. Asher, "Cyber Security Issues and Solution in Vehicular Networks," Available at SSRN 4181650, 2022.
20. J. Répás, "Definition of Forensic Methodologies for Autonomous Vehicles," Hadmérnök, vol. 18, no. 1, pp. 125-141, 2023.
21. M. A. Al-Shareeda, M. Anbar, S. Manickam, A. Khalil, and I. H. Hasbullah, "Security and privacy schemes in vehicular ad-hoc network with identity-based cryptography approach: A survey," IEEE Access, vol. 9, pp. 121522-121531, 2021.
22. N. I. Shuhaimi and T. Juhana, "Security in vehicular ad-hoc network with Identity-Based Cryptography approach: A survey," in 2012 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA), 2012: IEEE, pp. 276-279.
23. [23] S. Kumar, M. S. Gaur, P. S. Sharma, and D. Munjal, "A novel approach of symmetric key cryptography," in 2021 2nd international conference on intelligent engineering and management (ICIEM), 2021: IEEE, pp. 593-598.

24. F. M. Noori, A. Hafeez, H. Malik, M. Z. Uddin, and J. Torresen, "Source Linking Framework in Vehicular Networks for Security of Electric Vehicles using Machine Learning," in 2023 IEEE Vehicular Networking Conference (VNC), 2023: IEEE, pp. 207-214.
25. R. U. D. Refat, A. A. Elkhail, A. Hafeez, and H. Malik, "Detecting can bus intrusion by applying machine learning method to graph based features," in Intelligent Systems and Applications: Proceedings of the 2021 Intelligent Systems Conference (IntelliSys) Volume 3, 2022: Springer, pp. 730-748.
26. U. Khandelwal, A. Fan, D. Jurafsky, L. Zettlemoyer, and M. Lewis, "Nearest neighbor machine translation," arXiv preprint arXiv:2010.00710, 2020.
27. M. Girdhar, Y. You, T.-J. Song, S. Ghosh, and J. Hong, "Post-accident cyberattack event analysis for connected and automated vehicles," IEEE Access, vol. 10, pp. 83176-83194, 2022.
28. D. Wang, Y. Cao, F. Yan, Y. Liu, D. Tian, and Y. Zhuang, "Secure long-range autonomous valet parking: A reservation scheme with three-factor authentication and key agreement," IEEE Transactions on Vehicular Technology, vol. 72, no. 3, pp. 3832-3847, 2022.
29. C. Huang, R. Lu, X. Lin, and X. Shen, "Secure automated valet parking: A privacy-preserving reservation scheme for autonomous vehicles," IEEE Transactions on Vehicular Technology, vol. 67, no. 11, pp. 11169-11180, 2018.
30. A. Aggarwal, S. Gaba, J. Kumar, and S. Nagpal, "Blockchain and autonomous vehicles: Architecture, security and challenges," in 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022: IEEE, pp. 332-338.
31. Y. Koh, Y. Kim, M. Batzorig, and K. Yim, "Real vehicle-based attack dataset for security threat analysis in a vehicle," in International Conference on Broadband and Wireless Computing, Communication and Applications, 2022: Springer, pp. 137-146.
32. P. Kale and R. R. N. Bielby, "Security operations of parked vehicles," ed: Google Patents, 2022.
33. G. A. Francia III III, "Vehicle network security metrics," in Advances in Cybersecurity Management: Springer, 2021, pp. 55-73.
34. H. Alfehaid and S. El Khrdiri, "Cyber security attacks on identity And location of vehicle ad-hoc networks," in Selected Papers from the 12th International Networking Conference: INC 2020 12, 2021: Springer, pp. 207-223.
35. W. Terrance, K. Kouadio, and T. Youssef, "Understanding Open Charge Point Protocol," in SoutheastCon 2023, 2023: IEEE, pp. 559-564.
36. K. Gandhi and W. G. Morsi, "Impact of the open charge point protocol between the electric vehicle and the fast charging station on the cybersecurity of the smart grid," in 2022 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), 2022: IEEE, pp. 235-240.
37. Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis, and C. Douligeris, "Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (OCPP)," IEEE Communications Surveys & Tutorials, vol. 24, no. 3, pp. 1504-1533, 2022.
38. B. Vaidya and H. T. Mouftah, "Deployment of secure EV charging system using open charge point protocol," in 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), 2018: IEEE, pp. 922-927.
39. K. Kirihara and T. Kawabe, "Power System Frequency Control Architecture Combining Open Charge Point Protocol and Electric Vehicle Model Predictive Charge Rate Control," IEEE Access, vol. 10, pp. 104498-104511, 2022.
40. S. Y. Mattepu, M. Richter, and S. Balischewski, "OCSS: An application to simulate multiple charging stations which uses an Open charge point protocol for communication," in 2022 IEEE 13th International Symposium on Power Electronics for Distributed Generation Systems (PEDG), 2022: IEEE, pp. 1-5.
41. S. Deniz, "An empirical analysis of the openness dimension of OCPP standard," in 4th European Battery, Hybrid and Fuel Cell Electric Vehicle Congress, 2015.
42. S. H. V. Bhupathiraju, J. Sheldon, L. A. Bauer, V. Bindschaedler, T. Sugawara, and S. Rampazzi, "Emi-lidar: uncovering vulnerabilities of lidar sensors in autonomous driving setting using electromagnetic interference," in Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2023, pp. 329-340.
43. X. Jin, H. Yang, X. He, G. Liu, Z. Yan, and Q. Wang, "Robust LiDAR-based vehicle detection for on-road autonomous driving," Remote Sensing, vol. 15, no. 12, p. 3160, 2023.
44. T. Liu, Y. Wang, X. Niu, L. Chang, T. Zhang, and J. Liu, "LiDAR odometry by deep learning-based feature points with two-step pose estimation," Remote Sensing, vol. 14, no. 12, p. 2764, 2022.

45. J. Taher et al., "Feasibility of hyperspectral single photon lidar for robust autonomous vehicle perception," Sensors, vol. 22, no. 15, p. 5759, 2022.
46. Y. Cao, S. H. Bhupathiraju, P. Naghavi, T. Sugawara, Z. M. Mao, and S. Rampazzi, "You can't see me: Physical removal attacks on {lidar-based} autonomous vehicles driving frameworks," in 32nd USENIX Security Symposium (USENIX Security 23), 2023, pp. 2993-3010.
47. X. Sun, M. Wang, J. Du, Y. Sun, S. S. Cheng, and W. Xie, "A task-driven scene-aware LiDAR point cloud coding framework for autonomous vehicles," IEEE Transactions on Industrial Informatics, vol. 19, no. 8, pp. 8731-8742, 2022.
48. C. Vishnu, J. Khandelwal, C. K. Mohan, and C. L. Reddy, "EV AA-Exchange Vanishing Adversarial Attack on LiDAR Point Clouds in Autonomous Vehicles," IEEE Transactions on Geoscience and Remote Sensing, 2023.
49. Z. Cheng et al., "Fusion is Not Enough: Single Modal Attacks on Fusion Models for 3D Object Detection," arXiv preprint arXiv:2304.14614, 2023.
50. H.-J. Yoon, H. Jafarnejadsani, and P. Voulgaris, "Learning when to use adaptive adversarial image perturbations against autonomous vehicles," IEEE Robotics and Automation Letters, vol. 8, no. 7, pp. 4179-4186, 2023.
51. Y. Man, M. Li, and R. Gerdes, "Remote perception attacks against camera-based object recognition systems and countermeasures," ACM Transactions on Cyber-Physical Systems, vol. 8, no. 2, pp. 1-27, 2024.
52. O. Adeboye, A. Abdullahi, T. Dargahi, M. Babaie, and M. Saraee, "LIFT the AV: Location InFerence aTtack on Autonomous Vehicle Camera Data," in 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC), 2023: IEEE, pp. 1-6.
53. G. Aravind, S. Nambiar, and M. M. Krishnan, "Autonomous Vehicle Security Enhancement," in 2023 International Conference on Networking and Communications (ICNWC), 2023: IEEE, pp. 1-5.
54. A. Afdhal, A. Ahmadiar, and R. Adriman, "Sybil Attack Detection on ITS-V2X System using a Realistic Traffic Model-based Approach," in 2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT), 2022: IEEE, pp. 333-338.
55. D. D. Dunn, S. A. Mitchell, I. Sajjad, R. M. Gerdes, R. Sharma, and M. Li, "Regular: Attacker-induced traffic flow instability in a stream of semi-automated vehicles," in 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2017: IEEE, pp. 499-510.
56. I. Gokasar, A. Timurogullari, M. Deveci, and H. Garg, "SWSCAV: Real-time traffic management using connected autonomous vehicles," ISA transactions, vol. 132, pp. 24-38, 2023.
57. J. Ivanchev, D. Eckhoff, and A. Knoll, "System-level optimization of longitudinal acceleration of autonomous vehicles in mixed traffic," in 2019 IEEE Intelligent Transportation Systems Conference (ITSC), 2019: IEEE, pp. 1968-1974.
58. P. Galántai, "Assessment of dangerous traffic situations for autonomous vehicles," Periodica Polytechnica Transportation Engineering, vol. 50, no. 3, pp. 260-266, 2022.
59. T. Yang, C. Murguia, D. Nesic, and C. Yuen, "Attack-Resilient Design for Connected and Automated Vehicles," arXiv preprint arXiv:2306.10925, 2023.
60. X. Ge, Q.-L. Han, Q. Wu, and X.-M. Zhang, "Resilient and safe platooning control of connected automated vehicles against intermittent denial-of-service attacks," IEEE/CAA Journal of Automatica Sinica, vol. 10, no. 5, pp. 1234-1251, 2022.
61. X. Zhang, H. Du, Z. Jia, S. Jia, Y. He, and C. Cui, "Distributed adaptive platooning control for platoons under DoS attacks," in 2022 Australian & New Zealand Control Conference (ANZCC), 2022: IEEE, pp. 24-28.
62. F. Li, C. Wang, D. Mikulski, J. R. Wagner, and Y. Wang, "Unmanned ground vehicle platooning under cyber attacks: a human-robot interaction framework," IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 10, pp. 18113-18128, 2022.
63. S. Xiao, X. Ge, Q.-L. Han, and Y. Zhang, "Secure distributed adaptive platooning control of automated vehicles over vehicular ad-hoc networks under denial-of-service attacks," IEEE Transactions on Cybernetics, vol. 52, no. 11, pp. 12003-12015, 2021.
64. M. Maleki, M. Malik, P. Folkesson, B. Sangchoolie, and J. Karlsson, "Modeling and Evaluating the Effects of Jamming Attacks on Connected Automated Road Vehicles," in 2022 IEEE 27th Pacific Rim International Symposium on Dependable Computing (PRDC), 2022: IEEE, pp. 12-23.
65. S. Ucar, S. C. Ergen, and O. Ozkasap, "IEEE 802.11 p and visible light hybrid communication based secure autonomous platoon," IEEE Transactions on Vehicular Technology, vol. 67, no. 9, pp. 8667-8681, 2018.

66. C. Vitale et al., "CARAMEL: results on a secure architecture for connected and autonomous vehicles detecting GPS spoofing attacks," EURASIP Journal on Wireless Communications and Networking, vol. 2021, pp. 1-28, 2021.
67. M. Kamal et al., "A comprehensive solution for securing connected and autonomous vehicles," in 2022 Design, Automation & Test in Europe Conference & Exhibition (DATE), 2022: IEEE, pp. 790-795.
68. H. Taslimasa, S. Dadkhah, E. C. P. Neto, P. Xiong, S. Ray, and A. A. Ghorbani, "Security issues in Internet of Vehicles (IoV): A comprehensive survey," Internet of Things, vol. 22, p. 100809, 2023.
69. Z. Cui, Y. Guan, H. Ji, W. Pei, P. Liu, and W. Sun, "Overview of Malicious Information Propagation and Control in Internet of Vehicles," in 2023 IEEE International Conference on Unmanned Systems (ICUS), 2023: IEEE, pp. 1323-1328.
70. W. Wei, J. Shen, A. Telikani, M. Fahmideh, and W. Gao, "Feasibility analysis of data transmission in partially damaged IoT networks of vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 4, pp. 4577-4588, 2022.
71. J. Wang, L. Wu, H. Wang, K.-K. R. Choo, L. Wang, and D. He, "A secure and efficient multiserver authentication and key agreement protocol for internet of vehicles," IEEE Internet of Things Journal, vol. 9, no. 23, pp. 24398-24416, 2022.
72. T. Christensen, S. B. Mandavilli, and C.-Y. Wu, "The Dark Side of The Internet of Vehicles: A Survey of the State of IoV and its Security Vulnerabilities," arXiv preprint arXiv:2211.05775, 2022.
73. B. Asher and A. Dalton, "Security Methods in Internet of vehicles," Available at SSRN 4154862, 2022.
74. S. Liu, Y. Yu, W. Hu, Y. Peng, and X. Yang, "Intelligent vulnerability analysis for connectivity and critical-area integrity in IoV," IEEE Access, vol. 8, pp. 114239-114248, 2020.
75. S. Aarthi and N. Bharathi, "Analysis of security and privacy issues over vehicular communication in Internet Of Vehicles," in 2022 International Mobile and Embedded Technology Conference (MECON), 2022: IEEE, pp. 500-505.
76. P. Schafhalter, S. Kalra, L. Xu, J. E. Gonzalez, and I. Stoica, "Leveraging cloud computing to make autonomous vehicles safer," in 2023 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), 2023: IEEE, pp. 5559-5566.
77. A. Masood, D. S. Lakew, and S. Cho, "Security and privacy challenges in connected vehicular cloud computing," IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2725-2764, 2020.
78. M. Hataba, A. Sherif, and R. Elkhouly, "Enhanced obfuscation for software protection in autonomous vehicular cloud computing platforms," IEEE Access, vol. 10, pp. 33943-33953, 2022.
79. M. Hataba, A. Sherif, and R. Elkhouly, "A proposed software protection mechanism for autonomous vehicular cloud computing," in 2021 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS), 2021: IEEE, pp. 878-881.
80. S. Aurangzeb, M. Aleem, M. T. Khan, H. Anwar, and M. S. Siddique, "Cybersecurity for autonomous vehicles against malware attacks in smart-cities," Cluster Computing, vol. 27, no. 3, pp. 3363-3378, 2024.
81. S. Jha et al., "Ml-driven malware that targets av safety," in 2020 50th annual IEEE/IFIP international conference on dependable systems and networks (DSN), 2020: IEEE, pp. 113-124.
82. P. J. Bonczek and N. Bezzo, "Resilient Detection and Recovery of Autonomous Systems Operating under On-board Controller Cyber Attacks," in 2022 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), 2022: IEEE, pp. 1741-1747.
83. Shah, A. M., Aljubayri, M., Khan, M. F., Alqahtani, J., Sulaiman, A., & Shaikh, A. (2023). ILSM: Incorporated Lightweight Security Model for Improving QOS in WSN. Computer Systems Science & Engineering, 46(2).
84. M. El Mouhib, K. Azghiou, and A. Benali, "Connected and Autonomous Vehicles against a Malware Spread: A Stochastic Modeling Approach," in 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2022: IEEE, pp. 1-6.
85. C. P. Gonçalves, "Cyberattacks on Quantum Networked Computation and Communications--Hacking the Superdense Coding Protocol on IBM's Quantum Computers," arXiv preprint arXiv:2105.07187, 2021.
86. M. Shapna Akter et al., "Exploring the Vulnerabilities of Machine Learning and Quantum Machine Learning to Adversarial Attacks using a Malware Dataset: A Comparative Analysis," arXiv e-prints, p. arXiv: 2305.19593, 2023.
87. L. Hammood, İ. A. Doğru, and K. Kılıç, "Machine learning-based adaptive genetic algorithm for android malware detection in auto-driving vehicles," Applied Sciences, vol. 13, no. 9, p. 5403, 2023.
88. H. Ahn, J. Choi, and Y. H. Kim, "A mathematical modeling of Stuxnet-style autonomous vehicle malware," IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 1, pp. 673-683, 2022.

89. Z. Xiaojing, "An autonomous protection algorithm for android malware attacks based on multiple features," in Proceedings of 2019 International Conference on Information Science,-Medical and Health Informatics (ISMHI 2019). Institute of Management Science and Industrial Engineering, 2019, pp. 573-576.
90. A. Al-Sabaawi, K. Al-Dulaimi, E. Foo, and M. Alazab, "Addressing malware attacks on connected and autonomous vehicles: recent techniques and challenges," Malware Analysis Using Artificial Intelligence and Deep Learning, pp. 97-119, 2021.
91. M. Boughanja and T. Mazri, "Attacks and defenses on autonomous vehicles: a comprehensive Study," in Proceedings of the 4th International Conference on Networking, Information Systems & Security, 2021, pp. 1-6.
92. K. Lakshmi and M. Soranamageswari, "Enriched Model of Pigeon Inspired Pseudonym Generation for Privacy Preservation of Vehicles Location in VANET," in 2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2023: IEEE, pp. 173-177.
93. C. Shekhar, J. Debadarshini, P. K. Singh, and S. Saha, "A lightweight IoT-based framework for vehicular ad hoc network (VANET)," in 2023 15th International Conference on COMmunication Systems & NETworkS (COMSNETS), 2023: IEEE, pp. 19-24.
94. X. Chen et al., "Vehicle as a service (VaaS): Leverage vehicles to build service networks and capabilities for smart cities," IEEE Communications Surveys & Tutorials, 2024.
95. M. Haris, M. A. Shah, and C. Maple, "Internet of intelligent vehicles (IoIV): an intelligent VANET based computing via predictive modeling," IEEE Access, vol. 11, pp. 49665-49674, 2023.
96. A. K. Tyagi and N. Sreenath, "Vehicular ad hoc networks: New challenges in carpooling and parking services," in proceeding of international conference on computational intelligence and communication (CIC), 2016, vol. 14, pp. 13-24.
97. V. Kharchenko, A. Grekhov, and V. Kondratiuk, "Loss Estimation in VANET Communications," J Sen Net Data Comm, vol. 3, no. 1, pp. 47-59, 2023.
98. G. A. Issac and A. J. Mary, "Validation scheme for VANET," in 2019 2nd International Conference on Signal Processing and Communication (ICSPC), 2019: IEEE, pp. 11-15.
99. Z. U. Abideen, M. A. Bute, S. Khalid, I. Ahmad, and R. Amin, "A3d: Physical adversarial attack on visual perception module of self-driving cars," 2022.
100. M. S. Alam, S. M. Hossain, J. Oluoch, and J. Kim, "A Novel Secure Physical Layer Key Generation Method in Connected and Autonomous Vehicles (CAVs)," in 2022 IEEE Conference on Communications and Network Security (CNS), 2022: IEEE, pp. 1-6.
101. Z. Chen and Y. Feng, "Physically realizable adversarial attacks on 3d point cloud," in 2022 34th Chinese Control and Decision Conference (CCDC), 2022: IEEE, pp. 5819-5823.
102. R. Muller, Y. Man, Z. B. Celik, M. Li, and R. Gerdes, "Physical hijacking attacks against object trackers," in Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, 2022, pp. 2309-2322.
103. X. Han, G. Xu, Y. Zhou, X. Yang, J. Li, and T. Zhang, "Physical backdoor attacks to lane detection systems in autonomous driving," in Proceedings of the 30th ACM International Conference on Multimedia, 2022, pp. 2957-2968.
104. A. Z. Mohammed, Y. Man, R. Gerdes, M. Li, and Z. B. Celik, "Physical layer data manipulation attacks on the can bus," in Proceedings of the International Workshop on Automotive and Autonomous Vehicle Security (AutoSec), San Diego, CA, USA, 2022, vol. 24.
105. J. Lou, Q. Yan, Q. Hui, and H. Zeng, "SoundFence: Securing ultrasonic sensors in vehicles using physical-layer defense," in 2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), 2021: IEEE, pp. 1-9.
106. W. Jia, Z. Lu, H. Zhang, Z. Liu, J. Wang, and G. Qu, "Fooling the Eyes of Autonomous Vehicles: Robust Physical Adversarial Examples Against Traffic Sign Recognition Systems. arXiv 2022," arXiv preprint arXiv:2201.06192.
107. Z. Sun, S. Balakrishnan, L. Su, A. Bhuyan, P. Wang, and C. Qiao, "Who is in control? Practical physical layer attack and defense for mmwave-based sensing in autonomous vehicles," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 3199-3214, 2021.
108. P. Dash and K. Pattabiraman, "Recovering Autonomous Robotic Vehicles from Physical Attacks."