SECURITY OF CONNECTED AND AUTONOMOUS VEHICLES

Madhumita Shankar

110074752

Abstract-Connected and Autonomous vehicle is the backbone of next-gen vehicles, and it is the more researched automobile technology because it reduces user cost, increases transport safety, reduces the number of crashes on road, increased autonomy has the potential to eradicate risky and harmful driving practices, fuel-saving, drop-in human emissions, increase lane capacity, promote mobility and it creates more new job opportunities. Since it's all connected the vehicle is more prone to cyberattacks, and the malicious user can inject different kinds of attacks on the system. The computer controls the whole system, and it is wireless therefore there is an increase in cyberattacks and it is important to give priority to finding ways to prevent them. Autonomous vehicle interacts with the object in the environment and with other cars. The growth in surface attacks on vehicles raises the potential for security threats. This article discusses the different types of traditional and non-traditional cyberattacks.

I Introduction

Vehicles in the past are like a single unit where the driver gets into the car and drives the car to its destination. But the current trend in the automobile industry is blooming with various technology. Having closely witnessed many advancements in this field, be it the evolution of vehicles or humans driving a car to autonomous vehicles. Because we are getting introduced to new technologies such as the Internet of things (IoT), Blockchain, Big Data and Analytics, Shared Mobilities, Electrification, Vehicle Connectivity, Human-Machine Interface, Autonomous vehicles, Machine Learning, Cloud Computing, Smart Robotics in fostering innovation etc. When there is any enhancement in the technology there raises the issue of privacy and security. Security of the vehicle doesn't mean only the surface of the vehicle it is also about the passenger, environment and other factors. Charlie Miller and Chris Valasek demonstrated successfully hacked into a Jeep Cherokee in 2015 using computers connected to the Internet. They had control over the steering wheel, accelerator, air conditioning, radio, windshield wipers, and even the brakes, which may endanger the driver's life [1]. The destination data is provided as an input in the central processing unit when it comes to fully autonomous cars. If the wrong input is given, the vehicle may explode. Remote parking was made available in select automobiles in 2017, including the Audi A8, Tesla Model S, and Nissan Leaf EV. These systems are accomplished using a smartphone application. Some firms attempt to use car information provided across networks, known as telematics, for their operations. Autonomous driving is also linked to connected vehicles [2]. In 2018-model-year automobiles have reached level 3 self-driving, however, this is primarily accomplished by sensors attached to the vehicle itself. They constitute a system of systems when they are linked. As a result, it adds a key layer of communication and information infrastructure to mobility and transportation [2]. Apple established the CarPlay platform with the help of various car manufacturers, and this platform makes iPhone use in automobiles possible via the navigation system. CAVs have the potential to reduce traffic congestion, pollution, and automobile accidents. They constitute a system of systems when they are linked. As a result, it adds a key layer of communication and information infrastructure to mobility and transportation. Wireless technology i.e., 5G is an emerging technology. Connected and Autonomous Car (CAVs) is made up of sensors and different software. It is helpful in Vehicle-to-everything (V2X) communication. This prevents traffic accidents and saves lives by allowing the vehicle to interact with everything. For example, currently, everything is connected and if the vehicle is lost or stolen when it is connected to an application using GPS, we can find the location of the vehicle. But we can easily collect information by hacking into the public WIFI and hotspot. The attacker gets information about the vehicle. Here raise privacy, security and trust issues that affect the vehicle. There are several types of attacks that not only influence the attack surface but also operational safety. Due to the sheer safety implications, it is difficult to safeguard the security of cars and the infrastructure on which they rely. Inadequate security might result in vehicle theft, and data leakage or it can lead. to the death of occupants. Evaluating these security concerns in isolation is inadequate since vulnerabilities may and frequently are exploited in combination, resulting in increased threats with the potential for greater harm. As a result, security is introduced into the development process. Threat modelling is important in security requirements. Using threat modelling, potential risks such as structural vulnerabilities or the lack of suitable protection can be discovered, listed, and mitigations can be prioritized. Threat modelling is almost used in every stage of the vehicle's development process. The car's lifecycle of design and development is the concept, product, development, production, and operation. There are five major steps in threat modelling first, we must identify the security requirements i.e., what are the possible attacks on the vehicle and then we must create an application diagram, identify the threats, mitigate the threats and validate the threats that have been mitigated. There are many types of attacks, and those attacks are discussed here. The attack against automobiles has escalated over the years. Direct physical attacks, indirect physical vulnerabilities, sensor faking vulnerabilities, and wireless vulnerabilities are automotive cyberattacks.

II Types of Cyber Attacks

***Physical Access**:*

It is classified into invasive and non-invasive. This classification is done based on whether the device is attached to the vehicle or not [3].

A. Non-invasive attacks:

Side-Channel Attacks: A side-channel attack is a security issue that attacks the system's or hardware's indirect effects to get information from or affect the programme execution of a system rather than attacking the programme or its code directly. For example, Capturing and analyzing timing information, power usage, electromagnetic leakage, acoustic signal analysis, and data remanence are all examples of side-channel assaults. Asynchronous processing units and shielding devices are used as defences against side-channel assaults [4] [5].

B. Invasive Attacks:

1. Code Modification: An OBD-II scanner is a low-cost gadget that car owners and maintenance professionals may use to perform vehicle diagnostics. More advanced scanners may also include chip-tuning capabilities, allowing them to extract and change ECU codes. An attacker, on the other hand, may use similar tools to modify harmful code in order to infiltrate the system. To fight against such attacks, ensure that any vehicle connections are password-protected so that only authorized individuals have access, and that only approved and validated code updates are made [5].

2. Code Injection: Like code modification attacks, an adversary may introduce destructive codes into ECUs after obtaining access to the vehicle's networks and ECUs. Malicious programs such as viruses, Trojan horses, and malware may also enter an AV via this method. When one or more of the vehicle's components or sub-systems are non-compliant, car owners may inject codes with the intention of improving the performance of their vehicle or deceiving regulatory checks. One method of defending against this attack would be to use an intrusion detection system and finer granularity control over privileged access, which should only be granted to authorized personnel, which may not include the vehicle's owners in certain circumstances [5].

In-vehicle Attack:

In-vehicle network attacks are location trailing attacks, close proximity vulnerabilities, remote sensor attacks, GPS spoofing attacks, controller area network (CAN) and society of automotive engineers (SAE) J1939 buses vulnerabilities, ECUs software flashing attacks and integrated business service attacks.

1. Location Trailing Attacks: The hacker can track and locate the vehicle using this. By doing this, we can collect the driver's personal information and real-world data. For example, if a person used his driverless car to his work location and the attacker can track and locates his vehicle, he can easily get complete information about him. Here raises the privacy issue. He can also attack the vehicle. Here raises the security of the vehicle issue.

2. Close proximity vulnerabilities: This type of attack is used in short-range communication. This is achieved by a tire pressure monitoring system (TPMS), Bluetooth, keyless entry and ignition systems. Using TPMS, messages can be received up to 10 metres to 40 metres by a basic noise amplifier. Using keyless entry, When the driver tries to lock his car with a variety of devices, such as garage door openers and house light controllers/dimmers, the opponent may block the signals from the key fob [1].

3. GPS spoofing attacks: CAVs completely rely on GPS because using GPS the vehicle reaches the destination. The attacker can fake the GPS signal which is higher than the true signal. By GPS spoofing attack they can fake time and location so that the vehicle is attacked.

4. Remote Sensor Attacks: One of the primary concerns in the environment of CAVs is those different electrical components, such as ultrasonic radar, lidar, camera, and other sensors, are connected via an in-vehicle network. In terms of range, detecting capabilities, and reliability, each type of sensor has its own set of advantages and disadvantages. Furthermore, existing wireless access technologies can be used by other organizations to connect to sensors. As a result, the attacker in CAVs has a simpler time gaining access to a susceptible and peripheral sensor than in autonomous cars. The attacker will be able to capture the control of the sensor and launch remote sensor attacks as a result.

5.ECUs Software Flashing Attacks: It is an embedded system, which can control gear shift, servo steering, ignition system, electronic window lift, climate controls, etc. It is reprogrammable and helpful in correcting bugs and integrating functionalities without replacing them. It can be attacked by reverse engineering, fuzzing attacks, phlashing, and code modification.

6. CAN and SAE J1939 buses vulnerabilities: The main problem in CAN is it lacks authentication and encryption. The unauthenticated message can listen to any message if it is from an unauthorized node. So that the attacker can collect information about the driver including personal information, location, address book and contact location. It is also vulnerable to DoS attack [1] [6]. When a message is sent to a specified destination in connection mode on the SAE J1939 bus, both the sender and the receiver can break the connection. By delivering an abort message to either the sender or the recipient, the attacker can terminate the connection.

Vehicle to Everything Network Attacks.

The vehicle not only interacts with other vehicles it also interacts with other things in the environment. This enables to exchange of data among the connected vehicle and other things. The types of vehicles to everything network attacks are DoS attacks, Relay attacks, Routing attacks, Impersonation attacks, password and key attacks, Eavesdropping attacks and Data falsification attacks.

1. DoS attacks: DoS attacks occur when an attacker uses interference signals to block the whole communication channel [1]. Dos attacks are common and serious attacks. It generally takes place in the back end of the server [2]. On the network nodes, the attacker inserts useless messages or causes problems. As a result, authentic users are unable to access network services. Correct communications are unable to reach their intended recipients. DoS attacks can cause a delay in the receiver's response and interfere with it. In the context of CAVs, a slight delay might compromise the vehicle's driving safety. An accident can be caused or avoided in a fraction of a second. Furthermore, the need for reaction time is rather high. CAVs are vulnerable to DoS attacks, which can be deadly [3]. Example Tesla Model S [7] and Nissan Leaf [5].

2. Relay Attacks: Replay attacks are common in several authorizations and key agreement systems in order to spoof a real vehicle. The attacker basically collects and retransmits early acceptable at a later phase in replay attacks. It happens regularly only at the network or transport layer. It has the potential to mislead authorities, mislead the entire traffic, and even risk transportation safety.

3. Routing Attacks: Routing attacks make use of routing protocols vulnerabilities. The attacker might break the usual routing process or delete incoming packets in these attacks [5]. The types of routing attacks are wormhole attacks, blackhole attacks and grey hole attacks. A single hacked node or a group of cooperating nodes can launch a black hole attack [8]. In grey hole attack packets are dropped in a selected manner [9]. In a wormhole attack, two cooperative nodes are required. The attacker captures a packet at a location and stores it in another location [10].

4. Impersonation Attacks: The attacker sends fake messages, send modified messages and critical messages where he fakes his identity [1].

5. Password and key Attacks: The attacker cracks the password. Classified into rainbow table attacks, brute force attacks, and dictionary attacks [1].

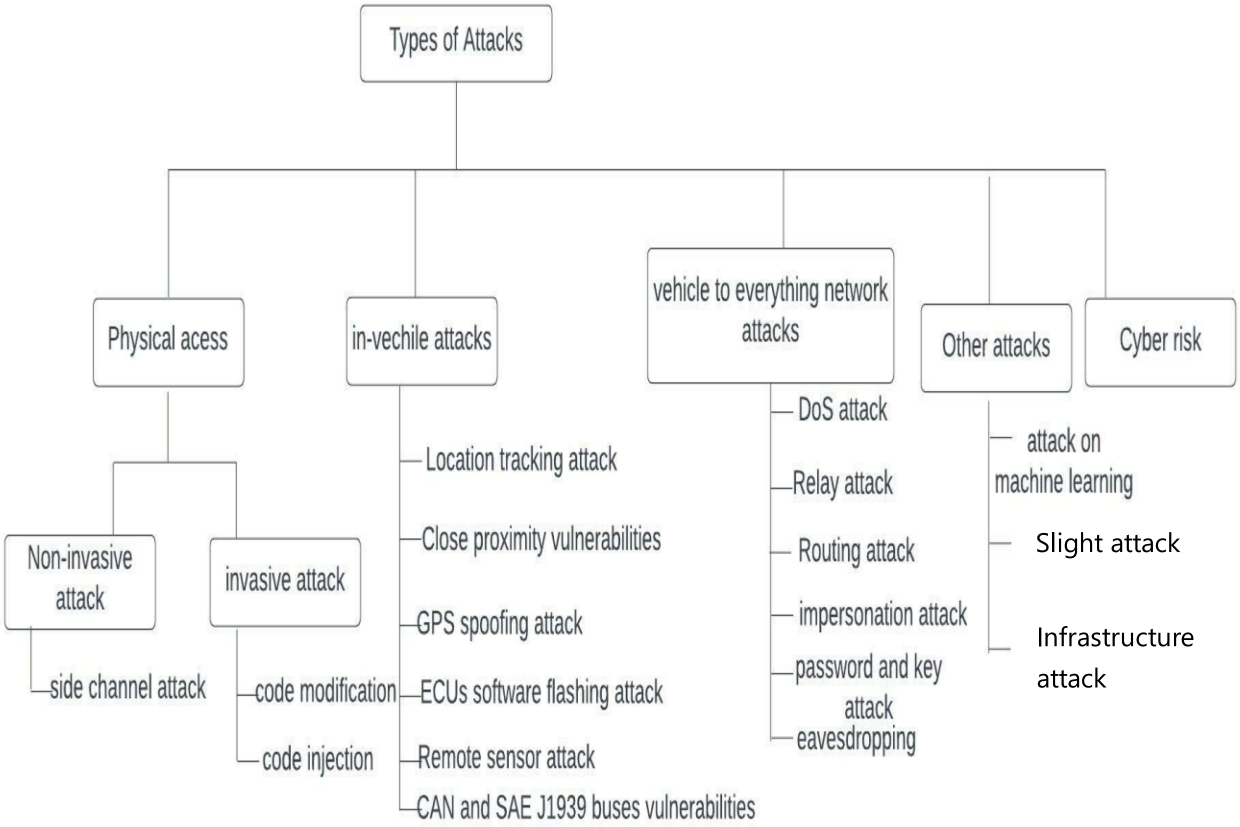

FIG 1 CLASSIFICATION OF ATTACKS

6. Eavesdropping Attacks: It is in short overhearing. Leaking the actual identity. This is mostly achieved in wireless medium [1].

Other Attacks:

Other attacks include Attacks on machine learning systems, Infrastructure attacks and slight attacks.

1. Attacks on machine learning: Machine Learning systems can be used for security-sensitive tasks such as vulnerability detection and security monitoring. This can be attacked in the phase of data collection, prediction and training [1]. The attacker can modify the original data and insert malicious data this will affect the algorithm. Without affecting the accuracy, it leaks the user's private information [1].

2. Slight Attacks: This method will be engaged if the difference between predicted and measured behaviours reaches a predefined level. In this instance, the pre-set security mechanism may be rendered ineffective. Even minor attacks can create dangerous situations and pose severe safety concerns for all cars in a CAVs fleet. The scientists stated that when CAVs are subjected to minor attacks, communicating locations are more hazardous than speeds. It is possible that a situation involving more automobiles under attack with a low severity is more dangerous than one with fewer vehicles under attack with high severity [1].

3. Infrastructure Attacks: Surface attack takes place. The attacker attacks the onboard unit, cloud server, roadside unit, intelligent traffic, traffic management centre etc. There are many entry points for the attacker this attack leads to accidents and several attacks on the vehicle.

Cyber risk:

Cyber risk is described as the risk of financial loss, interruption, or harm to an organization's reputation caused by a breakdown of its information technology systems.

III AUTONOMOUS VEHICLE SECURITY

To reduce the attack surface, several strong encryption and authentication methods and approaches may be used to assure autonomous vehicle security [11].

The step for designing security is

1. Determining the objective
2. Accessing the sensitivity
3. Estimating capabilities
4. Determining the control features [11].

As mentioned earlier the types of attacks in the CAVs, these attack causes a more severe impact as the degree of automation increases. In connected and autonomous vehicles, a huge number of data are transferred. These data must be safe. The security requirement for data transfer is availability, authorization, privacy, anonymity, data integrity, data confidentiality, authentication: user, source, location authentication, traceability and revocation: track malicious entities [11].

Defences for autonomous vehicles (AVs) are categorized into four types: active defences, preventive defences, passive defences, and collaborative defences. Having several lines of defence and layers of defence ensures a higher level of security preparation and resistance against threats.

A. Preventive defence is enhancing security measures to threaten an attack as it occurs. Authenticating the user and the in-vehicle device, securing communications, and managing network traffic are all part of this form of protection (through the firewall) [11]. It considers the system's regular operating settings and places less emphasis on the situations during or after an attack [5].

1. Secure Communication is Used to make sure that vehicle data transfer and encryption are safe because it is essential. The secrecy of data transmission can be ensured by encryption. It may also be feasible to rely on the keys to validate the sender's identity, depending on the encryption strategy employed. MAC (message authentication code) algorithms are also required to secure and verify the integrity of the data being received.

2. *In-Vehicle Device Authentication*: As recommended in [12], certificates can be produced to facilitate the authentication procedure, ensuring that the AV controllers can be trusted. Each controller will then have a certificate with its controller identity, public key, and authorization (i.e., the operations it is permitted to do). The gateway will store a list of public keys for all the vehicle's approved Original Equipment Manufacturers (OEMs). The corresponding controller and its authorization are added to the gateway's list of valid controllers if the authentication procedure is successful.

3. User Authentication: Using an extra, although a seamless layer of user authentication, such as biometric identification, is another technique to ensure the allowed use and management of the car Biometric.

B. Active defences can be implemented by continually checking the autonomous vehicle's security scales or by employing adaptive security. The latter is distinguished by redesigning the assault targets and enhancing techniques in order to have greater influence over the attack when it occurs [5].

1. Continuous Security Monitoring:

The infrastructure is a vital system with major repercussions if their security is compromised, near real-time situation awareness of their security health states is required [5]. As a result, continuous security monitoring is needed to give snapshots of their states at regular intervals in order to analyze their security status. It is also crucial to establish where and what to monitor so that critical components and interfaces are not caught off guard.

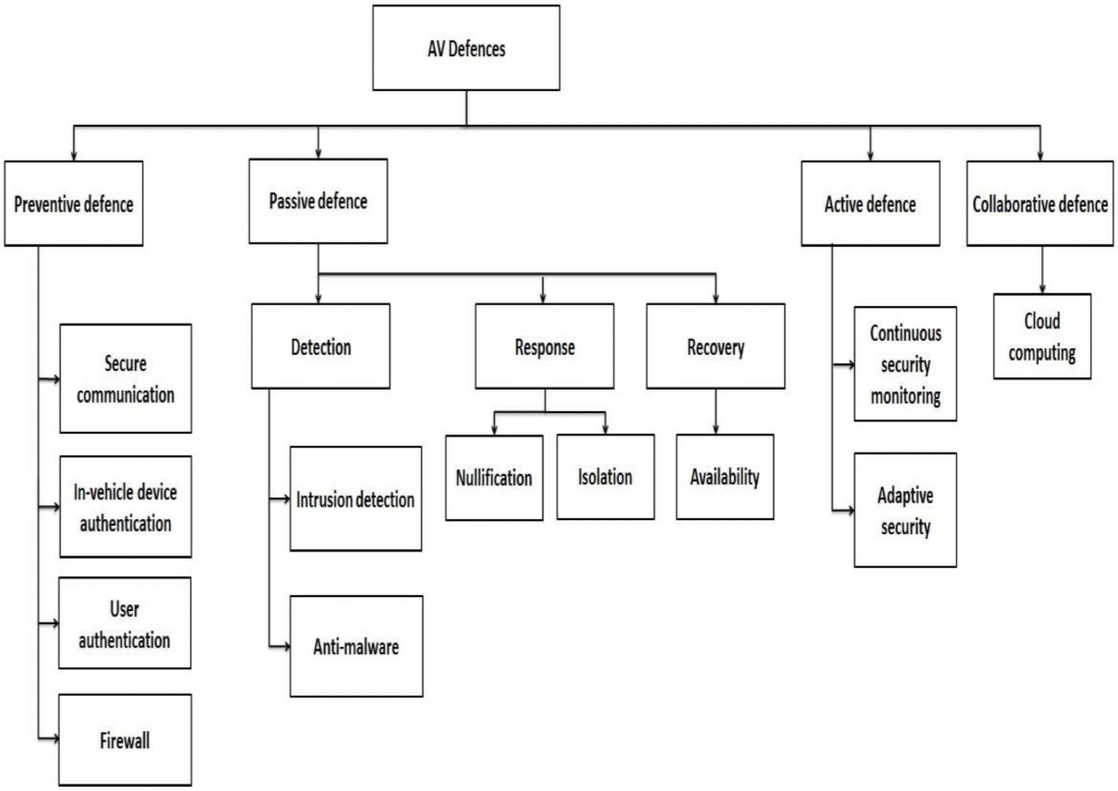

FIG 2 CLASSIFICATION OF SECURITY DEFENCE STRATEGY

2. Adaptive Security:

In today's environment, static defences are no longer sufficient, since assaults on systems, networks, and critical infrastructure continue to change at a rapid rate. As a result, it becomes vital to build and deploy defence measures that are moving targets themselves. Deception techniques and adaptive reconfiguration of assault targets can be used to gain greater control and tip the balance during an attack [5]. Furthermore, detection models should grow through self-learning during their operational lifespan in order to respond to new types of threats.

C. collaborative defence occurs in coordination with cloud services. Autonomous cars can work together to improve their cybersecurity. Vehicle-to-Internet-of-Things, or V2IOT, will be deployed into clouds in the future to minimize communication routes. As a result, attackers will have a more difficult time attacking autonomous vehicles [13]. This defence method mostly happens in Cloud computing.

D. Passive defences are implemented to identify, respond to, and recover from a security breach. It may be characterized as identifying methods to avoid malware, as well as code insertion and modification approaches. Responding to these attacks and mitigating their damage is accomplished using electrical or cyber capabilities, such as a GPS anti-jamming device or isolation. Isolation refers to disconnecting the autonomous car from the inter-vehicle communication network in order to prevent causing harm to others [11].

1. Attack Detection

Intrusion Detection

Modern automobiles can detect the existence of physical security threats and inform their owner or anybody in the neighbourhood with the use of vehicle alarms (e.g., glass break audio sensor). Cyber assaults influence the CAVs' activities, on the other hand, may be less visible or traceable. Nonetheless, many Intrusions Detection Systems (IDS) models for CAVs security have been suggested and verified using computational simulation scenarios [14], [15]. In an ideal world, innovation with CAVs IDSes should continue, with the goal of improving attack attempt detection accuracy [5].

Anti-Malware

Anti-malware solutions for AVs should be capable of defending the AVs against malicious software that attempts to penetrate the system, just as they are in normal computer systems. Because AV malware is still in its infancy, there may not be much malware out there. AV attack modelling, innovative malware built particularly for AVs, and behavioural-based malware detection and mitigation for AVs should all be prioritized by the research community.

2. Attack Response:

Nullification

The capacity of an entity to invalidate or negate a cyber-attack utilizing electronic or cyber capabilities are referred to as nullification. The adoption of GPS anti-jamming systems [16] is an example. Null forming is used in GPS anti-jamming technology to suppress interference from jamming devices. The nominal interference suppression capability of such systems can exceed 40 dB [5].

Isolation

During an attack, the self-isolation of the AV can help prevent other vehicles from obtaining false information. Ignoring ECU reprogramming while the engine is still running is another example. Aside from self-isolation, when an assault on an AV is undertaken, the vehicle should ideally reply in a way that alerts other cars nearby so that their apps may be updated [5].

3. Attack Recovery:

Availability

Availability becomes a significant concern in critical systems. In the case of autonomous vehicles, availability is critical since it is essential to ensure the safety of passengers and other road users. As a result, protection and fault tolerance methods must be implemented into the system to ensure the CAV's durability and ability to recover fast in the event of an attack [5].

IV RESEARCH ANALYSIS

A multi-layer security system is necessary to secure the vehicle. A multi-layered strategy to vehicle cybersecurity lowers the chances of a successful cyber-attack and mitigates the implications of a successful incursion. Security design, awareness and training, governance, collaboration with third parties for security, risk management and assessment, threats detection and protection are all essential areas in which specialization is required. A robust and constant Internet connection is required for the autonomous vehicle to convert into a sophisticated cyber-physical system. Cyber security is a movable target, with hackers continuously looking for new methods to exploit flaws, and automakers must be cautious and prepared to combat them. One of the most effective techniques is to integrate security into the connected car. This may be accomplished by incorporating an inbuilt firewall that can help identify and report risks, safeguard communication, such as V2V and external communication to the vehicle, prevent communication from unauthorized devices, encrypt data to preserve privacy, and secure the firewall. Plan for authentication and access control, external attack protection, detection, and incident response. The development of overall vehicle safety, security, and risk assessment are essential. The OTA system and scenario-based TARA are the two most important concerns in cybersecurity engineering. To develop a set of cybersecurity goals for a HADF, a step-by-step study must be performed to execute Threat Analysis and Risk Assessment (TARA) against probable vulnerabilities.

V CONCLUSION

This article discussed the types of attacks, vulnerabilities and how to protect the vehicle from these attacks i.e., the defence strategy. The type of attack and intensity of these attacks keeps increasing every day. This attack can happen from any direction, and they sometimes risk the life of the passenger. Make sure that these attacks are checked and find a potential way to make the effect less.

REFERENCE

[1] F. R. Y. F. a. P. Z. Xiaoqiang Sun, A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs).

[2] J. TAKAHASHI, An Overview of Cyber Security for Connected Vehicles.

[3] P. W. K. W. a. J. M. Simon Parkinson, "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges".

[4] K. D. a. S. B. Mustafa Saed, "A Survey of Autonomous Vehicle Technology and Security".

[5] V. L. L. T. a. J. Wu2, "Autonomous Vehicle Security: A Taxonomy of Attacks and Defences".

[6] M. S. a. O. B. J. Michael, "Driving Down the Rabbit Hole," *Proc. DEFCON Hacking Conference 25,* 2017.

[7] M. R. a. K. Mahaffey, "How To Hack a Tesla Model S".

[8] S. S. A. a. E. M. Fredericks, "Lightweight detection and isolation of black hole attacks in connected vehicles," *IEEE 37th Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW),* 2017.

[9] S. C. D. a. S. J. K. C. Purohit, "Mitigation and performance analysis of routing protocols under black-hole attack in vehicular ad-hoc network (VANET),".

[10] P. K. a. S. Verma, "Detection of wormhole attack in VANET".

[11] H. N. a. W. Z. E. B. Hamida, "Security of Cooperative Intelligent Transport Systems:

Standards, Threats, Analysis and Cryptographic Countermeasures," vol. vol. 4, 2015.

[12] A. W. a. C. P. M. Wolf, "Security in automotive bus systems," *The Workshop on Embedded Security in Cars,* 2004.

[13] A. C. a. K. Y. Lam, "Autonomous Vehicle: Security by Design," 2018..

[14] M.-J. K. a. J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PLoS ONE,* vol. 11, 2016.

[15] A. G. a. K. M.-M. K. M. A. Alheeti, "On the detection of grey hole and rushing attacks in self-driving vehicular networks," *Journal of Computers,* vol. 5, no. 2016.

[16] Z. M. a. C. Schmittner, "Threat Modeling for Automotive Security Analysis".