International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 03 | Mar 2024 www.irjet.net p-ISSN: 2395-0072

Cyber threats to autonomous vehicles: The risks of hacking, Ransomware, and other Cyber-Attacks

Mohammad sufiyan Rajapatel[1], Mangesh A Deshmukh[2]

[2]Design Engineer, Tata Technologies Ltd, Pune
[2]Manager, Tata Technologies Ltd, Pune

Abstract - *The emergence of autonomous vehicles promises to revolutionize transportation, but it also presents new cybersecurity threats. The growing sophistication of hacking, ransomware, and other cyber-attacks could lead to disastrous consequences for passengers and other road users. Therefore, strong cybersecurity protocols are crucial in mitigating the dangers of cyber threats to autonomous vehicles. These protocols include encryption, multi-factor authentication, and intrusion detection systems. Data privacy policies are also important to safeguard personal information collected by autonomous vehicles. To fix vulnerabilities, businesses must become aware of them and locate weak points in their hardware and software systems, applying security updates and patches. Employee education is necessary to teach them the risks of cyber threats and how to spot and react to them. Collaboration among technology companies, automakers, regulators, and other stakeholders is also necessary to establish best practices and guidelines for autonomous vehicle cybersecurity. Incident response planning is essential to ensure that protocols are in place to react quickly and effectively to cyber-attacks. Advanced sensor and perception systems are critical to identifying cyber threats and taking appropriate action. Companies must develop systems that can detect anomalies and potential threats in real-time and respond quickly. In conclusion, managing the risks of cyber threats to autonomous vehicles is crucial for the safe and effective operation of these vehicles. By implementing robust cybersecurity protocols, data privacy policies, risk assessment, employee training, partnerships, incident response planning, and advanced sensor and perception systems, companies can ensure the safety and security of autonomous vehicle operations and maintain the public's trust in this emerging technology.*

Key Words: RADAR, LiDAR, V2V Communication, Autonomous Vehicle, Self-driving vehicle.

1.INTRODUCTION

As the world moves towards IoT-based devices, where all the devices are communicating with each other to improve lifestyles and provide ease of operation. The automobile industry has also grown and is submerged in the pond of new technology, which opens a new era. Now the automobile industry has grown so much that it is reducing human dependencies through technologies such as adaptive cruise control, departure warning systems, automatic parking systems, Auto pilot. As the industry started to pack new features into vehicles with the help of different types of sensors, cameras, navigation units, etc., It gave the rise to new sort of vehicles such as self-driving Vehicles. As the vehicle depend on the different sort of sensor which communicates with each other and provide feedback to control system and start to run on its own. It has an abundant amount of potential to change the whole transportation system. Such vehicles will reduce human dependency and can be operated by disabled and elderly men. Also, they can be used in dangerous war zones where the chances of human life loss are higher. Instead of these, self-driving vehicles can reduce the issues created by the misuse of vehicles, such as traffic issues, fuel consumption, optimal use of roads, reduction in accidents, etc. These vehicles have various technologies packed into them, like radar, sensors, GPS, and on-board cameras, which help the vehicle understand its surroundings. The data of the surroundings, which were sensed by using these technologies, was fed into the advanced control system present in the vehicle. This system processes the data and makes relevant decisions regarding navigation and any obstacles that may be present on the way. Also, translate traffic signals and signage that allow the vehicle to reach its destination with incident while considering other cars on the surrounding road. Even though autonomous vehicles have many advantages, there are still challenges with them. As technology is in the early stages of the era It raises many issues, such as cyber-attacks, data breaches, privacy concerns about one's personal data, etc.

The technology isn't mature enough to completely rely on it. Many companies race around and try to capture the most of the market while trying to introduce a new sort of vehicle. This paper will look at the market penetration of the self-driving vehicle and the security issues involved in it..

2. HOW SELF-DRIVING (AUTONOMOUS) VEHICLE WORKS?

of "Sense, Understand & Act". In the sense phase, the vehicle observes the surroundings and generates data. In the understanding phase, the data generated in the trailing phase is processed and transmitted to the algorithms. Then algorithms decide what else needs to be done.

If we move deep into the vehicle algorithms. The autonomous vehicle has dependencies on sensors, radar, cameras, actuators, and powerful processing hardware. The vehicle creates maps of its surroundings with the help of the sensors, which are situated on the vehicle exterior. Radar prepares the data on the nearby vehicles. Then cameras produce the data from the traffic signals and signs. LiDAR detects the position of the vehicle, creates a map of the road edges, and identifies the lane markings. When all the data gets generated with the hardware, it moves to powerful machine learning software, where it gets processed. Which controls the steering, acceleration brake, etc. (Refer Figure 1.)

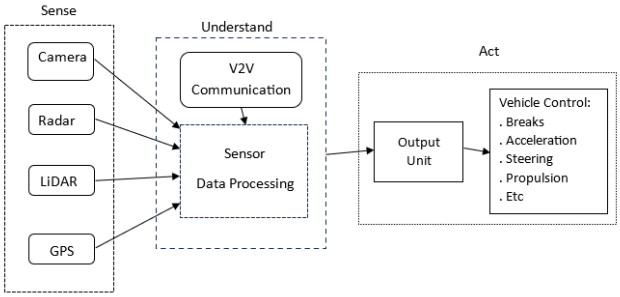

Fig -1: 3 Phases of Autonomous Vehicle.

3. MERITS OF THE AUTONOMOUS VEHICLES –

As mentioned earlier, autonomous vehicles have an abundant amount of potential to revolutionize the automobile industry by transforming the world of transportation, increasing the safety of passengers and goods, and improve workability in worst-case scenarios such as warzones and hazardous places. This section of the paper will discuss a few of the benefits of autonomous vehicles.

3.1 SAFETY -

As vehicles don't have human dependency, they will follow all the rules that were programmed in the software and reduce the chance of accidents by significant numbers. Also, many studies have found that drivers get distracted behind the wheel with respect to drunk driving, speeding, and the use of smartphones. But as vehicles are programmed to avoid accidents, Autonomous vehicles are designed to work on any sort of road line, and advancements in the technologies used in these vehicles have made them safer and more reliable. But in a few situations, the vehicle must be able to comprehend the circumstances and provide a workable remedy. If human life loss is unavoidable, then it is crucial to consider if the safety of the drivers and passengers of the vehicles is more essential than the safety of the pedestrians. So, to successfully use the autonomous vehicle and surrounding area consisting of roadside units and a V2V (vehicle-to-vehicle) communication system, it needs to be developed.

3.2 DRIVER INDEPENDENCY –

As the autonomous vehicle operates on its own, it avoids the dependency of the driver. It provides a safer and more enjoyable ride for passengers. These sorts of vehicles will have more advantages for the elderly, young and disabled people. These populations can be moved effectively to destination without the help of a third party. The vehicles can serve as mobile offices for those who are employed and can amuse passengers during long commutes. According to a recent survey, Youngster are attracting towards the public transport as they provide chance to use travel time for them. These individuals might be among the first to use autonomous vehicles. Shared autonomous vehicles can meet the needs of city dwellers if there is no public transit available there. Another benefit of the vehicle is the elimination of chauffeurs or the need to get driving licenses.

3.3 USE OF VEHICLES IN DIFFERENT SECTORS –

Numerous businesses, including the military, freight transportation, and mining, are increasingly implementing autonomous vehicle technology. The trucking sector is implementing autonomous vehicle technologies to facilitate long-distance transportation. The adoption has decreased the need for drivers and improved these trucks' fuel efficiency. These trucking companies deploy a large number of autonomous cars that travel in tandem to engage in a behavior known as platooning. Large autonomous earthmovers are utilized quite effectively in the mining sector. These earthmovers are incredibly efficient and follow a set path their destination. Because fewer people are working around large pieces of equipment, autonomous vehicles help to increase human safety. The productivity of autonomous mining vehicles is increased because they do not require specialized equipment operators. The defense industry has embraced autonomous vehicle technology very enthusiastically. The military views autonomous vehicles as a key enabler for the protection of its soldiers. Military vehicles with driverless technology can be used to distribute commodities and necessities without the need for human interaction in sensitive locations.

4. LIMITATION AND ISSUES WITH TECHNOLOGY –

Though using autonomous vehicles has many benefits, its applicability on a wide scale is still up for debate. Large-scale implementation studies are still being conducted in real-world settings, and ongoing study is required. The expenses of manufacture, liability in case of accidents, and licensing concerns all have a significant impact on how well autonomous vehicles are put into use. Security and privacy considerations are also a very essential area of research because these vehicles operate using computing technologies. This section will discuss a few of the limitations and issues with technology.

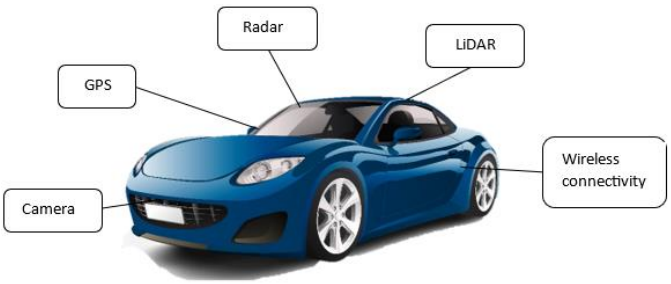

Fig -2: Various Sensor on AV

4.1 VEHICLE COST -

The autonomous vehicle uses various technologies such as sensors, GPS, LiDAR, and cameras, which are very expensive and require high-end software to operate. These technologies put the price of autonomous vehicles beyond the purchasing power of average people who own cars. Only if they are widely used will autonomous vehicles be successful, leading to further price reductions for the same vehicles. Like any technological adoption, whether it be electric automobiles or computers, future prices can only be decreased with technological advancements and mass production. Early adopters might pay higher prices, but expenses can eventually be reduced.

4.2 TECHNOLOGICAL & LIABILITY ISSUES –

Autonomous vehicles depend on the integrated sensor, cameras, LiDAR and processing unit. Any failure in the devices will cause a loss of control and raise the probability of a loss of human life. In ideal circumstances, every technology on autonomous vehicles has performed brilliantly. Extreme weather, such as hailstorms, torrential rain, or snow, will, however, cause the system to malfunction and interfere with the sensors and video systems. To determine how these vehicles will respond, further research must be done in these areas. Even though autonomous vehicles can drive themselves from one place to another, human assistance is still required to make sure they are operating securely. This might be a problem since future drivers might be too dependent on technology and might not remember how to operate a car safely. Autonomous vehicles are pre-programmed, and the use of artificial intelligence technologies enables them to adapt to changing road conditions and environments.

As the device integrated into the vehicle has a chance of failure, accidents may happen, and in the worst situations, lives can be lost. In this situation, the issue of liability for accidents arises. Who is to blame? Is it the person operating the car, the producer, or the person who created the algorithm? The insurance concerns for such accidents are another factor. Humans are typically protected from punishment when accidents happen for reasons beyond the driver's control. In the majority of the nations where autonomous vehicles may be used, there are also no legal precedents. Regarding accidents involving autonomous vehicles, there is no current legislation or legal requirement. There are no national centralized regulatory organizations in place to control the use of autonomous vehicles. The laws and regulations that apply in one state might not apply in another state.

4.3 ETHICAL AND SECURITY ISSUE –

The major concern of autonomous vehicles is the security of the vehicle. The hacker can break into the system and manipulate the operation of the vehicle. Given that the car might be used for criminal activities, this can be exceedingly risky. The bomb-laden truck can be used by terrorists to attack important locations. They can also be employed as rolling missiles that target certain areas of the road and cause havoc. Any malware can propagate swiftly via the complete automotive network to enter a large number of vehicles since cars are connected to and communicate with one another. These malwares have the potential to be harmful and can be used to conduct planned and well-executed attacks. Autonomous vehicles track and communicate location data as well. This might enable user tracking, which hackers could abuse for surveillance or, worse, criminals could exploit to track the position of victims.

Also, there are several non-technical ethical issues with the use of autonomous cars. Concerns about what to do in an emergency are being voiced. Whom should the car's occupants protect—the pedestrians or the drivers? Should the car make an effort to avoid any animals that might hurt the occupants by crossing the street? Who makes the decisions during these programs, and how should they be made in such situations? Human drivers are more than capable of handling ethical dilemmas, but autonomous vehicles may not be able to do so as they are ultimately machines that execute preprogrammed code. Before the widespread use of autonomous vehicles, the built-in processing software must reach a high level of maturity.

5. HACKING/ CYBER ATTACKS –

The reliability of autonomous vehicles has been improved regularly by the manufacturers. Increasing the accuracy of the data collected by the numerous sensors on these vehicles is the main way to accomplish these goals. There were many cases where, during the outdoor testing of the autonomous vehicle crashed into the surrounding vehicle, and in a few cases, it caused death. The significance of having precise sensors that function in typical driving conditions is made clear by this accident. The fact that the sensors shouldn't be open to outside input or hacking is much more crucial. Inputs from outside sources or successful hacks could result in inaccurate readings and sensor issues.

Table -1: Attack and their possible methods

Category	Types	Methods
Sensor Attacks	Sensor Spoofing	Malware, Ransomware
	GPS spoofing	False data packet Virus
	Proximity vulnerabilities	False data packet Virus
	CAN and SAE J1939 buses vulnerabilities	Malware, Ransomware
	ECUs software flashing	Reverse engineering, Malware, firewall bridging
Software Attacks	DoS attacks	Burette Force Data birding
	Impersonation attacks	Firewall False authentication Attack
	Data falsification attacks	Burette Force Data birding
	Eavesdropping attacks	Reverse engineering, Malware, firewall bridging
	Password and key attacks	False data packet Virus

5.1 ATTACK AGAINST SENSORS

Autonomous vehicles depend on sensors such as ultrasonic sensors, radar, LiDAR, GPS, etc. These sensors provide the surrounding data and encode it for the processing unit. LiDAR is a device that uses rotating laser beams. The tool aids in the autonomous vehicle's environmental navigation and is used to detect obstructions. The LiDAR system produces data that tells us where obstacles are located in the environment and where the autonomous vehicle is in relation to those obstacles. Road curves, infrastructure, vegetation, and elevation of roadways can all be seen in LiDAR data. Attackers can make noise, fabricate reflections, and spoof artificial objects when targeting a LiDAR system. Autonomous vehicles use GPS satellites to locate their own geographic positions. For the installation of autonomous vehicles to be successful, the geographic coordinates and vehicle identities provided by these satellites are crucial. Attack involving positioning—during this attack, a hostile person can take advantage of the behavior by employing a GPS satellite simulator. If the signal from this gadget is stronger than the real GPS satellites, it may be used to trick cars into believing they are somewhere else. The vehicles are tricked into believing they are somewhere other than where they are, which will interfere with how effectively they behave. Etc,

5.2 ATTACKS ON ON-BOARD CAMERAS –

In order to comprehend the visual identification of the environment where the autonomous vehicle is being operated, on-board cameras use visible light and optics. Particularly helpful are the cameras for detecting lanes, traffic lights, and road signage. The driving and stopping abilities of autonomous vehicles are improved with the help of this data. Conducting a blinding attack against on-board cameras is the most significant attack. The purpose of the assault is to affect the camera's sensor by exposing it to a bright light that prevents the camera from seeing actual traffic signals or objects for a short period of time. This type of attack can be carried out using a variety of light-emitting devices. Some of these common light-emitting gadgets are laser pointers and LED light sources. The camera needs 4 to 5 seconds to recover from such a blinding onslaught.

5.3 CYBER SECURITY ATTACKS-

Attacks that try to deny legitimate users access to the network and its resources are known as denial of service (DoS) attacks. Attackers overwhelm the network's active users by sending bogus messages, which lowers the network's effectiveness and performance. This attack is so significant that even if it is discovered, it will be incredibly challenging to stop. A vehicle in a network of cooperative cars has the ability to create a huge number of false identities and send bogus signals to other vehicles and RSUs. These fake communications may be deceptive and may prompt unexpected responses from other cars. In a distributed denial of service (DDoS) attack, several cars cooperate to launch simultaneous attacks from various places against a genuine vehicle. To prevent the target vehicle from being able to communicate with other cars or the RSU, multiple vehicles may assault it from various angles and at various times. These attacks are more likely because the autonomous car network uses a wireless channel. Additionally, because of the great mobility of vehicles and the quick changes in topology, there are more examples of these attacks, making detection more challenging. There were many more attacks that hackers can use to harm the vehicle and passengers, such as attacks via keyless entry, data falsification attacks, routing attacks, password brute force attacks, etc.

6. Defensive Strategies -

Protecting the safety and security of these vehicles and their occupants requires defensive measures against cyber-attacks on autonomous vehicles. Strong cybersecurity protocols must be implemented to safeguard autonomous vehicles from potential cyber threats. To prevent unwanted access to the vehicle's systems and data, authentication techniques, rigorous access controls, and encryption should be used. To fix known vulnerabilities and strengthen the

vehicle's resistance to new threats, regular software updates are necessary. The real-time monitoring, detection, and prevention of any attacks on the vehicle's network are all made possible by intrusion detection and prevention systems, or IDPS.

For the protection of data sent between the vehicle and external systems, secure communication methods are essential. Sensitive information is kept secure and encrypted by using protocols like Transport Layer Security (TLS). In order to reduce the danger of tampering and illegal alterations, secure boot processes and trusted execution environments are essential for ensuring that only authenticated and approved software runs on the vehicle's system. Strong data privacy safeguards should be put in place to preserve the privacy of personal information and telemetry data the vehicle collects, reducing data collection and storage to lower the risk of exposure to cyber threats. To inform people involved in the vehicle's development, maintenance, and operation of cybersecurity best practices, employee education, and awareness initiatives are crucial. An educated worker is better able to identify possible dangers and take appropriate action. Third-party penetration testing and security audits provide thorough assessments of the vehicle's systems, spotting vulnerabilities, and fixing potential shortcomings. Redundancy and fail-safe measures should be incorporated into the design of autonomous cars to guarantee that they will continue to operate even if some system safeguards are compromised. The sharing of best practices in cybersecurity is made possible by working with colleagues in the sector and taking part in information-sharing platforms.

Last but not least, an incident response strategy is essential in defining the steps to quickly identify, lessen, and recover from cyberattacks. These reaction plans are regularly tested and simulated to guarantee their efficiency. Manufacturers and operators of autonomous vehicles can improve the cybersecurity posture of their vehicles by implementing these defensive measures, which will increase public confidence in the deployment and general acceptance of autonomous transportation solutions.

Table -2: Few Preventions Strategies.

Category	Types	Prevention
Sensor Attacks	Sensor Spoofing	Strong authentication process
	GPS spoofing	Bias Estimation range check, GNSS Augmentation
	Proximity vulnerabilities	Strong data Encryption and Authentication Process
	CAN and SAE J1939 buses vulnerabilities	Hybrid Network encryption, Network breaker circuit.
	ECUs software flashing	Hybrid Network encryption, Network breaker circuit.
Software Attacks	DoS attacks	Integration of multi-level firewall
	Impersonation attacks	Integration of multi-level firewall
	Data falsification attacks	Strong data Encryption, Strong authentication process
	Eavesdropping attacks	Strong data Encryption and 2-way Data authentication.
	Password and key attacks	Malfunction Authentication

7. CONCLUSION –

Autonomous vehicles have already become accessible, and prominent automakers are stepping into this market. Vehicle manufacturers are embracing this technology. To successfully navigate and comprehend the area they are in, these vehicles rely on integrated sensors and technical equipment. For successful route planning, emergency movements, and route calculations, precise sensor data is essential. The main success criteria and barriers for autonomous vehicles have been covered in this essay. The importance of security is also discussed, along with a key component of autonomous vehicle security. Multiple security flaws in driverless vehicles have been discovered through attacks on various sensors and onboard cameras. Cooperative driving and wireless technologies are also essential for the development of autonomous vehicles. From other vehicles and their surroundings, the autonomous vehicles gather a range of data. The vehicles are vulnerable to malware and DoS attacks because of their wireless connectivity. A secure wireless solution that offers the highest level of privacy and security is essential for effective implementation.

References

1. Jafarnejad, S., Codeca, L., Bronzi, W., Frank, R. and Engel, T., "A Car Hacking Experiment: When Connectivity meets Vulnerability," 2015 IEEE Globecom Workshops (GC Wkshps), San Diego, CA, USA, 2015, pp. 1-6.

2. E. Schmidt, N. Gatsis, and D. Akopian, "A GPS spoofing detection and classification correlator-based technique using the LASSO," IEEE Trans. Aerosp. Electron. Syst., vol. 56, no. 6, pp. 4224–4237, Dec. 2020.

3. K. Greene, D. Rodgers, H. Dykhuizen, Q. Niyaz, K. Al Shamaileh, and V. Devabhaktuni, "A defense mechanism against replay attack in remote keyless entry systems using timestamping and XOR logic," IEEE Consum. Electron. Mag., vol. 10, no. 1, pp. 101–108, Jan. 2021.

4. K. Greene, D. Rodgers, H. Dykhuizen, Q. Niyaz, K. Al Shamaileh, and V. Devabhaktuni, "A defense mechanism against replay attack in remote keyless entry systems using timestamping and XOR logic," IEEE Consum. Electron. Mag., vol. 10, no. 1, pp. 101–108, Jan. 2021.

5. S. Kumar and K. S. Mann, "Prevention of DoS attacks by detection of multiple malicious nodes in VANETs," in Proc. Int. Conf. Automat., Comput. Technol. Manage. (ICACTM), Apr. 2019, pp. 89–94.

6. R. Moalla, H. Labiod, B. Lonc, and N. Simoni, "Risk analysis study of its communication architecture," in Network of the Future (NOF), 2012 Third International Conference on the. IEEE, 2012, pp. 1–5.I. Broster and A. Burns, "An analysable bus-guardian for event triggered communication," in Real-Time Systems Symposium, 2003. RTSS 2003. 24th IEEE. IEEE, 2003, pp. 410–419.

7. "Autonomous haulage: making mining safe and more productive today," [Online]. Available: http://www.cat.com/en_US/articles/customer-stories/mining/autonomous-haulage-making-mining-safer-and-more-productive-today.html.

8. "Google's Self-Driving Car Project Is Losing Out to Rivals," 2016. [Online]. Available: https://www.bloomberg.com/news/articles/2016-09-12/google-car-project-loses-leaders-and-advantage-as-rivals-gain