11-2023

A review of cyber attacks on sensors and perception systems in autonomous vehicle

Taminul Islam

Md. Alif Sheakh

Anjuman Naher Jui

Omar Sharif

Md Zobaer Hasan

Contents lists available at ScienceDirect

Journal of Economy and Technology

journal homepage: www.keaipublishing.com/JET

Review article

A review of cyber attacks on sensors and perception systems in autonomous vehicle

Taminul Islam[a,*], Md. Alif Sheakh[b], Anjuman Naher Jui[c], Omar Sharif[d], Md Zobaer Hasan[e]

[a] School of Computing, Southern Illinois University Carbondale, IL, United States
[b] Department of Computer Science and Engineering, Daffodil International University, Dhaka, Bangladesh
[c] Department of Computer Science and Engineering, University of Science and Technology, Chittagong, Bangladesh
[d] Department of Mathematics and Statistics, University of Texas Rio Grande Valley, TX, United States
[e] Lecturer, School of Science, Monash University Malaysia, Selangor D. E., Malaysia

ARTICLE INFO

Keywords:
Autonomous vehicle
Security threats
Artificial intelligence
Vulnerabilities
Machine learning
CAN
RONI

ABSTRACT

Vehicle automation has been in the works for a long time now. Automatic brakes, cruise control, GPS satellite navigation, etc. are all common features seen in today's automobiles. Automation and artificial intelligence breakthroughs are likely to lead to an increase in the usage of automation technologies in cars. Because of this, mankind will be more reliant on computer-controlled equipment and car systems in our daily lives. All major corporations have begun investing in the development of self-driving cars because of the rapid advancement of advanced driver support technologies. However, the level of safety and trustworthiness is still questionable. Imagine what the assailants could do if they had access to a car. Control of braking, acceleration and even steering by an attacker can have disastrous results. Most of the assaults against autonomous vehicle software and hardware are covered in this study, along with their prospective consequences. This work explores an extended analysis of the security threat and cyber-attacks on different sensors and perception systems in autonomous vehicles. This work also showed machine learning-based possible defensive techniques to prevent the security threat. An overview of most of the conceivable assaults against autonomous vehicle software and hardware and their prospective consequences is presented in this study.

1. Introduction

The integration of artificial intelligence in digital technology is rapidly expanding, with the automotive industry experiencing a surge in interest in connected to autonomous vehicles. An Autonomous Vehicle (AV) is a robotic or driverless vehicle that relies on sensors, machine learning techniques, complex algorithms, and actuators. These vehicles utilize powerful processors to execute software, eliminating the need for human intervention to control the vehicle (Badue et al., 2021).

Autonomous vehicle's leverage various technologies like vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2X) communications (Mun et al., 2022) to engage with their environment and operate safely. By sharing information on position, speed, and heading with other vehicles, these technologies help predict the vehicle's trajectory and navigate roads and terrains more easily

[*] Corresponding author.
E-mail address: taminul.islam@siu.edu (T. Islam).

https://doi.org/10.1016/j.ject.2024.01.002
Received 6 December 2023; Received in revised form 22 January 2024; Accepted 23 January 2024
Available online 28 January 2024

(Chattopadhyay and Lam, 2018). Different types of autonomous vehicles are emerging for transportation, including self-driving cars and unmanned aerial vehicles (UAVs) (Jones et al., 2023; Schirmer and Torens, 2022). According to industry reports (Khalid Khan et al., 2022), despite the $54 billion global market, only 16 % of consumers feel confident in autonomous vehicles as a secure transportation mode (Wong et al., 2021). This lack of trust can be attributed to cybersecurity threats that autonomous vehicles need to mitigate. For instance, electronic control units (ECUs) can potentially be hacked (Sugunaraj and Ranganathan, 2022), GPS signals spoofed (Pardhasaradhi and Cenkeramaddi, 2022), and sensor values altered (Van Wyk et al., 2020). As a result, the security vulnerabilities of networked autonomous vehicles are discussed, along with other challenges and difficulties (Wyglinski et al., 2013). When compared to conventional vehicles, autonomous vehicle's communication with other cars and infrastructure renders them a much more vulnerable target. Besides, the transportation industry may benefit from the novel traffic behaviors that AV allow, such as the use of reservations for controlling intersections to increase road capacity and decrease reaction times (Levin and Boyles, 2019). However, the analysis of massive amounts of data required for self-driving cars is vulnerable to adversarial assaults and may generate false positives as data volume grows due to the utilization of deep learning algorithms. Moreover, the im-maturity of the technology, both in hardware and software, means that it is impossible to ensure the security of AV in all circumstances (Plathottam and Ranganathan, 2018; Jafarnejad et al., 2015).

In addition to the security risks and technical challenges associated with AV, there are also ethical concerns to consider. For example, who is responsible if an AV gets into an accident and causes harm? How should an AV be programmed to make decisions in potentially life-threatening situations? These questions are still being debated and require further research and discussion (Lin et al., 2008). Furthermore, there are concerns about the potential impact of AV on employment, as the widespread adoption of this technology could lead to job displacement for millions of drivers around the world (Autonomous Vehicle Technology, 2023). As such, while the benefits of autonomous vehicles are significant, it is crucial to carefully consider the potential risks, ethical implications, and societal impacts associated with their adoption.

The technology for autonomous and unmanned vehicles has already reached a very advanced stage. Unmanned aerial vehicles (UAVs) (Valavanis, 2018) have been used for military reasons for the past three decades, and many current automobiles include conscience and advanced driver assistance capabilities that allow them to run independently. Within a few decades, self-driving automobiles, unmanned aerial vehicles, flying robots, and other robotic gadgets will be commonplace in our daily lives thanks to these breakthroughs in autonomous technology (Stephan et al., 2012). Autonomous vehicles have become popular for performing hazardous or labor-intensive tasks in military, business, and government settings due to their ability to carry out tasks effectively and safely (Rossiter, 2020). However, with the increasing use of artificial intelligence (AI) in autonomous systems, the risks associated with security threats and vulnerabilities have also risen. As these vehicles handle tasks that can affect human lives, they need to have the capability to operate securely even when faced with attacks from hackers or malfunctioning gear.

This paper focuses on the extensive review on works that has been used AI to address these risks and vulnerabilities and ensure the secure and efficient operation of autonomous systems. This research also focuses on reducing the security threat of vulnerability of autonomous vehicles. Bugs in software and systems should be controlled because hackers are looking for them (Sun et al., 2022). There are many ways for hackers to take advantage of flaws in systems, especially in automobiles (Burzio et al., 2018). When a car is referred to as 'connected,' it communicates with other equipment, networks, and automobiles (What is an Autonomous Car? – How Self-Driving Cars Work | Synopsys, n.d.). Additionally, there are even simpler ways for someone to attack a car that is powered by artificial intelligence, in addition to the issues about hacking autonomous vehicles. Policies and laws governing automotive cybersecurity can also aid in the prevention of assaults on driverless automobiles (Khan et al., 2021). To be effective, the car sector must treat this with the seriousness it deserves. To ensure that artificial intelligence is as secure as possible, it is necessary to include cybersecurity in the design and implementation processes from the beginning (Maple et al., n.d.).

Commercial vehicle-related mobile apps and other mobile applications have significant security risks, as highlighted in Table 1, which could result in serious consequences. This underscores the need for automakers and software developers to implement appropriate measures to safeguard their applications and systems against these threats. According to previous research findings, there are several security problems in current commercial vehicle-related mobile apps and other mobile applications. Mobile apps for car diagnostics are becoming increasingly popular, and various companies are taking advantage of the growing demand (Swan and Fischer, 2015). Unfortunately, the security issues in this area will put users at risk of death in some cases. Table 1 (Ryan et al., 2020; Sripada et al., 2021; Hägele et al., 2016; Wolcott and Eustice, 2014; Lampe and Meng, 2023; Zhang et al., 2022a) provides a summary

Table 1
Security Threats in Automotive Applications: Percentage of Vulnerabilities and Risks.

Applications	Percentages
Tele No. Leakage	21.1 %
URI Exposure	54.6 %
Component Exposure	57.3 %
Implicit Intent	6.1 %
Exposed Access Privilege	42.3 %
Repackage	42.3 %
Code Confusion	73.4 %
Unsecured	76.5 %
Man-in-the-Middle Attack	60.1 %

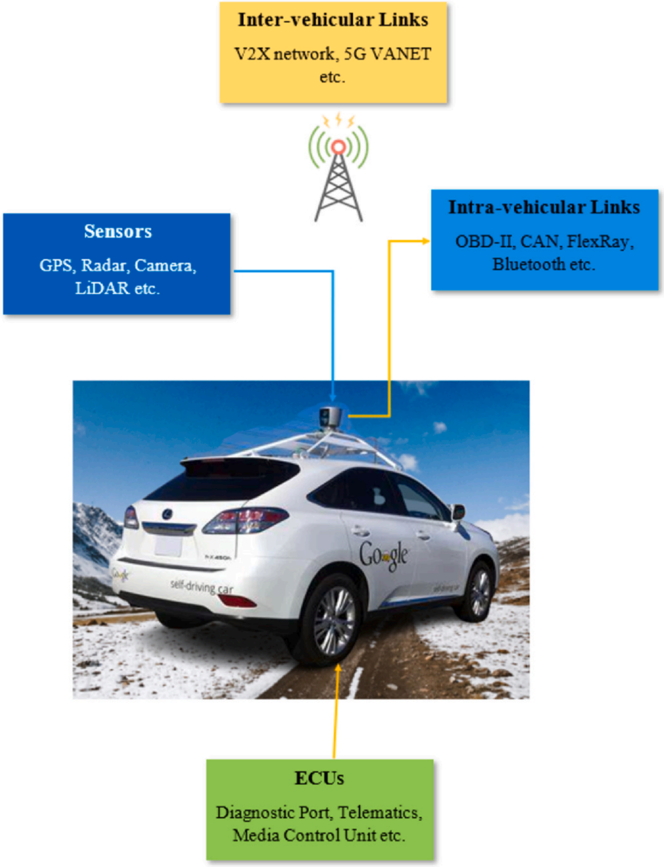
Inter-vehicular Links
V2X network, 5G VANET etc.
Sensors
GPS, Radar, Camera, LiDAR etc.
Intra-vehicular Links
OBD-II, CAN, FlexRay, Bluetooth etc.
ECUs
Diagnostic Port, Telematics, Media Control Unit etc.

Fig. 1. Basic components of an autonomous vehicle.

of the security threats present in automotive applications, along with the percentage of vulnerabilities and risks associated with each threat. The table highlights several significant security risks, including Unsecured applications (76.5 %), Code Confusion (73.4 %), Man-in-the-Middle Attacks (60.1 %), and URI Exposure (54.6 %). These risks could potentially result in serious consequences, such as data breaches, unauthorized access to sensitive information, and even physical harm to drivers and passengers. The table underscores the need for automakers and software developers to take security seriously and implement appropriate measures to safeguard their applications and systems against these threats.

According to (Le et al., 2018), vehicle diagnostic apps can pose a security risk due to multiple vulnerabilities found in commonly used apps. These vulnerabilities may allow attackers to access the user's driving profile and automobile information, potentially leading to identity theft and other malicious activities. It is important to note that these security risks are not unique to autonomous vehicles and are a common risk for all cars with an OBD interface (Koscher et al., 2010). Therefore, developers of vehicle diagnostic apps must prioritize security measures to protect user’s sensitive information.

From Fig. 1, we got the basic components and working procedure of an autonomous vehicle, which incorporates diverse sensors positioned at various points of the car to create and supervise a map of the surrounding environment. The autonomous vehicle will be declared safe and successful if it can make an accurate map as well as react appropriately based on the surrounding situation. A radar sensor (Nagy, 2023) is used to detect the specific location of nearby vehicles. Track other vehicles, road signs, and pedestrians all are detected by the video camera. By bouncing light pulses off the surroundings, the Lidar (Wolcott and Eustice, 2014) sensors calculate distances and detect lane markings as well as road edges. An ultrasonic sensor (Yang et al., 2023) is placed in the wheel to detect both curbs and other vehicles. The observation of the sensor will be provided to the software which will process all the input, Then, it will generate an instruction that will be sent to the car’s actuators. The actuator will perform the given instruction such as control steering, braking, or acceleration.

2. Related works

This section presents the author’s discussion about the different methods and systems used in vehicles for navigation, obstacle detection, control, etc. The first sensor discussed is the GPS sensor, which uses signals from GPS satellites to determine the vehicle's location. However, due to the open access to information, hackers can manipulate or mislead the GPS data to send misleading

Table 2
Analysis of existing and previous attacking techniques with advantages and disadvantages.

Reference	Attacking Techniques	Explanation of Attacking Techniques	Advantages	Disadvantages
(Autonomous Vehicle, 2023; Bendiab et al., 2023)	The method based on optimization	This method based on optimization is an attacking technique used to create adversarial samples for deep neural networks (DNNs). It involves optimizing the input data to the DNN such that the output is changed to a desired target. The main advantage of this technique is that it produces samples with the smallest possible impact on the input data.	The smallest possible impact Assault samples should be of the highest quality.	It takes a long time. Isn't capable of handling huge datasets
(Zhu et al., 2023)	First gradient sign method (FGSM)	The First gradient sign method (FGSM) is an adversarial attack technique that perturbs input data by adding a small value (epsilon) in the direction of the gradient of the loss function. This leads to the misclassification of the input data by the targeted machine learning model.	Faster than approaches based on optimization Assault samples should be of the highest quality.	The alteration isn't the best choice.
(Gangappa et al., n.d.a)	Iterative least-likely class method	The iterative least-likely class method is an attacking technique used to generate adversarial examples for deep neural networks. It is an iterative approach that generates adversarial examples by iteratively applying the first gradient sign method (FGSM). The algorithm finds the least-likely class by taking the direction that minimizes the likelihood of the correct class.	Fine-tuning of FFGSM FGSM's best adversarial case	There is a direct correlation between the number of iterations and performance.
(Amirkhani et al., 2022)	Deep Fool	Deep Fool is a type of adversarial attack that involves computing the minimum amount of perturbation required to misclassify an input image. It achieves this by iteratively projecting the input image onto a linearized version of the decision boundary, thus minimizing the Euclidean distance between the original image and the perturbed image.	Neural networks are assumed to be purely linear. It's quite effective.	No guarantee that the generated hostile samples are of a high enough quality.
(Gangappa et al., n.d.b)	Jacobian-based saliency map approach	The Jacobi-an-based saliency map approach is an attacking technique that exploits the sensitivity of neural networks to input perturbations. It involves calculating the gradient of the network's output concerning its input, and then using the gradient to identify the input features that are most important for the network's classification decision. The approach then generates adversarial examples by perturbing these important features.	Fine-tuning the perturbation is possible A nice compromise between the quantity and quality of adversarial samples can be found here.	Feed-forward DNNs are required as targets. Processing large, multi-dimensional datasets introduces a significant level of computational complexity.

Table 3
The state of the art in referred research works on autonomous vehicles.

Paper References	Author	Key Contribution	Journal Name	Year	Keyword
(Abu Bakar et al., 2022)	Abu Bakar et al.	The key contribution is to synthesize diverse national regulations into global guidelines to promote the safety and sustainability of autonomous vehicle testing.	Sustainability (Sustainability, 2023)	2022	autonomous vehicle; testing guideline; road testing; road safety; regulation
(Aldhyani and Alkahtani, 2022)	Aldhyani et al.	The authors proposed a high-performance system that uses deep learning to detect message attacks in the CAN bus and achieve superior performance compared with existing systems.	Sensors (Sensors, 2023)	2022	in-vehicle network; CAN; cybersecurity; intrusion detection; deep learning; artificial intelligence
(Sankaranarayanan et al., 2022)	Sankaranarayanan et al.	This work proposes a novel machine-learning approach for energy optimization in autonomous vehicles that can meet the demands of large traffic.	Computers and Electrical Engineering (Computers and Electrical Engineering, 2023)	2022	machine learning, energy optimization, autonomous vehicles, traffic
(Bathla et al., 2022)	Bathla et al.	The key contribution of this work is to survey recent methodologies and their comparative analysis for autonomous vehicles and to offer important future directions for research.	Mobile Information Systems (Mobile Information Systems, 2023)	2022	intelligent automation, autonomous vehicles, artificial intelligence, machine learning, internet of things
(Chattopadhyay et al., 2021)	Chattopadhyay et al.	This work is to identify the core issues of securing autonomous vehicles, and to develop a security-by-design framework for AV from the first principles.	IEEE Transactions on Intelligent Transportation Systems (IEEE Xplore, 2023)	2021	autonomous vehicles (av), security, security by design, cyber-physical systems (cps), sociotechnical systems

directions or affect the vehicle's course, compromising passenger safety and security. The second sensor discussed is the Light Detection and Ranging (LiDAR) technology, which uses laser pulses to create a 3D representation of the environment, enabling localization, detection, and avoidance of obstacles.

The third sensor discussed is the Inertial Measurement Unit (IMU), which uses gyroscopes and accelerometers to provide information on the vehicle's speed, acceleration, and orientation. Finally, the Electronic Control Unit (ECU) and the OBD port are discussed. Attackers can re-flash the ECU with modified firmware to induce harmful and unanticipated activities. At the same time, the OBD port provides information about the vehicle's malfunctions and performance through communication with the ECUs. In the methodology section, this study shows the state of the art in referred research works on autonomous vehicles in Table 3.

2.1. GPS sensor

Global Positioning System abbreviated as GPS (Al-Turjman, 2022). To identify and navigate a vehicle, GPS data may be used with high precision. Increased satellite count in the public eye was used to overcome challenges in obtaining GPS data. Due to open access to information, hackers can manipulate or mislead the data to send misleading directions or affect the vehicle's course. Passenger safety and security were compromised as a result of this. GPS fooling (Jiang et al., 2022) and jamming (Wang et al., 2023) are terms used to describe the act of sending false or misleading information to GPS satellites. As the GPS sensors are set to accept greater signals, the power of the fake signal grows, and the vehicle's location progressively deviates from the targeted goal (Madhu and Vijaya Kumar, 2022). The mathematical Eqs. (1–3) (Liu et al., 2022) for GPS sensors can be expressed as follows:

$$d1 = c*(t1 - t0) \tag{1}$$

$$d2 = c*(t2 - t0) \tag{2}$$

$$d3 = c*(t3 - t0) \tag{3}$$

Here, $d1$,2, $d3$ are the distances between the receiver and three GPS satellites, $t0$ is the time when the signal was transmitted from the GPS satellites. $t1$, $t2$, $t3$ are the times when the signal was received by the GPS receiver and c is the speed of light.

Using the distances $d1$, $d2$, and $d3$, the GPS receiver can determine its position using trilateration. The position (x, y, z) can be calculated by solving the following equations:

$$x^2 + y^2 + z^2 = (d1)^2 \tag{4}$$

$$(x - x2)^2 + (y - y2)^2 + (z - z2)^2 = (d2)^2 \tag{5}$$

$$(x - x3)^2 + (y - y3)^2 + (z - z3)^2 = (d3)^2 \tag{6}$$

Where: $(x2, y2, z2)$ and $(x3, y3, z3)$ are the coordinates of the other two GPS satellites. Solving this system of equations gives the GPS receiver's position in three-dimensional space.

2.2. Light detection and ranging

Localization, detection, and avoidance of obstacles are all possible using Light Detection and Ranging (LiDAR) technology (Alaba and Ball, 2022). The distance an item is from the vehicle is deter-mined by the time it takes for the information to travel to and from the vehicle. Assume the object is spotted if the hacker sends a message to the scanner with the same frequency. It slows or halts the vehicle's movement (Zhang et al., 2023). The mathematical equation for LiDAR can be expressed as follows:

$$d = \frac{ct}{2} \tag{7}$$

Here, d is the distance from the LiDAR sensor to an object in the environment. c is the speed of light, t is the time it takes for the laser pulse to travel from the LiDAR sensor to the object and back. The equation is divided by2 because the distance traveled by the laser pulse is the round-trip distance, and we only need to know the one-way distance.

By measuring the time, it takes for the laser pulse to travel to an object and back, LiDAR can create a 3D representation of the environment. As shown in Fig. 2, by sweeping the laser over a range of angles and distances, LiDAR can create a point cloud, which is a collection of 3D points that represent the surfaces of objects in the environment. This point cloud can be used for various applications, such as mapping, autonomous navigation, and environmental monitoring.

2.3. Inertial measurement unit

Gyroscopes and accelerometers work together to provide information on the vehicle’s speed, acceleration, and orientation (Kanwal et al., 2023). Changes in environmental dynamics such as these researchers also track a gradient. It is possible to alter or ignore the sensor data to account for the road's gradient. It causes the car to proceed at a slower speed on the incline roads, which in turn slows down the vehicles behind it (Kuschan et al., 2022). Detection of lanes, traffic signs, headlights, obstacles, and other dangers may all be accomplished with the use of video cameras. The use of high-beam torches or the headlights of the opposing vehicle can partially disrupt the operation of cameras. Erroneous or no detection of objects may be introduced as a safety concern.

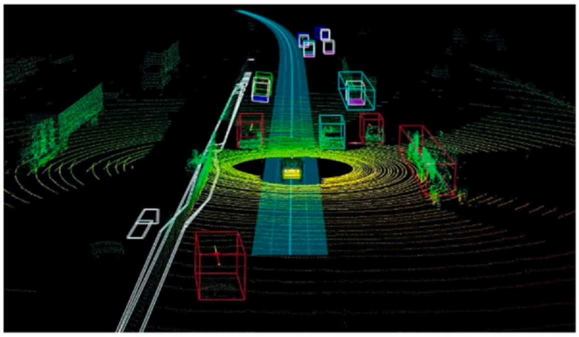

Fig. 2. Example of LiDAR point cloud.

2.4. *Electronic control units security*

Modern vehicles have over 100 electronic control units (ECUs) (Huang and Chen, 2022) that control various subsystems through sensors and actuators. These control units are designed with proprietary code, making them an attractive target for attackers looking to induce harmful and unanticipated activities. Attackers may re-flash the ECU with modified firmware to alter its functionality, tamper with ECU memory and security keys, and update the ECU firmware (Mayilsamy et al., 2022) using hashing methods and verification of the ECU firmware program and its upgrades. Full access attacks involve physical access to the ECU's external interface.

2.5. *The onboard diagnostics security*

The onboard diagnostics (OBD) port can be found in almost all vehicles and is used to gather diagnostic data (Saeed et al., 2023). The OBD port communicates with the ECUs using the controller area network (CAN) bus. Attackers may exploit vulnerabilities in the CAN protocol (Hoppe et al., 2011) or the ECM itself to gain unauthorized access to the vehicle's OBD connector. It's a portable device, similar to a USB flash drive, that connects to the vehicle's port under the dashboard, just across from the adjacent driver's seat either a wired USB port or wireless Bluetooth connection to the PC. PCs may communicate with the vehicle's electronic control units (ECUs) and exchange data between the two (Yan, 2016). The exploitation of this connection might lead to harmful data being sent into the vehicle's network (Almeida et al., 2002). For example, hackers can use a "CAN bus sniffer" to intercept and analyze messages sent over the CAN network, or they may use replay attacks or denial-of-service attacks to manipulate messages or disrupt the vehicle's normal operation (Lampe and Meng, 2022). To prevent such attacks, modern vehicles may use security measures such as encryption or digital signatures to secure the CAN protocol (Almeida et al., 2002) and tamper-resistant housings and secure boot mechanisms to protect the ECM from unauthorized access.

2.6. *Exploring the threats of cyberattacks on connected cars*

Connected car firmware upgrades have been a major update. Without sufficient safety and security improvements, these changes are unsafe. serious cyber assaults might disclose confidential information from the car (Bella et al., 2023). In this way, hackers may inject malware and take over the connected cars' firmware by exploiting security flaws in the system. There are two ways in which exploitation can take place which physical access and remote access.

Physical access - The physical layer is now directly connected to the ECUs, which raises the risk of cyberattacks. Hackers can directly exploit the sensor data, control, and communication components. Vehicle electronic modules can be targeted directly or indirectly, or the physical layer can be overloaded (Kumar et al., 2018).

Remote access- Different connectivity, such as Wi-Fi, Bluetooth, and 4G, can be used for remote access. The CAN bus is directly linked to the ECUs, which is not what the manufacturer wanted (Singh et al., 2022). Malware or virus files can be injected into the firmware while the device is connected to the internet. Neither the threats nor the measures to be taken to eliminate them are clear to automakers. Even the automobile manufacturers themselves are unsure about the best course of action to take in the wake of the financial crisis (Saez-Perez et al., 2023).

When it comes to data security and privacy, adversarial attacks aim to manipulate the training data distribution to alter parameters in machine learning models, degrading subsequent classification performance. These causative attacks target the training phase rather than already trained classifiers. Counterintuitively, adversarial samples and training data can expose sensitive information or induce misclassifications in machine learning models, which are the target models in this context.

These types of attacks can be broadly classified into two categories based on the attacker's knowledge - white-box and black-box attacks (Suryadi, 2023; Liu et al., 2016) A white-box attacker has full access to download and analyze the target models and training data. In contrast, a black-box attacker only knows the input/output patterns of the target models. Without a doubt, such attacks on machine learning models can violate privacy and endanger lives.

As an example, Sharif et al (Suryadi, 2023). showed an attack against facial recognition systems by having the attacker wear specially crafted glasses. This demonstrated the real-world feasibility and potential consequences of such white-box attacks.

Additional work (Liu et al., 2016) proved that transferable adversarial samples could be generated using ensemble learning, indicating that output patterns from one model can effectively attack others in a black-box manner.

Table 2 analyzes attacking techniques for autonomous vehicles, with advantages and disadvantages. Techniques include optimization-based, FGSM (Zhang et al., 2022a), iterative least-likely class, DeepFool (Moosavi-Dezfooli et al., 2016), and Jacobian-based saliency maps (Wang et al., 2022). The optimization method has minimal impact but is slow and doesn't scale. FGSM is faster but the perturbation may not be optimal. Iterative least-likely class fine-tunes FGSM but more iterations impact performance. DeepFool is effective but assumes linearity. Jacobian-based saliency balances quantity and quality but needs feed-forward DNNs and is computationally complex for large datasets.

3. Methodology

The majority of this study is based on previously published works. When it comes to research, it all comes down to the subject at hand. Additionally, we assimilate data and display it to our audience in a unique and inventive manner. It is not sufficient to offer a basic overview of the study; specific explanations are required. As a result, to get a complete grasp of the subject, it is necessary to familiarize yourself with its several sub-fields. To guarantee that we address all pertinent concerns in this study, we have addressed them all. The findings of the research are put to use for a variety of purposes, including testing. As a result, we now have the information we need to move on with our investigations. The findings of the research are put to use for a variety of purposes, including testing. Though this is a Review work that’s why in this work, data has been collected from the previously published work. Table 3 shows the core methodology. This table presents information about the refereed research work of this study.

Currently available machine learning defense mechanisms are discussed in this section, along with their merits and limitations. Machine learning security can be supported by a range of different tactics at various points in the lifecycle of the machine learning system. When adversarial training, defense distillation, and the RONI technique (Tobaruela and Rodríguez, 2017) are effective in defending against attackers during the training phase, the ensemble approach and the ensemble approach are useful for security during the testing or inferring stages. When it comes to data security and privacy, there are two important approaches: homomorphism encryption and differentiation.

3.1. The RONI technique

The RONI (Reactive Obstacle Navigation with Integral Action) technique (Tobaruela and Rodríguez, 2017) is an approach used in AV control to avoid obstacles while navigating a path. The technique uses information from sensors, such as LIDAR, radar, or cameras, to detect obstacles in the vehicle's path and then adjust the vehicle's trajectory to avoid them. The RONI technique is an extension of the proportional controller, which relies on the difference between the desired and actual states of a system to calculate the control action. The RONI technique adds an integral component to the controller, which allows the system to adjust for any steady-state error that may exist in the system (Mouad et al., 2012). The integral component integrates the error over time, resulting in a control action that is proportional to the ac-cumulated error. This technique can be expressed mathematically in (8) (de Lope and Maravall, 2003) as:

$$u(t) = Kp{*}e(t) + Ki{*}\int e(t)dt \tag{8}$$

Fig. 3. Autonomous vehicle with RONI - LIDAR obstacle detection.

Here, $u(t)$ is the control action at time t, Kp is the proportional gain, Ki is the integral gain, $e(t)$ is the error between the desired and actual states of the system and $\int e(t)dt$ is the integral of the error over time.

For example, let's consider an autonomous vehicle that needs to navigate through a cluttered environment. The vehicle's LIDAR sensor detects an obstacle in its path, and the RONI technique is used to adjust the vehicle's trajectory to avoid the obstacle. The error between the desired and actual states of the vehicle is calculated, and the control action is determined using the RONI equation. The proportional component of the control action adjusts the vehicle's direction, while the integral component ensures that the vehicle reaches its desired state. This technique is an effective way to control an autonomous vehicle while avoiding obstacles in its path. By using the proportional and integral components of the controller, the vehicle can adjust its trajectory to reach its desired state while avoiding obstacles in real-time.

Fig. 3 shows the visualization of an autonomous vehicle traveling down a road, which is equipped with a LIDAR sensor that is constantly scanning the surrounding environment. The LIDAR sensor detects an obstacle in the vehicle's path and sends this information to the vehicle's control system.

The control system calculates the error between the desired trajectory of the vehicle and the actual trajectory, taking into account the obstacle that was detected by the LIDAR sensor (Wolcott and Eustice, 2014). The RONI technique is used to determine the control action that the vehicle should take to avoid the obstacle and stay on course. The proportional component of the control action adjusts the vehicle's direction, causing it to steer away from the obstacle (Alaba and Ball, 2022). The integral component of the control action helps to correct any steady-state error in the system, ensuring that the vehicle eventually reaches its desired trajectory. Over time, the vehicle's control system continues to monitor the environment and adjust the vehicle's trajectory as necessary, using the RONI technique to ensure that the vehicle stays on course and avoids obstacles.

3.2. Cyber attacks and strategies

A high-level representation of a cyber-attack is displayed. Although there are several more subtle processes that take place between the steps outlined above, there are a few that are worth mentioning (reconnaissance, exploit, control, or data exfiltration) (Khan et al., 2022). A broad number of assault strategies are available to the adversary as a result of this, each of which can be adapted to the peculiarities of the situation at hand. There is no doubt that cyber-attacks are incredibly difficult to execute successfully.

Fig. 4 shows the cyber-attack procedure. A single machine-learning method can perform several subtasks with the same results. Object detection and position and movement prediction using regression algorithms are examples of such applications.

In Amid the rapid development of self-driving vehicles (Kockelman et al., 2016), several firms have encountered difficulties in protecting the CAV system from attacks, which has led to various issues on the road. System security is the subject of several studies. However, there is still room for improvement in the algorithm to achieve high performance. We applied deep learning techniques to real CAV datasets in this study.

3.3. CAN intrusion detection systems: recent advances and future directions

This section discusses the most recent advancements in the field of CAN intrusion detection systems, used an inception ResNet model (Tseng et al., 2023) to train the data from the vehicle network traffic to detect intrusion assaults on the network. Long-term memory (Robin et al., 2023), neural networks (Legaard et al., 2023), support vector machine (Qin and Li, 2023), the naive bayes approach (Islam et al., 2022a), the k-nearest neighbors model (Memiş et al., 2022), and decision tree (Islam et al., 2023) algorithms have all been tested and compared to the findings of this study. Zhang et al., developed an intrusion detection method to safeguard the CAN bus from being attacked (Zhang et al., 2022b). In order to message of the attack, the scientists used a hybrid model that included adaptive gain with a gradient descent momentum. Liang et al. used deep neural networks to detect intrusions into the CAN bus message frame, which they then monitored (Liu et al., 2021). The accuracy of this system has been demonstrated to be close to 98 % when the deep belief network function is used as the deep learning model during the training phase. A network traffic analysis system, such as the one implemented in the CAN bus by Hoppe et al. (Hoppe et al., 2011), intended for the purpose of discovering fresh patterns in network packets and comparing them with patterns IDS system, according to the researchers. When compared to the traditional system, they were able to achieve extremely high accuracy levels. Taylor et al (Taylor et al., 2016). built an LSTM model to detect CAN bus assaults in order to protect the network. Ye et al (Taylor et al., 2016; Ye et al., 2021). developed a hierarchical

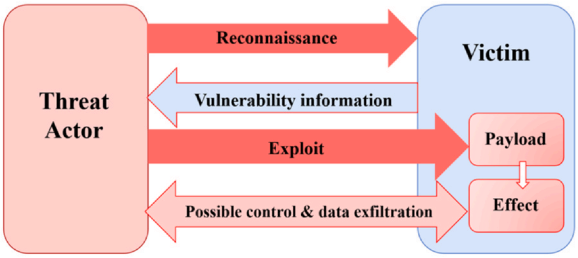
Threat Actor
Reconnaissance
Victim
Vulnerability information
Exploit
Payload
Effect
Possible control & data exfiltration

Fig. 4. Autonomous vehicle cyber-attack procedure overview.

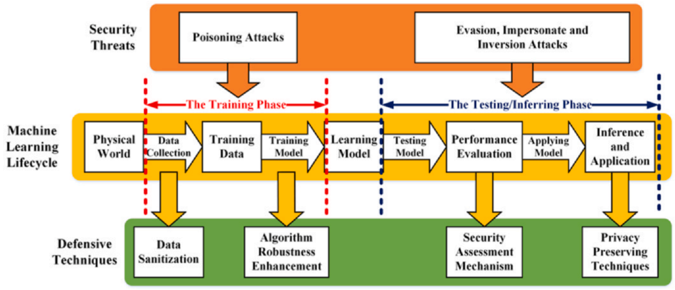
Security Threats
Poisoning Attacks
Evasion, Impersonate and Inversion Attacks
The Training Phase
The Testing/Inferring Phase
Machine Learning Lifecycle
Physical World
Data Collection
Training Data
Training Model
Learning Model
Testing Model
Performance Evaluation
Applying Model
Inference and Application
Defensive Techniques
Data Sanitization
Algorithm Robustness Enhancement
Security Assessment Mechanism
Privacy Preserving Techniques

Fig. 5. Machine learning defense strategies.

temporal memory strategy in anomaly categorization system. Many machine learning and Deep Learning techniques have been applied to predict CAN bus invasions (Hoppe et al., 2011). Deep neural networks applied Convolutional Neural Networks (CNN) (Islam et al., 2022b), and other techniques have been used to do so (CNNs).

3.4. Challenges in autonomous driving: object misclassification

Machine learning is being utilized to construct driver assistance systems that offer enhanced levels of perception and awareness of their environment, including self-driving automobiles. Specifically, camera-based mechanisms to identify and categorize objects. There have been notable progressions in LiDAR (Bilik, 2023) and radar technology.

Undoubtedly, one of the most challenging aspects of autonomous driving is the misclassification of objects (Feng et al., 2022). The vehicle's computerized control system collects and analyzes all data its numerous sensors obtain. In certain instances, an automobile may erroneously perceive a stop sign as a less consequential traffic sign, such as a speed limit indicator, owing to a disparity in a small number of pixels within the visual representation generated by the vehicle's camera technology. It is possible for a pedestrian to be misidentified as a stationary object, such as a lamp post, by the system. Furthermore, the system may be unable to anticipate the pedestrian's future movements. Fig. 5 depicts the defensive techniques employed in machine learning.

Machine learning can contribute to the safety of a vehicle by preventing system failures that could result in an accident. To examine onboard data, it is possible to employ machine learning. Data on the motor temperature, battery charge, oil pressure, and coolant levels are collected and analyzed by the system to provide an overall picture of the vehicle's health and motor performance to the driver. Indicators that indicate a problem with the car may alert the owner as well as the rest of the system that maintenance or repair is required.

By evaluating the data produced by a vehicle's electronics, machine learning can also ensure that the electronics do not fail and cause an accident. For sensors like cameras, lidar, and radar to be effective in providing a safe cruise, they must be adequately maintained.

4. Empirical investigations and analysis

According to, a taxonomy of security threats towards machine learning was proposed from three different perspectives, namely, the influence on classifiers, security violations, and attack specificity, as depicted in Fig. 6. which illustrates the taxonomy of security threats towards the autonomous technique. Security has an impact on classifiers from the perspective of there being two main types of dangers to machine learning. After in-depth analysis, this research finds key sensors and attacks that are responsible for autonomous vehicles.

4.1. Ultrasonic sensor

Sensors are used by autonomous vehicles to measure road conditions to make real-time decisions, and their security is heavily dependent on these sensor's reliability. Ultrasonic sensors are used to detect obstacles (Carullo and Parvis, 2001). Obstacles are detected by releasing ultrasounds and examining their reflections. To estimate the distance of an object, the ultrasonic sensor releases ultrasonic pulses and calculates the time of receiving the reflected pulses. The mathematical equation is –

$$d = 0.5 \cdot t_P \cdot v_s \tag{9}$$

Here, *tp* represents the ultrasonic pulses propagation time. In the air, the sound velocity is defined by using $vs(At200C343m/s)$.
Threat: Intruders can use spoofing, adaptive spoofing, and jamming attacks on the ultrasonic sensors.

4.2. Random spoofing attack

In this attack, previously recorded signals will be replied randomly at the correct time (Cao et al., 2022). At this moment, the received signals will not be canceled. This type of attacks can only fool the sensors into reporting a fabricated obstacle that is near than any actual barriers. We can write the sensor signal received in random spoofing attack in the following manner.

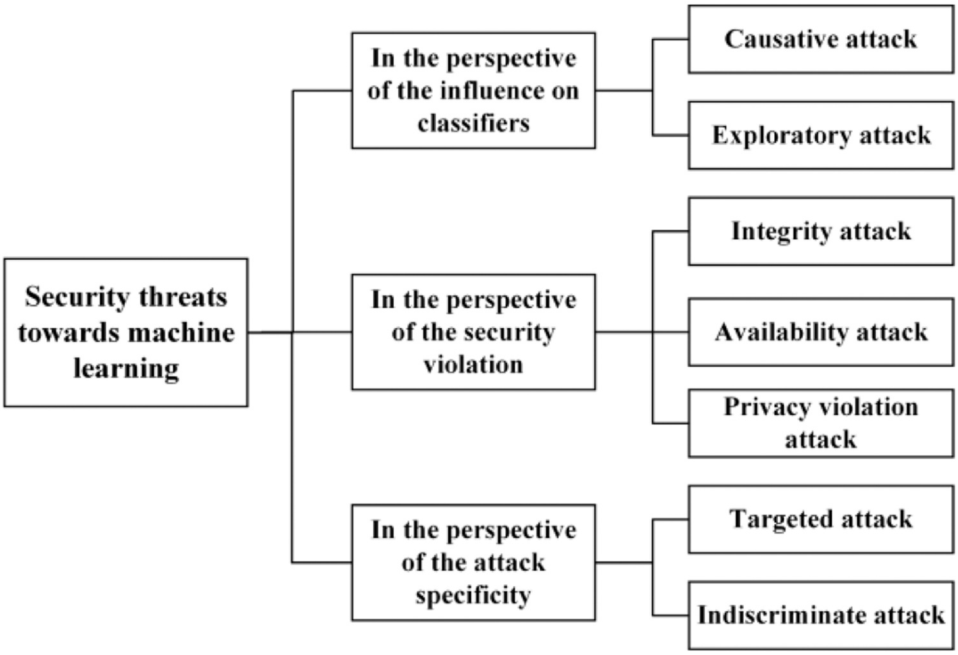
Security threats towards machine learning
In the perspective of the influence on classifiers
Causative attack
Exploratory attack
In the perspective of the security violation
Integrity attack
Availability attack
Privacy violation attack
In the perspective of the attack specificity
Targeted attack
Indiscriminate attack

Fig. 6. Security threats taxonomy for autonomous techniques.

$$\gamma_i = \psi_i(T_0) + \sum_{n=1}^{N} \psi_j^*(T_n) \tag{10}$$

Here, Ψi(τ) defines the cycle of the echo which is received at τ0.Ψ*j (τn) represents the spoof signal which is replayed on the basis of the previous cycle (j) which is achieved after Tn time. All spoof signals are counted and stored in the N.

4.3. Jamming attack

In this attack, the ultrasounds will be emitted continuously (Mpitziopoulos et al., 2009). We can write the received signal in this attack in the following manner.

$$\gamma_i = \psi_i(T_0) + \int_0^{T_0} A\cos(\omega t) \tag{11}$$

Here, the amplitude of the jamming is denoted by A and frequency is defined by the ω.

4.4. Adaptive spoofing attack

In The aim of this attack is to generate the non-existing barriers. We can define the signal which is received under this attack as follows:

$$\gamma_i = \psi_i(T_0) - \alpha\Psi_i(T_0 + \delta) + \Psi_i^*(T_1) \tag{12}$$

Here, the cancellation of the signal is denoted by α and the time delay is denoted by the δ.

Solution: To improve the protection of ultrasonic sensors as well as autonomous vehicles, the authors proposed two types of defense techniques-

Physical Shift Authentication (PSA): Despite ultrasound's drawbacks, PSA (Xu et al., 2018) permits a sensor to deliver random probing signals. As a result, it can reliably detect obstacles by determining whether the obtained echoes are from the sensors or not.

Multiple Sensor Consistency Check: At the system level, MSCC (Shu et al., ,) allows multiple sensors to work together to tackle more advanced attacks. It can identify spoofing attacks, calculate the distance in a resilient manner, and localize both real and attackers' obstacles. By using two assistance sensors, MSCC can improve its detection rate.

4.5. Threats in localization and navigation technologies for autonomous driving

Technologies of localization and navigation are the root elements of navigation as well as the planning of routes. By exploiting the loopholes of these technologies, the attacker can manipulate the navigation of autonomous vehicles. GPS, INS, and HD maps are the most common localization and navigation technologies. The following attacks are liable for the navigation technology threats.

- GPS spoofing Attack: The main goal of this attack is to manipulate the navigation (Tippenhauer et al., 2011). There are two steps in this attack. At first, false signals of GPS are created that are identical to legitimate ones but have sufficient power to replace the legitimate GPS signals. Then it changes navigation SMS or shifts the arrival time of the signals to handle the navigation.
- GPS jamming attack: This attack can be done by sending out a huge amount of radio noises on the GPS frequency (Ashourian and Sharifi-Tehrani, 2022). Furthermore, making and using a GPS jammer is very simple.
- GPS replay attack: The primary goal of GPS replay attack is to destroy the encryption as well as authentication security. It is one of the dangerous attacks (Aissou et al., 2022).
- GPS software attack: This attack is done by finding software loopholes (Moukahal et al., 2022).
- Message falsification attack: The aim of this attack is to upload huge amount of false message in order to update the HD maps.

4.6. GPS signal security

Because of unencrypted and unauthorized signals, Civil GPS (Mitch et al., 2011) is easy to affect by jamming. The possible solutions are –

- One viable method for preventing interference is to optimize the signal process of GPS.
- To make safe the GPS signals from spoofing attack, encrypt the signals of GPS by using private key can be the solution.
- Aside from improving GPS security, it is also essential to enhance the GPS terminal's ability to recognize false signals and collect real ones. To accomplish this, six methods can be used. They are front-end filtering, radio frequency interference detection, anti-interference filtering, integrated navigation, space-time adaptive and antenna enhancement. To improve the protection of HD maps, three methods can be used.

1. We must ensure the data collection's accuracy.
2. It is essential to create a safe update framework.
3. By using cloud services, HD maps will be updated. It is necessary to use safe cloud services.

4.7. Causative attack

To put it another way, it means that adversaries can alter the training data distribution, resulting in parameter changes in learning models that affect subsequent classification performance. This type of attack does not aim to alter classifiers that have already been trained (Gallagher et al., 2022). While it may seem counterintuitive, hostile samples and training data can be used to induce misclassifications or expose sensitive information in learning models.

4.8. Attack on integrity

It aims to enhance the number of false negatives of existing classifiers when it comes to identifying dangerous samples. For (b) an Availability attack, see (a). Instead, such an approach will increase the number of classifiers that identify harmless samples as false positives. (c) A breach of personal privacy. Because enemies may access training data and learning models, this means that they can gain sensitive and confidential information. Security threats to machine learning can be divided into two categories, based on attack specificity: An attack that is specifically tailored to the target. Classifiers' performance on a single sample or subset of samples is specifically targeted for degradation. Untargeted as-sault. The classifier is unable to distinguish between different types of samples because of this attack. In the field of autonomous security, a new battleground has emerged: secure deep learning. According to earlier studies, the security of DNNs is jeopardized by their counterintuitive nature. Even if adversarial samples are taken into consideration during model training and learning algorithms are strengthened, none of these strategies are sufficient to solve the problem outlined above. From this research, we found three vital aspects of security threats of an autonomous vehicle.

4.9. Firmware

ECU firmware (Chen et al., 2022) may be extracted and decoded by hackers. Additionally, this enables for the extraction of sensitive data such as encryption keys to be discovered in the firmware. It's possible that the vehicle's intellectual property, such as fuel economy and battery health, might be exposed if the vehicle's firmware is extracted. The safety of the system depends on the integrity and protection of these data.

4.10. Advanced/autonomous vehicle systems (semi and completely autonomous)

Cars equipped with high-tech connected car systems like radar, cameras, parking assistance systems, and collision-prevention systems can be used to bridge the gap between a cyber-attack and a physical one. These systems can be hacked and utilized to compromise the safety of a vehicle. As a result, verifying their integrity is crucial for the overall security of the vehicle.

Table 4
Analysis between existing and previous defensive techniques.

References	Defensive Techniques	Advantages	Disadvantages
(Li and Chan, 2014)	Reject on Negative impact (RONI)	When hostile samples are included into training data, it effectively removes them. A large variety of classification algorithms can be used.	It is a lack of thorough testing in a wide range of applications.
(Xu et al., 2021)	Adversarial training	It's simple to learn and put into practice. It can be used with a wide range of classification algorithms.	Adversarial samples used in the training phase determine the success of this technique.
(Goodfellow et al., 2014; Papernot et al., 2016)	Defence distillation	Reduced sensitivity to input perturbations results in a smoother DNN model. It enhances the DNN's ability to generalize. It effectively reduces the impact of FGSM-created hostile samples.	JSMA-created adversarial samples are too easy to defeat.
(Carlini and Wagner,; Sengupta et al., 2019; Tramèr et al., 2017)	Ensemble method	Multiple classifiers or defence mechanisms can be easily integrated.	With respect to adversarial samples, it does not have the transferability that is required.
(Abbasi and Gagné, 2017; Tschantz et al., 2011; Rubinstein et al., 2009)	Differential privacy	It safeguards the confidentiality of training data. In this way, the privacy of algorithms for learning is safeguarded.	A classifier's performance on authentic data is affected by this.
(Damgård et al., 2012)	Homomorphic encryption	It protects data confidentiality and security in the cloud.	As a result, additional processing time is required.

4.11. Wireless an Infotainment system

Wi-Fi, Bluetooth, Near Field Communication, and mobile Internet technologies give a plethora of additional entry points into the connected car and should be thoroughly scrutinized for flaws and vulnerabilities before implementation. The audio head unit, navigation system, USB, CD/DVD, and other physical interfaces on the car are all easily accessible, providing a possible entry point for hackers to get direct access to onboard components and firmware and compromise the vehicle's security.

5. Discussion

When a car is self-driving, it does not require the assistance of a human driver to makeover around its surroundings. Human passengers are not required to be present at any point during the process of taking control of the vehicle. Self-driving automobiles do not require the assistance of a human driver to traverse their environment. Human passengers are not necessary at any point during the process of taking control of the vehicle. Table 4 shows the analysis between existing and previous defensive techniques.

At various points in the machine learning lifecycle, a variety of defense mechanisms can be employed to provide security assistance. There are a number of useful techniques for ensuring data security and privacy, such as RONI for defending against attackers during the training phase, defensive distillation, the ensemble approach for testing, and differential confidentiality and homomorphic encryption for inferring. This research suggests some vital ways that can protect your autonomous vehicle.

- Make a strong password for your vehicle. If your car came with a default password, hackers may easily guess it. In 2023, for example, the default password of thousands of automobiles' GPS tracking applications was "123456."
- Rather than relying on a single network, cities could set up several. Connected automobiles are more vulnerable to cyberattacks if they rely on a single network. Cities may drastically lessen their vulnerability by establishing several tiny networks.
- When a car's software is up to date, it will have the most recent updates that defend the vehicle against known risks.
- When it comes to installing applications in automobiles, vehicle manufacturers should guarantee that the app developers are focused on making sure that the programs are secure prior to their installation.
- Using a technique called "GPS spoofing," it is possible to take control of a vehicle's GPS system by disabling the GPS signal. A radio signal is used by a bad actor to disrupt a GPS locating system. It is possible to stop an automobile in its tracks by deceiving it into thinking it has arrived at its destination via spoofing, for example. This is why having GPS turned on just when necessary is important.
- The enormous amount of complexity that underlies autonomous automobiles can make it harder to detect flaws, whereas a regular vehicle could be easier to identify. As a result, drivers should become comfortable with their self-driving cars before taking to the road.

Self-driving autos will eliminate a substantial source of human error since they are incapable of making mistakes in judgment. According to a study, self-driving cars might potentially save the lives of 29,447 individuals every year by preventing traffic accidents from occurring. Following the resolution of legislative and technological obstacles, it is possible that around 15 % of new automobiles delivered in 2030 will be totally self-driving. Commercial availability of fully driverless vehicles is unlikely to emerge before 2020, according to industry analysts. According to current projections, self-driving cars will generate more than 300 gigabytes of data each year in the future. The continuous progress of safety technology makes it possible to develop complex software-defined autonomous systems capable of navigating roadways with little to no human input. In the next four to five years, autonomous vehicles are expected to be commonplace on U.S. highways and highway interchanges.

Automation, Machine Learning is at the heart of big data, the Internet of Things (IoT), cloud computing, and artificial intelligence. There has been a lot of interest in security risks and their accompanying defense methods, both in academics and in industry. Research into machine learning security risks and defenses shows the following patterns, according to the available literature: Machine learning is under attack from a variety of new risks at any given time. There have been several frameworks, algorithms and optimization mechanisms developed, but research into the security of learning models and algorithms is only beginning. Researchers are increasingly looking on the security of AI-based decision systems in hostile situations. It is expected that a defender would become increasingly concerned about the security of decision systems as the number of machine learning-related security incidents rises. There is a new battleground in machine learning security: secure deep learning. The security of DNNs is compromised by their counterintuitive nature, according to previous research. Even if adversarial samples are considered during model training, and learning algorithms are made more resilient, none of these methods are strong enough to address the problem described above.

In this study, authors did a comprehensive survey on security issues of an autonomous vehicle. Machine learning security concerns have been re-examined in terms of the training and testing/inferring phases. Security assessment mechanisms, countermeasures during testing, and data privacy and security are some of the existing machine learning defence systems that have been grouped together. The quickly changing nature of technology and the associated security risks, which can make it challenging to stay current with the latest threats and vulnerabilities, is one of the main issues. Research in this field necessitates knowledge of both computer science and transportation engineering, which presents another obstacle. Large datasets and testbeds are also required to effectively assess the efficacy of machine learning defensive strategies. To address these issues, researchers should concentrate on following the most recent advancements in the field, interacting with leaders in adjacent fields, and creating and utilizing extensive datasets and testbeds to accurately assess the usefulness of their suggested solutions. To do successful research in this field, one will also need a solid grasp of cybersecurity principles, machine learning methods, and transportation engineering concepts.

6. Conclusions

In the coming years, there's a considerable probability that autonomous vehicles will have a significant impact on the economy and society. In the United States alone, lower crash rates and more efficient travel time might result in an annual social benefit of more than $750 billion due to reduced crash rates and increased efficiency in travel time usage. Automatic vehicles (AVs) have the potential to cut carbon emissions by improving vehicle energy efficiency; however, the increased use of road automobiles may outweigh this gain. Additionally, it is possible that this will have a negative impact on the positive impact that AVs could have on traffic. It is vital to consider options such as car sharing, flexible work schedules, and telecommuting in order to make the most of the potential benefits of autonomous vehicles. In this work, using a review of machine learning approaches, we conducted a thorough survey on security issues. Security concerns to machine learning have been re-examined in terms of the training and testing/inferring phases. Furthermore, we have grouped existing machine learning defence systems into security assessment mechanisms, defence during training, countermeasures during testing, and data security and privacy. All these repercussions are the result of the wide-spread use of audio-visual technology. Trust in the system will be based on aspects such as the moral concerns that were considered when developing the algorithms that are used in antivirus technologies, as well as the cybersecurity components and the overall system reliability. The most efficient application of this new technology needs tight collaboration across a variety of AV disciplines and industry players. We intend to go on with this research in the future by putting our findings into action. The outcomes of this study will be included in our forthcoming project work. We will decrease the critical factors contributing to an autonomous vehicle's vulnerability and security danger.

Funding

This research received no external funding.

Conflict of Interest

The authors declare that they have no conflict of interest.

References

Abbasi, M., & Gagné, C. (2017). Robustness to Adversarial Examples through an Ensemble of Specialists. *5th International Conference on Learning Representations, ICLR 2017 - Workshop Track Proceedings* . https://doi.org/10.48550/arxiv.1702.06856.

Abu Bakar, A.I., Abas, M.A., Muhamad Said, M.F., Tengku Azhar, T.A., 2022. Synthesis of autonomous vehicle guideline for public road-testing sustainability. Sustainability 14 (3), 1456. https://doi.org/10.3390/SU14031456

Aissou, G., Benouadah, S., El Alami, H., & Kaabouch, N. (2022). Instance-based Supervised Machine Learning Models for Detecting GPS Spoofing Attacks on UAS. *2022 IEEE 12th Annual Computing and Communication Workshop and Conference, CCWC 2022*, 208–214. https://doi.org/10.1109/CCWC54503.2022.9720888.

Alaba, S.Y., Ball, J.E., 2022. A survey on deep-learning-based LiDAR 3D object detection for autonomous driving. Sensors 22 (24), 9577. https://doi.org/10.3390/S22249577

Aldhyani, T.H.H., Alkahtani, H., 2022. Attacks to automatous vehicles: a deep learning algorithm for cybersecurity. Sensors 22 (1), 360. https://doi.org/10.3390/S22010360

Almeida, L., Pedreiras, P., Fonseca, J.A.G., 2002. The FTT-CAN protocol: Why and how. IEEE Trans. Ind. Electron. 49 (6), 1189–1201. https://doi.org/10.1109/TIE.2002.804967

Al-Turjman, F., 2022. A novel approach for drones positioning in mission critical applications. Trans. Emerg. Telecommun. Technol. 33 (3), e3603. https://doi.org/10.1002/ETT.3603

Amirkhani, A., Karimi, M.P., Banitalebi-Dehkordi, A., 2022. A survey on adversarial attacks and defenses for object detection and their applications in autonomous vehicles. Vis. Comput. 1–15. https://doi.org/10.1007/S00371-022-02660-6/METRICS

Ashourian, M., Sharifi-Tehrani, O., 2022. Application of semi-circle law and Wigner spiked-model in GPS jamming confronting. Signal, Image Video Process. 1–8. https://doi.org/10.1007/S11760-022-02276-2/METRICS

Autonomous Vehicle Cyber-Attacks Classification Framework | IEEE Conference Publication | IEEE Xplore. (n.d.). Retrieved February 23, 2023, from 〈https://ieeexplore.ieee.org/abstract/document/10041387〉.

Autonomous Vehicle Technology: A Guide for Policymakers - James M. Anderson, Kalra Nidhi, Karlyn D. Stanley, Paul Sorensen, Constantine Samaras, Oluwatobi A. Oluwatola - Google Books. (n.d.). Retrieved April 8, 2023, from https://books.google.com.bd/books?hl=en&lr=&id=y0WrAgAAQBAJ&oi=fnd&pg=PP1&dq=Anderson,+J.+M.,+Nidhi,+K.,+Stanley,+K.+D.,+Sorensen,+P.,+Samaras,+C.,+%26+Oluwatola,+O.+A.+(2014).+Autonomous+vehicle+technology:+A+guide+for+policymakers.+Rand+Corporation.&ots=-8M883FBSS&sig=gIA5rKLzYY-ldcFNMUkvR878G9I&redir_esc=y#v=onepage&q&f=false.

Badue, C., Guidolini, R., Carneiro, R.V., Azevedo, P., Cardoso, V.B., Forechi, A., De Souza, A.F., 2021. Self-driving cars: a survey. Expert Syst. Appl. 165, 113816. https://doi.org/10.1016/J.ESWA.2020.113816

Bathla, G., Bhadane, K., Singh, R.K., Kumar, R., Aluvalu, R., Krishnamurthi, R., Basheer, S., 2022. Autonomous vehicles and intelligent automation: applications, challenges, and opportunities. Mob. Inf. Syst. 2022. https://doi.org/10.1155/2022/7632892

Bella, G., Biondi, P., Tudisco, G., 2023. A double assessment of privacy risks aboard top-selling cars. Automot. Innov. 1, 1–18. https://doi.org/10.1007/S42154-022-00203-2/TABLES/8

Bendiab, G., Hameurlaine, A., Germanos, G., Kolokotronis, N., Shiaeles, S., 2023. Autonomous vehicles security: challenges and solutions using blockchain and artificial intelligence. IEEE Trans. Intell. Transp. Syst. 1–24. https://doi.org/10.1109/TITS.2023.3236274

Bilik, I., 2023. Comparative analysis of radar and lidar technologies for automotive applications. IEEE Intell. Transp. Syst. Mag. 15 (1), 244–269. https://doi.org/10.1109/MITS.2022.3162886

Burzio, G., Cordella, G.F., Colajanni, M., Marchetti, M., & Stabili, D. (2018). Cybersecurity of Connected Autonomous Vehicles: A ranking based approach. *2018 International Conference of Electrical and Electronic Technologies for Automotive, AUTOMOTIVE 2018* . https://doi.org/10.23919/EETA.2018.8493180.

Cao, H., Zou, W., Wang, Y., Song, T., & Liu, M. (2022). Emerging Threats in Deep Learning-Based Autonomous Driving: A Comprehensive Survey. https://doi.org/10.48550/arxiv.2210.11237.

Carlini, N., & Wagner, D. (n.d.). Defensive Distillation is Not Robust to Adversarial Examples. Retrieved from 〈http://tensorflow.org/〉.

Carullo, A., Parvis, M., 2001. An ultrasonic sensor for distance measurement in automotive applications. IEEE Sens J. 1 (2), 143.

Chattopadhyay, A., & Lam, K.Y. (2018). Security of autonomous vehicle as a cyber-physical system. *2017 7th International Symposium on Embedded Computing and System Design, ISED 2017, 2018-January*, 1–6. https://doi.org/10.1109/ISED.2017.8303906.

Chattopadhyay, A., Lam, K.Y., Tavva, Y., 2021. Autonomous vehicle: security by design. IEEE Trans. Intell. Transp. Syst. 22 (11), 7015–7029. https://doi.org/10.1109/TITS.2020.3000797

Chen, Z., Thomas, S.L., & Garcia, F.D. (2022). MetaEmu: An Architecture Agnostic Rehosting Framework for Automotive Firmware. *Proceedings of the ACM Conference on Computer and Communications Security*, 515–529. https://doi.org/10.1145/3548606.3559338.

Computers and Electrical Engineering | Journal | ScienceDirect.com by Elsevier. (n.d.). Retrieved April 11, 2023, from 〈https://www.sciencedirect.com/journal/computers-and-electrical-engineering〉.

Damgård, I., Pastro, V., Smart, N., & Zakarias, S. (2012). Multiparty computation from somewhat homomorphic encryption. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7417 LNCS, 643–662. https://doi.org/10.1007/978–3-642–32009-5_38/COVER.

Feng, D., Harakeh, A., Waslander, S.L., Dietmayer, K., 2022. A review and comparative study on probabilistic object detection in autonomous driving. IEEE Trans. Intell. Transp. Syst. 23 (8), 9961–9980. https://doi.org/10.1109/TITS.2021.3096854

Gallagher, M., Pitropakis, N., Chrysoulas, C., Papadopoulos, P., Mylonas, A., Katsikas, S., 2022. Investigating machine learning attacks on financial time series models. Comput. Secur. 123, 102933. https://doi.org/10.1016/J.COSE.2022.102933

Gangappa, D., Bhamsagar, M.B., Ag, N., Ponnana, P., K, P.H., & In, A. (n.d.a). Adversarial attacks and defence on autonomous vehicles. Retrieved from 〈www.irjmets.com〉.

Goodfellow, I.J., Shlens, J., & Szegedy, C. (2014). Explaining and Harnessing Adversarial Examples. *3rd International Conference on Learning Representations, ICLR 2015 - Conference Track Proceedings*. https://doi.org/10.48550/arxiv.1412.6572.

Hägele, M., Nilsson, K., Pires, J.N., Bischoff, R., 2016. Industrial robotics. Springe Handb. 1385–1422. https://doi.org/10.1007/978-3-319-32552-1_54/COVER

Hoppe, T., Kiltz, S., Dittmann, J., 2011. Security threats to automotive CAN networks—practical examples and selected short-term countermeasures. Reliab. Eng. Syst. Saf. 96 (1), 11–25. https://doi.org/10.1016/J.RESS.2010.06.026

Huang, S., Chen, J., 2022. Event-triggered model predictive control for autonomous vehicle with rear steering. SAE Technical Papers(2022). https://doi.org/10.4271/2022-01-0877

IEEE Xplore: IEEE Transactions on Intelligent Transportation Systems. (n.d.). Retrieved April 11, 2023, from 〈https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6979〉.

Islam, M.T., Ahmed, T., Raihanur Rashid, A.B.M., Islam, T., Rahman, M.S., & Tarek Habib, M. (2022b). Convolutional Neural Network Based Partial Face Detection. *2022 IEEE 7th International conference for Convergence in Technology, I2CT 2022*. https://doi.org/10.1109/I2CT54291.2022.9825259.

Islam, T., Kundu, A., Islam Khan, N., Chandra Bonik, C., Akter, F., Jihadul Islam, M., 2022a. Machine learning approaches to predict breast cancer: Bangladesh perspective. Smart Innov. Syst. Technol. 302, 291–305. https://doi.org/10.1007/978-981-19-2541-2_23/COVER

Islam, T., Kundu, A., Lima, R.J., Hena, M.H., Sharif, O., Rahman, A., Hasan, M.Z., 2023. Review analysis of ride-sharing applications using machine learning approaches: Bangladesh perspective. Comput. Stat. Methodol. Model. Artif. Intell. 99–122. https://doi.org/10.1201/9781003253051-7

Jafarnejad, S., Codeca, L., Bronzi, W., Frank, R., & Engel, T. (2015). A car hacking experiment: When connectivity meets vulnerability. *2015 IEEE Globecom Workshops, GC Wkshps 2015 - Proceedings* . https://doi.org/10.1109/GLOCOMW.2015.7413993.

Jiang, P., Wu, H., Xin, C., 2022. DeepPOSE: detecting GPS spoofing attack via deep recurrent neural network. Digit. Commun. Netw. 8 (5), 791–803. https://doi.org/10.1016/J.DCAN.2021.09.006

Jones, M.R., Djahel, S., Welsh, K., 2023. Path-planning for unmanned aerial vehicles with environment complexity considerations: a survey. ACM Comput. Surv. https://doi.org/10.1145/3570723

Kanwal, K., Rustam, F., Chaganti, R., Jurcut, A.D., Ashraf, I., 2023. Smartphone inertial measurement unit data features for analyzing driver driving behavior. 1–1. IEEE Sens. J. https://doi.org/10.1109/JSEN.2023.3256000

Khalid Khan, S., Shiwakoti, N., Stasinopoulos, P., 2022. A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles. Accid. Anal. Prev. 165, 106515. https://doi.org/10.1016/J.AAP.2021.106515

Khan, S.K., Shiwakoti, N., Khalid Khan, S., Stasinopoulos, P., & Warren, M. (2021). Dynamic assessment of regulation and policy framework in the cybersecurity of Connected and Autonomous Vehicles. Retrieved from 〈http://www.atrf.info〉.

Khan, Z., Chowdhury, M., & Khan, S.M. (2022). A Hybrid Defense Method against Adversarial Attacks on Traffic Sign Classifiers in Autonomous Vehicles, (1). https://doi.org/10.48550/arxiv.2205.01225.

Kockelman, K.M., Avery, P., Bansal, P., Boyles, S.D., Bujanovic, P., Choudhary, T., … Stewart, D. (2016). Implications of Connected and Automated Vehicles on the Safety and Operations of Roadway Networks: A Final Report.

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., Savage, S., 2010. Experimental security analysis of a modern automobile. Proceedings - IEEE Symposium on Security and Privacy 447–462. https://doi.org/10.1109/SP.2010.34

Kumar, A.D., Chebrolu, K.N.R., R, V., KP, S., 2018. A brief survey on autonomous vehicle possible attacks. Exploits Vulnerabilities. https://doi.org/10.48550/arxiv.1810.04144

Kuschan, J., Filaretov, H., & Kruger, J. (2022). Inertial Measurement Unit based Human Action Recognition Dataset for Cyclic Overhead Car Assembly and Disassembly. *IEEE International Conference on Industrial Informatics (INDIN)* , *2022-July*, 469–476. https://doi.org/10.1109/INDIN51773.2022.9976078.

Lampe, B., & Meng, W. (2022). IDS for CAN: A Practical Intrusion Detection System for CAN Bus Security. *2022 IEEE Global Communications Conference, GLOBECOM 2022 - Proceedings*, 1782–1787. https://doi.org/10.1109/GLOBECOM48099.2022.10001536.

Lampe, B., Meng, W., 2023. A survey of deep learning-based intrusion detection in automotive applications. Expert Syst. Appl. 221, 119771. https://doi.org/10.1016/J.ESWA.2023.119771

Le, V.H., den Hartog, J., Zannone, N., 2018. Security and privacy for innovative automotive applications: a survey. Comput. Commun. 132, 17–41. https://doi.org/10.1016/J.COMCOM.2018.09.010

Legaard, C.M., Schranz, T., Schweiger, G., Drgoňa, J., Falay, B., Gomes, C., Larsen, P.G., 2023. Constructing neural network based models for simulating dynamical systems. ACM Comput. Surv. https://doi.org/10.1145/3567591

Levin, M.W., & Boyles, S.D. (2019). Effects of Autonomous Vehicle Ownership on Trip, Mode, and Route Choice. https://doi.org/10.3141/2493–04, 2493, 29–38. https://doi.org/10.3141/2493–04.

Li, H., Chan, P.P.K., 2014. An improved reject on negative impact defense. Commun. Comput. Inf. Sci. 481, 452–459. https://doi.org/10.1007/978-3-662-45652-1_45/COVER

Lin, P.G., Bekey, K., & Abney, M.A. (2008). Autonomous Military Robotics: Risk, Ethics, and Design.

Liu, X., Liang, J., & Fu, J. (2021). A dynamic trajectory planning method for lane-changing maneuver of connected and automated vehicles. *https://doi.org/10.1177/0954407020982712,* 235(7), 1808–1824. https://doi.org/10.1177/0954407020982712.

Liu, Y., Chen, X., Liu, C., & Song, D. (2016). Delving into Transferable Adversarial Examples and Black-box Attacks. *5th International Conference on Learning Representations, ICLR 2017 - Conference Track Proceedings* . https://doi.org/10.48550/arxiv.1611.02770.

Liu, Y., Luo, Q., Zhou, Y., 2022. Deep learning-enabled fusion to bridge GPS outages for INS/GPS integrated navigation. IEEE Sens. J. 22 (9), 8974–8985. https://doi.org/10.1109/JSEN.2022.3155166

de Lope, J., & Maravall, D. (2003). Integration of Reactive Utilitarian Navigation and Topological Modeling, 103–139. https://doi.org/10.1007/978–3-7908–1767-6_4.

Madhu, G.C., Vijaya Kumar, P., 2022. A survey and analysis of different lightweight block cipher techniques for resource-constrained devices. Int. J. Electron. Secur. Digit. Forensics 14 (1), 96–110. https://doi.org/10.1504/IJESDF.2022.120039

Maple, C., Bradbury, M., Le, A.T., & Ghirardello, K. (n.d.). A Connected and Autonomous Vehicle Reference Architecture for Attack Surface Analysis. https://doi.org/10.3390/app9235101.

Mayilsamy, K., Ramachandran, N., Moses, B.J.S., Ravikumar, A., 2022. A hybrid approach to enhance data security in wireless vehicle firmware update process. Wirel. Pers. Commun. 125 (1), 665–684. https://doi.org/10.1007/S11277-022-09571-8/METRICS

Memiş, S., Enginoğlu, S., Erkan, U., 2022. Fuzzy parameterized fuzzy soft k-nearest neighbor classifier. Neurocomputing 500, 351–378. https://doi.org/10.1016/J.NEUCOM.2022.05.041

Mitch, R.H., Dougherty, R.C., Psiaki, M.L., Powell, S.P., O'Hanlon, B.W., Bhatti, J.A., & Humphreys, T.E. (2011, September 23). Signal Characteristics of Civil GPS Jammers. Retrieved from 〈http://www.ion.org/publications/abstract.cfm?jp = p&articleID = 9740〉.

Mobile Information Systems | Hindawi. (n.d.). Retrieved April 11, 2023, from 〈https://www.hindawi.com/journals/misy/〉.

Moosavi-Dezfooli, S.-M., Fawzi, A., Frossard´, P.F., Polytechnique, F., & De Lausanne, F. (2016). DeepFool: A Simple and Accurate Method to Fool Deep Neural Networks. Retrieved from 〈http://github.com/lts4/deepfool〉.

Mouad, M., Adouane, L., Khadraoui, D., & Martinet, P. (2012). Mobile Robot Navigation and Obstacles Avoidance based on Planning and Re-Planning Algorithm, 1714850. Retrieved from 〈https://hal.science/hal-01714850〉.

Moukahal, L., Zulkernine, M., & Soukup, M. (2022). AVSDA: Autonomous Vehicle Security Decay Assessment. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *13204 LNCS*, 20–37. https://doi.org/10.1007/978–3-031–02067-4_2/COVER.

Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., Pantziou, G., 2009. A survey on jamming attacks and countermeasures in WSNs. IEEE Commun. Surv. Tutor. 11 (4), 42–56. https://doi.org/10.1109/SURV.2009.090404

Mun, H., Seo, M., Lee, D.H., 2022. Secure privacy-preserving V2V communication in 5G-V2X supporting network slicing. IEEE Trans. Intell. Transp. Syst. 23 (9), 14439–14455. https://doi.org/10.1109/TITS.2021.3129484

Nagy, L., 2023. Microstrip antenna development for radar sensor. Sensors 23 (2), 909. https://doi.org/10.3390/S23020909

Papernot, N., McDaniel, P., Wu, X., Jha, S., & Swami, A. (2016). Distillation as a Defense to Adversarial Perturbations Against Deep Neural Networks. *Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016*, 582–597. https://doi.org/10.1109/SP.2016.41.

Pardhasaradhi, B., Cenkeramaddi, L.R., 2022. GPS spoofing detection and mitigation for drones using distributed radar tracking and fusion. IEEE Sens. J. 22 (11), 11122–11134. https://doi.org/10.1109/JSEN.2022.3168940

Plathottam, S.J., & Ranganathan, P. (2018). Next generation distributed and networked autonomous vehicles: Review. *2018 10th International Conference on Communication Systems and Networks, COMSNETS 2018*, 2018-January, 577–582. https://doi.org/10.1109/COMSNETS.2018.8328277.

Qin, Z., Li, Q., 2023. An uncertain support vector machine with imprecise observations. Fuzzy Optim. Decis. Mak. 1–19. https://doi.org/10.1007/S10700-022-09404-0/METRICS

Robin, P., Emmerich, T., Ismail, A., Niguès, A., You, Y., Nam, G.H., Bocquet, L., 2023. Long-term memory and synapse-like dynamics in two-dimensional nanofluidic channels. Science 379 (6628), 161–167. https://doi.org/10.1126/SCIENCE.ADC9931/SUPPL_FILE/SCIENCE.ADC9931_SM.PDF

Rossiter, A. (2020). The impact of robotics and autonomous systems (RAS) across the conflict spectrum. *https://doi.org/10.1080/09592318.2020.1743481*, 31(4), 691–700. https://doi.org/10.1080/09592318.2020.1743481.

Rubinstein, B.I.P., Bartlett, P.L., Huang, L., Taft, N., 2009. Learning in a large function space: privacy-preserving mechanisms for SVM learning. J. Priv. Confid. 4 (1). https://doi.org/10.48550/arxiv.0911.5708

Ryan, C., Murphy, F., Mullins, M., 2020. Spatial risk modelling of behavioural hotspots: risk-aware path planning for autonomous vehicles. Transp. Res. Part A: Policy Pract. 134, 152–163. https://doi.org/10.1016/J.TRA.2020.01.024

Saeed, Z., Masood, M., Khan, M.U., 2023. A review: cybersecurity challenges and their solutions in connected and autonomous vehicles (CAVs). JAREE (J. Adv. Res. Electr. Eng.) 7 (1). https://doi.org/10.12962/JAREE.V7I1.322

Saez-Perez, J., Wang, Q., Alcaraz-Calero, J.M., Garcia-Rodriguez, J., 2023. Design, implementation, and empirical validation of a framework for remote car driving using a commercial mobile network. Sensors 23 (3), 1671. https://doi.org/10.3390/S23031671

Sankaranarayanan, R., Umadevi, K.S., Bhavani, N.P.G., Jos, B.M., Haldorai, A., Babu, D.V., 2022. Cluster-based attacks prevention algorithm for autonomous vehicles using machine learning algorithms. Comput. Electr. Eng. 101, 108088. https://doi.org/10.1016/J.COMPELECENG.2022.108088

Schirmer, S., & Torens, C. (2022). Safe Operation Monitoring for Specific Category Unmanned Aircraft, 393–419. https://doi.org/10.1007/978–3-030–83144-8_16.

Sengupta, S., Chakraborti, T., & Kambhampati, S. (2019). MTDeep: Boosting the Security of Deep Neural Nets Against Adversarial Attacks with Moving Target Defense. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11836 LNCS, 479–491. https://doi.org/10.1007/978-3-030–32430-8_28/COVER.

Sensors | An Open Access Journal from MDPI. (n.d.). Retrieved April 11, 2023, from 〈https://www.mdpi.com/journal/sensors〉.

Shu, J., Hong, M., Zheng, W., Sun, L.-M., & Ge, X. (n.d.). Multi-sensor Data Fusion Based on Consistency Test and Sliding Window Variance Weighted Algorithm in Sensor Networks. https://doi.org/10.2298/CSIS110617004S.

Singh, J.N., Tripathi, A., Bhardwaj, K., Srivastava, S., & Gupta, K. (2022). Wireless Remote Connection for IOT Vehicles. *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2022* , 988–994. https://doi.org/10.1109/ICACITE53722.2022.9823762.

Sripada, A., Bazilinskyy, P., de Winter, J., 2021. Automated vehicles that communicate implicitly: examining the use of lateral position within the lane. Ergonomics 64 (11), 1416–1428. https://doi.org/10.1080/00140139.2021.1925353/SUPPL_FILE/TERG_A_1925353_SM2027.DOCX

Stephan, K.D., Michael, K., Michael, M.G., Jacob, L., Anesta, E.P., 2012. Social implications of technology: the past, the present, and the future. Proc. IEEE 100 (SPL CONTENT), 1752–1781. https://doi.org/10.1109/JPROC.2012.2189919

Sugunaraj, N., & Ranganathan, P. (2022). Electronic Control Unit (ECU) Identification for Controller Area Networks (CAN) using Machine Learning. *IEEE International Conference on Electro Information Technology*, 2022-May, 382–388. https://doi.org/10.1109/EIT53891.2022.9813928.

Sun, X., Yu, F.R., Zhang, P., 2022. A survey on cyber-security of connected and autonomous vehicles (CAVs). IEEE Trans. Intell. Transp. Syst. 23 (7), 6240–6259. https://doi.org/10.1109/TITS.2021.3085297

Suryadi, N.N.P. (2023). Rancang Bangun Fault Reporting System (FRS) Berbasis Internet Of Things (IoT) Untuk Mengoptimalkan Keandalan Atmospheric Water Generator (AWG) Pada Kapal Pelayaran Rakyat.

Sustainability | An Open Access Journal from MDPI. (n.d.). Retrieved April 11, 2023, from 〈https://www.mdpi.com/journal/sustainability〉.

Swan, M., Fischer, S., 2015. Connected car: quantified self becomes quantified car. J. Sens. Actuator Netw. 4 (1), 2–29. https://doi.org/10.3390/JSAN4010002

Taylor, A., Japkowicz, N., & Leblanc, S. (2016). Frequency-based anomaly detection for the automotive CAN bus. *2015 World Congress on Industrial Control Systems Security, WCICSS 2015*, 45–49. https://doi.org/10.1109/WCICSS.2015.7420322.

Tippenhauer, N.O., Pöpper, C., Rasmussen, K.B., & Čapkun, S. (2011). On the requirements for successful GPS spoofing attacks. *Proceedings of the ACM Conference on Computer and Communications Security*, 75–85. https://doi.org/10.1145/2046707.2046719.

Tobaruela, J.A., Rodríguez, A.O., 2017. Reactive navigation in extremely dense and highly intricate environments. PLoS ONE 12 (12). https://doi.org/10.1371/JOURNAL.PONE.0189008

Tramèr, F., Kurakin, A., Papernot, N., Goodfellow, I., Boneh, D., & McDaniel, P. (2017). Ensemble Adversarial Training: Attacks and Defenses. *6th International Conference on Learning Representations, ICLR 2018 - Conference Track Proceedings.* https://doi.org/10.48550/arxiv.1705.07204.

Tschantz, M.C., Kaynar, D., Datta, A., 2011. Formal verification of differential privacy for interactive systems (extended abstract). Electron. Notes Theor. Comput. Sci. 276 (1), 61–79. https://doi.org/10.1016/J.ENTCS.2011.09.015

Tseng, F.H., Yeh, K.H., Kao, F.Y., Chen, C.Y., 2023. MiniNet: Dense squeeze with depthwise separable convolutions for image classification in resource-constrained autonomous systems. ISA Trans. 132, 120–130. https://doi.org/10.1016/J.ISATRA.2022.07.030

Valavanis, K., 2018. Handbook of unmanned aerial vehicles. Springer International PU (Retrieved from). 〈https://link.springer.com/book/9783319483191〉.

Van Wyk, F., Wang, Y., Khojandi, A., Masoud, N., 2020. Real-time sensor anomaly detection and identification in automated vehicles. IEEE Trans. Intell. Transp. Syst. 21 (3), 1264–1276. https://doi.org/10.1109/TITS.2019.2906038

Wang, J., Su, W., Luo, C., Chen, J., Song, H., Li, J., 2022. CSG: classifier-aware defense strategy based on compressive sensing and generative networks for visual recognition in autonomous vehicle systems. IEEE Trans. Intell. Transp. Syst. 23 (7), 9543–9553. https://doi.org/10.1109/TITS.2022.3146038

Wang, J., Xiao, Y., Li, T., Chen, C.L.P., 2023. A jamming aware artificial potential field method to counter GPS jamming for unmanned surface ship path planning. IEEE Syst. J. 1–12. https://doi.org/10.1109/JSYST.2023.3237613

What is an Autonomous Car? – How Self-Driving Cars Work | Synopsys. (n.d.). Retrieved April 11, 2023, from 〈https://www.synopsys.com/automotive/what-is-autonomous-car.html〉.

Wolcott, R.W., & Eustice, R.M. (2014). Visual localization within LIDAR maps for automated urban driving. *IEEE International Conference on Intelligent Robots and Systems*, 176–183. https://doi.org/10.1109/IROS.2014.6942558.

Wong, S.D., Walker, J.L., Shaheen, S.A., 2021. Bridging the gap between evacuations and the sharing economy. Transportation 48 (3), 1409–1458. https://doi.org/10.1007/S11116-020-10101-3/TABLES/15

Wyglinski, A.M., Huang, X., Padir, T., Lai, L., Eisenbarth, T.R., Venkatasubramanian, K., 2013. Security of autonomous systems employing embedded computing and sensors. IEEE Micro 33 (1), 80–86. https://doi.org/10.1109/MM.2013.18

Xu, W., Yan, C., Jia, W., Ji, X., Liu, J., 2018. Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles. IEEE Internet Things J. 5 (6), 5015–5029. https://doi.org/10.1109/JIOT.2018.2867917

Xu, X., Zhang, J., Li, Y., Wang, Y., Yang, Y., Shen, H.T., 2021. Adversarial attack against urban scene segmentation for autonomous vehicles. IEEE Trans. Ind. Inform. 17 (6), 4117–4126. https://doi.org/10.1109/TII.2020.3024643

Yan, W. (2016). A two-year survey on security challenges in automotive threat landscape. *2015 International Conference on Connected Vehicles and Expo, ICCVE 2015 - Proceedings*, 185–189. https://doi.org/10.1109/ICCVE.2015.1.

Yang, J., Liu, B., Ma, F., Jiao, Q., 2023. Target recognition using rotating ultrasonic sensor for an amphibious ROV. Eng. Res. Express. https://doi.org/10.1088/2631-8695/ACBD13

Ye, F., Zhang, S., Wang, P., & Chan, C.Y. (2021). A survey of deep reinforcement learning algorithms for motion planning and control of autonomous vehicles. *IEEE Intelligent Vehicles Symposium, Proceedings, 2021-July*, 1073–1080. https://doi.org/10.1109/IV48863.2021.9575880.

Zhang, J., Lou, Y., Wang, J., Wu, K., Lu, K., Jia, X., 2022a. Evaluating adversarial attacks on driving safety in vision-based autonomous vehicles. IEEE Internet Things J. 9 (5), 3443–3456. https://doi.org/10.1109/JIOT.2021.3099164

Zhang, K., Liu, Y., Mei, F., Jin, J., Wang, Y., 2023. Boost correlation features with 3D-MiIoU-based camera-LiDAR fusion for MODT in autonomous driving. Remote Sens. 15 (4), 874. https://doi.org/10.3390/RS15040874

Zhang, X., Chan, F.T.S., Yan, C., Bose, I., 2022a. Towards risk-aware artificial intelligence and machine learning systems: an overview. Decis. Support Syst. 159, 113800. https://doi.org/10.1016/J.DSS.2022.113800

Zhang, X., Jiang, Y., Lu, Y., Xu, X., 2022b. Receding-horizon reinforcement learning approach for kinodynamic motion planning of autonomous vehicles. IEEE Trans. Intell. Veh. 7 (3), 556–568. https://doi.org/10.1109/TIV.2022.3167271

Zhu, Y., Adepu, S., Dixit, K., Yang, Y., & Lou, X. (2023). Adversarial Attacks and Mitigations on Scene Segmentation of Autonomous Vehicles, 46–66. https://doi.org/10.1007/978–3-031–25460-4_3.