International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I1P111

Volume 72 Issue 1, 101-116, January 2024

Original Article

Cybersecurity in Autonomous Vehicles: A Comprehensive Review Study of Cyber-Attacks and AI-Based Solutions

Guirrou Hamza[1], Youssef Taher[2], Mohamed Zeriab Es-sadek[3], Amal Tmiri[4]

[1,3,4]*ENSAM, Mohammed V University in Rabat, Morocco.*
[2]*Center of Guidance and Planning of Education in Rabat, Morocco.*

[1]*Corresponding Author: hamza.guirrou@gmail.com*

Received: 09 August 2023 Revised: 10 November 2023 Accepted: 12 December 2023 Published: 07 January 2024

Abstract *- Cyber-attacks on autonomous vehicles (AVs) are becoming increasingly sophisticated and pose serious risks, including loss of control of the vehicle or compromise of personal data. Preventing intrusion into AV systems requires protecting against various cyberattacks by adopting appropriate countermeasures. One of these advanced countermeasures is using Artificial Intelligence (AI) technologies as an efficient and effective solution for AV security. Thanks to the increasing prevalence of AI, AV systems can detect, prevent, and mitigate attacks more efficiently than traditional software-driven approaches. In this context, the goal of this paper is to present a summary of recent developments in AI-based cybersecurity for AVs in order to identify knowledge gaps and provide recommendations for future studies. We discuss the relevant standards and regulations related to cybersecurity in AVs. We examine the high-risk AV components that are vulnerable to cybersecurity attacks. Furthermore, we review the most critical cyber-attacks that may affect these critical systems and their possible AI-based cybersecurity solutions.*

Keywords *- Cybersecurity, Artificial Intelligence, Autonomous vehicles.*

1. Introduction

The way we transport people and things could be completely transformed by AVs. This technological innovation offers significant sustainability, safety, and convenience benefits. However, the reliance on software and communication networks exposes these vehicles to many possible flaws that could be exploited by intruders or attackers and raise serious threats and risks (loss of control of the car, the theft of personal information, or even physical injury to the occupants or other road user). Consequently, preventing and protecting AVs against these attacks based on advanced technologies is one of the current major concerns of AVs Research Groups (AVRG). One of these advanced solutions that can be used to rapidly examine millions of events and identify many different types of threats is AI. Indeed, AI-based cybersecurity solutions have emerged as promising tools in the field of cybersecurity for AVs, offering adaptive defences that can react to new and developing threats, giving a more thorough and potent defence. For example, by using Machine Learning (ML) models or Deep Learning (DL) networks, AV systems can analyse massive volumes of data (events) and identify new threats in real-time, making it possible to detect, prevent, and respond to cyberattacks more successfully. In recent years, many AVRG groups have started investigating the possibility of AI-based cybersecurity systems. For example, the Automotive Information Sharing and Analysis Center (Auto-ISAC) offered 2014 a forum for discussion and the exchange of knowledge regarding cybersecurity issues facing the sector. Standards and best practices for AI-based cybersecurity solutions have been developed as a result of this collaboration in the automobile sector [10]. Following the passage of the Security and Privacy in Your Car (SPY Car) Act in 2018 [11], the National Highway Traffic Safety Administration (NHTSA) was mandated to create cybersecurity standards for automobiles. On the other hand, several scientific investigations have shown how AI-based cybersecurity can be used in AVs. As examples of important recent studies. Mecheva et al. defined the broad contours of the intelligent transportation systems ITS architecture and security challenges. The main areas of focus for security approaches are device configuration and initialization during manufacturing at the perception layer, anonymous node authentication in VANET at the network layer, defence of fog-based structures at the support layer, description and standardization of the complex model of data and metadata, and defence of AI-based systems at the application layer [1].

Sharma et al. provide a comprehensive review of digital forensics and cyberattacks on connected autonomous vehicles (CAVs). Before illustrating the existing security, the authors first review each component of a typical CAV network. Sensors, communication networks, and actuators were the three main CAV parts examined. Additionally, investigations into conventional and AI-based cyber-defense strategies were presented together with the extension of cybersecurity and forensic difficulties. Finally, they highlight the unresolved issues and potential research directions for creating effective forensic and cybersecurity solutions specifically for CAVs [2]. Girdhar et al. examine adversarial attacks on the ecosystem for automated driving and discuss adversarial defense models to strengthen defenses against assaults on ML components in AVs. The authors have specifically highlighted the significance of generic defense strategies in order to increase resilience and secure the ML and training data for AVs [3]. Bendiab et al. investigate the potential use of a hybrid blockchain-and-AI approach to AV security. The authors established a classification of potential security and privacy risks associated with the use of AVs. Then, they gave a summary of the research on the use of blockchain and AI to secure AVs. Finally, based on their systemic evaluation, they emphasized the potential drawbacks and difficulties associated with integrating Blockchain and AI with AVs and proposed possible future lines of inquiry [4]. Mudhivarth et al. provide a summary of potential attacks and countermeasures against networked and autonomous vehicles.

The attacker's domain of autonomous and connected vehicles and any related defenses are classified into three categories: safety system attacks, connection assaults, and diagnostics attacks. The authors also provided a domain analysis to appreciate the situations in this domain, recommendations, and future potential in this sector for further research [5]. Khan et al. present the CAV communication structure in a realistic manner with a graphical flow chart to give a clear image of all the interfaces of CAV cyber-attacks in the Intelligent Transport System.

The authors discussed how conventional cyber-physical system cybersecurity measures for CAVs were ineffectual. They summarized cyberattacks on CAVs, the accompanying CAV communication system, their impact, and the corresponding mitigation measures. Additionally, they indicated prospective directions that must be taken for the timely and effective defense against cyberattacks [6]. Guan et al. Consider the causes of the present car network's susceptibility to network attacks.

The authors listed the criteria for vehicular networks' security, various security assaults on intelligent vehicle systems, and difficulties associated with them. In addition, they have assigned grades to the security-enhancement solutions for intelligent, networked vehicles based on how well they defend against known assaults.

Discovering some benefits and drawbacks of the suggested defenses was their main goal. They concluded by thoroughly examining three popular techniques for aberrant intrusion detection in-vehicle networks [7]. Wong et al. set out to carefully examine the security concerns raised by connected and autonomous vehicle technologies, to assess the impact of cyberattacks on CAV performance, and to describe the remedies in an appropriate manner. The authors discussed the effects of cyberattacks on the functionality of CAVs from the perspectives of both intra-vehicle systems and inter-vehicle systems. For CAVs to be used in practice safely and reliably, they emphasized that ensuring their perception and operations would be the most important prerequisite. In addition, they recommended using cloud and fresh AI techniques to fight against cunning cyber-attacks against CAVs. automobile network intrusion detection [8]. Dibaei et al. highlight a few significant security assaults on the linked, intelligent vehicles. Based on these attacks, the authors thoroughly analyse the existing countermeasures and divide them into four groups: software vulnerability identification, network security, cryptography, and malware detection. They also look at potential future strategies for guarding against attacks on sophisticated vehicle systems [9].

Improving the existing AI-based cyber-security solutions or innovating alternative AI models entails identifying the most risky and critical AV components. Identifying the potential threats to each component. Selecting and implementing the cybersecurity best practices, techniques, advanced technology and measures to mitigate the most possible threats and attacks on AVs. In this context, the present investigation aims to systematically summarize different cyber attacks on critical AV components to review corresponding AI-based approaches in cyber-security in AV systems. In the first step, we review and summarize in detail the pertinent AV cyber-security standards. In the second step, we identify the most risky AV components and the most common and most dangerous types of cyber attacks affecting each AV component. Finally, we review the corresponding AI-based solutions in cyber-security in AV systems.

2. Review of AV Security Standards

Using AI-Based solutions in Autonomous Vehicles requires the coordination of many AV security levels (people, processes, technology). Numerous cybersecurity standards have been created to ensure careful coordination, especially for AV systems. These standards (guidelines / best practices) offer a framework for handling cybersecurity threats through the development of AVs and disposal at the end of their useful lives. Integrating AI-Based solutions with these guidelines or best practices offers a set of rules, suggestions, models, and technical solutions to address a number of cybersecurity-related topics, including risk assessment, threat monitoring, incident response, access control, and security assessment and authorization. The paragraphs summarize below the most pertinent AV cyber-security standards.

2.1. ISO/SAE 21434

Road vehicles Cybersecurity engineering: is an extensive cybersecurity system created especially for self-driving cars. For the whole lifecycle of the vehicle, from conception to decommissioning, it offers guidelines to ensure cybersecurity concerns are addressed. The standard specifies requirements for incident response, security testing, threat modeling, and risk assessment. In order to ensure a coordinated approach to cybersecurity, it also underlines the significance of cooperation amongst many stakeholders, including manufacturers, suppliers, and regulators. In addition to promoting customer confidence in this new technology, adherence to the ISO/SAE 21434 standard can assist in safeguarding the security and safety of autonomous cars and the people they transport [32].

2.2. SAE J3061

The Society of Automotive Engineers (SAE) produced the Cybersecurity Guidebook for Cyber-Physical Vehicle Systems standard to address cybersecurity risks in the design and usage of AVs. The standard offers a thorough framework for handling cybersecurity threats all the way through the lifecycle of a vehicle, from conception to disposal at the end of its useful life. It describes a risk-based strategy for cybersecurity that entails ongoing assessment of threats and vulnerabilities, risk assessment, and risk reduction tactics.

The standard focuses on the value of cooperation between various stakeholders, including producers, suppliers, and regulators, and offers instructions on how to set up efficient information-sharing and communication processes. Compliance with SAE J3061 can help guarantee that AVs are planned and deployed with strong cybersecurity measures, lowering the danger of cyberattacks and aiding in developing trust in this emerging technology [33].

2.3. NIST SP 800-53 Rev. 5

The National Institute of Standards and Technology (NIST) developed Security and Privacy Controls for Information Systems and Organizations to assist enterprises in managing and securing their information systems. Although it is not specifically designed for AV cybersecurity, it can be utilized in this context. The recommendations offer a thorough framework for managing cybersecurity risks and contain measures for locating, evaluating, and reducing those risks. With a focus on ongoing monitoring and assessment of threats and vulnerabilities, the framework stresses a risk-based approach to cybersecurity.

The controls cover a wide range of topics, such as incident response, access control, and security assessment and authorization. Adopting NIST SP 800-53 Rev. 5 will enable enterprises to create a thorough cybersecurity program that tackles the particular problems presented by AVs and helps to lessen the dangers connected with this cutting-edge technology [34].

2.4. UN Regulation No. 155

The United Nations Economic Commission for Europe (UNECE) developed the Cyber Security and Cyber Security Management System to address cybersecurity risks associated with designing and using connected CAVs. Risk assessment, threat monitoring, and incident response are only a few of the cybersecurity standards and guidelines provided by the legislation for CAV.

Additionally, it sets a system for type approval, under which manufacturers must prove that their CAVs adhere to the required cybersecurity requirements before they can be supplied in the participating nations. In addition to promoting international harmonization of cybersecurity standards for this developing technology, compliance with UN Regulation No. 155 can aid in ensuring the security and safety of CAVs and those who ride in them [35].

2.5. IEC 62443-4-2

Security for industrial automation and control systems Part 4-2: is an industrial automation and control systems IACS-specific cybersecurity standard created by the International Electrotechnical Commission (IEC). It offers instructions for creating, putting into use, and maintaining secure IACS networks, including those used in self-driving cars.

In order to defend IACS networks against online dangers, including malware, denial-of-service attacks, and unauthorized access, the standard contains a set of security controls and countermeasures. It also offers risk evaluation and administration recommendations, including developing security principles and practices. By lowering the danger of cyberattacks and fostering the safe and dependable functioning of these cars, compliance with IEC 62443 part 4-2 can help assure the security and resilience of autonomous vehicle networks [36].

2.6. UL 4600

Standard for Safety for the Evaluation of Autonomous Products: is a safety standard created by Underwriters Laboratories (UL) for autonomous vehicle systems. Although not explicitly focused on cybersecurity, it incorporates cybersecurity considerations as part of the overall safety framework. The standard offers standards for creating and testing autonomous vehicle technologies to ensure they are trustworthy and safe for usage on public roads.

It also outlines procedures for testing and validating autonomous vehicle systems and specifications for risk assessment, hazard detection, and mitigation measures. Compliance with UL 4600 can guarantee that AVs are developed and deployed with a focus on safety and reliability, which can, therefore, help to reduce cybersecurity risks by lowering the probability of mishaps or other occurrences brought on by software or hardware faults [37].

3. Related Work

3.1. Research Methodology

The research methodology used for this comprehensive review article is a thorough and in-depth examination of the current literature on cybersecurity concerns and solutions in the context of autonomous cars. The first phase entails thoroughly assessing scholarly databases, peer-reviewed journals, conference proceedings, and respectable books, focusing on studies relevant to cyber-attacks and AI-based cybersecurity solutions in autonomous vehicles. During this literature review, key themes such as the kinds of cyber attacks, vulnerabilities, and the use of artificial intelligence to improve cybersecurity will be diligently identified. Inclusion and exclusion criteria will be developed to ensure the selection of recent and relevant studies, focusing on those that significantly contribute to the knowledge of cybersecurity challenges in autonomous cars. The data extraction procedure will entail systematically gathering information on the methodology used in the selected research; important discoveries highlighted problems, and the success of AI-based cybersecurity solutions. A detailed comparison study was undertaken to assess the techniques' strengths and limitations across the evaluated literature. The findings synthesis seeks to provide a comprehensive overview of the present state of knowledge in cybersecurity for autonomous vehicles, including insights into prevalent risks, mitigation tactics, and the role of AI in enhancing security measures. We start by identifying and inventorying the most risky AV components. We present in the second step a comprehensive review study of cyber-attacks in AVs systems. In the third phase, we study the most advanced AI-based solutions to mitigate the most dangerous and extreme attacks in AV systems and limit their impacts. We summarize the AI-based cybersecurity solutions that reduce the risk of appropriate types of attacks. Figure 1 summarizes our research methodology.

3.2. Identification and Inventory of the Exposed AV Components for Cyber Attacks

AV systems depend on a sophisticated network of interconnected systems/subsystems (sensors, control systems, entertainment systems, and more) and software susceptible to cyber threats. To invest in developing and implementing an effective and efficient AI-based cybersecurity solution, it is crucial as a first process to inventory the main components of AVs that are susceptible to cyberattacks and identify the potential threats to each component. In this context, we review the main AVs components considered most risky in the paragraph below.

3.2.1. Remote Access Interfaces

Engineers and technicians can access the autonomous car's systems from outside the vehicle using remote access interfaces. This can help complete maintenance, upgrades, or diagnostics without physically accessing the car. These interfaces, however, can also be a point of vulnerability for online crimes.

Attackers might be able to alter or interfere with the vehicle's systems if they get illegal access to the remote access interface, leading to malfunction or even a crash. Furthermore, default or weak passwords on remote access interfaces that are simple to guess or hack could provide attackers access to the vehicle's systems [12, 13].

3.2.2. Cellular and Wireless Communication Interfaces

Without cellular and wireless communication interfaces, AVs cannot connect with other vehicles, infrastructure, or the cloud. The vehicle can exchange its own data with other vehicles and the cloud through these connections and access real-time traffic statistics, maps, and software updates. These portals for communication, though, can also be a weak spot for online threats. The car's security may be jeopardized if an attacker manages to intercept, block, or manipulate the data being transmitted, putting passengers at risk. Additionally, attackers may be able to take advantage of flaws in cellular and wireless communication interfaces, such as shoddy encryption or readily guessable or hackable default settings [14, 15].

3.2.3. Navigation Systems

Autonomous vehicle navigation systems give the vehicle vital information regarding its position, speed, and direction of travel. These technologies help the car navigate and safely avoid obstacles by combining sensors, GPS, and mapping data. However, cyberattacks can also target navigation systems. An attacker may be able to alter the mapping data or manipulate the sensor data, which might lead to the vehicle making bad decisions or losing its bearings [16].

3.2.4. Infotainment Systems

Streaming music and videos, internet access, speech recognition, and other features and services are all available to passengers by infotainment systems in AVs. These systems improve the entire driving experience and offer convenience and entertainment to passengers. Infotainment systems, however, can also be the subject of cyberattacks. An attacker might be able to acquire confidential information or seize control of the car's systems by taking advantage of flaws in the system. For instance, an attacker could utilize an internet-connected USB drive infected with malware to launch a remote attack or inject malicious code into the infotainment system [17].

3.2.5. In-Vehicle Networks

The technologies in AVs that allow various parts of the vehicle to connect and exchange data with one another are known as in-vehicle networks. These networks allow the car's different systems, including the steering, brakes, and engine, to operate together smoothly and safely. In-vehicle networks, however, can potentially be an area of vulnerability for online crimes. The vehicle's systems could be manipulated or interfered with by an attacker if they are able to access the network, leading to a malfunction or perhaps a crash [18, 19].

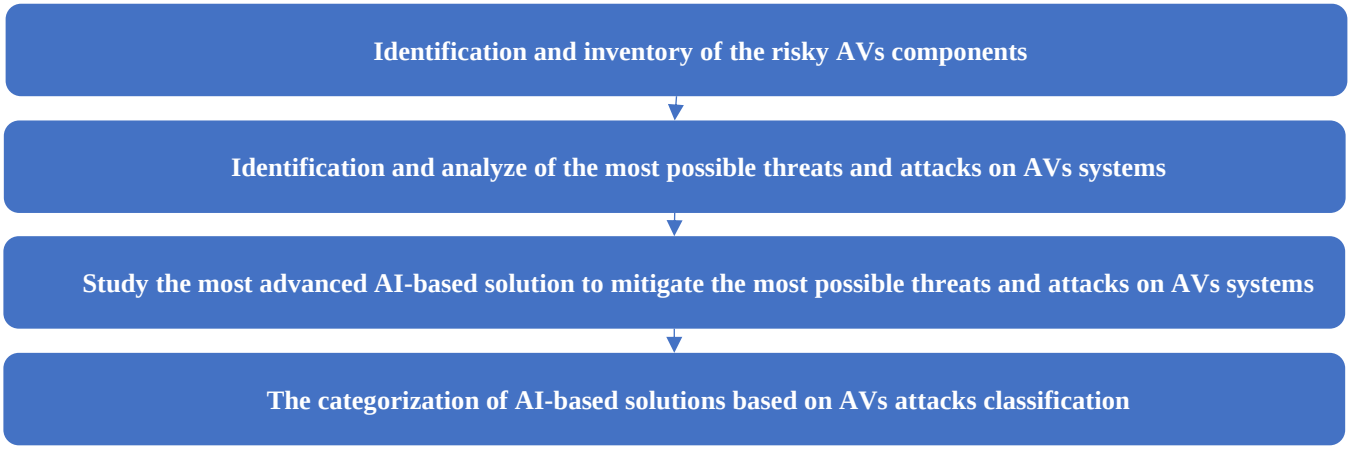

Fig. 1 Research methodology

3.2.6. Sensor Systems

Sensor systems in AVs are essential for gathering information about the environment around the vehicle, such the distance to other vehicles, the state of the road, and the movements of pedestrians. These systems gather and examine information about the environment around the vehicle using a range of sensors, such as lidar, radar, and cameras. However, cyberattacks against sensor systems are also a possibility. The sensor data may be susceptible to manipulation or spoofing by an attacker, which might lead to the vehicle making poor decisions or losing its bearings [20, 21].

3.2.7. Control Systems

The operation of an autonomous vehicle, including acceleration, braking, and steering, is managed by control systems. These systems analyze data from multiple sensors and utilize sophisticated algorithms and software to decide how the car should run. Control systems, however, can potentially be the target of cyberattacks. The vehicle might behave erratically or possibly cause an accident if an attacker manages to access the system and modify the algorithms [22].

3.2.8. Electronic Control Units

AVs Electronic Control Units (ECUs) are in charge of managing a number of electrical systems, including the engine, transmission, and brakes.

These systems analyze data from multiple sensors and utilize sophisticated algorithms and software to decide how the car should run. ECUs, however, may also be the target of cyberattacks. The vehicle might behave erratically or possibly cause an accident if an attacker manages to enter the system and modify the algorithms [23, 24].

3.2.9. Human-Machine Interfaces

The technologies in AVs that enable drivers and passengers to communicate with the various parts and systems of the vehicle are known as human-machine interfaces (HMIs).

These interfaces enable users to operate the car's functions and obtain operational data, including touch displays, voice-activated assistants, and other input devices.HMIs, however, can also be a point of weakness for online crimes. A hacker who gains access to the system may be able to alter the data shown on the screen or introduce harmful code into the HMI, which could confuse or distract the driver [25, 26].

3.2.10. Data Storage Systems

Data storage systems in AVs are in charge of keeping track of various data kinds, including navigational information, sensor readings, and driver preferences, that are gathered by the vehicle's sensors and other systems. These systems store the data on various storage devices, including solid-state drives and flash memory.

Data storage systems, however, can potentially be the target of cyberattacks. A hacker might be able to enter the system and take trade secrets, personally identifiable information (PII), or other sensitive data. Additionally, a hacker might be able to introduce malware or malicious code into the storage system, which could lead to data loss or corruption [27].

3.2.11. Software and Firmware Updates

Software and firmware updates are necessary for the various systems in AVs to continue operating as intended and to patch any newly identified vulnerabilities. The automaker or independent companies may offer these upgrades and send over-the-air (OTA) or through physical media, like a USB drive. Software and firmware updates, however, might also be the subject of cyberattacks.

Malicious code could be injected into the update process by an attacker, possibly compromising the entire vehicle's system. Additionally, a hacker may be able to take advantage of holes in the updating system itself, which could lead to a malfunction or even an accident [28, 29].

3.2.12. Emergency Systems

In the case of an emergency, AVs are equipped with emergency systems to protect both the occupants and the vehicle. These systems might have functions like automatic shut-off during a collision, emergency braking, and collision avoidance. However, cyberattacks can also be directed towards emergency systems. These systems might be vulnerable to assault; if they are, an accident might occur, or the system might fail to react correctly in an emergency [31].

3.3. Major Cyber Attacks in AVs

Any malicious action intended to compromise or alter the vehicle's systems or data is considered a cyber assault on AVs. Phishing attacks, malware injection, denial of service attacks, and direct physical assaults on the vehicle's hardware are among the many examples of the various ways that cyberattacks can manifest. A successful cyber attack on an autonomous car might have devastating effects, including loss of control, system failures, and even physical injury to other drivers and passengers. Implementing a thorough security strategy that includes features like access controls, network security, encryption and authentication, as well as frequent security testing and audits, is crucial to preventing cyber attacks against AVs. Additionally, it is critical to be informed of the most recent cybersecurity threats and vulnerabilities and regularly update and enhance security precautions to handle new hazards as they manifest.

3.3.1. Remote Control Hijacking

Remote control hijacking is a serious cyber attack that could target AVs. In this kind of attack, the attacker remotely takes over the car's steering, braking, and acceleration functions. Potentially, the attacker may steer the car in a dangerous direction or even cause it to crash. Insecure wireless communication routes or shoddy authentication procedures in the vehicle's software can lead to remote control hijacking. Given how heavily AVs depend on software and communication networks to function securely, this kind of attack should be of special concern. Strong security measures must be implemented to avoid remote control hijacking, including encryption, firewalls, and regular software upgrades to fix any known flaws. Additionally, manufacturers must consider putting in place fail-safe systems that permit the car to halt or slow down in the case of an attack [38, 39].

3.3.2. Sensor Spoofing

Sensor spoofing is yet another sort of cyberattack that might be employed against AVs. The goal of this assault is to cause the car to make poor decisions or possibly crash by fooling its sensors with bogus data. For instance, a perpetrator might use a tool to broadcast erroneous signals to a car's radar or lidar sensors, giving the impression that a bogus obstacle is on the road when it is not. This can lead to a swerve or abrupt braking in the car, which might result in an accident. The vehicle's perception of traffic signals and other road indicators can be manipulated using sensor spoofing, leading it to disregard or misinterpret crucial messages.

Secure communication protocols must be established between the sensors on the vehicle and other systems to prevent sensor spoofing. Additionally, it is crucial to use a variety of sensors to cross-check data and spot discrepancies. Algorithms for ML can also be used to identify prospective attacks by spotting anomalies in sensor data [21, 40, 41].

3.3.3. Denial of Service (DoS) Attacks

A Denial of Service cyber attack is a kind of cyberattack that might be used to target AVs. In this attack, the attacker overwhelms the systems or networks of the vehicle with traffic or requests, rendering the system inaccessible or unresponsive. This may interfere with the vehicle's ability to operate properly or possibly result in its complete shutdown.

For instance, a DoS assault on a vehicle's navigation system could be launched by an attacker, preventing it from accessing vital location data and leading to the vehicle getting lost or confused. It is crucial to employ network security measures, such as firewalls and intrusion detection systems, to detect and block malicious traffic to prevent DoS assaults. Furthermore, putting redundancy and failover methods into place can aid in making sure that crucial systems continue to function even if one system is hacked. Regular security testing and audits can also assist in locating and resolving possible flaws that might be used in a DoS attack [42, 43].

3.3.4. Malware Injection

Malware injection is a sort of cyberattack that might be employed against autonomous cars. In this attack, malicious malware is inserted into the vehicle's onboard computer systems, giving the attacker access to take control or steal information. Using a software flaw, an attacker could, for instance, implant malware into the car's infotainment system, which could then spread to other systems, such as the steering or brake systems. With this access, the attacker may take over the vehicle, steal confidential information, or even bring about a collision. Malicious downloads, infected software updates, or direct physical access to the vehicle's systems are just a few ways that malware might be injected. It is crucial to put strong security measures in place to avoid malware injection, including secure boot procedures, code signing, and regular software updates to fix any known imperfections. In addition, malware attacks may be detected and handled using intrusion detection and response systems [44, 45].

3.3.5. Physical Attacks

A Physical, cyber attack is a kind of cyberattack that entails physically accessing the vehicle's hardware or systems in order to hack or alter them. In this type of attack, the attacker acquires access to the vehicle's physical parts, such as its sensors, CPUs, or communication modules, and makes use of this access to alter the way the vehicle behaves or steal private information. For instance, a physical altercation with the vehicle's braking system by the assailant could result in system failure and the possibility of an accident.

Implementing physical security measures, such as tamper-proof hardware and secure boot procedures, to prevent unauthorized access to the vehicle's components is crucial to preventing physical cyber attacks. Furthermore, even if physical access is acquired, installing robust encryption and authentication procedures can help to protect data and communications. Regular security testing and audits can also assist in locating and addressing possible flaws that might be used in a real-world cyberattack [46, 47].

3.3.6. GPS Jamming

GPS jamming is a kind of cyberattack that might be used to target AVs. The attacker interferes with the vehicle's GPS signal in this assault, making it challenging for the car to navigate or function properly. Using equipment that emits radio signals at the same frequency as GPS signals can result in GPS jamming, interfering with the vehicle's capacity to receive precise positioning information. This could result in the car getting lost or confused, which could put other people's safety in danger or cause a collision. Since AVs rely so largely on GPS data to navigate and function securely, GPS jamming can be very troublesome for them. It is crucial to use redundant positioning systems, such as several GPS receivers or other positioning technologies, including inertial navigation or camera-based systems, to prevent GPS jamming. Further reducing the effects of GPS jamming attempts is using signal filtering and jamming detection systems [48, 49].

3.3.7. Phishing Attacks

Phishing attacks are an example of a cyberattack that might target AVs. In this assault, the attacker deceives the users or operators of the vehicle into disclosing confidential information or engaging in malicious behavior. An attacker might, for instance, send a phishing email to a vehicle operator while impersonating a trustworthy source, like a manufacturer or service provider, and asking for private data or access to the car's systems.

The driver can unintentionally provide the attacker access to the vehicle's systems or sensitive information if they fall for the phishing scam. The car's systems can also be infected with malware or other harmful software through phishing tactics. It is crucial to inform users and operators about the dangers of social engineering attacks and to put robust authentication and access control measures in place to restrict access to sensitive data and systems to prevent phishing attacks. Regular security awareness training and phishing simulation exercises can also assist in educating users and operators on how to spot and react to phishing attempts [50].

3.3.8. Ransomware

Ransomware is a kind of cyberattack that might be used to target AVs. In this attack, the attacker employs malicious software to lock down or encrypt the vehicle's systems, preventing them from functioning until a ransom is paid.

Ransomware attacks can happen in a number of ways, including through phishing emails, software flaws, or malicious downloads. The attacker will often request money after the vehicle's systems have been encrypted or locked down in exchange for a decryption key or to regain access to the vehicle's systems. Because AVs rely so much on software and communication networks to function securely. Strong security procedures, such as routine software updates and backups, should be implemented to address any known vulnerabilities and guarantee that data can be restored during an attack. A thorough incident response plan should also be in place to enable timely detection and reaction to possible ransomware attacks [51, 52].

3.3.9. Man-In-The-Middle Attacks

A Man-in-the-middle (MITM) attack is a kind of cyberattack that might be used to target AVs. The attacker in this attack intercepts and modifies communications between the car's systems and other gadgets or systems, like a remote control or a cellular network. The attacker can then alter the information being sent between the two systems, possibly leading to the car acting unexpectedly or disclosing private information. For instance, a remote control signal could be intercepted and altered by an intruder, sending the vehicle off course or accelerating suddenly. Passengers or other motorists may be put at risk for injury as a result of this. Strong encryption and authentication procedures must be used to safeguard communications between the vehicle's systems and other devices or systems to prevent MITM attacks. Implementing intrusion detection and response systems can also aid in the real-time identification and mitigation of potential MITM threats [53-55].

3.3.10. Social Engineering

Social engineering is a kind of cyberattack that might be used to target AVs. In this assault, the attacker deceives users or operators into disclosing sensitive information or engaging in destructive behavior by using psychological manipulation. Social engineering attacks can take many different shapes, such as phishing, pretexting, or baiting. In order to fool the operator into giving access to the vehicle's systems or critical information, the attacker, for instance, could appear as an authorized service provider or vehicle manufacturer. Alternatively, a hacker may employ social engineering to access the vehicle's systems physically, for example, by pretending to be a mechanic or maintenance staff member. Due to the dependence of AVs on the reliability of their onboard equipment and the trust of their operators, social engineering attacks can be particularly worrying. It is crucial to inform users and operators about the dangers of social engineering and to implement robust access control and authentication procedures to prevent social engineering attacks. Regular security awareness training can also assist in educating users and operators on spotting and reacting to potential social engineering threats [56, 57].

3.3.11. Wireless Network Attacks

A wireless network cyber attack is a sort of cyberattack that might be employed against autonomous cars. In this assault, the attacker takes advantage of flaws in the vehicle's Wi-Fi or Bluetooth wireless networks to obtain unauthorized access to its systems or data. The attacker may then exploit this access to make the car act inadvertently or leak private data. A hacker could, for instance, utilize a Wi-Fi network to access the car's infotainment system and then install malware that would give them remote access to the car's controls.

Alternately, an attacker may use a Bluetooth connection to access the vehicle's diagnostic systems and change the performance or safety features of the vehicle. Strong encryption and authentication procedures must be used to safeguard wireless communications between the vehicle's systems and other devices or systems to prevent wireless network attacks. It is also crucial to establish intrusion detection and response systems to identify and stop any attacks quickly, as well as to update software and hardware regularly to fix any known vulnerabilities [58, 59].

3.3.12. Brute Force Attacks

A Brute force cyber attack is a sort of cyberattack that might be employed against autonomous cars. In this attack, the attacker tries to access the vehicle's systems or data by guessing passwords or other authentication credentials. In most cases, the attacker makes use of automated systems that can quickly test thousands of potential passwords. Suppose the attacker is able to guess the right password. In that case, they might potentially get access to the vehicle's systems and data, which would give them the power to make the car do unexpected things or divulge private data.

An attacker could, for instance, conduct a brute force attack to get into the car's control systems and change the speed or direction. Employing multi-factor authentication techniques, which demand additional verification beyond a basic password, and using strong, complicated passwords are crucial steps in preventing brute-force assaults. Furthermore, brute force attacks can be avoided by changing passwords regularly and minimizing the number of unsuccessful login attempts [60].

3.3.13. Supply Chain Attacks

A Supply chain cyber attack is a kind of cyberattack that might be used to target AVs. The supply chain of the vehicle, which consists of all the parts and systems required in its construction and operation, is the object of this attack. The attacker may be able to obtain unauthorized access to the car's systems or data by compromising one or more supply chain components, which would give them the ability to make the vehicle act unexpectedly or divulge private data. For instance, a hacker could gain access to the networks of a component manufacturer, enabling them to insert malware into the firmware of a vital automobile part, such as the brake system. This might allow the attacker to control the vehicle's functionality or safety systems from a distance. To prevent supply chain assaults, it is crucial to examine all parts and suppliers for security flaws thoroughly and to put strong security controls in place throughout the whole supply chain. The use of robust encryption and authentication systems, as well as routine security audits and testing, can all be used to safeguard communications and data along the whole supply chain [61, 62].

3.3.14. ECU Reprogramming

An Electronic Control Unit (ECU) reprogramming cyber attack is a category of cyber attack that involves tampering with the software or firmware that regulates the systems and parts of the vehicle. In this attack, the attacker gains illegal access to the vehicle's ECU, which is in charge of managing vital systems like the engine, gearbox, and brakes, and alters the programming to make the car act in an unpredictable or hazardous manner.

For instance, a hacker may modify the ECU to disable vital safety measures like brakes or airbags, which could result in a serious accident. Strong access restrictions and authentication procedures must be implemented to stop unauthorized access to the car's systems and stop ECU reprogramming assaults. Further preventing data and communications from the car from being intercepted or tampered with is the implementation of strong encryption and authentication systems. Regular security testing and audits can also aid in identifying and addressing potential flaws that might be used in an ECU reprogramming cyber attack [63, 64].

3.3.15. Side-Channel Attacks

A Side-channel cyber attack is a sort of cyberattack that might be employed against autonomous cars. In this attack, the attacker takes advantage of flaws in the hardware or software of the target vehicle to obtain unauthorized access to its systems or data.

In order to obtain sensitive information, such as passwords or cryptographic keys, the attacker frequently employs sophisticated algorithms to analyze the signals and power usage of the vehicle's components. The key used to encrypt the wireless communications of the vehicle, for instance, could be extracted by an attacker through a side-channel assault, enabling them to intercept and control these conversations. Utilizing strong encryption and authentication techniques resistant to side-channel attacks is crucial to preventing side-channel assaults. The use of physical security measures, such as tamper-proof hardware and secure boot procedures, can also aid in preventing attackers from physically accessing the vehicle's systems or components. Regular security audits and testing can also assist in finding and fixing any vulnerabilities before they are used against you [65, 66].

3.4. AI-Based Cyber Solutions for AVs

AI is becoming a growing important cybersecurity solution for AVs. These vehicles are becoming more linked and dependent on technology, which increases their susceptibility to cyber threats, including hacking, malware, and ransomware assaults. AI can assist in addressing these dangers by offering cutting-edge threat detection and mitigation capabilities. To do this, ML algorithms must scan vast amounts of data from numerous sources, including sensors, cameras, and network traffic, in order to spot possible dangers as they emerge. AI can also learn from previous security problems and spot new attack patterns, improving the effectiveness of security teams' responses. AI can also be utilized to improve user education initiatives and raise overall security awareness among motorists.

3.4.1. Intrusion Detection Systems

Intrusion Detection Systems (IDS) are an essential part of cybersecurity solutions for AVs that use AI. IDS monitor the vehicle's network and looks for any attempts at unauthorized entry or harmful behavior using ML methods. This assists in identifying potential cyber threats before they harm the car or its occupants. Using AI in IDS enables them to learn and adjust to new threats as they appear, ensuring that the vehicle's cybersecurity is always current and efficient. IDS can assist in preventing significant security breaches and ensuring that AVs are kept safe and secure by detecting and responding to intrusions in real-time [67-69].

3.4.2. Threat Intelligence

Threat intelligence is yet another significant AI cybersecurity solution for AVs. AI can find potential dangers and system vulnerabilities by evaluating data from various sources, including social media, the dark web, and other threat intelligence feeds. This makes it possible for security teams to take proactive steps to stop cyberattacks before they happen. Threat information can also be used to spot patterns and trends in cybercrime, which will help with better preparing for and responding to new threats. AVs can benefit from real-time threat intelligence with the aid of AI, adding an extra layer of security against potential cyberthreats [70, 71].

3.4.3. Behavioral Analysis

Behavioral analysis is an effective AI cybersecurity solution for self-driving cars. AI can identify any unusual behaviour that would point to a hack by tracking how the vehicle's systems behave. This includes unusual system activity, network traffic anomalies, and other signs of compromise. AI can quickly recognize potential cyber risks by analyzing this data in real-time and notifying security professionals so they can respond appropriately. Security teams can better respond to emerging threats using behavioral analysis to spot previously undiscovered attack behaviors. The defense against various cyber threats for AVs can be improved by integrating behavioral analysis with existing AI cybersecurity solutions [72].

3.4.4. Anomaly Detection

Anomaly detection is another essential AI cybersecurity solution for AVs. AI is used in anomaly detection to find out-of-the-ordinary patterns or departures from norms in data produced by the vehicle's systems. Anomalies in network traffic, system logs, and other data sources can be examples.

AI can alert security personnel to impending cyberattacks and aid in the prevention of significant security breaches by spotting these irregularities. Security teams can respond to emerging attacks more successfully by using anomaly detection to spot previously unidentified attack patterns. AVs can gain from improved security against various cyber attacks by utilizing AI to monitor aberrant activity constantly [73-75].

3.4.5. Secure Communication

Secure communication is an essential AI cybersecurity solution for AVs. The communication between the car and other systems must be secured and safe, given the growing amount of data collected by these vehicles. AI can assist in accomplishing this by putting in place secure communication protocols and making sure that data is delivered and received securely.

This involves encryption techniques to prevent data from being intercepted and other types of cyberattacks. A significant security breach can be avoided by using AI to monitor communication channels for any indications of illegal access or data manipulation. When communicating securely, AVs can function with the assurance that their data is secure and shielded from potential cyber threats [76, 77].

3.4.6. Authentication And Access Control

Authentication and access control are fundamental AI cybersecurity solutions for AVs. AI can aid in preventing unwanted access to the systems and data of the vehicle by introducing multi-factor authentication and access control methods. Ensuring that only authorized people can access the vehicle's functions and data involves implementing biometric authentication, such as facial recognition or fingerprint scanning. Additionally, AI can watch over login attempts and notify security professionals of any unusual behaviour, assisting in preventing future cyberattacks. AVs can put in place strong authentication and access control controls with the aid of AI, guaranteeing that only authorized users have access to the vehicle's systems and data and assisting in preventing significant security breaches [78, 79].

3.4.7. Predictive Maintenance

Predictive maintenance is an additional crucial AI cybersecurity solution for AVs. Potential problems or malfunctions can be identified before they happen by utilizing AI to monitor the vehicle's systems and parts. Thus, significant safety or security breaches can be avoided by maintenance staff taking early steps to rectify any flaws.

As a result, maintenance staff can make data-driven decisions that enhance the vehicle's performance. AI can also evaluate data from the vehicle's sensors and other systems to discover potential areas for optimization or improvement. With predictive maintenance, AVs may run confidently because potential flaws are found and fixed before they have a chance to cause significant difficulties [80, 81].

3.4.8. Incident Response

Incident response is an essential AI cybersecurity solution for self-driving cars. In the case of a cyberattack, AI can support quick detection and response, reducing the impact on the vehicle's systems and occupants. This involves utilizing ML algorithms to categorize the attack type and the degree of damage, enabling security teams to react more quickly. Additionally, AI may automate incident response procedures like contacting emergency services or shutting down impacted systems, which can speed up reaction times and help avoid catastrophic security breaches. AVs that use AI may implement efficient incident response processes, ensuring that possible cyber risks are found and dealt with right away [82].

3.4.9. Data Protection

Data protection is an essential AI cybersecurity solution for self-driving cars. It is crucial to guarantee that data is protected from potential cyber threats, given the vast amounts of sensitive data created by these cars, including location data, biometric data, and other personal information.

Data encryption and other data protection techniques can be used by AI to safeguard the data produced by the vehicle's systems, which can aid in achieving this goal. Additionally, AI can keep track of how data is accessed and used, warning security staff of any questionable activity and assisting in preventing data breaches. AVs use of AI can ensure that private information is safeguarded and secure, lowering the possibility of significant security lapses and safeguarding passengers' safety and privacy [83].

3.4.10. Threat Modeling

Threat modeling is an essential AI cybersecurity solution for AVs. In order for security teams to develop efficient mitigation measures, this entails detecting and assessing potential cyber threats and vulnerabilities. In order to find potential attack vectors and vulnerabilities, AI can assist in achieving this by evaluating data from the vehicle's systems and sensors.

AI can help security teams respond more effectively by employing ML algorithms to detect possible cyber attacks and discover new attack patterns. Robust threat modeling tactics can be implemented by AVs using AI, guaranteeing that any possible vulnerabilities are found and fixed before being used by cyber attackers. This lessens the possibility of significant security lapses and safeguards passenger privacy and safety [84, 85].

3.4.11. Secure Software Development

Secure software development is an important AI cybersecurity solution for self-driving cars. This entails putting security measures in place throughout the entire software development lifecycle, from design to deployment. This can be accomplished with the help of AI, which can analyze code and spot potential security flaws or vulnerabilities, enabling developers to fix them before cybercriminals can take advantage of them.

As a result of AI's ability to use ML algorithms, developers of future software releases will be able to add more robust security features by learning from previous security incidents and spotting new attack patterns. AVs can use AI to implement secure software development practices, ensuring that vehicle systems are safeguarded from potential cyber threats and that passengers are safe and secure [86].

3.4.12. Patch Management

Patch management is yet another essential AI cybersecurity approach for AVs. It is crucial to ensure the vehicle's systems are up-to-date and secured from potential vulnerabilities, given the frequent release of software updates and security patches. This can be done with the aid of AI, which can automate the patch management procedure and ensure that all systems and components are updated as soon as new patches are released.

As a result, there is a lower possibility of cyberattacks, and the overall performance and dependability of the vehicle are maintained. AI can also analyze data from earlier patches to find potential issues using ML algorithms, allowing maintenance teams to address any problems before they arise. Implementing efficient patch management methods by AVs with AI will keep their systems current and secure from future cyber threats [87, 88].

3.4.13. Network Segmentation

Network segmentation is another significant AI-based cybersecurity solution for driverless vehicles. In order to lower the possibility of potential cyber threats spreading throughout the entire network, this entails segmenting the vehicle's network into smaller, more secure sections.

By examining network traffic and spotting potential vulnerabilities, AI can assist in achieving this goal and allow security teams to create efficient network segmentation solutions. AI can also learn from prior network attacks and spot new attack patterns by utilizing ML algorithms, which enables security teams to react more quickly. AVs can apply effective network segmentation protocols with the aid of AI, ensuring that possible cyberthreats are controlled and handled before they can seriously harm the vehicle's systems or its occupants. This keeps the car's general functionality and dependability high while simultaneously ensuring the security and privacy of its occupants [89].

Table 1. AVs cyber-attacks and their possible related AI-based cybersecurity solutions

Most dangerous attacks in critical AVs components	AI-based Solutions	Type	Description
Remote control hijacking	Intrusion Detection Systems, Secure communication	Prevention	IDS can detect anomalous activity, and secure communication ensures that remote control of the vehicle cannot be established.
Sensor spoofing	Behavioral analysis, Anomaly detection, Threat modeling	Prevention Detection	Threat modeling proactively identifies weaknesses that can be exploited through sensor spoofing, while behavioral analysis and anomaly detection can spot strange patterns of behavior.
Denial of Service attacks	Intrusion Detection Systems, Network segmentation	Prevention Detection	Network segmentation can isolate the attack and stop it from spreading, while IDS can identify traffic spikes that may be suggestive of a DoS attack.
Malware injection	Secure software development, Data protection, Patch management	Prevention Detection	Data protection can shield data in the event that malware can infiltrate the system, while secure software development can reduce vulnerabilities that can be exploited by malware injection. Patch management can guarantee that any identified vulnerabilities are immediately fixed.
Physical attacks	Secure hardware design, Incident response	Prevention Detection Response	Incident response can recognize and react to physical attacks; secure hardware design can prevent physical tampering.
GPS jamming	Secure communication	Prevention	Secure communication can ensure that location data is not spoofed or tampered with due to GPS jamming attacks.
Phishing attacks	Authentication and access control, User education	Prevention	Users can learn to recognize and avoid phishing efforts through user education, while authentication and access control can stop unwanted access caused by phishing assaults.
Ransomware	Incident response, Secure software development, Data protection	Detection/ Response	Secure software development and data protection can lessen the effects of an attack and safeguard against data loss, and incident response can detect and respond to ransomware attacks.
Man-in-the-middle attacks	Secure communication, Authentication and access control	Prevention	Secure communication can ensure that data is delivered securely and that no data is intercepted, while authentication and access control can guarantee that data is only accessible to those who are permitted.
Social engineering	User education	Prevention	User education can teach users how to recognize and avoid social engineering techniques that aim to trick them into disclosing sensitive information.
Wireless network attacks	Secure communication, Threat intelligence	Prevention Detection	Threat intelligence can identify possible wireless network assaults and proactively fix weaknesses, while secure communication can guarantee that wireless network data is transmitted safely.
Brute force attacks	Authentication and access control, Threat modeling	Prevention	Access control and authentication can stop brute force assaults from gaining illegal access, while threat modeling can proactively find potential weaknesses that can be exploited.
Supply chain attacks	Incident response, Threat intelligence	Detection Response	Identifying potential supply chain vulnerabilities and incident response can detect and respond to supply chain threats.
ECU reprogramming	Secure software development, Incident response, Patch management	Prevention Detection Response	Incident response and patch management can detect and stop any such assaults, and secure software development can reduce vulnerabilities that can be used for ECU reprogramming.
Side-channel attacks	Secure hardware design	Prevention	Ensuring that hardware is created to limit unauthorized access to data and having a secure hardware design can stop side-channel attacks.

3.4.14. Secure Hardware Design

Secure hardware design is an important AI cybersecurity solution for AVs. Security measures must be put in place at the hardware level to safeguard the vehicle's systems from potential cyber threats. By assessing hardware design and spotting possible weaknesses, AI can assist in achieving this goal by allowing designers to correct these problems before the vehicle is produced. Future hardware releases will feature more effective security measures thanks to AI's ability to use ML algorithms to anticipate new attack trends and learn from previous security problems. AVs can use AI to apply secure hardware design standards, guaranteeing that passengers are safe and secure and that the vehicle's systems are secured from potential cyber threats. This safeguards the security and privacy of passengers while also maintaining the overall performance and dependability of the vehicle [90].

3.4.15. User Education

User education is an essential AI cybersecurity solution for AVs. This entails training users on safe and secure behaviors to lower the danger of potential cyber risks, such as drivers and passengers. AI can assist in achieving this by evaluating user behavior data and identifying possible risk areas, enabling educators to develop focused training programs that address these problems. ML algorithms allow AI to predict emerging security trends and learn from past user issues, allowing educators to create training programs with more effectiveness in the future. A complete user education program can be put in place by AVs with AI, ensuring that all users are aware of potential cyber threats and can respond accordingly. This helps to maintain the car's overall security posture and ensures the privacy and safety of its occupants [31].

3.5. AI-based Cybersecurity Solutions to Appropriate Type of Attacks

Table 1 presents an overview of the most serious attacks targeting essential components in AVs and suggests AI-based solutions for prevention, detection, and reaction. The table's goal is to raise awareness about potential vulnerabilities and provide suggestions for mitigating these risks. Each attack is described, and the associated AI-based solutions are offered to combat the specific threat.

AV developers and users may improve the security and integrity of these vehicles, protecting the safety of passengers and the general public by identifying the risks and applying appropriate countermeasures. Creating and implementing cybersecurity solutions for AVs based on AI presents several difficulties that need creative solutions and ongoing improvements. One of the biggest obstacles is the complexity of autonomous vehicle systems, which can make it difficult to create AI-based cybersecurity solutions that can effectively handle all potential risks. Furthermore, because cyber threats are ever-evolving, they need to be updated and modified frequently to counter new and emerging threats. Finally, integrating AI-based cybersecurity solutions with current infrastructure calls for coordination and cooperation across stakeholders, including automakers, government regulators, and cybersecurity professionals. These issues can be resolved by future research, which will also improve the efficiency of AI-based cybersecurity solutions for AVs. For instance, research might concentrate on creating intrusion detection systems that are more effective and can immediately identify and stop remote hacking attempts against AVs. Research can also concentrate on creating more powerful and efficient data encryption and privacy protection technologies to secure the security and privacy of the data gathered by AVs.

4. Conclusion

In conclusion, AI-based cybersecurity solutions may be able to handle the growing cybersecurity issues that AVs are currently facing. With the aid of AI, it is possible to identify and stop cyber-attacks on the car's systems in real-time, increasing the security and dependability of the vehicle. Using AI algorithms and ML models together can also aid in spotting possible weaknesses and creating preventative measures to counteract them. However, adopting AI-based cybersecurity measures for self-driving cars comes with its own set of difficulties, such as the requirement for stringent data protection laws and the potential for AI-based assaults. For the deployment of AVs on our roads to be safe and secure, further research and development in this area are required. Overall, AI-based cybersecurity solutions show significant promise for the development of autonomous cars, and further research into their ability to improve the security and safety of these vehicles is essential.

References

[1] Teodora Mecheva, and Nikolay Kakanakov, "Cybersecurity in Intelligent Transportation Systems," *Computers*, vol. 9, no. 4, pp. 1-12, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Prinkle Sharma, and James Gillanders, "Cybersecurity and Forensics in Connected Autonomous Vehicles: A Review of the State-of-the-Art," *IEEE Access*, vol. 10, pp. 108979-108996, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Mansi Girdhar, Junho Hong, and John Moore, "Cybersecurity of Autonomous Vehicles: A Systematic Literature Review of Adversarial Attacks and Defense Models," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 417-437, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Gueltoum Bendiab et al., "Autonomous Vehicles Security: Challenges and Solutions Using Blockchain and Artificial Intelligence," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 4, pp. 3614-3637, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Bhavesh Raju Mudhivarth, Prabhat Thakur, and Ghanshyam Singh, "Aspects of Cyber Security in Autonomous and Connected Vehicles," *Computers*, vol. 13, no. 5, pp. 1-20, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Shah Khalid Khan et al., "Cyber-Attacks in the Next-Generation Cars, Mitigation Techniques, Anticipated Readiness and Future Directions," *Accident Analysis & Prevention*, vol. 148, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] Tian Guan et al., "An Overview of Vehicular Cybersecurity for Intelligent Connected Vehicles," *Sustainability*, vol. 14, no. 9, pp. 1-17, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Zhendong Wang et al., "Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey," *Sustainability*, vol. 14, no. 19, pp. 1-29, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Mahdi Dibaei et al., "An Overview of Attacks and Defences on Intelligent Connected Vehicles," *arXiv*, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[10] McCarthy Charlie et al., "*Assessment of the Information Sharing and Analysis Center Model*," (Report No. DOT HS 812 076) Washington, DC: National Highway Traffic Safety Administration, 2014. [Google Scholar] [Publisher Link]

[11] Wilson Joe, H.R.701 - 115th Congress (2017-2018): SPY Car Study Act of 2017, 2019. [Online]. Available: https://www.congress.gov/bill/115th-congress/house-bill/701/all-info?s=1&r=84

[12] Sasan Jafarnejad et al., "A Car Hacking Experiment: When Connectivity Meets Vulnerability," *IEEE Globecom Workshops (GC Wkshps)*, San Diego, CA, USA, pp. 1-6, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[13] Subir Halder, Amrita Ghosal, and Mauro Conti, "Secure OTA Software Updates in Connected Vehicles: A Survey," *arXiv Preprint*, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[14] Mikhail Buinevich, and Andrei Vladyko, "Forecasting Issues of Wireless Communication Networks' Cyber Resilience for an Intelligent Transportation System: An Overview of Cyber Attacks," *Information*, vol. 10, no. 1, pp. 1-22, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[15] Muhammad Sameer Sheikh, Jun Liang, and Wensong Wang, "Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey," *Wireless Communications and Mobile Computing*, vol. 2020, pp. 1-25, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] Boris Svilicic et al., "A Study on Cyber Security Threats in a Shipboard Integrated Navigational System," *Journal of Marine Science and Engineering*, vol. 7, no. 10, pp. 1-11, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[17] A. Rustamov, K. Sharipov, and T. Pulatov, "Vulnerability Analysis of Emergency Response System Based on Navigational Units in Case of Vehicle Accidents," *Technical Science and Innovation*, vol. 2020, no. 2, pp. 14-18, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[18] Géza Dévényi, "Functional Safety of Road Vehicle Infotainment Systems," *Safety and Security Sciences Review*, vol. 2, no. 1, pp. 39-48, 2020. [Google Scholar] [Publisher Link]

[19] Emad Aliwa et al., "Cyberattacks and Countermeasures for In-Vehicle Networks," *ACM Computing Surveys*, vol. 54, no. 1, pp. 1-37, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] Narayan Khatri, Rakesh Shrestha, and Seung Yeob Nam, "Security Issues with In-Vehicle Networks, and Enhanced Countermeasures Based on Blockchain," *Electronics*, vol. 10, no. 8, pp. 1-33, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] Zeinab El-Rewini et al., "Cybersecurity Attacks in Vehicular Sensors," *IEEE Sensors Journal*, vol. 20, no. 22, pp. 13752-13767, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[22] L. Erhan et al., "Smart Anomaly Detection in Sensor Systems: A Multi-Perspective Review," *Information Fusion*, vol. 67, pp. 64-79, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[23] Kyounggon Kim et al., "Cybersecurity for Autonomous Vehicles: Review of Attacks and Defense," *Computers & Security*, vol. 103, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[24] Beniel Dennyson, and C. Jothikumar, "A Review on Controller Area Network and Electronic Control Unit in Automotive Environment," *Journal of Positive School Psychology*, vol. 6, no. 4, pp. 269-277, 2022. [Google Scholar] [Publisher Link]

[25] Hamza Khemissa, and Pascal Urien, "Centralized Architecture for ECU Security Management in Connected and Autonomous Vehicles," *13th International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, Korea, Republic of, pp. 1409-1414, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[26] Jianan Lyu, Zalay Abdul Aziz, and Nor Syazwani Binti Mat Salleh, "A Study of Trends on Human-Machine Interface Design in Modern Vehicles," *Scientific Programming*, vol. 2022, pp. 1-9, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[27] Kang Wang, "Human-Computer Interaction Design of Intelligent Vehicle-Mounted Products Based on the Internet of Things," *Mobile Information Systems*, vol. 2021, pp. 1-12, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[28] Muhammad Umar Javed et al., "Blockchain-Based Secure Data Storage for Distributed Vehicular Networks," *Applied Sciences*, vol. 10, no. 6, pp. 1-22, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[29] Shahid Mahmood et al., "A Model-Based Security Testing Approach for Automotive Over-The-Air Updates," *IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, Porto, Portugal, pp. 6-13, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[30] James Howden, Leandros Maglaras, and Mohamed Amine Ferrag, "The Security Aspects of Automotive Over-the-Air Updates," *International Journal of Cyber Warfare and Terrorism*, vol. 10, no. 2, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[31] Zouhair Elamrani Abou Elassad et al., "The Application of Machine Learning Techniques for Driving Behavior Analysis: A Conceptual Framework and A Systematic Literature Review," *Engineering Applications of Artificial Intelligence*, vol. 87, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[32] Road Vehicles — Cybersecurity Engineering, ISO/SAE 21434, 2021. [Online]. Available: https://www.iso.org/standard/70918.html

[33] Cybersecurity Guidebook for Cyber-Physical Vehicle Systems - J3061_201601, 2016. [Online]. Available: https://www.sae.org/standards/content/j3061_201601/

[34] Joint Task Force, "NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations," *Computer Security Resource Center*, 2017. [Google Scholar] [Publisher Link]

[35] UN Regulation No. 155 - Uniform Provisions Concerning the Approval of Vehicles with Regards to Cyber Security and Cyber Security Management System, 2021. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/a5081378-8079-11eb-9ac9-01aa75ed71a1

[36] International Electrotechnical Commission, Security for Industrial Automation and Control Systems – Part 4-2: Technical Security Requirements for IACS Components, IEC 62443-4-2, 2019. [Online]. Available: https://webstore.iec.ch/cart&d=Fri%20Dec%2015%202023%2015:45:47%20GMT+0530%20(India%20Standard%20Time)

[37] UL 4600: Standard for Safety for the Evaluation of Autonomous Products, 2020. [Online]. Available: https://users.ece.cmu.edu/~koopman/ul4600/index.html#:~:text=of%20Autonomous%20Products-,UL%204600%3A%20Standard%20for%20Safety%20for%20the%20Evaluation%20of%20Autonomous,second%20edition%20issued%20March%202022.

[38] Markus Zoppelt, and Ramin Tavakoli Kolagari, "UnCle SAM: Modeling Cloud Attacks with the Automotive Security Abstraction Model," *The Tenth International Conference on Cloud Computing, GRIDs, and Virtualization, Cloud Computing*, 2019. [Google Scholar] [Publisher Link]

[39] Sekar Kulandaivel et al., "Cannon: Reliable and Stealthy Remote Shutdown Attacks via Unaltered Automotive Microcontrollers," *IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, pp. 195-210, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[40] Rony Komissarov, and Avishai Wool, "Spoofing Attacks Against Vehicular FMCW Radar," *Proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security*, pp. 91-97, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[41] Rohith Reddy Vennam et al., "mmSpoof: Resilient Spoofing of Automotive Millimeter-wave Radars using Reflect Array," *IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, pp. 1807-1821, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[42] Nataša Trkulja, David Starobinski, and Randall A. Berry, "Denial-of-Service Attacks on C-V2X Networks," *arXiv*, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[43] Yulei Wang et al., "Resilient Path-Following Control of Autonomous Vehicles Subject to Intermittent Denial-of-Service Attacks," *IET Intelligent Transport Systems*, vol. 15, no. 12, pp. 1508-1521, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[44] Aiman Al-Sabaawi et al., "Addressing Malware Attacks on Connected and Autonomous Vehicles: Recent Techniques and Challenges," *Malware Analysis Using Artificial Intelligence and Deep Learning, Springer Link*, pp. 97–119, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[45] Sana Aurangzeb et al., "CyberSecurity for Autonomous Vehicles Against Malware Attacks in Smart-Cities," *Cluster Computing*, pp. 1-16, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[46] Zhi Sun et al., "Who is in Control? Practical Physical Layer Attack and Defense for mmWave based Sensing in Autonomous Vehicles," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3199-3214, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[47] Yulong Cao et al., "Invisible for both Camera and LiDAR: Security of Multi-Sensor Fusion based Perception in Autonomous Driving under Physical-World Attacks," *IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, pp. 176-194, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[48] Ali Krayani et al., "Integrated Sensing and Communication for Joint GPS Spoofing and Jamming Detection in Vehicular V2X Networks," *2023 IEEE Wireless Communications and Networking Conference (WCNC)*, Glasgow, United Kingdom, pp. 1-7, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[49] Mohsin Kamal et al., "GPS Location Spoofing Attack Detection for Enhancing the Security of Autonomous Vehicles," *IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*, Norman, OK, USA, pp. 1-7, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[50] Syed Ghazanfar Abbas et al., "Identifying and Mitigating Phishing Attack Threats in IoT Use Cases Using a Threat Modelling Approach," *Sensors*, vol. 21, no. 14, pp. 1-25, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[51] Pranshu Bajpai, Richard Enbody, and Betty H.C. Cheng, "Ransomware Targeting Automobiles," *Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security*, pp. 23-29, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[52] Manuela Horduna, Simona-Maria L˘az˘arescu, and Emil Simion, "A Note on Machine Learning Applied in Ransomware Detection," *Cryptology ePrint Archive*, 2023. [Google Scholar] [Publisher Link]

[53] Felix Klement, Henrich C. Pöhls, and Stefan Katzenbeisser, "Man-in-the-OBD: A Modular, Protocol Agnostic Firewall for Automotive Dongles to Enhance Privacy and Security," *International Workshop on Attacks and Defenses for Internet-of-Things*, pp. 143-164, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[54] Seong-Kyu Kim, and Eun-Sill Jang, "The Intelligent Blockchain for the Protection of Smart Automobile Hacking," *Journal of Multimedia Information System*, vol. 9, no. 1, pp. 33-42, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[55] András Gazdaga, Csongor Ferenczib, and Levente Buttyán, "Development of a Man-in-the-Middle Attack Device for the CAN Bus," *1st Conference on Information Technology and Data Science*, 2020. [Google Scholar] [Publisher Link]

[56] Matthias Bergler et al., "Social Engineering Exploits in Automotive Software Security: Modeling Human-targeted Attacks with SAM," *Proceedings of the 31st European Safety and Reliability Conference*, pp. 2502-2509, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[57] Joachim Draeger, "Safety, Security, and Social Engineering — Thoughts, Challenges and A Concept of Quantitative Risk Assessment," *Nova Science Publishers*, pp. 141-175, 2020. [Google Scholar]

[58] Mikhail Buinevich, and Andrei Vladyko, "Forecasting Issues of Wireless Communication Networks' Cyber Resilience for an Intelligent Transportation System: An Overview of Cyber Attacks," *Information*, vol. 10, no. 1, pp. 1-22, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[59] Liqun Yang et al., "Real-Time Intrusion Detection in Wireless Network: A Deep Learning-Based Intelligent Mechanism," *IEEE Access*, vol. 8, pp. 170128-170139, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[60] Stephen Kahara Wanjau, Geoffrey Mariga Wambugu, and Gabriel Ndung'u Kamau, "SSH-Brute Force Attack Detection Model based on Deep Learning," *International Journal of Computer Applications Technology and Research*, vol. 10, no. 1, pp. 42-50, 2021. [Google Scholar] [Publisher Link]

[61] Shipra Pandey et al., "Cyber Security Risks in Globalized Supply Chains: Conceptual Framework," *Journal of Global Operations and Strategic Sourcing*, vol. 13, no. 1, pp. 103-128, 2020.[CrossRef] [Google Scholar] [Publisher Link]

[62] Nikhil Gupta et al., "Additive Manufacturing Cyber-Physical System: Supply Chain Cybersecurity and Risks," *IEEE Access*, vol. 8, pp. 47322-47333, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[63] Azeem Hafeez et al., "Machine Learning based ECU Detection for Automotive Security," *17th International Computer Engineering Conference (ICENCO)*, Cairo, Egypt, pp. 73-81, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[64] John Heneghan et al., "Enabling Security Checking of Automotive ECUs with Formal CSP Models," *49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, Portland, OR, USA, pp. 90-97, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[65] Amit Garg, and Nima Karimia, "Leveraging Deep CNN and Transfer Learning for Side-Channel Attack," *22nd International Symposium on Quality Electronic Design (ISQED)*, Santa Clara, pp. 91-96, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[66] Anuj Dubey et al., "Guarding Machine Learning Hardware Against Physical Side-Channel Attacks," *ACM Journal on Emerging Technologies in Computing Systems*, vol. 18, no. 3, pp. 1-31, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[67] Sampath Rajapaksha et al., "AI-Based Intrusion Detection Systems for In-Vehicle Networks: A Survey," *ACM Computing Surveys*, vol. 55, no. 11, pp. 1-40, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[68] Md Delwar Hossain et al., "LSTM-Based Intrusion Detection System for In-Vehicle Can Bus Communications," *IEEE Access*, vol. 8, pp. 185489-185502, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[69] Pengzhou Cheng et al., "TCAN-IDS: Intrusion Detection System for Internet of Vehicle Using Temporal Convolutional Attention Network," *Symmetry*, vol. 14, no. 2, pp. 1-15, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[70] Jun Zhao et al., "TIMiner: Automatically Extracting and Analyzing Categorized Cyber Threat Intelligence from Social Data," *Computers & Security*, vol. 95, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[71] Thomas D. Wagner et al., "Cyber Threat Intelligence Sharing: Survey and Research Directions," *Computers & Security*, vol. 87, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[72] Yang Xing et al., "Toward Safe and Smart Mobility: Energy-Aware Deep Learning for Driving Behavior Analysis and Prediction of Connected Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4267-4280, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[73] Abdul Rehman Javed et al., "Anomaly Detection in Automated Vehicles Using Multistage Attention-based Convolutional Neural Network," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4291-4300, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[74] Yiyang Wang, Neda Masoud, and Anahita Khojandi, "Real-Time Sensor Anomaly Detection and Recovery in Connected Automated Vehicle Sensors," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 3, pp. 1411-1421, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[75] Aiguo Zhou, Zhenyu Li, and Yong Shen, "Anomaly Detection of CAN Bus Messages Using a Deep Neural Network for Autonomous Vehicles," *Applied Sciences*, vol. 9, no. 15, pp. 1-12, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[76] Elmustafa Sayed Ali et al., "Machine Learning Technologies for Secure Vehicular Communication in Internet of Vehicles: Recent Advances and Applications," *Security and Communication Networks*, vol. 2021, pp. 1-23, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[77] Ikram Ali et al., "An Efficient and Provably Secure ECC-Based Conditional Privacy-Preserving Authentication for Vehicle-to-Vehicle Communication in Vanets," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1278-1291, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[78] Chen Wang et al., "B-TSCA: Blockchain Assisted Trustworthiness Scalable Computation for V2I Authentication in Vanets," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 3, pp. 1386-1396, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[79] Aleksandr Ometov et al., "Challenges of Multi-Factor Authentication for Securing Advanced IoT (A-IoT) Applications," *IEEE Network*, vol. 33, no. 2, pp. 82-88, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[80] Andreas Theissler et al., "Predictive Maintenance Enabled by Machine Learning: Use Cases and Challenges in the Automotive Industry," *Reliability Engineering & System Safety*, vol. 215, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[81] Battula Bhavya et al., "Prediction of Vehicle Safety System Using Internet of Things," *Journal of Green Engineering (JGE)*, vol. 10, no. 4, pp. 1786-1798, 2020. [Google Scholar] [Publisher Link]

[82] Atif Ahmad et al., "How Integration of Cyber Security Management and Incident Response Enables Organizational Learning," *Journal of the Association for Information Science and Technology*, vol. 71, no. 8, pp. 939-953, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[83] Chia-Nan Wang et al., "Wireless Communications for Data Security: Efficiency Assessment of Cybersecurity Industry—A Promising Application for UAVs," *Drones*, vol. 6, no. 11, pp. 1-21, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[84] Wenjun Xiong et al., "Cyber Security Threat Modeling based on the MITRE Enterprise ATT&CK Matrix," *Software and Systems Modeling*, vol. 21, no. 1, pp. 157-177, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[85] Xiong Wenjun, and Robert Lagerström, "Threat Modeling – A Systematic Literature Review," *Computers & Security*, vol. 84, pp. 53-69, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[86] Nijat Rajabli et al., "Software Verification and Validation of Safe Autonomous Cars: A Systematic Literature Review," *IEEE Access*, vol. 9, pp. 4797-4819, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[87] Imanol Mugarza, Jose Luis Flores, and Jose Luis Montero, "Security Issues and Software Updates Management in the Industrial Internet of Things (IIoT) Era," *Sensors*, vol. 20, no. 24, pp. 1-22, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[88] Jaewan Seo, Jiwon Kwak, and Seungjoo Kim, "Formally Verified Software Update Management System in Automotive," *Symposium on Vehicles Security and Privacy*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[89] Ryan Elder, Courtney Westrick, and Peter Moldenhauer, "Cyberattack Detection and Bus Segmentation in Ground Vehicles," *Proceedings of the Ground Vehicle Systems Engineering and Technology Symposium*, 2020. [Google Scholar] [Publisher Link]

[90] Carson Labrado, and Himanshu Thapliyal, "Hardware Security Primitives for Vehicles," *IEEE Consumer Electronics Magazine*, vol. 8, no. 6, pp. 99-103, 2019. [CrossRef] [Google Scholar] [Publisher Link]