International Journal of Smart Sensor and Adhoc Network

Volume 3
Issue 4 *Role of Emerging & Intelligent Technologies for the Society.*
Article 7

January 2023

# Effect of Cyber Vulnerabilities on the Adoption of Self-Driving Vehicles – A Review

Vidhi Shah
*University Of the Cumberlands*, shahvidhi90210@gmail.com

# Effect of Cyber Vulnerabilities on the Adoption of Self-Driving Vehicles – A Review

[1]Vidhi Shah, [2]Azad Ali

[1]University of the Cumberlands, KY USA

[2]Indiana University of Pennsylvania, PA USA

[1]shahvidhi90210@gmail.com

***Abstract***—One of the leading disruptive technologies in the upcoming technological revolution is Self-Driving vehicles. However, the absence of security is the greatest obstacle to adoption. This study looks at how cyber security impacts the adoption of driverless cars. The purpose of this paper is to perform a literature review supporting the in-depth analysis of cyber security and its impacts on the slower adoption rate of Self-Driving Vehicles. The study's primary goal is to determine the connection between worries about cyber security and the rate of adoption of self-driving vehicles. Driverless vehicles are the most effective and cutting-edge technology in the transportation sector, yet there are barriers to their widespread adoption because of cyber security worries. As a result, this study will clarify the cyber security issues that contributed to the slower deployment of autonomous vehicles. The NIST Cyber security Framework serves as the study's theoretical foundation. This paradigm consistently identifies the barriers to new technology adoption in cyber security.

***Keywords***—Critical infrastructure, Cyber security Framework, Self-Driving Vehicles, Autonomous Vehicles, AV Vulnerabilities, Driverless Cars, NIST, Technology Adoption

## I. INTRODUCTION

In this modern era, self-driving cars will revolutionize how we travel[1].Autonomous Vehicles (AV) technology offers us the prospect of reducing accidents and traffic bottlenecks while enhancing mobility. For many people who don't drive, it opens a new mode of mobility. The automotive sector has transformed thanks to this technology. All the big automakers are competing to be the first to introduce their fleet of self-driving cars. Even if the technology seems promising, it also presents specific unique difficulties. Unexpected human-robot interaction, surround detection, and cyber security are a few of our biggest problems. Additional research is needed in several of these areas. Human intervention is one of the areas where research is most lacking.

This article is focused on performing a literature review on how cyber security concerns contribute to adopting Self-Driving Vehicles. The very first section describes the theoretical Framework that governs cyber security technology adoption. The article deep dives into types of attacks previously encountered in Self Driving vehicles. This gives a clear understanding of the vulnerabilities associated with Self Driving Vehicles (SDV) and reluctance for its complete adoption. The study continues to explore the factors influencing Attack feasibility. The article then further elaborates on the Limitation of AV and potential research gaps. This also highlights the scope for future studies and avenues that have not yet been explored. This article concludes with a note of how cyber security concerns significantly contribute to the slower adoption rate of Self Driving Vehicles.

The effect of cyber security on self-driving cars is one of the new study trends. The human aspect must be thoroughly investigated because it is the most frequent cause of a successful cyber-attack, according to [2].The likelihood of an assault can be decreased, significantly improving. In 2015, a hack of the MMI system of a Jeep car caused a cyber attack. For researchers navigating their cyber security studies, this was enlightening.

For the sustainable development of smart cities, the article [3] authors have identified privacy and cyber security threats of self-driving cars. In their research, they highlight the measures taken by the government to reduce these risks and significantly contribute to forming Regulatory Compliances in the future.

There is a sizeable significant gap in transportation laws regarding new AV technologies. There is a considerable knowledge gap regarding routing behaviors, and connected vehicle technology (CAV) offers a potential chance for an effective traffic routing system,

claim Bagliee et al. [4].Studies in this field may result in revolutionary changes to the policies. The article's authors [5] examine several technological concerns related to self-driving cars and suggest how the government might create regulations to reduce those risks. The report also emphasizes how the US has initiated to development of legislation that can handle such technical dangers related to cyber security and privacy. The National Highway Traffic Safety Administration (NHTSA) released two documents this fall outlining its proposed guidance regarding the regulation of two interrelated developments in motor vehicle design and operation - self-driving vehicle technologies and concerns about the cyber security of vehicles.

One of the main worries and a significant barrier to deploying self-driving cars is cyber attacks. Numerous instances, such as GPS spoofing assaults, put the safety of vehicles in jeopardy, and the CARAMEL project suggests an architecture that can lessen the risk of spoofing. The H2020-CARAMEL project's primary objective is to close cyber security vulnerabilities caused by the new technical spheres used by modern cars using, among other things, cutting-edge AI and machine learning approaches [6].In their article, Ansari et al. [7] make the case that one of the main priorities for a broader market acceptance of AV should be minimizing cyber dangers and taking prevention. As a result, he presents a framework that can do just that. Authors contend that if manufacturers are held responsible for third-party software security, cyber security threats may be somewhat diminished.

Connected and self-driving vehicles (CAV) are most susceptible to data exploitation and cyber-attacks, according to [8].They claim that inter-institutional conversations with experts can be constructive in addressing these cyber security issues. In their article, they looked at various concerns related to the use of self-driving cars. Given that the majority of a self-driving vehicle's components are networked and that their principal means of communication make them particularly vulnerable to cyber attacks, a thorough understanding of the possibilities for cyber trespassing is necessary. This paper examines how criminological theory, precisely a viewpoint on everyday actions, may be used to mitigate these technical dangers [9].

A literature survey in the domain related explicitly to V2V and V2I architectures and their effects from a security perspective can also be assessed. We also examine a few cyber-attempts against self-driving cars to determine their target areas and the subsequent mitigation measures. The study will also discuss any prospective cloud-based safety promotion ideas and solutions. Additionally, the suggestion would be to set up a productive Incident Response team that only works during a cyberattack on AV. It is possible to investigate their roles and responsibilities. A literature analysis must be conducted to examine the military potential because one of the paper's primary sections will emphasize the future of AV. The security aspect of antivirus software will continue to be the focus of the literature review, along with how digital forensics can contribute.

## II. NIST CYBERSECURITY FRAMEWORK

It takes a sophisticated process to safeguard firms from cyber-attacks and ensure they follow regulations and standards. The NIST cyber security framework offers a platform for laying the groundwork for autonomous vehicles in this aspect. This article has tried to define the common fundamental Framework as advice for identifying cyber security components and making autonomous vehicles compliant. Numerous standards and specifications were examined during the literature research. The analysis demonstrated that the NIST cyber security framework was the most pertinent in autonomous cars.CIS CSC, COBIT, ISA, and other sources supported some of the standards.

Many authors have illustrated the connections between several frameworks and how NIST developed the critical components from various frameworks and mapped them together.(Jay et al.,2019).Without a solid structure, it is almost impossible to implement a cybersecurity plan [10, 11].Adherence to a framework is essential for achieving operational compliance, according to numerous firms across numerous industries.

The Biological Sciences Division (BSD) Success Story from the University of Chicago illustrates how business has used the Framework Cybersecurity Framework to help with program organization and alignment across numerous BSD departments. The details of the NIST framework are highlighted in the figure below (see Fig 1).

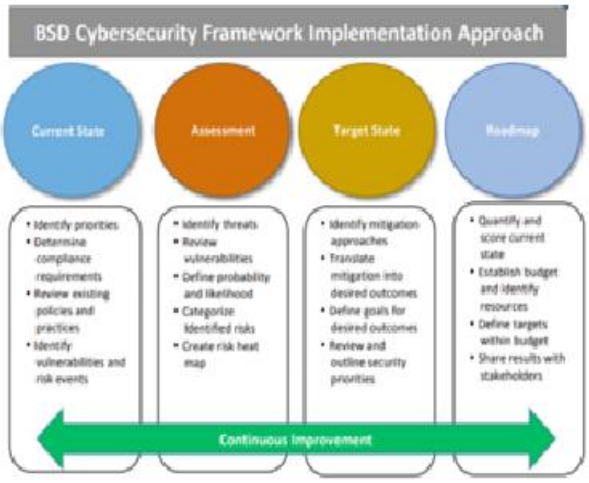


**Fig 1.** Uses and Benefits of NIST Cybersecurity Framework.(Shen, L. 2014).[12]

## III. TYPES OF ATTACK

### A. *Jamming Attack*

In this kind of attack, the attackers will jam the sensors within a distance range within a frequency range of 76-77 GHz [13].The results of a jamming attack are very prominent and can affect the vehicle and driver badly. This approach can hinder autonomous vehicle communication systems from hearing intended signals clearly, or perhaps altogether in some situations. The vulnerability of autonomous cars to jammer assaults stems primarily from their dependence on the inherently open wireless network for communication. Jamming can prevent an autonomous vehicle from receiving GPS or GNSS signals. Attackers can utilize jammer assaults to interrupt the short- and long-range wireless transmission of autonomous cars. Attackers can also use signal generators to blind autonomous vehicle radar systems by jamming the RF signals that their radar emitters broadcast and receive. These blocking attacks disable the vehicles' capacity to communicate via cellular networks by prohibiting them from producing or receiving wireless signals from outside the facility.


**Fig 2**.Autopilot with Jamming behavior [13]

### B. *Blinding Attack*

Poltergeist or blind attack is an assault against camera-based computer-vision systems, such as those used in autonomous vehicles, that uses noise to trigger the image stabilization features of the camera sensor and blur the picture, fooling the machine learning system into disregarding objects in its path [13].It attacks the vehicle's vision and central camera processing unit and does the maximum damage to the main operating unit.

### C. *Spoofing Attack*

Spoofing attacks entail sending fake data to sensors, cameras, and receivers.
Spoofing attacks on autonomous vehicle communication systems entail delivering fake messages, warnings, or signals to the receiving cars to change their paths or behavior, and attackers may spoof autonomous vehicles with relative simplicity and at a minimal cost. Attackers can use low-power lasers and pulse generators to fool autonomous vehicle cameras and Lidar systems into slowing down, altering direction, or remaining stationary to avoid hitting nonexistent objects.

Attackers can also use Arduinos, open-source electronics platforms that can accept sensor input and operate lights, motors, and other actuators, to spoof autonomous cars. Using Arduinos and ultrasonic transducers, attackers may trick ultrasonic driving and parking sensors into "seeing" nonexistent things. Advances in software-defined radio tool technology allow inexperienced criminals to build powerful GPS and GNSS spoofing devices, and even the most effective known spoofing countermeasures are not perfect [14].

### D. *Relay Attack*

Relay attack uses a flaw in passive keyless entry systems, which allow drivers to access and start their vehicles without having to remove the keyless fob from their pocket. In pairs, one criminal holds a gadget against the automobile door, increasing the signal it radiates across the vehicle's perimeter [15].Another man waits near a house's front wall or porch, holding a gadget that transfers the key's signal to his accomplice.

The automobile is essentially duped into believing that the owner is within a specific range (often two meters) and approaching the vehicle with their key [13].The door opens, and the signal is repeated, causing the engine to start. The machine will not restart if the key is not present. Keyless entry fobs are not the same as usual remote fobs. If you have to press a button on the fob to obtain entrance, your automobile does not have a keyless system and is not prone to relay theft.

## IV. ATTACK FEASIBILITY

Here we will study the feasibility of different attacks, knowledge threshold, and detection by driver and system.

### A. *Influential Factors*

After all, numerous factors influence attack success, including distance, angle, weather, surroundings, equipment performance, and sensor design. We will solely talk about distance and angle [13].Distance and angle are critical influencing elements for this sort of assault.

**Distance** - Due to air attenuation and the high jamming noise amplitude necessary in ultrasonic assaults, jamming is generally maintained within 1 meter. Spoofing is possible within a few meters.

**Angle** - The best performance in ultrasonic assaults is obtained at a perpendicular. This is simple to grasp since sound is a longitudinal wave that will transfer most of its energy forward. But only up to 75 meters.

### B. *Knowledge Threshold*

To attack a vehicle sensor, a specific level of understanding is required, including the system model, functioning principle, necessary physics, and the ability to build or run hardware equipment. Because attack tactics for one type of sensor cannot be utilized when dealing with another, learning and studying must be restarted, which may be time-consuming [14].Ultrasonics is the easiest of the three sensors we investigated, while radar is the most difficult (see Fig 3).

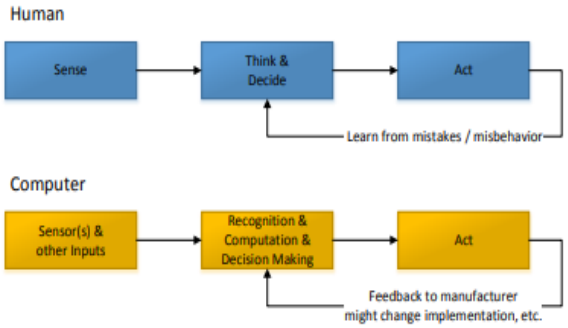


**Fig 3**.Knowledge threshold - human vs. Computer

### C. *Hardware cost*

An Arduino and a transducer for ultrasonic sensors cost $23, and it's considerably cheaper if you create your own. A few dollars worth of laser pointers may permanently destroy the camera, whether it is turned on or off. However, there are no off-the-shelf tools for MMW Radar. General equipment, such as the ones we used, is more expensive than the Tesla Model S [13].

### D. *Detection by System*

The system generates no "malicious attack" or "system failure" alarms for any of the assaults outlined in this research. The system either shows the faked distance, no detection, or no display during ultrasonic assaults.[15] In the presence of ultrasonic noise, "the system responds as a rule by notifying a problem to the driver or a pseudo-obstacle at a distance shorter than possibly genuine impediments." Remember that in a jamming assault, the distance is fudged to the maximum (which implies no detection), and no warning is issued [16].The identified object vanishes during a radar assault, but no alert of radar system malfunction of any type is given, and the Autopilot mode is not disabled.

### *E. Detection by Driver*

Due to the imperceptibility of ultrasound and MMW radio, the driver is unlikely to detect an ultrasonic or radar attack. Unless the damage is done in advance, a laser strike on a camera is highly likely to be noticed [13, 16].
Because the driver may grow suspicious of the device, it is vital to properly conceal or diminish the size of the equipment [17].

## V. LIMITATIONS AND FUTURE WORK

Furthermore, for most attacks, we could only observe the findings from the car display rather than from the sensors themselves, so we were unsure if the problems were from the sensors or the ECUs [18].We intend to evaluate the autonomous driving system further and monitor all states to understand system security better.

To avoid attacks, businesses must broaden the attack range by producing better-performing equipment and using the ultrasonic cancellation system [19].Due to the test yard's limitations, we could not evaluate the attack performance of MMW Radar at various distances and angles [20].We intend to do more tests in an open area and when the Tesla is driving. For cameras, we aim to conduct more studies on the viability of spoofing attacks.

Several publications are centered on safeguarding autonomous vehicles, and many of these articles mention protecting communications over VANETs. Depending on the kind of communication being used, VANETs make use of a variety of different communication protocols. Mishra et al. [21] present the most prominent communication technologies in VANET, such as IEEE 802.16, also known as WiMAX, which provides a communication range of 30 miles, and 802.11p, which is utilized for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) operating at a 5.9 GHz, a frequency licensed by Intelligent-Transport-Systems. Both of these technologies deliver communication (ITS).Authentication, dependability, integrity, anonymity, availability, delay handling, and confidentiality are some of the features that a security system should be able to provide for its users before it can be considered adequate.

Researchers are faced with a variety of security difficulties as a result of the deployment of VANETs. These challenges can be broken down into two categories: socio-economic and technical. Mishra et al. [21], Vaibhav et al. [22], and Hasrouny et al. [23] have all covered a number of these difficulties in their studies. Hartenstein and Laberteaux [25], two authors who examine such problems, state that the primary concerns regarding data authenticity are that incorrect information can be sent to vehicles, data transmitted through road infrastructure can be manipulated, and vehicles can be impersonated. By disregarding or mistrusting certain users' knowledge, trustworthy networks can help mitigate the problem [24, 25].

## VI. CONCLUSIONS

The robotics and automobile industries have evolved to become essential parts of people's lives. Using AI cyber prevention, self-driving cars have also helped to minimize the number of accidents. Like any other computer hardware, this robotics may be subject to various attacks. Our paper prioritizes security and anti tampering in AVs. We investigated numerous cyber hazards to human life, such as self-driving cars and driver robots. We reviewed the flaws and potential improvements to robotics.

This research proves that security is a significant concern for the safety of autonomous cars. Three types of sensors are explored and evaluated used in Automated Driving Systems and deployed with Autopilot. Jamming and spoofing attacks have been conducted against these sensors indoors and outdoors, causing a malfunction in the automotive system, potentially leading to collisions and compromising the safety of self-driving cars.

## REFERENCES

[1] Hamers, L. (2016).The Future of Cars.Science News, 190(13), 34–35.
[2] Linkov, V., Zámečník, P., Havlíčková, D., & Pai, C.-W. (2019). Human Factors in the Cybersecurity of Self-Driving Vehicles: Trends in Current Research. Frontiers in

Psychology, 10. https://doi.org/10.3389/fpsyg.2019.00995

[3] Lim, H. S. M., &Taeihagh, A. (2018). Self-Driving Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications.Energies (19961073), 11(5), 1062.https://doi.org/10.3390/en11051062

[4] Baglee, D., Knowles, M., Kinnunen, S. K., &Galar, D. (2016).A proposed maintenance strategy for a wind turbine gearbox using condition monitoring techniques. *International Journal of Process Management and Benchmarking*, *6*(3), 386-403.

[5] Taeihagh, A., & Lim, H. S. M. (2018). Governing Self-Driving vehicles: Emerging Responses for safety, liability, privacy, cybersecurity, and Industry Risks.Transport Reviews, 39(1), 103–128.https://doi.org/10.1080/01441647.2018.1494640

[6] Vitale, C., Piperigkos, N., Laoudias, C., Ellinas, G., Casademont, J., Escrig, J., Kloukiniotis, A., Lalos, A. S., Moustakas, K., Diaz Rodriguez, R., Baños, D., RoquetaCrusats, G., Kapsalas, P., Hofmann, K.-P., &Khodashenas, P. S. (2021). CARAMEL: results in a secure architecture for connected and Self-Driving vehicles detecting GPS spoofing attacks.EURASIP Journal on Wireless Communications & Networking, 2021(1), 1–28.https://doi.org/10.1186/s13638-021-01971-x

[7] Ansari, M. F., Sharma, P. K., & Dash, B. (2022).Prevention of phishing attacks using AI-based Cybersecurity Awareness Training.International Journal of Smart Sensor and Adhoc Network., 61–72.https://doi.org/10.47893/ijssan.2022.1221

[8] Liu, N., Nikitas, A., & Parkinson, S. (2020). Exploring expert perceptions about the cyber security and privacy of Connected and Self-Driving Vehicles: A thematic analysis approach.Transportation Research: Part F, 75, 66–86.https://doi.org/10.1016/j.trf.2020.09.019

[9] Dash, B., & Ansari, M. F. (2022).An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy.

[10] Maloney, T. (2016, February).Self-Driving vehicles by 2030?Not so fast [Review of Self-Driving cars by 2030?Not so quickly].The Globe and Mail.

[11] He, Q., Meng, X., & Qu, R. (2020). Towards a Severity Assessment Method for Potential Cyber Attacks to Connected and Self-Driving Vehicles.Journal of Advanced Transportation, 1–15.https://doi.org/10.1155/2020/6873273

[12] Shen, L. (2014).The NIST cybersecurity framework: Overview and potential impacts. *Sci-Tech Lawyer*, *10*(4), 16.

[13] Yan, C., Xu, W., & Liu, J. (2016). Can you trust autonomous vehicles: Contactless attacks against self-driving vehicle sensors. *Def Con*, *24*(8), 109.

[14]Holstein, T., Dodig-Crnkovic, G., &Pelliccione, P. (2018).Ethical and social aspects of self-driving cars. arXiv preprint arXiv:1802.04103.

[15] Pisarov, J. L., &Mester, G. (2022). Self-Driving Robotic Cars: Cyber Security Developments.In *Research Anthology on Cross-Disciplinary Designs and Applications of Automation* (pp. 969-1001).IGI Global.

[16] Gutierrez, S. (2021, May 25). The relay attack: Guidance for concerned car owners.Thatcham.Retrieved October 5, 2022, from https://www.thatcham.org/relay-attack/

[17] M. Noll and P. Rapps. Ultraschallsensorik. In HandbuchFahrerassistenzsysteme, pages 110–122. Springer, 2012.

[18] Dash, B., Ansari, M. F., Sharma, P., & Ali, A. (2022).Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review.International Journal of Software Engineering & Applications, 13(5), 13–21.https://doi.org/10.5121/ijsea.2022.13502

[19] C. Valasek and C. Miller. Adventures in Automotive Networks and Control Units.Technical White Paper, page 99, 2013.

[20] H. Winner.Automotive radar.In Handbook of Driver Assistance Systems: Basic Information, Components, and Systems for Active Safety and Comfort pages 325–403.Springer, 2016.

[21] Mishra, R., Singh, A., & Kumar, R. (2016, March).VANET security: Issues, challenges, and solutions.In 2016 international conference on electrical, electronics, and optimization techniques (ICEEOT) (pp. 1050-1055).IEEE.

[22] Vaibhav, A., Shukla, D., Das, S., Sahana, S., & Johri, P. (2017). Security challenges, authentication, application, and trust models for vehicular ad hoc network-a survey.IJ Wireless and Microwave Technologies, 3, 36-48.

[23] Hasrouny, H., Samhat, A. E., Bassil, C., &Laouiti, A. (2017). VANet security challenges and solutions: A survey.Vehicular Communications, 7, 7-20.

[24] Sharma, P., Dash, B., & Ansari, M. F. (2022). Anti-phishing techniques–a review of Cyber DefenseMechanisms.https://doi.org/10.17148/IJARCCE.2022.11728

[25]Hartenstein, H., &Laberteaux, L. P. (2008). A tutorial survey on vehicular ad hoc networks. IEEE Communications magazine, 46(6), 164-171.