WORLD ATLAS INTERNATIONAL JOURNAL OF EDUCATION & MANAGEMENT
VOL 9 NO 1, FEBRUARY 2026, NEW YORK CITY. *ISSN: 2667-1069*

CYBER SECURITY, A SERIOUS CONCERN ON AUTONOMOUS VEHICLES: THE NEED FOR PROTECTION FROM HACKING AND EFFECTS ON SAFETY

By

Dr Lucky W. WILLIAMS
Department of Engineering
Faculty of Engineering & Technology
University Avenue W
Waterloo, Ontario N2l 3g1
Canada
North America

And

AKPAN, E. Ebenezer, Ph.D., FCICN, AP, PPGDCA, PHDCDPM
Corporate institute of Research and Computer Science
140 Ikot Ekpene Road
Uyo, Akwa Ibom State

ABSTRACT

This study examined cybersecurity as a critical concern in autonomous vehicles, with emphasis on the need for protection against hacking and its implications for safety. The research explored the concepts of cybersecurity, autonomous vehicles, and hacking, highlighting their interconnections within modern intelligent transportation systems. It was established that autonomous vehicles rely heavily on advanced technologies such as artificial intelligence, sensor systems, and network connectivity, which significantly increase their vulnerability to cyber threats. The study identified various forms of cyberattacks, including malware injection, sensor spoofing, denial-of-service attacks, and unauthorized system access, all of which pose serious risks to vehicle functionality and passenger safety. Findings further revealed that cyberattacks on autonomous vehicles could result in loss of control, system malfunction, traffic disruptions, financial losses, and reduced public trust in autonomous technology. The study also examined key cybersecurity measures such as encryption, intrusion detection systems, secure communication protocols, and sensor fusion techniques as effective strategies for mitigating these risks. Additionally, strengthening mechanisms including fail-safe system design, real-time monitoring, over-the-air updates, and regulatory compliance were identified as essential for enhancing both safety and security. The study concluded that robust cybersecurity frameworks are indispensable for the successful deployment and sustainability of autonomous vehicles. One of the reccommendation made was that manufacturers of autonomous vehicles should integrate advanced security systems such as end-to-end encryption, intrusion detection systems, and multi-layer authentication protocols to prevent unauthorized access.

KEYWORDS: Autonomous Vehicles, Cybersecurity, Hacking, Vehicle Safety, Protection.

INTRODUCTION

The rapid advancement of digital technology has significantly transformed various sectors of human life, including transportation. One of the most groundbreaking innovations in this regard is the development of autonomous vehicles, also known as self-driving cars. These vehicles are designed to operate with minimal or no human intervention by utilizing advanced technologies such as artificial intelligence (AI), machine learning, sensors, and communication networks. While autonomous vehicles promise improved efficiency, reduced human error, and enhanced mobility, they also introduce complex cybersecurity challenges that cannot be overlooked.

Cybersecurity, which involves the protection of computer systems, networks, and data from unauthorized access and cyber threats, has become a fundamental concern in today's interconnected world. As noted by Akpan and Wilson (2023), cybersecurity is not limited to internet users alone but is essential for all individuals and systems that rely on digital infrastructure. Similarly, Farahmand, Navimipour, and Hosseinzadeh (2020) emphasized that cybersecurity encompasses protective measures designed to safeguard systems against disruptions, data theft, and infrastructure damage. With the integration of intelligent technologies into transportation systems, cybersecurity has become increasingly important in ensuring the safe operation of autonomous vehicles.

Autonomous vehicles depend heavily on interconnected systems such as Vehicle-to-Vehicle (V2V) and Vehicle-to-Everything (V2X) communication, as well as sensor technologies like LiDAR, radar, and cameras to perceive their environment and make driving decisions. According to Sharma, Bhatia, and Singh (2020), these vehicles rely on complex artificial intelligence systems to analyze data and navigate safely without human input. However, this heavy reliance on digital and networked systems makes them highly susceptible to cyberattacks. Bai et al. (2024) further explained that autonomous vehicles integrate perception, decision-making, and control systems, all of which can be exploited if proper cybersecurity measures are not implemented.

One of the major threats to autonomous vehicles is hacking, which involves unauthorized access to computer systems and networks with the intent to manipulate, disrupt, or steal information. Hacking has evolved from a practice of system improvement to a serious cybersecurity threat involving malicious activities such as data breaches, malware attacks, and system manipulation (Sarker et al., 2020). In the context of autonomous vehicles, hacking can have severe real-world consequences, including loss of vehicle control, accidents, and threats to passenger safety. Cybercriminals may exploit vulnerabilities in vehicle software, communication networks, or sensor systems, thereby compromising the integrity and reliability of autonomous driving systems.

The effects of cybersecurity breaches on autonomous vehicles are far-reaching. Beyond immediate safety risks, cyberattacks can lead to economic losses, damage to

manufacturers' reputations, and reduced public trust in autonomous technology. Seetharaman et al. (2020) highlighted that cyberattacks can disrupt vehicle control systems, leading to dangerous situations such as unintended acceleration or braking failure. Furthermore, Meyer et al. (2021) noted that attacks on connected vehicle systems could result in traffic inefficiencies and large-scale transportation disruptions. These risks underscore the urgent need for strong cybersecurity frameworks in autonomous vehicle systems.

To address these challenges, various cybersecurity measures and strengthening mechanisms have been developed. These include intrusion detection systems, encryption techniques, secure communication protocols, sensor fusion, and artificial intelligence-based anomaly detection systems. Additionally, fail-safe system designs, real-time monitoring, over-the-air updates, and adherence to regulatory standards such as ISO 26262 and ISO/SAE 21434 play crucial roles in enhancing both safety and security. These strategies not only help in detecting and preventing cyberattacks but also ensure that autonomous vehicles can respond effectively to potential system failures.

CONCEPT OF CYBER SECURITY

Cybersecurity is the practice of defending computers, servers, networks, mobile devices, and data from malicious digital attacks, unauthorized access, or damage. Cybersecurity is not only an issue for "Internet users" but for all citizens. (Akpan & Wilson, 2023). As illustrated by Farahmand, Navimipour&Hosseinzadeh (2020), cybersecurity is the protection of computer systems and networks from cyber threats that aim to disrupt operations, steal data, or damage digital infrastructure. Effective cybersecurity necessitates ongoing monitoring, risk assessment, and the implementation of defensive mechanisms like encryption and intrusion detection systems. However, they also bring challenges such as cybersecurity risks, job displacement due to automation, and ethical concerns regarding data privacy and AI decision-making. (James & Kingsley, 2025)

As noted by Sarker, Kayes, &Badsha (2021), cybersecurity involves the protection of digital systems, networks, and data from unauthorized access, cyberattacks, and data breaches. This explains how cutting-edge technology like artificial intelligence, encryption methods, and intrusion detection systems are used in modern cybersecurity to detect and eliminate threats instantly. Cybersecurity and financial risks dominate, but strategic risk management remains an underexplored area, indicating an unmet need in the area of integrated enterprise-wide AI application. (Adesemowo, A.O, 2024).

CONCEPT OF AUTONOMOUS VEHICLES

An autonomous vehicle (AV), often called a self-driving car, driverless vehicle, or robocar, is a vehicle capable of sensing its environment and navigating without human input. Using technologies like lidar, cameras, radar, and AI, they manage steering, braking, and navigation. AI algorithms are employed to analyze road conditions, detect

deficiencies (potholes or other road deficiencies), and prioritize maintenance and repair efforts (Amuzat, 2025). They range from advanced driver-assistance systems (Level 1-2) to fully autonomous systems (Level 5).

As noted by Sharma, Bhatia, & Singh (2020), an autonomous vehicle is a self-driving system capable of sensing its environment and navigating without human intervention. To observe their environment, make decisions, and safely manage motion, these vehicles rely on a variety of sensors, including LiDAR, radar, and cameras, in addition to artificial intelligence systems. Artificial intelligence is an umbrella term for a wide variety of automated technologies (Ariseloka, 2025).

According to Bai, Zhang, Liu, & Chen (2024), autonomous vehicles are advanced intelligent systems that integrate perception, decision-making, and control modules to enable self-driving capability without human intervention. To enable safe navigation in challenging settings, these systems use deep learning algorithms and multi-sensor fusion (LiDAR, radar, and cameras).

CONCEPT OF HACKING

The act of locating, gaining access to, and modifying computer systems, networks, or digital devices—often by taking advantage of weaknesses or getting around security measures—is referred to as hacking. Although the phrase first referred to talented programmers who innovatively altered systems to enhance performance, it has since expanded to encompass both benign and malevolent cybersecurity actions. Hacking is frequently classified according to authorization and intent. White-hat hacking, often known as ethical hacking, is the practice of approved security experts testing systems to find vulnerabilities and bolster defenses. To increase system resilience, these people adhere to organizational policies and legal frameworks. Malicious hacking, often known as black-hat hacking, on the other hand, entails illegal access with the goal of stealing information, interfering with services, or causing harm. A third category, gray-hat hacking, falls between the two, where individuals may access systems without permission but do not necessarily intend harm, though their actions may still be unlawful (Sarker., 2020).

Cybersecurity risks and vulnerabilities are strongly related to the idea of hacking. Phishing, virus attacks, ransomware, and software vulnerability exploitation are examples of contemporary hacking strategies. The attack surface for hackers has greatly increased due to the quick development of digital technologies, cloud computing, and the Internet of Things (IoT). As a result, organizations face increasing risks related to data breaches, financial loss, and privacy violations (Conti. 2021). Strong security measures are necessary to combat these attacks. These consist of intrusion detection systems, encryption, multi-factor authentication, and frequent software updates. Cybersecurity experts and ethical hackers are essential in proactively spotting vulnerabilities before they can be exploited. Additionally, governments and international bodies have

developed regulations and standards to promote safer digital environments (Alshamrani. 2022).

EFFECTS OF CYBER SECURITY ON AUTONOMOUS VEHICLES

Autonomous vehicle (AV) development, deployment, and operation now depend heavily on cybersecurity. These cars are extremely susceptible to cyberattacks because they rely so largely on software, sensors, artificial intelligence, and communication networks like Vehicle-to-Everything (V2X). Therefore, cybersecurity has a multifaceted impact on autonomous vehicles, affecting scientific advancement, safety, performance, trust, and economic feasibility.

The direct impact of cybersecurity on autonomous cars' dependability and safety is one of its main effects. Since autonomous cars are cyber-physical systems, any cyberattack could have tangible repercussions in the real world. Malware or hacker assaults, for example, can disrupt car control systems, causing unexpected acceleration, braking issues, or loss of steering control. According to research, hackers have the potential to jeopardize passenger safety, increase communication delays, and threaten vehicle autonomy. Adversarial attacks against artificial intelligence models employed in perception systems might also cause cars to misinterpret obstructions or road signals, raising the likelihood of an accident (Seetharaman., 2020). Therefore, whereas inadequate security leaves AVs vulnerable to potentially disastrous failures, strong cybersecurity improves operational safety.

Vehicle performance and system efficiency are two more important effects. Vehicle networks must be protected by cybersecurity measures such encryption, intrusion detection systems, and authentication processes. Nevertheless, latency and processing overhead may be introduced by these approaches. For instance, AVs' real-time decision-making processes may be slowed down by more security checks in communication networks. However, in the lack of cybersecurity, systems are vulnerable to attacks that could interfere with vehicle communication, resulting in traffic congestion and inefficiencies. Research shows that traffic data manipulation by cyberattacks on connected cars might lead to ineffective routing and decreased system performance (Meye., 2021) As a result, cybersecurity strikes a balance between performance optimization and protection.

The financial and commercial sides of autonomous vehicles are significantly impacted by cybersecurity. Cyberattacks can result in monetary losses due to vehicle damage, system outages, legal ramifications, and damage to manufacturers' reputations. For instance, a successful cyberattack on a fleet of self-driving cars might cause major economic repercussions and interfere with transportation services. The total cost of AV production is also increased by the need for businesses to make significant investments in cybersecurity technology, research, and standard compliance. But these expenditures are required since the cost of cyber catastrophes is frequently much higher than the cost of prevention (Girdhar. 2023).

HOW TO PROTECT AUTONOMOUS VEHICLES FROM CYBER HACKING

Autonomous vehicles (AVs) are advanced cyber-physical systems that depend on sensors, artificial intelligence (AI), and network connectivity to operate without human drivers. While this connectivity enables smart driving, it also exposes vehicles to cyber threats such as hacking, malware injection, sensor spoofing, denial-of-service (DOS) attacks, and unauthorized access. As noted by Dibaei (2020), the high level of connectivity in intelligent vehicles significantly increases their vulnerability to cyber-attacks, especially through in-vehicle networks and external communication systems

Intrusion detection systems (IDS) are a key component of autonomous vehicle security. Ids continuously scans external communication channels and internal vehicle networks (like CAN buses) for unusual activity. It supports innovations like autonomous vehicles, remote surgery, and seamless real-time communication (Kingsley & James, 2025). These systems help identify cyber threats in real time before they affect vehicle safety.

Another important protection method is encryption and secure communication protocols. The need for an efficient, modern telecommunication sector is now regarded as crucial to economic development in transition countries (Akpan2022).Wireless technologies like Vehicle-to-Vehicle (V2V) and Vehicle-to-Everything (V2X) communication are crucial to autonomous cars. Attackers can intercept or alter transmitted data in the absence of encryption.

Redundancy and sensor security are also important aspects of protection. To comprehend their surroundings, autonomous cars employ a variety of sensors, including radar, LiDAR, cameras, and GPS. Cybercriminals may try to interfere with these sensors by faking or interfering with signals.Strong cyber security standards must be implemented to safeguard procurement platforms from identity theft, hacking, and data manipulation as procurement becomes more and more online (Amuzat2025). Sensor fusion techniques are used to cross-check data from several sources in order to prevent this. Unusual patterns in vehicle behavior are also found using AI-based anomaly detection systems. In order to identify typical driving behavior and spot abnormalities that might point to cyber-attacks, machine learning models are trained.

GENERAL STRENGTHENING MECHANISMS OF AUTONOMOUS VEHICLES FOR SAFETY AND SECURITY

The hardware, software, and cognitive decision-making systems that autonomous vehicles (AVs) rely on must all be improved in order to guarantee both security and safety. Robust mechanisms are needed to prevent accidents, withstand cyber assaults, and sustain dependable performance across a variety of settings because these vehicles run with little to no human assistance.

- **Sensor redundancy and fusion**

Sensor redundancy and fusion is one important mechanism. To sense their surroundings, autonomous cars rely on various sensors, including LiDAR, radar, cameras, and ultrasonic systems. By combining these sensors using sophisticated data fusion techniques, safety can be strengthened by making sure that other sensors can compensate in the event that one fails or delivers erroneous data. Sensor fusion algorithms improve object detection accuracy and reduce the risk of misinterpretation in complex driving environments (Feng, 2020; Yurtsever, 2020).

- **Robust artificial intelligence and machine learnin**

Robust machine learning and artificial intelligence validation are another crucial mechanism. Deep learning models, which are a subset of machine learning that uses neural networks with many layers, play a major role in AV (autonomous vehicle) perception and decision-making. Thorough training, testing, and validation utilizing a variety of datasets—including edge cases like bad weather or peculiar traffic situations—are necessary to strengthen these systems. Techniques like adversarial training and explainable AI (XAI) help detect vulnerabilities and improve transparency in decision-making processes (Zhang., 2021; Kuutti., 2020).

- **Cyber security frameworks and intrusion detection systems (IDS)**

Intrusion detection systems (IDS) and cybersecurity frameworks are also essential. Autonomous vehicles are networked systems that interact with cloud platforms, infrastructure, and other vehicles (V2V, V2I). They are vulnerable to cyberattacks because of this interconnectedness. Implementing encryption methods, secure communication channels, and real-time intrusion detection systems that keep an eye out for unusual network activity are all part of strengthening security. Blockchain-based approaches have also been proposed to secure data exchange and prevent unauthorized access (Sharma., 2021; Cui., 2022).

- **Fail-safe and fault-tolerant system design**

Furthermore, the design of a system must be fault-tolerant and fail-safe. AVs must be able to identify internal malfunctions and, if needed, switch to a safe state by slowing down or stopping. Redundant control systems, backup power supplies, and real-time diagnostics ensure that the vehicle can handle unexpected malfunctions without endangering passengers or other road users (Koopman& Wagner, 2020).

- **Real-time monitoring and over-the-air (OTA) updates**

Over-the-air (OTA) upgrades and real-time monitoring are additional strengthening mechanisms. Manufacturers can find and address issues after deployment thanks to ongoing monitoring. Without requiring physical access to the car, OTA updates allow for

timely security patches and performance enhancements. However, these updates must themselves be secured to prevent malicious interference (Rao, 2023).

- **Regulatory compliance and safety standards**

Lastly, safety standards and regulatory compliance are important. The design and implementation of safe and secure AV systems are guided by standards like ISO 26262 (functional safety) and ISO/SAE 21434 (cybersecurity). Compliance ensures that manufacturers follow best practices in risk assessment, hazard analysis, and system validation (Hawkin, 2021).

CONCLUSION

In conclusion cybersecurity is a fundamental requirement in the development and deployment of autonomous vehicles. While these technologies offer remarkable benefits in terms of efficiency and convenience, their dependence on interconnected digital systems exposes them to significant risks. The possibility of hacking and unauthorized access poses a direct threat to human life, public safety, and transportation infrastructure. This study highlights that without strong cybersecurity measures, the advantages of autonomous vehicles may be overshadowed by potential dangers. Therefore, ensuring the integrity, confidentiality, and reliability of vehicle systems is not optional but essential. Stakeholders in the automotive and technology industries must recognize that safety in autonomous mobility extends beyond physical engineering to include digital protection against cyber threats.

RECOMMENDATIONS

- Manufacturers of autonomous vehicles should integrate advanced security systems such as end-to-end encryption, intrusion detection systems, and multi-layer authentication protocols to prevent unauthorized access.
- Continuous updates should be implemented to fix vulnerabilities and strengthen system defenses against newly emerging cyber threats.
- Regulatory bodies should establish strict cybersecurity standards for autonomous vehicles, including mandatory safety certifications before deployment on public roads.
- Artificial intelligence should be used to monitor vehicle systems in real time, detect unusual activities, and respond immediately to potential cyberattacks.

REFERENCES

Adesemowo, A. O., (2024).AI-enabled frameworks for strategic risk management: a systematic review and model for organizational resilience and decision-making support.*Shared Seasoned International Journal of Topical Issues,* 10(1),125-129.

Akpan E. E (2022) A Strategic Assessment of Telecommunication Infrastructure Development and Economic Growth: A Panel Data Approach.*International Journal of Current Innovations in Education* 3(1) 1-3

Akpan, E.E., &Wilson, D.K.,(2023),The menace of cybercrimes: studying the strategies of strengthening cyber security and resilience to mitigate cybercrimes in Nigeria and the globe.*International Journal of Eminent Scholars*, 9(1),23-25.

Alsaade, F. W., & Al-Adhaileh, M. (2023).*Cyber attack detection for self-driving vehicle networks*. Sensors. DOI: 10.3390/s23084086

Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2022). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials*, 24(2), 120–152.

AmuzatO(2025) Combating Procurement Fraud In The Public Sector.Modern Anthology In Education Administration, Science And Technology. 24-37

Amuzat,O.,(2025).How AI will shape up government of alberta and the benefits it can reap and become more competitive globally by the strategic application of AI. *Shared Seasoned International Journal of Topical Issues*.12 (1).1-13.

Ariseloka, O.A., (2025).Leveraging AI-driven Autostore systems to enhance emergency response and crisis management; a focus on grocery stores.*Academic Journal Of Global Who Is Who In Academia,* 6(1),1-13.

Bai, Y., Zhang, X., Liu, H., & Chen, Y. (2024). Deep learning-based perception and decision systems for autonomous driving: A review. *IEEE Transactions on Intelligent Vehicles,* 9(2), 145–162

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2021). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, 78, 544–546.

Cui, J., Zhang, Y., Zhong, H., &Xu, Y. (2022). Secure communication in autonomous vehicles: A blockchain-based approach. *IEEE Transactions on Vehicular Technology*, 71(2), 1357–1369.

Dibaei, M., Zheng, X., Jiang, K., Abbas, R., Liu, S., Zhang, Y., Xiang, Y., & Yu, S. (2020). Attacks and defences on intelligent connected vehicles: A survey. Digital

Communications and Networks, 6(4), 399–421. https://doi.org/10.1016/j.dcan.2020.04.007

Farahmand, F., Navimipour, N. J., &Hosseinzadeh, M. (2020).A survey on cyber security challenges and solutions in modern information systems.*Journal of Information Security and Applications,* 55(3), 102–112

Feng, D., Haase-Schutz, C., Rosenbaum, L., et al. (2020). Deep multi-modal object detection and semantic segmentation for autonomous driving: Datasets, methods, and challenges. *IEEE Transactions on Intelligent Transportation Systems*, 22(3), 1341–1360.

Girdhar, M., Junho Hong, Moore, J. (2023).*Cybersecurity of autonomous vehicles: Adversarial attacks and defense models*. IEEE Open Journal. DOI: 10.1109/OJVT.2023.3265363

Hawkins, R., Habli, I., & Kelly, T. (2021). Assurance cases for safety and security in autonomous vehicles. *Safety Science*, 134, 105034.

James, C., & Kingsley, P.K.,(2025),The barriers to effective information dissemination by mass media: assessing the mitigating strategies using modern technologies in the 21st century.*Gaspro International Journal of Language and Linguistics* 5(1), 53-56.

Kim, K., Kim, J. S., Jeong, S., Park, J. H., & Kim, H. K. (2021). Cybersecurity for autonomous vehicles: Review of attacks and defense. Computer & Security 103, 102150.https://doi.org/10.1016/j.cose.2020.102150

Kim, K., S., Jeong, S., Park, J., [b], Kim, Huy K. (2021). *Cybersecurity for autonomous vehicles: Review of attacks and defense*. Computers & Security. DOI: 10.1016/j.cose.2020.102150

Kingsley P. A & James C (2025)The Barriers To Effective Information Dissemination By Mass Media: Assessing The Mitigating Strategies Using Modern Technologies In The 21st Century. *Gaspro International Journal Of Language And Linguistics* 5(1) 54-59

Koopman, P., & Wagner, M. (2020). Autonomous vehicle safety: An interdisciplinary challenge. *IEEE Intelligent Transportation Systems Magazine*, 12(1), 90–96.

Kuutti, S., Fallah, S., Katsaros, K., et al. (2020).A survey of deep learning applications to autonomous vehicle control.*IEEE Transactions on Intelligent Transportation Systems*, 22(2), 712–733.

Meyer, S. F., Elvik, R. & Johnsson, E. (2021).*Risk analysis for forecasting cyberattacks against connected and autonomous vehicles*.Journal of Transportation Security. DOI: 10.1007/s12198-021-00236-4

Rao, Q., Frtunikj, J., & Chen, B. (2023). Over-the-air updates for autonomous vehicles: Security challenges and solutions. *IEEE Internet of Things Journal*, 10(4), 3210–3222.

Sarker, I. H., Kayes, A. S. M., &Badsha, S. (2021). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data,* 8(1),1–27

Sarker, I. H., Kayes, A. S. M., & Watters, P. (2020).Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, 7(1), 41.

Seetharaman, A., Patwa**, N.,** Jadhav, V., Saravanan, A. S., &Sangeeth, D.(2020). *Impact of factors influencing cyber threats on autonomous vehicles*.Taylor & Francis. DOI: 10.1080/08839514.2020.1799149

Sharma, A., Bhatia, M., & Singh, R. (2020). Autonomous vehicles: Technologies, challenges, and future trends. *International Journal of Vehicle Autonomous Systems,* 18(2), 101–118.

Sharma, P. K., Singh, S., Jeong, Y. S., & Park, J. H. (2021). DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks. *IEEE Communications Magazine*, 59(2), 78–84.

Yurtsever, E., Lambert, J., Carballo, A., & Takeda, K. (2020). A survey of autonomous driving: Common practices and emerging technologies. *IEEE Access*, 8, 58443–58469.

Zhang, J., Chen, Y., & Li, Z. (2021). Adversarial attacks and defenses in autonomous driving: A survey. *IEEE Transactions on Intelligent Vehicles*, 6(3), 399–414.