Analysing Cyber Challenges: Towards Enhancing Autonomous Vehicle Cybersecurity Resilience

Tanisha Soldini, Elena Sitnikova, Karl Sammut
College of Science and Engineering
Flinders University
Adelaide, Australia
e-mail: {tanisharose.soldini | elena.sitnikova | karl.sammut}@flinders.edu.au

***Abstract*—Autonomous vehicles' rise in society represents an important technological advancement in the transportation sector, promising improved financial investments, mobility, and efficiency. Connectivity to cloud-based or fifth generation cellular networks increases autonomous vehicles' exposure to cyber threats, compromising vehicle safety, privacy, and economic stability. Ensuring resilient cyber security measures are critical for safeguarding transportation's critical infrastructure. This paper presents a taxonomy of cyber attacks and mitigation mechanisms of autonomous vehicles. Analysis of recent literature reveals a diverse range of threats, from Global Positioning System spoofing to malware attacks, countered by mitigation mechanisms, such as cryptography, software and network security solutions. Examination of current challenges has identified several future research directions, such as architectural solutions and adversarial machine learning, presenting continuous opportunities for innovation and advancement in the transportation field. Developing robust cyber security mechanisms is essential to closing the gap in protecting autonomous vehicles and ensuring the integrity of transportation infrastructure.**

Keywords-autonomous vehicles; critical infrastructure; cyber security; cyber resilience; taxonomy.

I. Introduction

Autonomous Vehicles (AVs) represent a continuing technological innovation in the transportation sector. The evolution of AVs includes state-of-the-art sensor technology, computing power, and Artificial Intelligent (AI) Systems. Employing AVs in the urban transport landscape has the potential to improve efficiency, lower costs, reduce emissions, increase mobility and accessibility [1][2][3]. AVs function through their interconnected systems and communication protocols, increasing the potential attack surface. Consequences of such attacks include compromised safety, breaches of information, financial losses, and damage to reputation [4]. Current taxonomies for understanding and mitigating cyber attacks on AVs address various elements of cyber security but fails to include all critical areas of AV security. These gaps in knowledge poses risks of accidents, financial losses, and widespread transportation disruptions [5][6][7][8]. Following research questions are developed to address the gaps in securing AVs:

1) What types of cyber-attacks are most pertinent to AV systems, and how can they be categorised?
2) What are the effective mitigation mechanisms for these attacks, and how can they be systematically classified?

This paper proposes a new taxonomy of cyber attacks and mitigation mechanisms on AVs. The taxonomy will classify attack types and countermeasures, facilitating improved identification of system vulnerabilities and offer areas for future research to safeguard transportation infrastructure.

The remainder of the paper is as follows: Section II introduces AVs, discussing their architecture, and impact on society. Section III presents a taxonomy of cyber-attacks, categorising them based on attack types. In Section IV, mitigation mechanisms are investigated, labelling them as network security, software security, and cryptography. Section V provides an analysis of current challenges in securing AVs and Section VI outlines potential areas for future research in developing resilient cyber security measures.

II. Introduction to Autonomous Vehicles

First introduced in the 1980s, AVs integrate physical and computational processes to improve safety, mobility and efficiency [9].

A. Architecture of Autonomous Vehicles

AVs architecture can be separated into three distinct layers: perception and sensor integration, decision and control, and chassis [10][11].

Perception and Sensor Integration: AVs integrate various sensors, such as Radio Detection and Ranging (Radar), Light Detection and Ranging (LiDAR), Cameras (Image sensors), Global Positioning System (GPS) to perceive the vehicle's surroundings and position localisation.

Decision and Control: Processed sensor data is used to perform higher-level decision-making to outline pathways, predict actions, avoid obstacles, and control vehicle motion.

Chassis: The chassis layer interfaces with the decision and control layer, regulating vehicle mechanical components.

B. Level of Vehicle Autonomy

The Society of Automotive Engineers (SAE) defines vehicle automation into six levels, ranging from 0 (requiring full human control) to 5 (complete automation), dependent on the extent of human interaction necessary for operation [9][12]. The six levels are defined as follows:

- **Level 0:** All tasks accomplished by human drivers.
- **Level 1:** Human driver controls the vehicle, automation systems can assist.
- **Level 2:** Human driver controls driving process and monitors the environments with automated functions applied.

Copyright (c) IARIA, 2024. ISBN: 978-1-68558-186-2

- **Level 3:** Automated vehicle with human operator prepared to assume command of the vehicle at any instance.
- **Level 4:** Under specific circumstances, automated driving occurs, otherwise the operator can assume control of the vehicle.
- **Level 5:** Under all conditions, automated driving occurs, and the operator can take control of the vehicle.

Societal impact of AVs is multifaceted and largely dependent on their autonomy level. These levels of autonomy have potential to increase independence and access to transportation, and improve road safety.

III. Taxonomy of Cyber Attacks

A. Methods of Cyber Attacks and Targeted Components

Several attack pathways in AVs exist. These include:

- **Remote Access and Control:** Exploitation of electronic control systems, gaining unauthorised access and critical functions control [6].
- **Sensor Manipulation:** AVs' reliance on sensor technology for manoeuvring in their surroundings, poses a significant threat. Attackers can spoof sensor data or jam signals, causing the system to misinterpret its environment. Such manipulation could result in hazardous driving and breach of privacy [13][14].
- **Wireless Networks:** Utilised by AVs facilitate communication with nearby vehicles and infrastructure, this reliance introduces vulnerabilities exploitable by attackers. By targeting these communication networks, adversaries can disrupt operations or inject false information into the vehicle's system. This interference can lead to confusion or incorrect decision-making by the vehicle's system, compromising its ability for safe and reliable operation [15]. These include vehicle-to-vehicle (V2V), vehicle-to-network (V2N), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) [16].
- **Software Vulnerabilities:** AVs operate as sophisticated computer systems using a variety of algorithms and software. Consequently, software vulnerabilities emerge as a prominent threat to vehicle safety and security. Malicious software, such as ransomware, poses a potential risk to AV operations by disrupting operations or extorting users for financial gain [17].
- **Hardware Vulnerabilities:** Hardware components, such as the Electronic Control Units (ECUs), On-Board Diagnostic Port (OBD) and Controller Area Network (CAN), can pose potential weaknesses to their physical components and systems. These vulnerabilities may be exploited by through tampering and unauthorised access [5]. Developing a taxonomy of cyber attacks and and identifying corresponding mitigation mechanisms is essential for protecting AVs.

B. Motivations and Perpetrators Behind Cyber Attacks

Cyber attacks on AVs are typically perpetrated by hackers, cyber criminals, and disgruntled individuals. Motivations behind these attacks can be divided into three principal objectives: operational disruptions, gaining vehicle control, and data theft [16].

- **Operational Disruptions:** Compromises critical AV components that are essential for driving functionality, rendering autonomous driving inoperative.
- **Gaining Vehicle Control:** Allows attackers to manipulate critical vehicular functionalities, such as route deviation, emergency braking, and speed modulation.
- **Data Theft:** Stealing data from AV systems, potentially fuelling subsequent cyber attacks.

Cyber criminals can infect the AVs' network with malware, disrupting system operations, harming users, their surroundings, and causing financial losses [18].

C. Cyber Attack Classification

Cyber attacks on AVs can be classified as follows:

- **Man-in-the-Middle (MITM) Attacks:** MITM attacks occur when attackers intercept and alter communications between two components, compromising the integrity and confidentiality of the data exchanged. Methods include intercepting and tampering with vehicle communications, impersonating legitimate entities, exploiting wireless interfaces, rerouting messages and attacking dynamic rerouting [19].
- **Infection Attacks:** Infection attacks involve injecting malicious code into a vehicle's systems, which can potentially compromise its functionality and safety. Methods include exploiting software vulnerabilities, violating wireless interfaces, supply chain attacks, infecting removable media, and compromising backend systems [20].
- **Tampering Attacks:** These attacks involve the unauthorised manipulation of data, software, or hardware components on AVs, potentially affecting their performance and safety. Methods include sensor data tampering, such as intercepting camera perception by physically obscuring its view, spoofing LiDAR signals, jamming or injecting noise into sensors [21]. Communication mechanisms can be tampered with by injecting malicious data or MITM attacks. Software/firmware tampering exploits vulnerabilities in the vehicle's ECUs by introducing malicious code into the in-vehicle infotainment system or compromising vehicle software through supply chain attacks. Physically tampering with AVs can grant access to the vehicle's internal networks and components. Rogue commands can be sent from the CAN bus through internal access, and actuators can be tempered with to control AV driving operations [5].

1) Identity-based:

- **Spoofing Attacks:** An attacker feeds false information to vehicle systems or sensors to disrupt their data. Spoofing can occur with sensors and communication systems [6].
- **Impersonation Attacks:** Attackers disguise themselves as legitimate entities to access or influence AV systems. Methods include spoofing vehicle identities, impersonating infrastructure, compromising wireless interfaces and cryptographic keys [21].

- **Sybil Attacks:** A single malicious entity creates multiple identities to gain influence. Methods include impersonating multiple vehicles, overwhelming legitimate entities, disrupting platoon operations, exploiting authentication vulnerabilities, and colluding with malicious insiders [6].
- **Replay Attacks:** Capturing and replaying valid data transmissions to bypass authentication. Replay attacks can target GPS signals, sensor data, and communication mechanism. Cryptographic and sensor fusion replay attacks exist [6].

2) Service-based:

- **Denial of Service (DoS) Attacks and Distributed Denial of Service (DDoS) Attacks:** DoS and DDoS attacks overwhelm systems with data to impair operations. Methods include flooding wireless communication channels, jamming sensor signals, exploiting software vulnerabilities, and targeting backend infrastructure [22].
- **Jamming Attacks:** Jamming attacks interfere with wireless communication channels. Methods include jamming sensor and wireless communications [16].
- **Routing Attacks:** Routing attacks disrupt routing protocols to create network instability. Methods include wormhole attacks, sinkhole attacks, black hole attacks, and grey hole attacks [6].

3) Software-based:

- **Malware Attacks:** Introduces malicious code to compromise systems. Methods include exploiting software vulnerabilities, compromising wireless interfaces, supply chain attacks, removable media infection, and compromising backend systems [7].

4) Data Privacy:

- **Location Trailing Attacks:** Monitors a vehicle's location without authorisation. Methods include exploiting localisation algorithms, compromising wireless communications, and exploiting GPS vulnerabilities [4].
- **Eavesdropping Attacks:** Intercepts and accesses private data transmissions. Methods include intercepting wireless communications, exploiting vulnerabilities in communication protocols, and compromising wireless access points [5].

In classifying each type of cyber attack, their characteristics, techniques, and goals are identified.

D. Potential Consequences of Cyber Attacks on Autonomous Vehicles

Cyber attacks on AVs can cause harm to their users and surroundings. Potential consequences are as follows:

- **Safety Risks:** Effective cyber attacks can cause accidents and endanger surroundings by allowing malicious actors to hijack critical vehicle functions, including path control, acceleration, and braking. Spoofing or jamming of the sensors can disrupt navigation. Based on disrupted collected data, incorrect decisions can lead to vehicle malfunctions. If vehicles used for public transport, emergency services or law enforcement are compromised, public safety can be endangered [5].
- **Loss of Vehicle Control:** Malicious attacks have the potential to gain unauthorised remote access to a vehicle's ECUs, paralysing the car or causing erratic behaviour. Software vulnerabilities allow attackers to compromise safety-critical functions [5].
- **Privacy and Data Breaches:** Sensitive data collected by AVs, such as location tracking, driver behaviour, and other personal information, could be exposed by cyber attacks. If this data is breached, it could enable stalking, identity theft, and other privacy violations [6].
- **Traffic Disruptions and Infrastructure Damage:** Compromised AVs could be rerouted or have their navigation systems manipulated, potentially causing major traffic jams, road blockages, and damage to infrastructure [21].
- **Financial Losses and Legal Liabilities:** Cyber attacks may lead to a loss of public trust, potentially resulting in costly vehicle recall and legal liabilities [6].

Securing AVs from cyber attacks is essential to the formulation of mitigation methods in harm prevention.

IV. Mitigation Mechanisms

Mitigation mechanisms are classified as follows:

A. Network Security

Network security mitigation mechanisms protect AV communication networks and systems from cyber attacks.

1) Intrusion Detection Systems: Intrusion detection systems (IDSs) are employed to detect and mitigate various network-based attacks. There are four main IDSs implemented to secure AVs [6][23]:

- **Signature-based IDS:** Functions by comparing observed behaviour against a database of known signatures.
- **Anomaly-based IDS:** Operates by recognising anomalies in a vehicle's behaviour that deviate from the normal or expected patterns.
- **Specification-based IDS:** Monitors a vehicle's behaviour against a set of predefined rules or specifications.
- **Hybrid-based IDS:** Combines the strengths of signature-based and anomaly-based detection methods to defend against a broader spectrum of cyber threats.

B. Malware Detection

Malware detection systems, an extension of IDSs, employ signature and behaviour-based techniques to mitigate cyber attacks. In addition to these, malware detection includes [7]:

- **Heuristic-based Techniques:** Employ heuristic rules and algorithms to identify potential malware based on characteristics or patterns associated with malicious code.
- **Cloud-based Techniques:** Leverages cloud computing services for efficient and scalable malware detection in AVs.

1) Machine Learning and Deep Learning for Intrusion Detection: Network IDSs in AVs utilise Machine Learning (ML) and Deep Learning (DL) models for their fast detection and response times to cyber threats, and ability to leverage insights from data analytics. Models include k-nearest neighbour (KNN), decision trees, auto-encoders and long short-term memory (LSTM) networks [23].

These mechanisms can mitigate cyber attacks, such as spoofing, flooding, modifying hardware components, replay attacks, firmware attacks, and identifying unauthorised access [7].

C. Software Security

1) Machine Learning Algorithms: ML models are employed for various security tasks, including intrusion detection, malware analysis, and vulnerability assessment. Similar to ML for IDSs, ML models detect anomalies and deviations in normal software behaviour, identifying previously unseen attack vectors and zero-day exploits [6].

2) Software Analysis Techniques: Static and dynamic analysis methods are used to analyse AV software for potential vulnerabilities and malicious code [7]:

- **Static:** Examines code without executing it to identify potential vulnerabilities.
- **Dynamic:** Executes code in a controlled environment and monitors for anomalies.

Software techniques can address vulnerabilities like code injection and memory corruption, while ML models counter spoofing, flooding, and replay attacks [21].

D. Cryptography

1) Encryption Techniques: Encryption (symmetric and asymmetric) techniques are used to secure data transmissions and communications in AVs. Public-key cryptography is employed for secure key distribution and authentication in V2V/V2I communications [16].

- **Symmetric:** Encrypts data transmissions in V2V/V2I communications.
- **Asymmetric:** Secures key distribution and authentication in V2V/V2I communications.

Encryption helps mitigate attacks like eavesdropping, spoofing, and MITM attacks, safeguarding the privacy and integrity of transmitted data [16].

2) Authentication Technique:

- **Digital Signatures:** Authenticate the source and integrity of messages or data transmitted between vehicles and infrastructure.
- **Message Authentication Codes:** Provide data origin authentication and integrity verification for V2V/V2I communications.

3) Blockchain Technology: Blockchain (BC) technology is used to store and share information on an advanced database. Each dataset is stored in blocks, linked together in a chain. BC technology has gained popularity with its ability to prevent cyber attacks through its inherent security measures of decentralisation, transparency, encryption, and immutability [24].

These mitigation mechanisms can counter attacks like spoofing, replay attacks, and injection of fake data [16].

E. Comparison of Existing Literature

A systematic review of current literature on cyber attack taxonomies and mitigation mechanisms for AVs was conducted for comparison Table I presents a comparison of existing literature [6][8][16][17][23][25]. This method is performed to reduce bias in the literature. All literature presents a detailed classification of cyber attacks and mitigation mechanisms. Papers [6][8][17][23][25] are lacking in conveying the motivation behind cyber attacks and those responsible. While papers [8][16][17][23][25] do not detail AV architecture.

TABLE I. Comparison of Existing Literature

Literature	[17]	[16]	[6]	[23]	[25]	[8]	Analysis of Paper
Architecture of AV	✗	✗	✓	✗	✗	✗	✓
Motivation and Perpetrators of cyber attacks	✗	✓	✗	✗	✗	✗	✓
Cyber Attack Classification	✓	✓	✓	✓	✓	✓	✓
Target Components	✓	✓	✓	✓	✓	✓	✓
Potential Consequences on Society	✓	✓	✓	✗	✓	✗	✓
Mitigation Mechanisms	✓	✓	✓	✓	✓	✓	✓
Current Challenges and Future Work	✓	✓	✗	✓	✓	✓	✓

Comparison of literature reveals significant gaps in current research on AV cyber security taxonomies, highlighting the need for the proposed taxonomy.

V. Discussion

A. Current Challenges in Securing Autonomous Vehicles from Cyber Attacks

The complexity of cyber attacks and securing AVs will continue to grow with advancements in technology. AVs are computers comprised of complex software algorithms, large amounts of data, and a multitude of electronic components, making them difficult to integrate into traditional security approaches. Their complex and interconnected nature allows for multiple potential entry points for attack points, making it a complicated task to secure all these vectors.

Real-time operation is critical for functioning AVs. High volumes of data must be processed and analysed to detect and combat cyber security risks in real-time. Advancements in high-speed computer processing systems and algorithms are imperative for such progress. AV architecture should be designed to manage system faults and scalability issues [5].

Securing vehicle communication is essential to successful functionality. Breaches in AVs have sequential impacts on critical infrastructure, vice versa. V2X technologies require robust protective methods and the implementation of secure communication networks to ensure reliability. Existing mitigation mechanisms against DDoS attacks in V2V communications are largely theoretical and require verification in a trusted testing environment [16].

AVs depend on ML algorithms to decipher real-time data and formulate operational decisions. These algorithms can be vulnerable to adversarial attacks, manipulating sensor data and leading to potentially hazardous decisions. Errors, such as misclassification, can be triggered by specifically crafted adversarial inputs in deep-learning models. Updating these models with new incoming data from the vehicle has the potential to leak private information [20][26].
These challenges in cyber security provide potential areas for future research.

VI. Conclusion and Future Work

A. Future Work

1) Securing Sensor Data: Securing sensor data is vital for AVs to accurately observe their surroundings, make informed decisions, and ensure safe performance. Research is required to improve sensor fusion techniques to combine data from various sensors, providing an accurate view of the environment.

2) Adversarial Machine Learning Algorithms: Restricted availability of standardised datasets has limited the development of Adversarial Machine Learning (AML) mitigation mechanisms against cyber attacks. Current datasets do not account for advancement in AML and adversarial attacks. Compiling an accessible, up-to-date dataset that represents different attack scenarios and network traffic diversity is critical for developing effective AML mitigation mechanisms [27].

3) Real time decision making: AVs require sophisticated algorithms and computing processors to effectively evaluate vast amounts of data, posing challenges in real-time decision making [5].

4) Securing Autonomous Vehicles with AI and BC Technologies: BC technologies demonstrate promise in preventing cyber attacks through their inherent security measures of decentralisation, transparency, encryption, and immutability. In comparison to traditional security approaches, AI has shown greater efficiency and a faster detection rate when addressing cyber threats. There is a lack of research concerning the interrelationship between BC and AI, and consequently, an understanding of AVs' security and privacy [24].

5) Communication Mechanisms: Challenges exist in implementing strong communication networks in AVs. These systems require networks that can manage low-latency communications, high volumes of complex data flows, and resilient connectivity in harsh environments. 5G cellular V2X products are still under development and security attacks have currently not been prominent. Security features are well defined and rely on authentication and encryption. However, their effectiveness needs to be tested before and after AV deployment [16] [23].

6) Architectural Solution: Future research has the potential to combine an architectural solution for AVs with Supervisory Control and Data Acquisition (SCADA) integration. A hierarchical self-aware architectural solution allows for real-time operational analysis, decision formulation, and integration with remote locations. The architecture includes four layers: monitoring, analysis, decision-making, and visualisation. A Security-specific In-vehicle Black Box (STCB) is employed to execute the security models and algorithms within a trusted environment [28]. This architectural solution provides security coverage through multiple hierarchical layers, enabling proactive and tailored security measures. SCADA has multiple integration points:

- Monitoring layer collects data from various sensors.
- Analysis layer uses machine learning techniques for anomaly detection.
- Decision layer determines the severity of incidents and triggers appropriate responses.
- Visualisation layer is a human-machine interface (HMI) module.

Integration of in-vehicle security components with an external Virtual Security Operation Centre (VSOC) facilitates coordinated responses across vehicle fleets. The STCB enhances situational awareness and timely mitigations through security-specific logging and analysis, real-time threat detection, and automated responses. Leveraging SCADA's capabilities, the hierarchical self-aware architecture can be implemented for unified security management of AVs.

B. Conclusion

The increasing reliance on connectivity in AVs has introduced vulnerabilities to cyber attacks, posing significant risks to safety, privacy, and economic stability. This paper has provided a taxonomy of cyber attacks, mitigation mechanisms, and future research areas. Analysis of current challenges reveals the potential for a multidisciplinary approach that integrates an architectural solution with SCADA systems to counter the diverse range of threats facing AVs. As the transportation sector continues to evolve, it is imperative that resilient cyber security methods are developed and implemented to safeguard AVs while maintaining the integrity of critical infrastructure. Future research should focus on addressing the identified challenges and developing innovative solutions to ensure secure and reliable operation of AVs.

References

[1] E. Kassens-Noor *et al.*, "Sociomobility of the 21st century: Autonomous vehicles, planning, and the future city", *Transport Policy*, vol. 99, pp. 329–335, Dec. 2020, ISSN: 0967070X. DOI: 10.1016/j.tranpol.2020.08.022.

[2] D. Bissell, T. Birtchnell, A. Elliott, and E. L. Hsu, "Autonomous automobilities: The social impacts of driverless vehicles", *Current Sociology*, vol. 68, no. 1, pp. 116–134, Jan. 1, 2020, Publisher: SAGE Publications Ltd, ISSN: 0011-3921. DOI: 10.1177/0011392118816743.

[3] R. Bennett, R. Vijaygopal, and R. Kottasz, "Willingness of people with mental health disabilities to travel in driverless vehicles", *Journal of Transport & Health*, vol. 12, pp. 1–12, Mar. 2019, ISSN: 22141405. DOI: 10.1016/j.jth.2018.11.005.

[4] A. Algarni and V. Thayananthan, “Autonomous vehicles: The cybersecurity vulnerabilities and countermeasures for big data communication”, *Symmetry*, vol. 14, no. 12, p. 2494, Dec. 2022, Number: 12 Publisher: Multidisciplinary Digital Publishing Institute, ISSN: 2073-8994. DOI: 10.3390/sym14122494.

[5] A. Giannaros *et al.*, “Autonomous vehicles: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions”, *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, pp. 493–543, 2023, Publisher: MDPI AG, ISSN: 2624-800X. DOI: 10.3390/jcp3030025.

[6] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, “Cybersecurity for autonomous vehicles: Review of attacks and defense”, *Computers & Security*, vol. 103, p. 102 150, Apr. 1, 2021, ISSN: 0167-4048. DOI: 10.1016/j.cose.2020.102150.

[7] S. Aurangzeb, M. Aleem, M. T. Khan, H. Anwar, and M. S. Siddique, “Cybersecurity for autonomous vehicles against malware attacks in smart-cities”, *Cluster Computing*, Oct. 3, 2023, ISSN: 1573-7543. DOI: 10.1007/s10586-023-04114-7.

[8] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and Y. Chen, “Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions”, *Accident Analysis & Prevention*, vol. 148, p. 105 837, Dec. 1, 2020, ISSN: 0001-4575. DOI: 10.1016/j.aap.2020.105837.

[9] C. Morrison, E. Sitnikova, and S. Shoval, “A review of the relationship between cyber-physical systems, autonomous vehicles and their trustworthiness”, in *International Conference on Cyber Warfare and Security*, Num Pages: 611-621,XV, Reading, United Kingdom: Academic Conferences International Limited, 2018, pp. 611–621, XV.

[10] W. Zong, C. Zhang, Z. Wang, J. Zhu, and Q. Chen, “Architecture design and implementation of an autonomous vehicle”, *IEEE Access*, vol. 6, pp. 21 956–21 970, 2018, Conference Name: IEEE Access, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2018.2828260.

[11] M. Pipicelli *et al.*, “Architecture and potential of connected and autonomous vehicles”, *Vehicles*, vol. 6, no. 1, pp. 275–304, Mar. 2024, Number: 1 Publisher: Multidisciplinary Digital Publishing Institute, ISSN: 2624-8921. DOI: 10.3390/vehicles6010012.

[12] “SAE levels of driving automation™ refined for clarity and international audience”, [Online]. Available: https://www.sae.org/site/blog/sae-j3016-update (visited on 05/30/2024).

[13] Y. Wang, Q. Liu, E. Mihankhah, C. Lv, and D. Wang, “Detection and isolation of sensor attacks for autonomous vehicles: Framework, algorithms, and validation”, *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 8247–8259, Jul. 2022, Conference Name: IEEE Transactions on Intelligent Transportation Systems, ISSN: 1558-0016. DOI: 10.1109/TITS.2021.3077015.

[14] Z. El-Rewini *et al.*, “Cybersecurity attacks in vehicular sensors”, *IEEE Sensors Journal*, vol. 20, no. 22, pp. 13 752–13 767, Nov. 2020, Conference Name: IEEE Sensors Journal, ISSN: 1558-1748. DOI: 10.1109/JSEN.2020.3004275.

[15] A. Al-Sabaawi, K. Al-Dulaimi, E. Foo, and M. Alazab, “Addressing malware attacks on connected and autonomous vehicles: Recent techniques and challenges”, in *Malware Analysis Using Artificial Intelligence and Deep Learning*, M. Stamp, M. Alazab, and A. Shalaginov, Eds., Cham: Springer International Publishing, 2021, pp. 97–119, ISBN: 978-3-030-62582-5. DOI: 10.1007/978-3-030-62582-5_4.

[16] M. Pham and K. Xiong, “A survey on security attacks and defense techniques for connected and autonomous vehicles”, *Computers & Security*, vol. 109, p. 102 269, 2021, Publisher: Elsevier BV, ISSN: 0167-4048. DOI: 10.1016/j.cose.2021.102269.

[17] S. Parkinson, P. Ward, K. Wilson, and J. Miller, “Cyber threats facing autonomous and connected vehicles: Future challenges”, *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 11, pp. 2898–2915, Nov. 2017, Conference Name: IEEE Transactions on Intelligent Transportation Systems, ISSN: 1558-0016. DOI: 10.1109/TITS.2017.2665968.

[18] A. Seetharaman, N. Patwa, V. Jadhav, A. S. Saravanan, and D. Sangeeth, “Impact of factors influencing cyber threats on autonomous vehicles”, *Applied Artificial Intelligence*, vol. 35, no. 2, pp. 105–132, Jan. 28, 2021, ISSN: 0883-9514, 1087-6545. DOI: 10.1080/08839514.2020.1799149.

[19] R. Gothwal, G. Dharmani, R. S. Reen, and E. G. AbdAllah, “Evaluation of man-in-the-middle attacks and countermeasures on autonomous vehicles”, in *2023 10th International Conference on Dependable Systems and Their Applications (DSA)*, Tokyo, Japan: IEEE, Aug. 10, 2023, pp. 502–509, ISBN: 9798350304770. DOI: 10.1109/DSA59317.2023.00070.

[20] M. C. Chow, M. Ma, and Z. Pan, “Attack models and countermeasures for autonomous vehicles”, in *Intelligent Technologies for Internet of Vehicles*, N. Magaia, G. Mastorakis, C. Mavromoustakis, E. Pallis, and E. K. Markakis, Eds., Cham: Springer International Publishing, 2021, pp. 375–401, ISBN: 978-3-030-76493-7. DOI: 10.1007/978-3-030-76493-7_12.

[21] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, and R. Das, “Attacks on self-driving cars and their countermeasures: A survey”, *IEEE Access*, vol. 8, pp. 207 308–207 342, 2020, Conference Name: IEEE Access, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.3037705.

[22] A. El-Ghamry and M. Elhoseny, “Detecting distributed DoS attacks in autonomous vehicles external environment using machine learning techniques”, in *The 3rd International Conference on Distributed Sensing and Intelligent Systems (ICDSIS 2022)*, Hybrid Conference, Sharjah, United Arab Emirates: Institution of Engineering and Technology, 2022, pp. 292–308, ISBN: 978-1-83953-818-6. DOI: 10.1049/icp.2022.2479.

[23] T. Limbasiya, K. Z. Teng, S. Chattopadhyay, and J. Zhou, *A systematic survey of attack detection and prevention in connected and autonomous vehicles*, Aug. 5, 2022. arXiv: 2203.14965[cs].

[24] G. Bendiab, A. Hameurlaine, G. Germanos, N. Kolokotronis, and S. Shiaeles, “Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence”, *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 4, pp. 3614–3637, Apr. 2023, Conference Name: IEEE Transactions on Intelligent Transportation Systems, ISSN: 1558-0016. DOI: 10.1109/TITS.2023.3236274.

[25] X. Sun, F. R. Yu, and P. Zhang, “A survey on cybersecurity of connected and autonomous vehicles (CAVs)”, *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 6240–6259, Jul. 2022, Conference Name: IEEE Transactions on Intelligent Transportation Systems, ISSN: 1558-0016. DOI: 10.1109/TITS.2021.3085297.

[26] M. Sadaf *et al.*, “Connected and automated vehicles: Infrastructure, applications, security, critical challenges, and future aspects”, *Technologies*, vol. 11, no. 5, p. 117, Oct. 2023, Number: 5 Publisher: Multidisciplinary Digital Publishing Institute, ISSN: 2227-7080. DOI: 10.3390/technologies11050117.

[27] S. Mokhtari, A. Abbaspour, K. K. Yen, and A. Sargolzaei, “A machine learning approach for anomaly detection in industrial control systems based on measurement data”, *Electronics*, vol. 10, no. 4, p. 407, Jan. 2021, Number: 4 Publisher: Multidisciplinary Digital Publishing Institute, ISSN: 2079-9292. DOI: 10.3390/electronics10040407.

[28] A. Adu-Kyere, E. Nigussie, and J. Isoaho, “Self-aware cybersecurity architecture for autonomous vehicles: Security through system-level accountability”, *Sensors*, vol. 23, no. 21, p. 8817, Jan. 2023, Number: 21 Publisher: Multidisciplinary Digital Publishing Institute, ISSN: 1424-8220. DOI: 10.3390/s23218817.