sciendo

Ybl Journal of Built Environment, Volume 9. Issue 2. (2024)
10.2478/jbe-2024-0015

CREATING A SECURE AUTONOMOUS VEHICLE SYSTEM USING A NEURO-FUZZY SYSTEM THAT MERGES ARTIFICIAL NEURAL NETWORKS AND FUZZY INTERFACE SYSTEMS

Ahmed Douzi[1], Judit Lukacs[2]

[1]PhD Student, Óbuda University, Doctoral School on Safety and Security, Budapest, Hungary
ahmed.douzi@phd.uni-obuda.hu

[2]Full Professor, Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, Hungary
lukacs.judit@bgk.uni-obuda.hu

***Abstract*:** *This paper provides an overview of the potential use of Neuro-Fuzzy Systems (NFS) in safeguarding autonomous vehicles (AVs) against cyber-attacks. As innovative technology continues to permeate various aspects of daily life, the integration of advanced technologies, such as Artificial Neural Networks (ANN) and fuzzy inference systems (FIS), holds promise for enhancing the security of intelligent transport systems. With the increasing prominence of autonomous vehicles and self-driving cars in smart city systems, it is imperative to address vulnerabilities that may compromise their security. Existing vulnerabilities, including insecure applications and data-gathering vulnerabilities, pose significant obstacles to the widespread adoption of this technology. The potential consequences of security breaches in autonomous vehicles, such as endangering the lives of individuals both inside and outside of the vehicle, underscore the critical need for comprehensive security measures. By leveraging NFS, this study explored the feasibility of mitigating cyber-attacks targeting AVs, thereby bolstering their security and resilience against malicious intrusions.*

Keywords: *Neuro-Fuzzy system, Autonomous vehicles,Cyber-attacks, Artificial Neural Network, Fuzzy interface, Electronic Control Units*

1. INTRODUCTION

The integration of advanced technologies such as Artificial Neural Networks (ANN) and Fuzzy Inference Systems (FIS) into the smart transport system holds promise for enhancing the security of autonomous vehicles (AVs). The increasing prominence of autonomous vehicles and self-driving cars in smart city systems highlights the need to address vulnerabilities that may compromise their security. This paper explores the feasibility of mitigating cyber-attacks targeting AVs using Neuro-Fuzzy Systems (NFS), thereby bolstering their security and resilience against malicious intrusions. With the increasing integration of artificial intelligence and autonomous systems in various industries, including the automotive sector, ensuring the security of these vehicles becomes crucial to prevent potential cyber-attacks. One approach that

has been explored is the use of neuro-fuzzy systems, which combine the power of neural networks and fuzzy logic to enhance the security measures implemented in autonomous vehicles [1]. These neuro-fuzzy systems can effectively detect and mitigate cyber threats, offering a higher level of protection for autonomous vehicles. To further understand the potential of securing autonomous vehicles against cyber-attacks using neuro-fuzzy systems, it is IMPORTANT to examine the current and expected prospects for their development in various applications, including military and civilian use. Furthermore, exploring the mathematical structures and algorithms employed in neuro-fuzzy systems. Neuro-fuzzy systems can analyze complex data patterns and identify anomalies, making them well-suited for detecting cyber threats in autonomous vehicles. These systems can adapt and learn from past attacks, continuously improving their ability to detect and prevent future cyber-attacks. In addition to their potential to enhance the security of autonomous vehicles, neuro-fuzzy systems also offer advantages in terms of real-time responsiveness and adaptability. This allows them to quickly respond to evolving cyber threats and adjust their security measures, accordingly, ensuring the continuous protection of autonomous vehicles. Furthermore, it is essential to consider the societal attitudes towards the use of neural network algorithms in military applications.

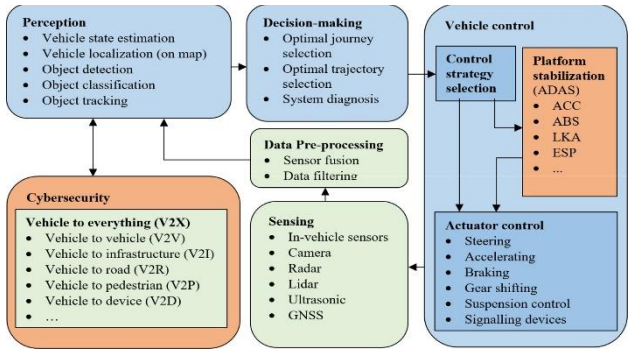

Figure 1 Areas of developing AVs technology [1].

2. AUTONOMOUS VEHICLES AND CYBER-SECURITY CHALLENGES

Autonomous vehicles rely on a vast array of sensors, communication modules, and control systems to navigate and interact with their environment. This interconnectedness, coupled with the increasing adoption of connected technologies, has exposed autonomous vehicles to a wide range of cyber-security threats. Potential attack vectors include:

Sensor Spoofing: Attackers may manipulate sensor data, such as GPS signals or camera feeds, to mislead the decision-making algorithms of the vehicle[2].

Communication Hijacking: Unauthorized access to vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communication channels can allow attackers to intercept, modify, or inject malicious data.

Software Vulnerabilities: Exploiting vulnerabilities in the software of the vehicle, including operating systems, firmware, or applications, can enable attackers to gain control of the systems of the vehicle.

Physical Access Attacks: Unauthorized physical access to the internal components can allow attackers to tamper with the hardware and compromise the security of the vehicle.

Addressing these cyber-security challenges is crucial to ensure the safe and reliable operation of autonomous vehicles, as a successful attack could have catastrophic consequences.

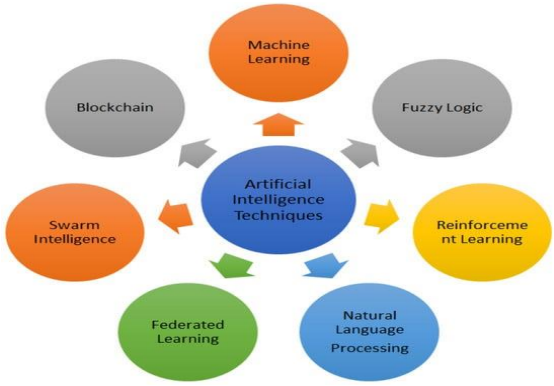

Figure 2 Artificial intelligence techniques involving the fuzzy logic.[3]

Fuzzy logic is a mathematical tool applicable in autonomous vehicles to manage uncertainty and imprecision during decision-making. Within autonomous vehicles, fuzzy logic aids in replicating human-like decision-making processes by incorporating multiple variables that influence driving scenarios, including weather conditions, traffic congestion, road conditions, pedestrian actions, and most importantly, the prevention of cyber-attacks.

3. APPLICATION OF NEURO-FUZZY SYSTEMS

3.1.Tailoring Neuro-Fuzzy Systems for Cyber Threat Detection

Neuro-fuzzy systems present a unique blend of thelearning capabilities of neural networks and the tolerance to uncertainty, making them highly suitable for the complex tasks of cyber threat detection in autonomous vehicles. To tailor these systems for AV security, researchers focus on creating models that can interpret the massive amount of data generated by the sensors of the vehicle and communication systems. These models rely on characteristic patterns of network traffic and user behavior to distinguish between normal operations and potential security threats. By integrating techniques such as Adaptive Resonance Theory and Convolutional Neural Networks, the neuro-fuzzy systems can adapt and evolve to recognize new threats as they arise, thus continuously fortifying the defense mechanisms [2][3[4]].

3.2 Assessing Performance in Real-World Scenarios

The effectiveness of neuro-fuzzy systems in AV security needs to be validated in real-world scenarios to ensure they are not only theoretically sound but also practical. This involves rigorous hardware-in-the-loop testing, which simulates cyber-attacks under controlled conditions to observe the system response. In civilian contexts, this could mean testing against hacking attempts or unauthorized data breaches, while in military applications, it encompasses resistance against targeted attacks by adversaries employing more sophisticated methods. These tests should aim to evaluate both the accuracy of the system in threat detection and its capability to initiate appropriate countermeasures without hindering the vehicularoperation [2 [5]] [4[6]].

3.3 Confronting Deployment Challenges

Deploying neuro-fuzzy systems in AVs is not without challenges. One major hurdle is the computational load these systems demand. AVs must process and respond to threats in real-time, which requires significant processing power and could potentially impact vehicle functions. To address this, researchers are looking into optimizing algorithms to reduce complexity without compromising on performance. Edge computing presents a promising solution by distributing processing loads across the network, thereby reducing the computational burden on individual vehicles. Additionally, the development of specialized hardware capable of running these complex calculations efficiently can further alleviate this concern [5][7].

4. NEURO-FUZZY SYSTEMS FOR AUTONOMOUS VEHICLE SECURITY

In the rapidly evolving landscape of autonomous vehicles, the need for robust security measures has become increasingly paramount. Neuro-fuzzy systems, a blend of neural networks and fuzzy logic, offer a promising solution to address the complex security challenges faced by autonomous vehicles. These vehicles are equipped with a myriad of sensors, communication modules, and decision-making algorithms that work in tandem to navigate the roads safely and efficiently. However, these complex systems are also vulnerable to various cyber threats, ranging from malicious hacking attempts to software glitches and sensor failures.

Neuro-fuzzy systems present a unique approach to enhancing the security of autonomous vehicles by combining the strengths of neural networks and fuzzy logic. Neural networks, with their ability to learn from vast amounts of data and identify intricate patterns, are well-suited for detecting anomalies and potential threats within the systems of the autonomous vehicle. Fuzzy logic, on the other hand, provides a flexible and human-like approach to decision-making, allowing the system to handle uncertainties and ambiguities that may arise during the operation of the vehicle. By integrating these two complementary techniques, neuro-fuzzy systems can effectively identify and mitigate various security threats, from unauthorized access attempts to sensor spoofing and software vulnerabilities.

Neuro-fuzzy systems offer a promising approach to enhancing the cybersecurity of autonomous vehicles by leveraging the strengths of artificial neural networks and fuzzy logic. These hybrid systems combine the learning capabilities of neural networks with the interpretability and reasoning of fuzzy logic, providing a robust framework for real-time threat detection and mitigation[8], [9].

The architecture of a neuro-fuzzy system for autonomous vehicle security typically consists of several key components[10]:

- Sensor Data Preprocessing: Incoming sensor data from various sources (e.g., cameras, LiDAR, GPS) is preprocessed to extract relevant features and prepare the data for analysis.
- Neuro-Fuzzy Anomaly Detection: A neuro-fuzzy model is trained to learn the normal behavior patterns of the autonomous vehicle's systems. This model can then detect anomalies in real-time, identifying potential cyber-attacks.
- Fuzzy Inference System: The fuzzy inference system leverages expert knowledge and rules to interpret the detected anomalies and determine the appropriate response, such as triggering alerts or initiating mitigation actions.
- Neural Network-based Mitigation: A neural network component is responsible for dynamically adjusting the control systems of the vehicle to mitigate the detected cyber-attacks, ensuring the safe and reliable operation of the autonomous vehicle.

The integration of neuro-fuzzy systems in autonomous vehicles offers several key benefits[11]:

- Adaptability: Neuro-fuzzy systems can adapt to changing cyber-security threats and evolving attack patterns, ensuring the continuous protection of autonomous vehicles.
- Interpretability: The fuzzy logic component of the system provides interpretable rules and decision-making processes, allowing for better understanding and trust in the security mechanisms.
- Real-time Performance: The hybrid nature of neuro-fuzzy systems enables fast and efficient threat detection and mitigation, crucial for the safety-critical applications of autonomous vehicles.
- Robustness: Neuro-fuzzy systems can handle uncertainties and incomplete information, making them resilient to the complex and dynamic nature of cyber-attacks.

By incorporating neuro-fuzzy systems into the security architecture of autonomous vehicles, researchers and developers can enhance the protection against various cyber threats, including sensor spoofing, communication hijacking, and software vulnerabilities.

5. NEURO-FUZZY ARCHITECTURE FOR AUTONOMOUS VEHICLE SECURITY

The architecture of a neuro-fuzzy system designed to enhance the security of autonomous vehicles is a critical component in safeguarding these vehicles against cyber-attacks. This architecture typically comprises several key elements that work synergistically to detect and mitigate potential threats effectively[12].

- Sensor Data Preprocessing: The initial stage involves preprocessing incoming sensor data from various sources such as cameras, LiDAR, and GPS. This preprocessing step aims to extract relevant features and prepare the data for further analysis within the neuro-fuzzy system.
- Neuro-Fuzzy Anomaly Detection: A crucial aspect of the architecture is the neuro-fuzzy anomaly detection module. This component is responsible for training a model to learn the normal behavior patterns of the systems of the autonomous vehicle. By detecting anomalies in real-time, this module can effectively identify potential cyber-attacks and trigger appropriate responses.
- Fuzzy Inference System: The fuzzy inference system plays a vital role in interpreting the detected anomalies and determining the suitable response mechanisms. Leveraging expert knowledge and predefined rules, this system can make informed decisions based on the identified threats.
- Neural Network-based Mitigation: Another integral part of the architecture is the neural network-based mitigation module. This component dynamically adjusts the control systems to promptly mitigate the detected cyber-attacks. By leveraging the learning capabilities of neural networks, this module ensures the safe and reliable operation of the autonomous vehicle in the face of security threats.

By integrating these components into a cohesive neuro-fuzzy architecture, autonomous vehicles can benefit from a comprehensive and adaptive security framework that effectively detects, interprets, and mitigates cyber-attacks in real-time. This architecture offers a robust defense mechanism against a wide range of threats, including unauthorized access attempts, sensor spoofing, and software vulnerabilities, ensuring the safety and reliability of autonomous vehicle operations.

6. CASE STUDIES AND SIMULATION RESULTS

To validate the efficacy of neuro-fuzzy systems in enhancing the cybersecurity of autonomous vehicles, several case studies and simulation results were conducted to assess their performance in detecting and mitigating cyber-attacks. These studies aimed to simulate real-world attack scenarios and evaluate the response of the neuro-fuzzy system in safeguarding the autonomous vehicle against potential threats.

6.1 Study Case: Enhancing CAN Bus Security Using Neural-Fuzzy Systems

Autonomous Vehicles represent an increasingly appealing innovation within Intelligent Transportation Systems. However, despite the technological progress, vehicles predominantly rely on a Controller Area Network bus system for the internal communication of various electronic control units. Although the CAN bus is highly effective in transmitting messages, it presents notable security vulnerabilities due to its unsegmented, unencrypted, and authentication-deficient network architecture. Consequently, there is a critical need to establish additional security measures to safeguard the continued utilization of CAN in vehicles [13].

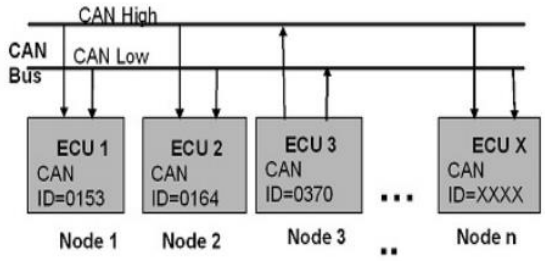

Figure 3 ECU nodes interconnected with the CAN bus[13]

The absence of security measures in the CAN bus system exposes it to potential threats compromising its confidentiality, integrity, and availability.[14]. The primary vulnerability of the CAN bus system lies in its broadcast of all messages from the Electronic Control Units (ECUs) without implementing encryption or authentication mechanisms, thereby rendering it susceptible to security breaches[15]. As a result of this vulnerability, malicious actors can exploit and manipulate Electronic Control Units (ECUs), leading to significant harm to a vehicle[16]. The CAN bus system is particularly susceptible to three primary types of attacks: Denial of Service (DoS) attacks, Fuzzing attacks, and Impersonation attacks[17].

The Controller Area Network (CAN) bus system is a critical component in modern vehicles, responsible for facilitating communication between various electronic control units. However, the CAN bus protocol lacks encryption, authentication, and integrity checking, making it vulnerable to cyber-attacks that can compromise the integrity and security of the vehicle.

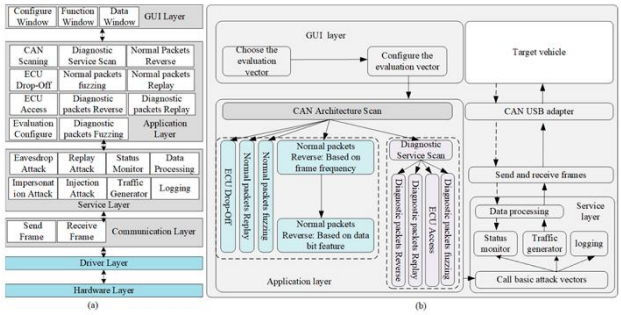

Figure 3 CANsec architecture: (a) The framework of CANsec; (b) Automatic evaluation flow[18]

The objective of this study case is to demonstrate how neural-fuzzy systems can be leveraged to enhance the security of CAN bus systems, mitigate cyber threats, and safeguard the integrity of vehicle communications.

6.2 Simulation Scenario: Securing the CAN Bus in Autonomous Vehicles

In a simulated environment inspired by real-world AV operations, a neural-fuzzy system is deployed to protect the automotive communication networks, sensor data, and control systems from cyber threats. The simulation includes scenarios such as sensor spoofing attacks, communication hijacking attempts, and software vulnerabilities that mimic potential risks faced by AVs in operational settings.

In this simulation scenario, Controller Area Network (CAN) bus of a highly automated vehicle is equipped with a neural-fuzzy system to enhance its security against cyber-attacks. The simulation aims to demonstrate the effectiveness of this approach in detecting and mitigating threats targeting the CAN bus.

The simulation setup includes:

- CAN Bus Network: The autonomous vehicle is modeled with a realistic CAN bus architecture, including multiple Electronic Control Units (ECUs) communicating over the bus.
- Attack Scenarios: Various cyber-attack scenarios are simulated, such as:
  - Unauthorized access attempts to the CAN bus
  - Injection of malicious data packets
  - Spoofing of legitimate ECU messages
  - Denial-of-Service (DoS) attacks disrupting CAN bus communication
- Neural-Fuzzy Security System: A neural-fuzzy system is integrated into the CAN bus architecture to monitor network traffic, detect anomalies, and identify potential cyber-attacks. The system combines the learning capabilities of neural networks with the interpretability of fuzzy logic to classify suspicious activities.

Training and Adaptation: The neural-fuzzy system is trained using a dataset of known cyber-attacks and normal CAN bus operations. It learns to recognize patterns indicative of malicious activity and adapts its detection rules accordingly.

During the simulation, the neural-fuzzy system continuously monitors the CAN bus traffic. When an attack scenario is triggered, the system analyzes the network data in real-time, leveraging its trained models to detect anomalies and classify the type of attack.

Upon detecting a cyber-attack, the neural-fuzzy system initiates appropriate mitigation actions, such as:

Isolating the affected ECUs or CAN bus segments

Triggering alerts to the security systems

Implementing countermeasures to block malicious traffic

Rerouting critical messages through alternative channels

The simulation results demonstrate the effectiveness of the neural-fuzzy system in enhancing CAN bus security. Key performance metrics include:

- Attack detection accuracy
- False positive rate
- Response time to detected attacks
- Resilience against evolving attack patterns

By incorporating this neural-fuzzy security system into the CAN bus architecture, autonomous vehicle manufacturers can significantly improve the protection of their vehicles against cyber threats targeting the CAN bus. The simulation serves as a proof-of-concept for this approach and highlights its potential in ensuring the safe and secure operation of autonomous vehicles.

6.3 Results:

Through the implementation of the neural-fuzzy system, the AV successfully detects and mitigates cyber-attacks in real-time. The adaptive learning capabilities of the system enable it to identify anomalies in sensor data, detect unauthorized access attempts, and respond proactively to potential threats. The neural-fuzzy system showcases high accuracy in classifying suspicious activities and triggering appropriate responses to safeguard the AV's cybersecurity.

7. CONCLUSION

This paper has delved into the feasibility of countering cyber-attacks aimed at AVs through the utilization of Neuro-Fuzzy Systems (NFS), thereby enhancing their resilience against malicious intrusions. By harnessing the amalgamation of neural networks and fuzzy logic, NFS offer a robust security framework that can effectively detect and mitigate cyber threats, elevating the level of protection afforded to autonomous vehicles.

The exploration of neuro-fuzzy systems has shed light on their capacity to analyze intricate data patterns, identify anomalies, and adapt to evolving cyber threats. Their real-time responsiveness and adaptability position them as formidable tools in safeguarding autonomous vehicles against a spectrum of security risks.

Looking ahead, it is crucial to consider the broader implications and societal attitudes towards the deployment of neural network algorithms, particularly in military applications. By further investigating the mathematical structures and algorithms underpinning neuro-fuzzy systems, we can continue to enhance their efficacy in securing autonomous vehicles and advancing cybersecurity measures in the automotive sector.

As we navigate the evolving landscape of autonomous vehicles and smart city technologies, the integration of neuro-fuzzy systems stands as a beacon of innovation and progress in fortifying the security of autonomous vehicles against cyber-attacks. Through ongoing research, collaboration, and technological advancements, we can pave the way for a safer and more secure future in autonomous transportation.

ACKNOWLEDGMENT

I would like to express my gratitude to the researchers and authors cited in the sources provided, and I would like to thank my supervisor Dr. Judit Lukacs for her valuable contributions. This acknowledgment is a testament to the collaborative efforts and innovative research that have studied the way for advancements in cybersecurity for autonomous vehicles.

REFERENCES

[1] **V. Skrickij, E. Šabanovič, and V. Žuraulis**, "Autonomous road vehicles: recent issues and expectations," *IET Intelligent Transport Systems*, vol. 14, no. 6, pp. 471–479, Jun. 2020, doi: 10.1049/IET-ITS.2018.5513.

[2] **R. Komissarov and A. Wool**, "Spoofing Attacks Against Vehicular FMCW Radar," pp. 91–97, Nov. 2021, doi: 10.1145/3474376.3487283.

[3] **M. Sadaf et al.**, "Connected and Automated Vehicles: Infrastructure, Applications, Security, Critical Challenges, and Future Aspects," *Technologies 2023, Vol. 11, Page 117*, vol. 11, no. 5, p. 117, Sep. 2023, doi: 10.3390/TECHNOLOGIES11050117.

[4] **X. Wang, X. Lin, and M. Li**, "Aggregate modeling and equilibrium analysis of the crowdsourcing market for autonomous vehicles," *Transp Res Part C Emerg Technol*, vol. 132, p. 103362, Nov. 2021, doi: 10.1016/J.TRC.2021.103362.

[5] **R. W. Chalmers, D. H. Scheldt, T. M. Neighoff, S. J. Witwicki, and R. J. Bamberger**, "Cooperating unmanned vehicles," *Collection of Technical Papers - AIAA 1st Intelligent Systems Technical Conference*, vol. 1, pp. 244–251, 2004, doi: 10.2514/6.2004-6252.

[6] **T. Davenport, A. Guha, D. Grewal, and T. Bressgott**, "How artificial intelligence will change the future of marketing," *J Acad Mark Sci*, vol. 48, no. 1, pp. 24–42, Jan. 2020, doi: 10.1007/S11747-019-00696-0/FIGURES/2.

[7] **L. Jia et al.,** "On autonomous transportation systems", doi: 10.1108/SRT-06-2022-0015.

[8] **B. Selma and S. Chouraqui,** "Neuro-fuzzy controller to navigate an unmanned vehicle," *Springerplus*, vol. 2, no. 1, pp. 1–8, 2013, doi: 10.1186/2193-1801-2-188.

[9] "(PDF) Autonomous System Controller for Vehicles Using Neuro-Fuzzy." Accessed: May 10, 2024. [Online]. Available: https://www.researchgate.net/publication/259080180_Autonomous_System_Controller_for_Vehicles_Using_Neuro-Fuzzy

[10] **K. Asha et al.**, "Analysis of Automotive Security Risk using Cyber Security," *2023 International Conference on Network, Multimedia and Information Technology, NMITCON 2023*, 2023, doi: 10.1109/NMITCON58196.2023.10275969.

[11] **S. R. Shetty and D. H. Manjaiah,** "Adaptive Neuro-Fuzzy Technique for Jamming Detection in VANETs," *Lecture Notes in Networks and Systems*, vol. 479, pp. 571–580, 2023, doi: 10.1007/978-981-19-3148-2_49.

[12] **B. Amar Bensaber, C. G. Pereira Diaz, and Y. Lahrouni,** "Design and modeling an Adaptive Neuro-Fuzzy Inference System (ANFIS) for the prediction of a security index in VANET," *J Comput Sci*, vol. 47, p. 101234, Nov. 2020, doi: 10.1016/J.JOCS.2020.101234.

[13] **R. Gundu and M. Maleki,** "Securing CAN Bus in Connected and Autonomous Vehicles Using Supervised Machine Learning Approaches", doi: 10.1109/eIT53891.2022.9813985.

[14] **C. Young, J. Zambreno, H. Olufowobi, and G. Bloom**, "Survey of automotive controller area network intrusion detection systems," *IEEE Des Test*, vol. 36, no. 6, pp. 48–55, Dec. 2019, doi: 10.1109/MDAT.2019.2899062.

[15] **X. Mo, P. Chen, J. Wang, and C. Wang,** "Anomaly Detection of Vehicle CAN Network Based on Message Content," *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 284, pp. 96–104, 2019, doi: 10.1007/978-3-030-21373-2_9.

[16] **V. H. Le, J. den Hartog, and N. Zannone**, "Security and privacy for innovative automotive applications: A survey," *Comput Commun*, vol. 132, pp. 17–41, Nov. 2018, doi: 10.1016/J.COMCOM.2018.09.010.

[17] **A. Rehman Javed, S. ur Rehman, M. Ullah Khan, M. Alazab, S. Member, and T. G. Reddy**, "CANintelliIDS: Detecting In-Vehicle Intrusion Attacks on a Controller Area Network Using CNN and Attention-Based GRU", doi: 10.1109/TNSE.2021.3059881.

[18] **H. Zhang, X. Meng, X. Zhang, and Z. Liu**, "CANsec: A Practical in-Vehicle Controller Area Network Security Evaluation Tool", doi: 10.3390/s20174900.