ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/suresh-sureddi/372

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 2 & Iss: 4

Research Article

The Use and Impact of AI in Enhancing Automotive Cyber Protection

Suresh Sureddi*

Citation: Sureddi S. The Use and Impact of AI in Enhancing Automotive Cyber Protection. J Artif Intell *Mach Learn & Data Sci 2024*, 2(4), 1717-1719. DOI: doi.org/10.51219/JAIMLD/suresh-sureddi/372

Received: 02 November, 2024; **Accepted:** 18 November, 2024; **Published:** 20 November, 2024

***Corresponding author:** Suresh Sureddi, USA, E-mail: ssureddi@gmail.com

ABSTRACT

The integration of Artificial Intelligence (AI) in the automotive industry has transformed various facets of vehicle design, manufacturing and operation. One of the most critical areas where AI is making a significant impact is in enhancing automotive cybersecurity. As vehicles become increasingly connected and autonomous, the need for robust cybersecurity measures has become more crucial. This article explores the use and impact of AI in boosting automotive cyber protection.

Keywords: Vehicular network, intelligent connected vehicle, cyber security, Artificial intelligence, Cloud computing

1. Introduction

The advancements in connected and autonomous vehicles, enabling communication with other vehicles, road infrastructure and cloud-based services, bring abundant benefits but makes vehicles vulnerable to cyber threats. For example, in mid-2023, a vulnerability was discovered in the Ford Sync 3[1] infotainment system by security researcher, which uses QNX as its operating system. This issue was due to a flaw in Wi-Fi driver. This vulnerability assisted remote code execution in the QNX OS. As traditional cyber security methods struggle to address the continuously evolving threats, AI could help to proactively address the threats in real time. This paper first lists the current ongoing security challenges in the connected cars and then provide the benefits of AI in addressing those challenges. It also briefly lists the complexity involved in using AI for cyber protection.

2. Cyber threats in Connected and autonomous vehicles

Smart key systems which involve wireless communication between the key fob and vehicle, eliminate the need for physical key, makes vulnerable to vehicle theft such as replay attack.

2.1. Cloud based features: In the past, vehicle owner used to get a fixed set of features at the time of purchase and it requires a visit to dealership to get upgrades. But now a days, vehicles regularly communicate with OEM's cloud and third-party cloud services for Over the air (OTA) software updates and for online subscription features. This extended connectivity increases vulnerability to cyber-attacks.

2.2. ADAS (Advanced Driver Assistance Systems): ADAS features has transformed the driving experience and drastically enhanced the safety of the vehicles. These functions depend on complex sensors such as cameras, radar, Lidar and GPS etc to interpret the surroundings and make real time decisions. However, recent studies exposed the vulnerabilities, specifically involving the manipulation of camera [2] inputs.

2.3. V2X communications (Vehicle to Everything): Vehicle-to-Everything (V2X) communication empowers vehicles to interact with each other and with infrastructure, such as roadside units (RSU), traffic lights and road signs. These V2X communications are vulnerable to cyber-attacks. Categorization of the general cyber-attacks in connected and autonomous vehicles [CAV] [3] include Attacks on authentication, Attacks on availability,

Attacks on non-repudiation, Attacks on confidentiality and Attacks on privacy.

2.4. Vehicle Network and Diagnostics (OBD Port access): At dealership, diagnostics tools are connected to the vehicle network (CAN) over the OBD port and collects various data from different ECU. This makes vehicle network vulnerable to cyber-attacks.

3. Benefits of using AI in automotive cybersecurity:

Advanced threat intelligence or Real-time threat detection:

Machine learning is vital in identifying and mitigating cybersecurity threats in real-time. Machine learning algorithms analyzes vast amounts of data from vehicle systems and detect patterns that indicate potential threats or unusual activities.

Categories of machine learning algorithms used in threat detection include:

- **Supervised Learning:** Classifying known threats based on labeled/tagged data, such as previous malware signatures.
- **Unsupervised Learning:** Helps identify new and emerging threats by detecting anomalies in vehicle behavior that do not match established patterns.
- **Reinforcement Learning:** Continuously improves threat detection accuracy by learning from past responses and adapting to new threats.

AI established Intrusion Prevention Systems (IPS) can analyze large amounts of data from several sources in real-time to identify emerging threats, analyze attack methodologies and provide real-time threat intelligence reports. This helps Cybersecurity experts become proactive and implement security measures before the attack occurs[4].

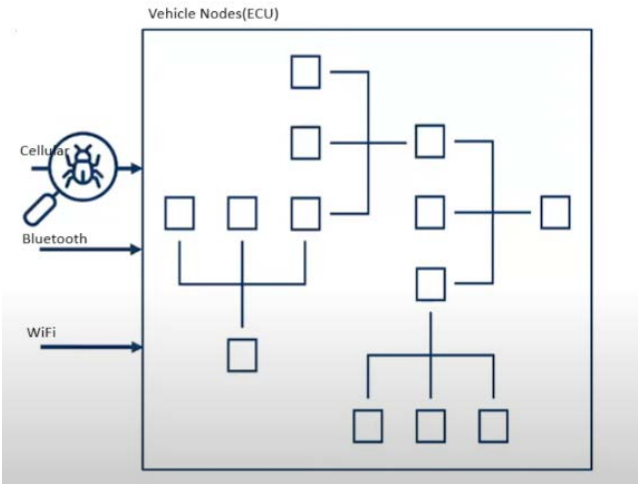

Figure 1: Intrusion Preventive Systems (IPS).

AI supported Intrusion Detection Systems (IDS) can analyze large amounts of data in real time to identify suspicious activities, analyze the network traffic and provide timely warnings to security teams. Also, the AI enabled IDS can continuously learn from new threat patterns to update its algorithms.

3.1. Use of AI for securing V2X communications

V2X communications are critical for autonomous vehicles. AI helps securing these communications from cyber threats by monitoring the real time data exchange and identifying potential vulnerabilities. AI algorithms analyze traffic patterns detect anomalies and block suspicious data transfers.

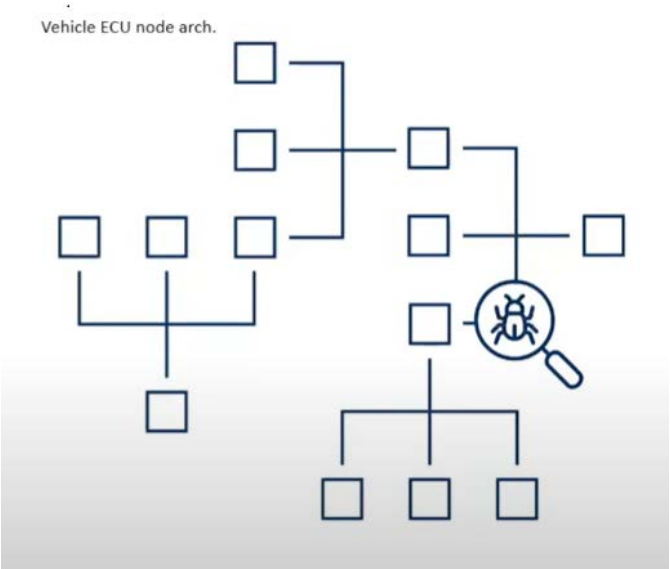

Figure 2: Intrusion Detection Systems (IDS).

3.2. Use of AI in OTA (Over the Air) updates

Over-the-Air (OTA) updates helps manufacturers to remotely update vehicle software with new features and security patches. AI algorithms monitor and secures these software and firmware updates. AI helps by ensuring only the safe and verified SW is used before the installation and prevents installation of malicious software[5].

3.3. Use of AI in securing Autonomous driving systems

Autonomous vehicles depend on AI for navigation, decision-making and control. AI can be used to continuously monitor the autonomous systems, checking for anomalies in sensor data and navigation decisions and take corrective action if any issues are detected.

3.4. Use of AI in protecting connected vehicle Ecosystems

Vehicles are connected to external systems like Cloud and data centers for providing enhanced features like remote operations and subscription management etc. AI secures data exchange between the vehicle and backend systems like cloud, ensuring data integrity and preventing security breaches.

3.5. Use of Predictive Maintenance

By analyzing data from various sensors and historical maintenance records, AI can predict when a part is likely to fail and schedule maintenance accordingly. This proactive approach enhances vehicle reliability and ensures that security vulnerabilities are addressed before they can be exploited by attackers.

3.6. Attack Prevention

AI can analyze emails and messages through NLP (Natural language processing) to detect phishing attempts by recognizing suspicious patterns, misleading information and malicious URLs. NLP is also used to interpret and secure V2X communications. NLP allows vehicles to understand and act on voice commands and AI ensures these interactions are secure. For instance, BMW uses NLP for secure communication.

3.7. Vulnerability and patch management

AI can support vulnerability scanning by analyzing code (static and dynamic analysis), identifying potential weaknesses and by building queries to check affected.

AI can also support patch management by supporting appropriate patches and suggesting mitigation measures for identified vulnerabilities.

3.8. Incident management

AI can support incident management rapid response by handling initial incident reports, automating ticket system and providing the first level support.

3.8.1. Automated response: AI can immediately neutralize threats, such as isolating affected systems or shutting down compromised communication channels, without human intervention.

4. Challenges of AI in automotive cybersecurity

4.1. Complexity in developing AI systems

Developing AI systems for automotive cybersecurity is complex because they must address various potential threats of hardware and software vulnerabilities. Integrating AI with vehicles having legacy systems can be even more technically challenging.

4.2. AI system itself could be vulnerable

AI systems themselves can become targets for cyber attackers. Small manipulations in data could cause AI to make incorrect decisions. AI systems themselves shall continuously adapt and evolve to come up with counter measures to control the rising threat of AI-generated or enhanced attacks.

4.3. Performance vs AI security

AI algorithms with strong security measures could slow down the overall performance of the systems in the vehicle. OEMs and suppliers need to make sure the systems or ECUs with real-time decision-making capability are not impacted due to the potential overhead of AI based security measures.

5. Emerging trends of AI in automotive cyber security

OEMs are exploring the use of deep learning capabilities to anticipate and counterattack the threats before they materialize.

AI systems are expected to become more advanced at predicting through continuous learning and adaption.

5.1. Integration of AI with Quantum computing

Quantum computing helps AI driving cybersecurity by enabling faster and more complex calculations. This could help development of robust encryption methods and rapid detection of security threats.

OEMs are working with regulatory bodies to create a unified framework to ensure vehicles' cybersecurity. Also, automotive industry finds the need for international collaboration to develop standards for AI in automotive cybersecurity.

6. Conclusion

Artificial Intelligence (AI) is transforming the way vehicles are secured against cyberattacks. AI can be beneficial in several areas of automotive industry from Advanced threat intelligence to attack prevention to securing V2X communications and autonomous driving systems to secure OTA (Over the air updates), AI can play a crucial role in ensuring the safety and security of modern vehicles. With the continuous evolution of automotive industry, the advancements in AI technologies such as quantum computing and deep learning is essential to ensure vehicles are protected against critical cyber-attacks. Also, it is essential for automotive industry to collaborate globally to develop standards for AI in automotive cybersecurity. AI can be misused by cyber attackers in saving time to determine the attack methods, provide malicious code and enhance the attacks on the systems. Cybersecurity remains a highly competitive field where experts on both side of the law compete. Automotive industry, governments and researchers shall be ahead of the game in effectively utilizing the AI capabilities to protect the auto users from cyber-attacks.

7. References

1. https://fordauthority.com/2023/08/ford-says-sync-3-vehicles-have-a-security-vulnerability/
2. https://www.teslarati.com/tesla-not-ai-training-compute-constrained-elon-musk/
3. https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/itr2.12504
4. https://www.youtube.com/watch?v=COaqxNPouF8&list=PLFrXHXT1jl_wkH7wCArSqHIWFQRTIQk2p&index=
5. https://redresscompliance.com/ai-in-automotive-Cybersecurity/#AI_Technologies_in_Vehicle_Cybersecurity