IoT in Autonomous Vehicles

Krishnakanth Kuruvachira Sabu

22078053

A report submitted for

INFS7008 (SCC Term 3 2024) Systems and Network Security
in partial fulfillment of the requirements for the degree of
Master of Data Science

Unit Convenor : Dr Hanh Vo

School of Computer, Data and Mathematical Sciences
Western Sydney University
January 2025

Contents

List of Figures

Chapter 1

Introduction

In this Modern Era the integration of the Internet of Things also termed as IoT, into autonomous vehicles (AVs) is revolutionizing the transportation industry which enhance safety, efficiency, and user convenience. Through interconnected sensors, module used for communication, real time data processing, AVs can operate with a minimal human involvement, paving the way for intelligent transportation systems. However, these technologies advancements come up with a significant security risk that can actually compromise the safety, reliability, and most importantly privacy of both passengers and broader transport networks.

Among the numerous cybersecurity concerns in IoT that enabled Avs, GPS spoofing, data breaches and malware attacks stand out as some of the most critical. GPS spoofing involves manipulation of navigation systems by transmitting fake signals, leading vehicles as off the right path and posing safety hazards. Data Breaches that threaten the confidentiality and integrity of sensitive data, potentially allowing unauthorized sources to access vehicle controls or user information. Malware and ransomware attacks can disrupt vehicle operations and performance, compromise safety functions, and extort customers or manufacturers.

Figure 1.1: System architecture of AIoT in autonomous vehicles

The increasing connectivity of Avs creates a larger attack surface, exposing vehicles to complex and evolving cyber attacks or threats. Addressing all these challenges requires a comprehensive understanding of the underlying backend architectures, potential vulnerabilities, and effective security solutions. This report explores the IoT architecture in Autonomous vehicles which examines key security threats, and process robust measures to mitigate these risks and issues [1].

Chapter 2

Architectures and applications

Autonomous vehicles are mostly relied on a multi layered IoT architecture that facilitates seamless communication, real time data processing and autonomous decision making. This architecture includes various components working together to ensure the safety and efficient operation of the vehicles in a big complex environment.

2.1 IoT Architectural Layers in AVs

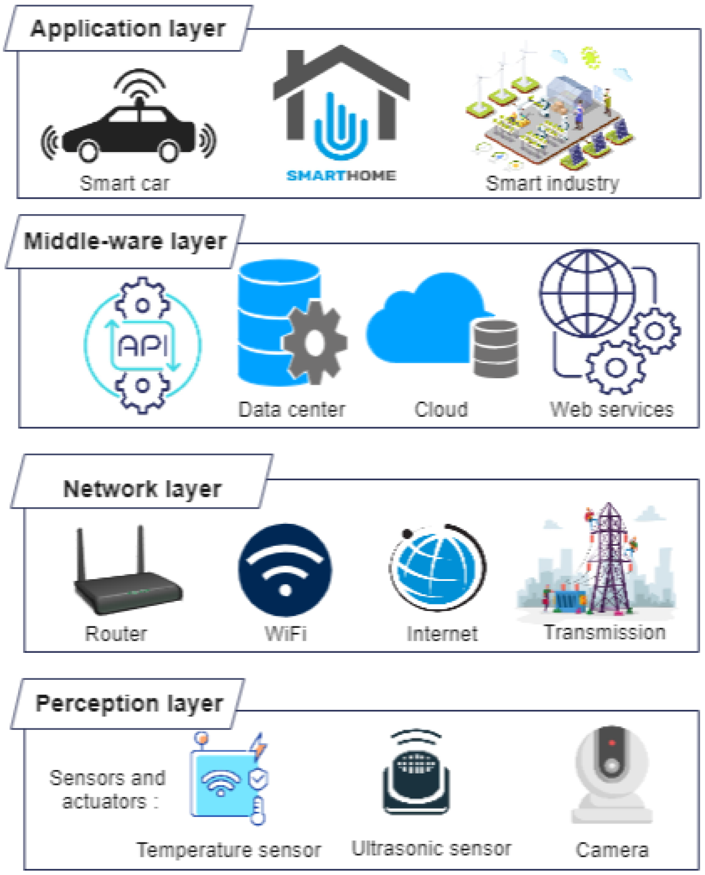

Figure 2.1: IoT Architectural Layers in AVs

1. **Perception Layer:**
   This foundational layer which includes various sensors and devices responsible for environmental data collections. These sensors such as LiDAR, Radar, Ultrasonic sensors, GPS modules, and cameras which gathers a crucial and critical information for navigation, object detection in low visibilities on the conditions. These sensors work in collaboration to deliver accurate real time data for autonomous navigation

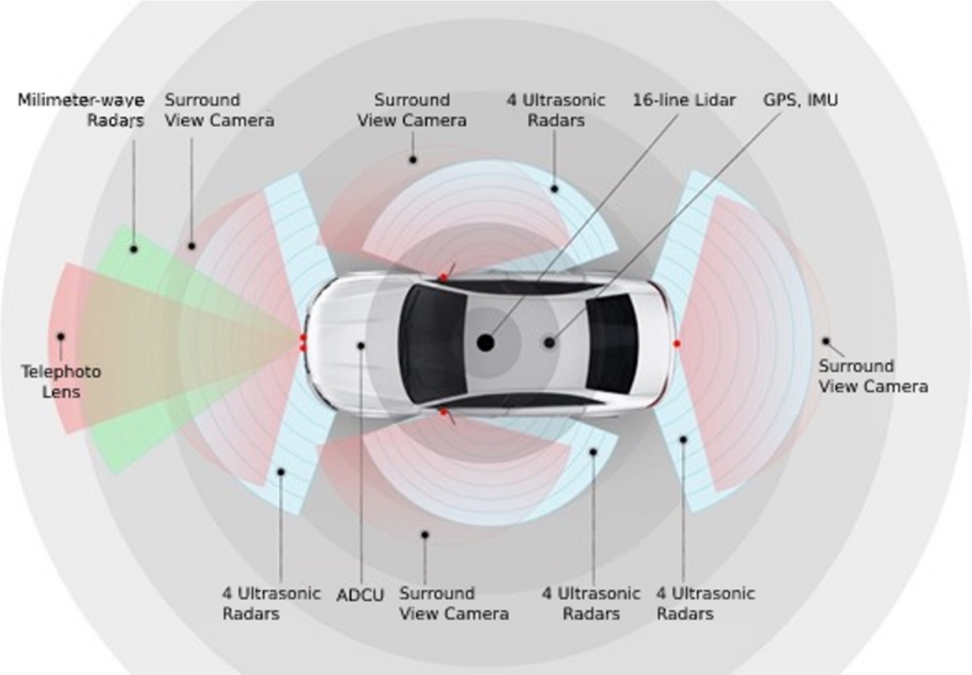

Figure 2.2: Diagram of sensors in autonomous vehicles

2. **Network Layer:**
   This layer depicts the communication between the vehicle components, infrastructure and other vehicles. Technologies such as Vehicle to Vehicle(V2V), Vehicle to Infrastructure (V2I), and Vehicle-to-Everything (V2X) this technologies exchange real time data. The involvement of 5G networks supports high speed processing, low tatect communication, essential for rapid decision making in dynamic environments. [1][3]

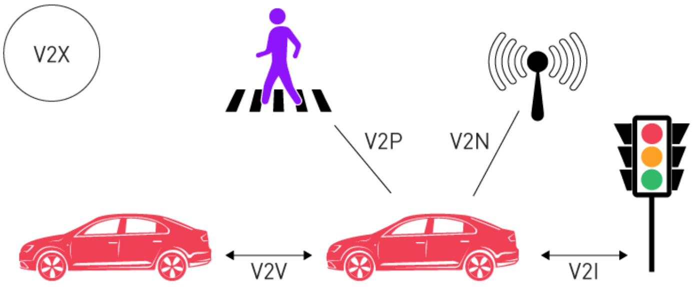

Figure 2.3: V2X communication diagram for autonomous vehicles

The reliance on interconnected systems exposes the Network Layer to several vulnerabilities:

MITM (Man in the middle) attackes : Attackers intercept and manupilate data exchanged between vehicles and infrastructures.
Denial of Service (DoS): Flooding the network with massive traffic can disrupt communication, potentially causing accidents or traffic issues.
Unauthorized access: Weak authentication procedures can allow hackers to infiltrate the network, gaining control of the vehicles functioning or can lead to stealing the data.

3. **Processing Layer:**
   Edge Computing and cloud infrastructures from the processing layer, where massive data streams are analyzed and processed .Edge computing processes time sensitive data locally, minimizing the latency and enhancing responses. The cloud computing handles large scaled data storage and complex data analysis, which support advanced features like machine learning for predictive maintenance and route optimization.[2][3]

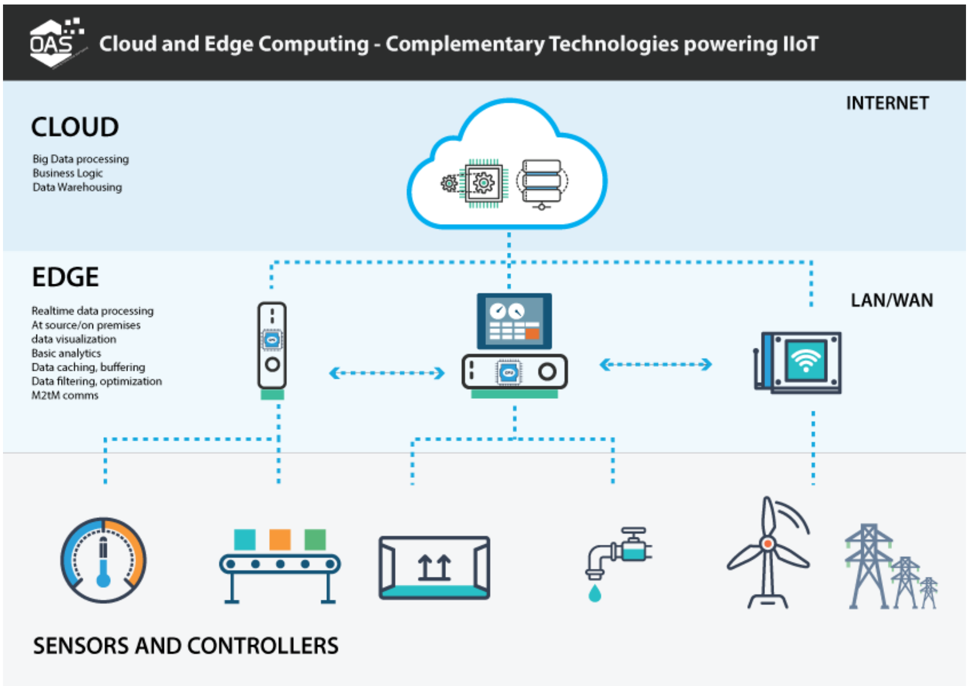

Figure 2.4: Edge and cloud computing architecture for IoT in AVs

4. **Application Layer:** This layer controls or also governs decision making algorithms, user interfaces, and vehicle control systems. It interprets processed data to activate safety features, optimize navigation, and improve user experience. Functions include adaptive cruise control, collision avoidance, and real-time route adjustments.

The seamless involements of these layers ensures that the autonomous vehicles can operate efficiently while navigating towards the complex traffic scenarios. However, each layer also presents potential security vulnerabilities that need to be addressed to maintain system integrity [1][3]

2.2 Applications of IoT

The application of IoT in autonomous vehicles shows various critical applications that increase the efficiency, safety, and overall performance of the vehicles. These applications have interconnected systems and real time data to improve the functionality of AVs:

1. **Real-Time Navigation:**
   GPS and sensor data enable accurate and precise route planning and obstacle avoidance for the vehicles.

2. **Traffic Management:**
   V2V and V2I communication enhance the traffic flow and reduce congestion in roades and the environments in.

3. **Predictive Maintenance:**
   Continuous monitoring of vehicle components helps predict failures and schedule timely maintenance.

4. **Passenger Safety:**
   Advanced Driver Assistance Systems improve safety of the vehicle and the passenger by detecting potential hazards and taking preventive measures for reducing.[2]

Chapter 3

Security Issues in IoT-Enabled Autonomous Vehicles

The IoT integration in AVs provides more advantages, it also shows these systems to a wide range of cybersecurity threats as well. The interconnected nature of IoT devices creates multiple entry points for this attacks, making AVs particularly vulnerable to exploitation. These vulnerabilities can compromise the safety, privacy, and operational trust, showing significant risks to passengers, infrastructure, and manufacturers.

3.1 GPS Spoofing and Navigation Attacks

GPS spoofing involves the transmission of false signals to confuse a vehicle's navigation system in autonomous vehicles, this can redirect the vehicle to a different locations, route planning that throw into confusion, or even cause accidents. GPS signals, which are weak and often unencrypted, are particularly capable to spoofing attacks.

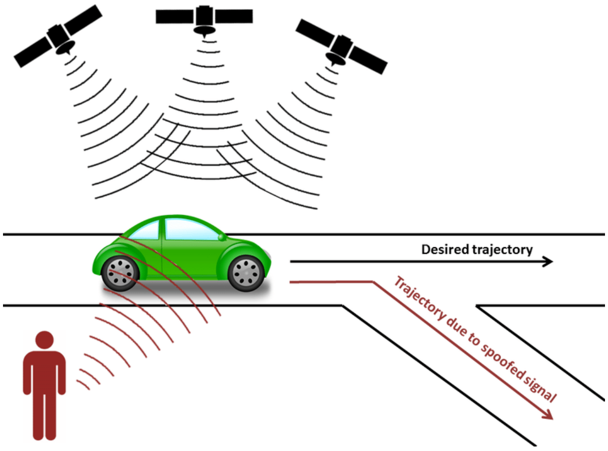

Figure 3.1: GPS Spoofing and Navigation Attacks

Attackers can transmit fake GPS signals that replace the orginal ones, misleading the vehicle's navigation system. This manipulation could result in detours, hijacking, or accidents. The risk will make worse in urban environments where signal reflections and interference are usual. To mitigate this risk, AVs need to incorporate unnecessary navigation systems and robust signal authentication precedures.[1]

3.2 Data Breaches and Unauthorized Access

Autonomous vehicles generate and transmit huge amounts of sensitive data, including personal information, vehicle diagnostics, and operational commands. This data can be vulnerable to breaches if communication channels and also the storage systems are poorly secured. Hackers can exploit vulnerabilities in wireless networks or cloud storage to gain unauthorized access which will lead to:

1. **Theft of Personal Data:**
   showing sensitive user data, such as location history and personal details.

2. **Unauthorized Vehicle Control:**
   Exploiting system flaws to take over the vehicle functioning.

3. **Corporate Espionage:**
   Accessing strong matching algorithms and businessinformation.

Weak encryption, weak access controls, and insecure APIs increase the likelihood of being in data breaches. advanced encryption and secure authentication systems are essential to protect AV data. [2]

3.3 Malware and Ransomware Attacks

Malware attacks take advantage of software vulnerabilities in AVs to compromise the functionality of the system. The Ransomware which is a subset of malware, can lock vehicle systems and can lead to demand of payment for the release of lock. Malicious code can manipulate essential systems like braking, acceleration, and steering, posing life threatening risks to the environment.

Figure 3.2: Jeep Cherokee hack in 2015

A main example is the Jeep Cherokee hack in 2015, where researchers remotely controlled vehicle functions by exploiting software vulnerabilities. Such incidents highlight the need for careful cybersecurity measures in AV software development. Regular security updates, trespass detection systems, and secure software design are critical to preventing malware attacks.

Chapter 4

Security Solutions

This section explores in-depth solutions for three critical issues: GPS spoofing, data breaches, and malware attacks, this section provides important strategies to show key cybersecurity challenges in IoT-enabled AVs. Implementing these solutions requires support among manufacturers and technology providers, to have attention need for a proactive and unified approach to cybersecurity. Additionally, as threats increases and evolves, updated research and innovation in AI-driven security systems, blockchain systems, and advanced encryption technologies and techniques will be crucial in place. These measures will ensure that IoT-enabled AVs remain safe, reliable, and resilient in an complex connected world.

4.1 Countermeasures Against GPS Spoofing

GPS spoofing manipulates the navigation systems of AVs by transmitting false signals, leading to fake and unsafe routes. This vulnerability can compromise vehicle safety and operational problems. To counter this threat, the following strategies are essential:

1. Signal Encryption and Authentication:
   Encrypting GPS signals ensures that only authenticated data from trusted sources is processed by the AV. Advanced cryptographic techniques, such as Public Key Infrastructure, validate the integrity of incoming signals to the system, making it harder for attackers to introduce counter attacks to the data.

2. Multi Sensor Fusion:
   Combining GPS data with inputs from other sensors, such as LiDAR, radar, and inertial measurement units, enhances flexibility against spoofing attacks. For instance, LiDAR and IMU data can confirm the vehicle's actual position even if GPS signals are compromised by the attackers. This strong matches minimizes reliance on any source of information.

3. Anomaly Detection Systems:
   AI-driven non consistent detection algorithms can identify non uniform GPS signals, such as sudden position jumps or signal variablity. These systems can doubt in safety protocols, such as switching to manual mode or engaging alternate navigation systems, when spoofing is done.

4. Interference-Resilient GPS Receivers:
   Advanced GPS receivers designed to filter out malicious signals can improve resilience. These receivers use frequency hopping and signal strength analysis to differentiate between legitimate and spoofed signals.

By carefuly considering these countermeasures, AVs can maintain accurate navigation, ensuring passenger safety and trust in autonomous systems.[1]

4.2 Mitigating Data Breaches and Unauthorized Access

Data breaches in IoT-enabled AVs shows a significant threats to user's privacy, security, and reputation of the company. The highly interconnected nature of AVs increases their chances of unauthorized access. The following measures can surpass these risks:

1. End-to-End Encryption:
   Securing data transmission through encryption protocols such as AES-256 ensures that sensitive information remains protected from involvement. This is crucial and critical for communications between vehicles and cloud servers.

2. Zero-Trust Architecture:
   The zero-trust model operates like on the principle of "never trust, always verify" requiring continuous authentication procedure and validation of every user, device, and system that attempting to access the network or the system. This approach minimizes the risk of unauthorized access of internal and external hands.

3. Multi-Factor Authentication (MFA):
   Implementing MFA strengthens the system by having multiple verification steps, such as biometrics scans, physical scan or tokens, and passwords. For example, AV operators could use fingerprint scanners or facial recognition in addition to old methods.

4. Blockchain for Data Integrity:
   Blockchain technology provides a decentralized and closed and protected framework for sending and receiving data. Each transaction or communication is recorded as a verifiable process, ensuring transparency and preventing unauthorized changes.

5. Regular Vulnerability Assessments:
   Regular security changes and timely arraingement of patches can address turn up vulnerabilities. Over the air (OTA) updates allow manufacturers to give main security improvements without requiring physical access to the vehicle.

These solutions not only protect sensitive user data but also strengthen the overall security of the AV ecosystem.[2]

4.3 Preventing Malware and Ransomware Attacks

Malware and ransomware attacks are among the most common threats to IoT-enabled autonomous vehicles, targeting critical systems and rendering them in operatable for use.

Malware can sneak into AVs through unsecured software updates, compromised third party applications on the system, or unsecured communication networks or channels. Once inside the system, it can manipulate main functions such as braking, steering, or acceleration, leading to severe safety risks for passengers and things or people in the road. Ransomware, a part or subject of malware, encrypts and locks critical vehicle systems, asking payment from users or train operators to restore functionality. These attacks can disrupt travel, disable the entire fleets, or stop logistics operations, causing economic and operational problems. The interconnected nature of AVs add to these risks, as a single infected vehicle can act as an entry point to replicate or called compromised an entire network of vehicles. understanding these threats requires a fast combination of security measures, real-time monitoring to ensure that AV systems remain strong against evolving malware attacks.[2][3]

Chapter 5

Conclusion

The use of IoT in autonomous vehicles brings many benefits, such as improved safety and efficiency. However, it also creates new security challenges, like GPS spoofing, data breaches, and malware attacks. To keep passengers safe and protect data, these issues need to be addressed. Solutions like authenticating GPS signals, encrypting data, and preventing malware can make autonomous vehicles more secure and trustful. Ongoing research and development in cybersecurity will play a key role in making these vehicles safer and more reliable for the future.

Chapter 6

Reference

1. Biswas, A. Wang, H.-C., 2023. Autonomous vehicles enabled by the integration of IoT, edge intelligence, 5G, and blockchain. Sensors, 23(4), p.1963. Available at: https://doi.org/10.3390/s23041963 .

2. Ud Din, I., Almogren, A. Rodrigues, J.J.P.C., 2024. AIoT integration in autonomous vehicles: Enhancing road cooperation and traffic management. IEEE Internet of Things Journal, 11(22), pp.35942-35949.Available at: https://doi.org/10.1109/JIOT.2024.3387927.

3. Nautiyal, A.P. Bathla, N., 2024. Revolutionizing urban mobility: Smart transportation vehicle-to-infrastructure communication – A review. International Journal of Future and Modern Research (IJFMR), 6(5), pp.1-10. Available at: https://doi.org/10.36948/ijfmr.2024.v06i05.27578.