Contents

[Introduction 2](#_Toc180429611)

[Functional Summary 3](#_Toc180429612)

[Assumptions 5](#_Toc180429613)

[Functional Requirements 6](#_Toc180429614)

[System Context 6](#_Toc180429615)

[Requirements List 6](#_Toc180429616)

[Technical Investigation 8](#_Toc180429617)

[CAN Bus Security and Odometer Data Authentication 8](#_Toc180429618)

[Vulnerabilities in the CAN Bus Protocol 8](#_Toc180429619)

[SecOC 9](#_Toc180429620)

[Encryption on the CAN bus 10](#_Toc180429621)

[Telematics Systems and Vehicle-to-Cloud Communication 11](#_Toc180429622)

[TLS 11](#_Toc180429623)

[Large-scale data management 11](#_Toc180429624)

[References 12](#_Toc180429625)

# Introduction

The goal of my project is to investigate mileage tampering and create a solution on how it can be prevented or minimised.   
  
The recent increase of complexity within vehicle electronics and systems has led to new opportunities for vehicle exploitation. One of the most popular forms of automotive fraud in the automotive market is odometer tampering also known as mileage fraud. Odometer tampering is the illegal practice of altering the mileage displayed on a vehicle’s odometer which results in the vehicle displaying a lower mileage than the vehicle has actually travelled.   
  
Mileage fraud effects many in the automotive space such as buyers in the second-hand market, vehicle manufactures and vehicle leasing companies. Mileage fraud can be used against vehicle manufacturers who have a warranty in place for their vehicles which includes a maximum mileage limit before the vehicle is out of warranty. This is a very relevant topic as more manufactures begin to sell electric cars that come with a warranty cover on the battery itself, such as Hyundai Ireland who grant warranty on their batteries for 8 years or up to 160,000 kms. Similarly with leased vehicles they will come with an annual mileage limit which typically falls between 8,000 and 15,000 kilometres and mileage fraud can be used to exceed this limit to avoid addiction charges.  
  
To combat the issues of mileage fraud there has been several regulations been put in place at both national and international levels. In the European Union one of the key directive addressing the issue is [EU Directive 2014/45/EU](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0045#:~:text=(25),by%20the%20Commission.). This Directive mandates that Member States are required to conduct periodic vehicle inspections along with recording the odometer readings at the time of the inspection. This solution is not a 100% fix to the problem and includes some gaps

* **Cross Border Sales:** One major problem with this solution is that mileage records are typically only accessible with a single Member State, this meaning once a vehicle is exported to a different state the records for that vehicle are often not transferred.
* **Technological Limitations:** With the current regulation in place it heavily relies on manual inspections which is not a sufficient solution to combat mileage blockers as they are and active device fitted to the vehicle which blocks mileage or blocks a percentage of mileage from being recorded.

The aim for this project is to address the problems with mileage tampering and to develop a solution to include a large amount of vehicle manufactures. I will attempt this by using Vector standards along with using Vector tools to develop my solution along with using Vector CANoe to demonstrate the solution to prevent mileage tampering.

# Functional Summary

What I plan to do to accomplish this project idea includes the following but that may be subject to change:

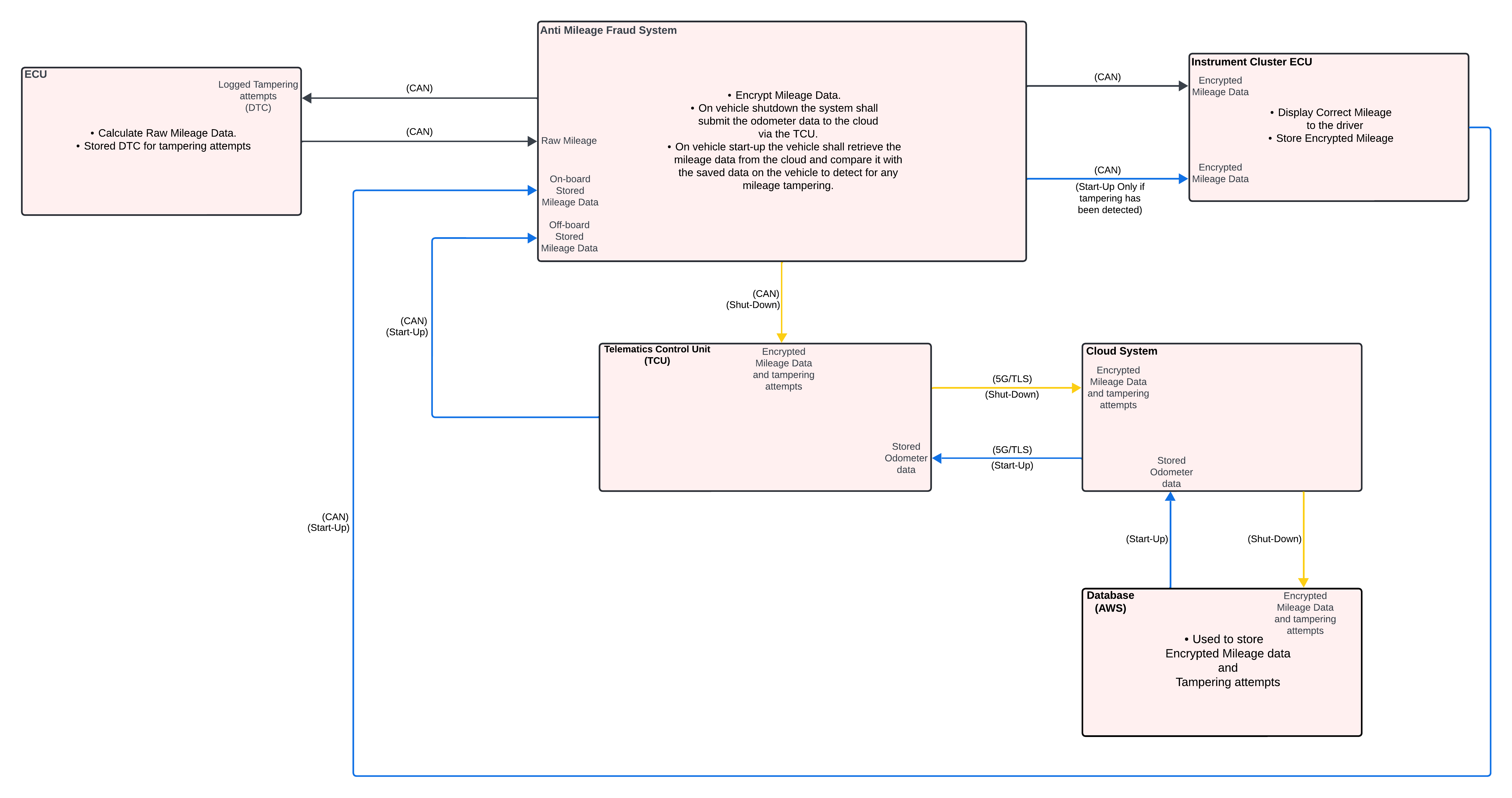
* **Research Impact of mileage blocker on industry and second-hand market.** 
  + Study how odometer fraud affects the used car market. Research the financial losses, consumer trust issues, and regulatory concerns.
  + Explore legal cases or studies documenting the extent of mileage tampering fraud.
* **Research the estimated usage of mileage blockers.**
  + Research the prevalence of mileage tampering devices (like blockers) across different regions or industries.
  + Explore how often these devices are used and in which types of vehicles e.g. high-value cars, commercial vehicles.
* Understand How Mileage Blockers Work.
  + **Hardware Research**: Investigate how mileage blockers interact with a vehicle’s systems e.g. CAN bus, ECUs.
  + Learn about the software protocols that can interfere with odometer readings.
  + **Vehicle Systems**: CAN bus communication, and ECU architecture.
* Research the software tools what I may need to research and develop this project.
  + Vector tools.
  + Cloud tools.
  + Database tools.
* Development:
  + **Mileage Tracking:** The system will continuously monitor and display accurate odometer readings using data collected from the vehicle’s ECUs.
  + **Tamper Detection:** The system will detect any attempt to modify or block the odometer data. It will log all tampering attempts and store these logs securely.
  + **Secure Data Storage:** Odometer data will be stored both onboard and offboard, ensuring that the mileage data is tamper proof and can be verified at any time.
  + **Data Integrity Verification:** The system will provide mechanisms to verify the authenticity of odometer data. In case of a discrepancy, the offboard stored data will serve as a reference to verify legitimate mileage.
  + **Reporting of Tampering Attempts:** Any tampering or inconsistency in mileage data will trigger alerts and generate logs that can be accessed for reporting.

# Assumptions

* **Vehicle Compatibility:** This project assumes that the vehicle models targeted for testing have standardised communication protocols such as OBD-II and CAN bus, which will allow for easy access to odometer data.
* **Regulatory Compliance:** It is assumed that the system will be designed within the bounds of current automotive regulations regarding data logging and tamper protection.
* **Network Connectivity:** The offboard storage system assumes stable internet connectivity for transmitting odometer data securely.
* **Tamper Detection Mechanisms:** It is assumed that mileage tampering can be detected based on either change in the communication patterns of the vehicle’s ECUs or the failure of the system to log mileage data at regular intervals.
* **Onboard Storage Capacity:** It is assumed that the onboard storage capacity in the vehicle’s hardware is sufficient to store encrypted odometer data locally.

# Functional Requirements

## System Context



## Requirements List

* **Data Management:** 
  + The system shall read odometer data from the vehicle's ECU periodically.
  + The system shall store odometer data onboard in encrypted form to prevent unauthorized modifications.
  + The system shall transmit odometer data to offboard storage after each vehicle shutdown or at regular intervals.
* **Tamper Detection:** 
  + The system shall detect any attempt to manipulate odometer readings or disrupt the communication flow between the ECU and the odometer.
  + The system shall log all tampering attempts in a secure and non-tampering format.
  + The system shall detect any tampering attempts and log such attempts via onboard diagnostics and offboard storage.
* **Data Integrity:**
  + The system shall use encryption and cryptographic signatures to verify the integrity of odometer data stored onboard and offboard.
  + The system shall compare onboard odometer data with offboard stored data to verify its authenticity upon each vehicle startup.
* **Security:**
  + The system shall use industry standard encryption algorithms for storing data.
  + The system shall employ user authentication to access mileage data logs e.g. data is only accessible to main dealers.

# Technical Investigation

## CAN Bus Security and Odometer Data Authentication

### Vulnerabilities in the CAN Bus Protocol

The CAN (Controller Area Network) bus is the primary communication protocol used in modern vehicles to allow communication between various ECUs (Electronic Control Units). CAN is lightweight, efficient and cheap the protocol has many vulnerabilities, particularly when it comes to security. CAN was designed in the 1980s with reliability and real time communication in mind so now as modern vehicle technology grows CAN lacks the built in support for cybersecurity features.

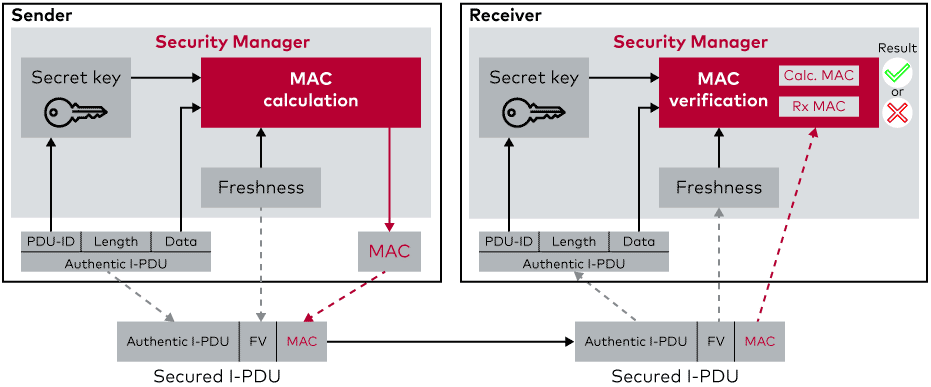
In this investigation I will focus on the key vulnerabilities of the CAN protocol that can be exploited for mileage fraud.

* **Lack of Authentication:** The CAN protocol does not authenticate messages that are being send around the CAN bus, meaning any ECU on the bus can send and receive messages without verifying their where they came from. This is how false data can be injected such as false mileage readings.
* **Message broadcast on CAN:** Any ECU that is connected to the CAN bus will receive every message broadcasted over the network. This opens the opportunity for tapping into the CAN bus and would allow for eavesdropping, message spoofing and injection of false data on the CAN bus. For example, an attacker could broadcast manipulated mileage data that is accepted by the odometer without the system noticing.
* **Message Tampering:** Since CAN messages lack any form of integrity checks, it is possible to modify CAN messages while they are in transit. An attacker could intercept a message containing odometer data and modify it to reflect a lower mileage before it reaches the destination ECU.
* **Replay Attack:** CAN is vulnerable to replay attacks, this is when a previously recorded message is rebroadcasted onto the network to manipulate something like the odometer reading.

(Understanding CAN Bus Vulnerabilities and How Blockchain Can Amplify Security, 19-09-24 )

### SecOC

SecOC (Secure Onboard Communication) was first introduced by AUTOSAR in 2015 to provide secure onboard communication for automotive systems that use CAN and CAN-FD networks. Over the years the AUTOSAR (Automotive Open System Architecture) standard has continued to refine SecOC to improve its functionality and integration into modern vehicles along with aligning with continuously evolving automotive cybersecurity standards such as ISO/SAE 21434.

SecOC is a security protocol designed to ensure the integrity and authenticity of messages exchanged between ECUs on the CAN bus network. SecOC doesn’t include encryption but it is highly effective at protecting data from tampering and replay attacks, both of which are critical concerns when it comes to securing odometer data.  
  
  
Figure 1 (Secure Onboard Communication, no date)

SecOC uses MACs (Message Authentication Codes) to detect any modification of messages. Each CAN message is appended with a MAC which is calculated using a secret key shared between ECUs. These keys must be distributed among each ECU that intends to receive the data from the sender. The necessary input values such as secret key and freshness values are stored in the Security Manager (Secure Onboard Communication, no date).

SecOC verifies the authenticity of the data by ensuring that it originates from a legitimate ECU, this prevents any attempt at injecting incorrect mileage values into the system.

Another security method implemented into SecOC is the use of freshness values. This helps stop the use of a replay attack. A replay attack occurs when a valid data transmission is fraudulently repeated to mislead the system, for example in the case of this project it would be used to send an older and lower mileage reading.  
*This is done by the SecOC module on the sender side creating a secured I-PDU by adding Authentication Information to the outgoing Authentic I-PDU. When using the Freshness counter, the Freshness counter should be incremented by the freshness manager prior to providing the Authentication Information to the receiver side.*

*On the receiver side, the SecOC module checks the freshness and authenticity of the authentic I-PDU by verifying the Authentication information that has been appended by the sending side SecOC Module. To verify the authenticity and freshness of an Authentic I-PDU, the secured I-PDU provided to the receiving side SecOC should be the same secured I-PDU provided by the sending side SecOC and the receiving side SecOC should have knowledge of the Freshness Value used by the sending side SecOC during creation of the Authenticator.* (Specification of Secure Onboard Communication Protocol, 30-11-2020 ).

SecOC is a lightweight solution to providing data integrity across ECUs where bandwidth and processing power is limited. (Specification of Secure Onboard Communication Protocol, 30-11-2020 ).

### Encryption on the CAN bus

The CAN bus network was designed without considering the need for cybersecurity, it also lacks native encryption leaving it vulnerable to data interception such as tampering and replay attacks. I will explore the feasibility and challenges of introducing encryption into CAN communications with a focus on protecting data like mileage readings.

1. **CAN Bus Architecture and Constraints:**The CAN protocol is highly efficient for real time communication with its simple architecture designed to prioritise message delivery as quick as possible. However this also introduces constraints:

* **Frame Size:** The CAN frames are limited to 8 bytes of data which makes for a significant challenge to introduce encryption. Encryption algorithms generally add overhead in the form of initialisation vectors, padding or keys which may result in exceeding the available payload of a single message. This would then introduce the need for message fragmentation.
* **Low Latency:** CAN is designed for low latency communication between ECUs. Encryption introduces overhead which could delay the transmission and processing of the data.

1. **Lightweight Cryptographic Algorithms and Integration:**

Regarding the limitations of the CAN bus, lightweight cryptographic algorithms may be more appropriate than standard cryptographic algorithms such as AES-256. AES-128 would be a good candidate due to its lower computational complexity compared to AES-256 but still being able to provide a high level of security.  
  
Encryption on the CAN bus requires careful integration to avoid breaking the fundamental principle of the protocol. The following aspects need to be considered:

* **Key Management:** Securely distributing and managing encryption keys is an essential. Key distribution schemes are also important to decide such as Symmetric key encryption for AES.
* **Encryption Placement:** Determining wherethe encryption should be applied in the CAN message is also important. Deciding whether the whole message should be encrypted or just the portion that included sensitive data such as mileage data.

1. **CAN-FD as an Alternative:**

Using CAN-FD as an alternative to standard CAN would allow for a lot more flexibility on the encryption side. CAN-FD allows for a larder frame size which is up to 64 bytes. This larger frame size would give more room for encryption overhead making it more suitable for implementing encryption while still maintaining compatibility with legacy CAN systems.

1. **The Impact of Encryption on the CAN Bus Performance:**

Implementing encryption in the CAN bus system will without a doubt have an impact on performance such as transmission latency, CPU load on ECUs and network bandwidth.

* **Latency and Real time Communication:**

Encryption increased message processing time and since CAN networks prioritise real time communication encryption may potentially lead to some delays. It will be important to investigate the affect that the added latency may have on the network.

* **Simulation of encrypted CAN traffic:**

Using software simulation I will evaluate how different encryption algorithms impact latency on the network.

* **Bandwidth Overhead:**

Encryption will add overhead in terms of addition data fields like initialisation vectors and padding which will reduce the effective payload capacity of CAN frames. This means that more frames may be required to transmit the same amount of data which may increase the overall bandwidth usage.

* **ECU Resource Utilisation:**

ECUs in vehicles have limited computing power, memory and power resources. Encrypting and decrypting messages can be expensive for these systems particularly for light weight ECUs.

## Telematics Systems and Vehicle-to-Cloud Communication

### TLS

### Large-scale data management

# References

Understanding CAN Bus Vulnerabilities and How Blockchain Can Amplify Security   
( 19-09-24 ) | Medium. <https://medium.com/@chaincom/understanding-can-bus-vulnerabilities-and-how-blockchain-can-amplify-security-a58388bf1fb4>. ( Accessed: 18-10-2024 )

Specification of Secure Onboard Communication Protocol ( 30-11-2020 ) | AUTOSAR. Available at: <https://www.autosar.org/fileadmin/standards/R20-11/FO/AUTOSAR_PRS_SecOcProtocol.pdf>. ( Accessed: 18-10-2024 )

Secure Onboard Communication ( no date ) | Vector. Available at: <https://www.vector.com/us/en/products/solutions/safety-security/automotive-cybersecurity/security-manager/#c212393>. ( Accessed: 18-10-2024 )