Secure Data Transmission in ECU Data Acquisition Systems based on MQTT and TLS

João Paulo Bedretchuk, Tiago Porsch Dopke, Thiago Martins, Giovani Gracioli, Anderson Wedderhoff Spengler
Software/Hardware Integration Lab (LISHA)
Federal University of Santa Catarina (UFSC)
{jpbedretchuk, porsch, tmartins, giovani, anderson}@lisha.ufsc.br

***Abstract*—Electronic Control Units (ECUs) play a critical role in modern automotive systems, providing data for performance analysis, calibration, and validation. Traditional commercial acquisition tools are widely used but often limited by high costs, dependency on high-performance computers, and restricted integration with modern cloud and edge-processing infrastructures. To overcome these limitations, we developed the Intelligent Acquisition and Analysis System for ECUs (IASE), an embedded platform designed for real-time data acquisition and calibration. This paper presents a secure communication architecture for the second generation of the system (IASE v2), enabling remote connectivity through 4G networks while ensuring confidentiality, integrity, and authenticity of transmitted data. The architecture integrates MQTT over TLS with per-device certificates and mutual authentication (mTLS). We validate the solution through experiments under real-world 4G conditions, demonstrating reliable performance, secure Over-The-Air (OTA) updates, and message delivery consistency. Results show that the proposed approach ensures robust data security without compromising scalability, making it suitable for modern automotive testing environments.**

Keywords—ECU Data Acquisition, MQTT, TLS, Mutual Authentication, Embedded Automotive Systems.

I. Introduction

The development of vehicles in the automotive industry largely follows the V-model of production, in which each project stage is validated until the final integration of the prototype [1], [2]. In the testing and validation phase, Electronic Control Units (ECUs) provide essential data on performance, calibration, and emissions. For this purpose, manufacturers rely on commercial data acquisition solutions provided by companies such as ETAS, Vector, ATI, and Bosch. Although consolidated in the sector, these tools present relevant limitations: high cost, dependence on external high-performance computers, and restrictions on integration with modern processing architectures and remote servers [3], [4], [5], [6].

To address these limitations, previous works introduced the Intelligent Acquisition and Analysis System for ECUs (IASE) [7], a low-cost embedded platform for real-time data acquisition and calibration, supporting integration with remote servers and mobile interfaces. The first generation of the system implemented automotive communication protocols, standardized data handling, and modular firmware based on state machines [8]. In its evolution to IASE v2, new hardware resources were added, along with support for Over-The-Air (OTA) updates and remote configuration of experiments, broadening its applicability in different testing scenarios.

With the use of mobile connectivity, the need arose to ensure secure communication between the embedded platform and the cloud server. In mobile networks such as 4G, data transmission can be exposed to threats such as spoofing, replay, and man-in-the-middle attacks [9], [10]. This paper proposes a secure communication architecture for ECU data acquisition systems, based on MQTT over TLS with unique per-device certificates, enabling mutual authentication (mutual TLS – mTLS). The solution ensures confidentiality, integrity, and authenticity of the transmitted data, while maintaining the lightness and scalability required in automotive embedded systems.

The remainder of this paper is organized as follows. Section II reviews related work and the state of the art in secure communication for automotive systems. Section III describes the proposed architecture. Section IV discusses the communication workflow and presents results obtained in preliminary tests. Section V concludes the paper and outlines future work.

II. Background

Lightweight protocols such as MQTT have been widely adopted for IoT and vehicular applications due to their scalability and low overhead [11]. Recent studies highlight the use of MQTT over TLS to provide confidentiality and integrity while maintaining acceptable performance in constrained devices [12], [13].

Mutual TLS (mTLS) has also been investigated as a mechanism for device-level authentication, particularly in large-scale deployments requiring secure key and certificate management [14]. However, integration of mTLS in automotive data acquisition platforms remains limited.

Compared to these approaches, the IASE v2 system represents an advance by combining secure MQTT/TLS communication, certificate-based authentication, OTA update mechanisms, and a complete server-side infrastructure tailored to ECU data acquisition scenarios.

III. System Architecture

The proposed architecture ensures secure and reliable data transmission between the embedded acquisition platform and a remote server during ECU testing and validation. Fig. 1 illustrates the overall structure of the system, composed of the

IASE v2 board, the 4G communication channel, and the server infrastructure.

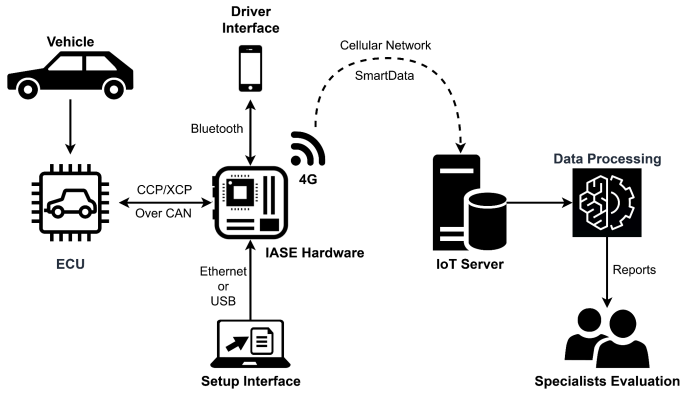

Fig. 1. IASE v2 overall structure

A. Embedded Platform

The IASE v2 board integrates an embedded processor and a 4G modem, enabling direct communication with a remote server without external computers. Each device is provisioned with a unique digital certificate and private key, issued by an internal public key infrastructure (PKI). These credentials are used to authenticate the device and establish secure connections through mutual TLS (mTLS). The firmware also supports Over-The-Air (OTA) updates, allowing remote installation of new experiments, firmware versions, and updated certificates.

B. Server Infrastructure

The server side is implemented using the Django framework and a MySQL database for storing firmware versions, certificates, experiment configurations, and update history. An Nginx reverse proxy provides an additional security layer by enforcing mTLS authentication before forwarding requests to the Django server. This setup ensures that both the client and the server authenticate each other before any data exchange. The server also manages certificate distribution, update policies, and experiment association to specific boards, guaranteeing that each device receives the correct software and configuration.

C. Secure Communication Layer

Communication between the IASE board and the server is based on the MQTT protocol over TLS 1.3. MQTT provides a lightweight publish/subscribe mechanism, which is particularly suitable for resource-constrained embedded systems and scenarios requiring efficient data transmission. By combining MQTT with TLS and unique per-device certificates, the system ensures:

- Confidentiality, through end-to-end encryption of messages.
- Integrity, by protecting data against tampering during transmission.
- Authenticity, via mTLS authentication where the client proves its identity with a certificate and the server validates it using the CA.

The complete mTLS authentication workflow is shown in Fig. 2. In this process, the server first sends its certificate to the client for validation. The client then presents its unique device certificate, which is verified by the server. The MQTT over TLS channel is established if, and only if, both sides are authenticated.

D. Data Exchange

It is necessary that all the data arrives in-order and once-and-only-once, however, MQTT QoS 2 is not an option for the volume of data and amount of MQTT messages the IASE v2 firmware sends every second, as it would need an extremely low latency of under 4 ms.

In order to achieve the guarantees and speeds necessary, the data exchange was implemented using MQTT QoS 1 (guarantees that the message will be received at least once) and an embedded sequence number on each message. With these two decisions, the receiver is able to process each message once-and-only-once and in-order.

E. OTA Update and Certificate Management

The OTA mechanism supports secure updates of firmware and certificates. Devices periodically check for new versions, download validated binaries through secure endpoints, and log update operations in the server database. By using HTTPS requests protected by mTLS, the architecture guarantees that only authenticated devices receive authorized updates.

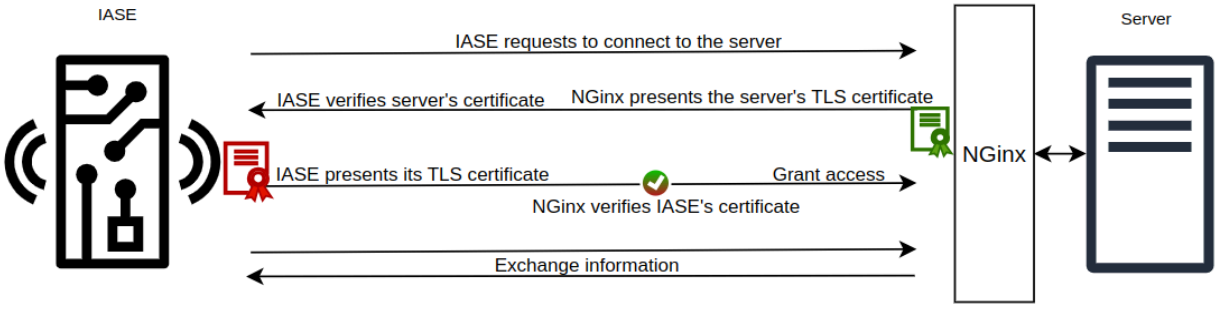

Fig. 2. Mutual TLS (mTLS) authentication flow between the IASE board and the remote server.

F. *Security Guarantees*

By integrating MQTT, TLS, and per-device certificates, the architecture protects the communication channel against common network threats such as spoofing, replay attacks, and man-in-the-middle (MITM) attacks. Furthermore, the OTA update process guarantees that only authenticated and authorized devices can download new firmware or certificates, preventing unauthorized software from being installed in the embedded platform.

IV. Results and Validation

To validate the proposed architecture, a series of experiments were conducted using the IASE v2 board connected to a remote server over a 4G mobile network. Each device was provisioned with a unique certificate and private key, enabling secure authentication with the server through mutual TLS (mTLS). The tests aimed to evaluate the impact of the security layer on communication performance, resource usage, and reliability under real-world conditions.

A. *Experimental Setup*

The evaluation environment consisted of:

- Client side: IASE v2 board with embedded processor, 4G modem, and firmware supporting MQTT over TLS.
- Server side: Django framework with MySQL database, fronted by an Nginx reverse proxy enforcing mTLS authentication.
- Network: Commercial 4G mobile network, subject to typical latency and bandwidth variations.

The experiments included the transmission of ECU acquisition data encapsulated in MQTT messages, as well as OTA updates of firmware and certificates.

B. *Performance Evaluation*

Fig. 3 shows how, when using HTTP, the message sending queue kept growing when under a spotty 4G connection and a full experiment generating a lot of data. Under identical conditions, the proposed MQTT over TLS system successfully handled high-throughput data streams, demonstrating stable queue management despite the additional TLS overhead. This difference arises because HTTP incurs substantial overhead from repeated request–response cycles and full header transmission, making it unable to recover efficiently from short periods of low bandwidth or intermittent connectivity. As a result, the queue grows continuously and cannot drain fast enough to sustain real-time throughput.

By contrast, MQTT's lightweight framing, persistent sessions, and asynchronous publish–subscribe model enable rapid recovery after transient link degradation. Although brief spikes in the MQTT queue occur due to the small size of individual messages, the protocol drains the backlog quickly once the connection stabilizes. These results indicate that MQTT over TLS provides significantly better resilience and efficiency than HTTP in variable 4G environments, making it more suitable for continuous ECU data acquisition.

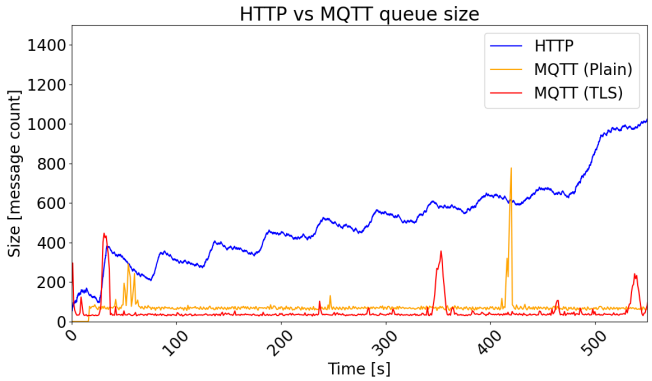

Fig. 3. Message queue evolution under HTTP, plain MQTT, and MQTT with TLS in a 4G environment.

By contrast, MQTT's lightweight framing, persistent sessions, and asynchronous publish–subscribe model enable rapid recovery after transient link degradation. Although brief spikes in the MQTT queue occur due to the small size of individual messages, the protocol drains the backlog quickly once the connection stabilizes. These results indicate that MQTT over TLS provides significantly better resilience and efficiency than HTTP in variable 4G environments, making it more suitable for continuous ECU data acquisition.

Fig. 3 also shows that plain MQTT exhibits larger queue peaks than MQTT over TLS. This behavior results from the lower protocol overhead of plain MQTT, which enables a higher maximum throughput. Under the same data-generation rate, this higher efficiency causes the queue to grow more rapidly during brief 4G interruptions. With TLS, the added encryption overhead slightly reduces the effective transmission rate, leading to slower queue accumulation and smaller peaks.

C. *Reliability Tests*

The IASE v2 firmware saves a local copy of every single byte of data it acquires from a vehicle's ECU. This allows the byte-by-byte verification of everything that the server received.

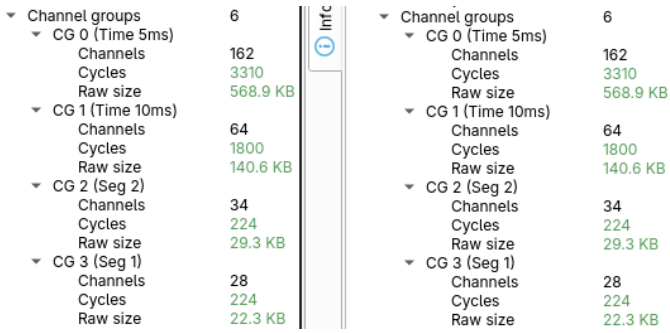

Fig. 4. Comparison of the number of data cycles from a server-generated data file and a locally-generated data file.

Tests were run where the 4G connection was unstable, or even unavailable for some period of time. In all test scenarios, the server-generated data files were byte-to-byte identical to

locally stored copies, confirming lossless and reliable data transmission even under unstable 4G connectivity, as can be seen on Fig. 4.

V. Conclusion and Future Work

This paper presented a secure communication architecture for the IASE v2 platform, enabling reliable ECU data acquisition over mobile networks. By combining MQTT, TLS 1.3, and per-device mTLS authentication, the proposed system ensures confidentiality, integrity, and authenticity of ECU data, while maintaining the lightweight operation required in embedded automotive systems.

Experimental results demonstrated that the architecture provides robust message delivery and OTA update security under real-world 4G network conditions, with negligible performance degradation compared to unsecured communication.

Future work will focus on extending the validation to 5G and Wi-Fi 6 networks, and scaling the certificate management infrastructure for large fleets of test vehicles.

Acknowledgment

This work was supported by Fundação de Desenvolvimento da Pesquisa - Fundep Mover/Linha V 27192.02.INT01/2022.01-00. We would like to thank Renault do Brasil for the support of this project.

References

[1] K.-H. Dietsche e K. Reif, *Automotive Handbook*, 11th Edition, Revised and Extended. Karlsruhe: Bosch, 2022.

[2] J. Weber, *Automotive Development Processes: Processes for Successful Customer Oriented Vehicle Development*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. doi: 10.1007/978-3-642-01253-2.

[3] B. Du e L. Sterpone, "An FPGA-based testing platform for the validation of automotive powertrain ECU", em *2016 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*, set. 2016, p. 1–7. doi: 10.1109/VLSI-SoC.2016.7753553.

[4] J. Andert, S. Klein, R. Savelsberg, S. Pischinger, e K. Hameyer, "Virtual shaft: Synchronized motion control for real time testing of automotive powertrains", *Control Engineering Practice*, vol. 56, p. 101–110, nov. 2016, doi: 10.1016/j.conengprac.2016.08.005.

[5] D. Guse, J. Andert, S. Walter, e N. Meyer, "Next Level of Testing - Extended Frontloading through Latency-optimized EiL Test Benches", *MTZ Worldw*, vol. 81, nº 10, p. 44–49, out. 2020, doi: 10.1007/s38313-020-0278-7.

[6] "VH4110 - IoT Enabler Manual", Vector Informatik GmbH. Acesso em: 27 de setembro de 2025. [Online]. Disponível em: https://www.vector.com/br/pt/download/vh4110-iot-enabler-manual

[7] J. P. Bedretchuk, S. Arribas García, T. Nogiri Igarashi, R. Canal, A. Wedderhoff Spengler, e G. Gracioli, "Low-Cost Data Acquisition System for Automotive Electronic Control Units", *Sensors*, vol. 23, nº 4, p. 2319, jan. 2023, doi: 10.3390/s23042319.

[8] S. Arribas, J. Bedretchuck, A. Spengler, e T. Nogiri, "Desenvolvimento de Software Embarcado para Aquisição e Calibração de ECUs Automotivas", em *Blucher Engineering Proceedings*, Blucher Proceedings, set. 2022, p. 50–60. doi: 10.5151/simea2022-PAP10.

[9] B. Bhushan, G. Sahoo, e A. K. Rai, "Man-in-the-middle attack in wireless and computer networking — A review", em *2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall)*, set. 2017, p. 1–6. doi: 10.1109/ICACCAF.2017.8344724.

[10] M. Conti, N. Dragoni, e V. Lesyk, "A Survey of Man In The Middle Attacks", *IEEE Communications Surveys & Tutorials*, vol. 18, nº 3, p. 2027–2051, 2016, doi: 10.1109/COMST.2016.2548426.

[11] "Miller, C. and Valasek, C. (2015) Remote Exploitation of an Unaltered Passenger Vehicle. Black Hat USA. - References - Scientific Research Publishing". Acesso em: 27 de setembro de 2025. [Online]. Disponível em: https://www.scirp.org/reference/referencespapers?referenceid=2387001

[12] Z. Kegenbekov e A. Saparova, "Using the MQTT Protocol to Transmit Vehicle Telemetry Data", *Transportation Research Procedia*, vol. 61, p. 410–417, jan. 2022, doi: 10.1016/j.trpro.2022.01.067.

[13] F. Chen, Y. Huo, J. Zhu, e D. Fan, "A Review on the Study on MQTT Security Challenge", em *2020 IEEE International Conference on Smart Cloud (SmartCloud)*, nov. 2020, p. 128–133. doi: 10.1109/SmartCloud49737.2020.00032.

[14] I. L. B. M. Paris, M. H. Habaebi, e A. M. Zyoud, "Implementation of SSL/TLS Security with MQTT Protocol in IoT Environment", *Wireless Pers Commun*, vol. 132, nº 1, p. 163–182, set. 2023, doi: 10.1007/s11277-023-10605-y.