Embedded Selforganizing Systems

Multi-Layer Hybrid Encryption: A Novel Approach for Enhanced V2X Security

Hasan Aljzaere
Faculty of Computer Science,
Professorship of Computer Engineering
Technische Universität Chemnitz
Chemnitz, Germany
hasan.aljzaere@informatik.tu-chemnitz.de

Amr Gad
Faculty of Computer Science,
Professorship of Computer Engineering
Technische Universität Chemnitz
Chemnitz, Germany
amr.gad@s2021.tu-chemnitz.de

Omar Elsayed
Faculty of Computer Science,
Professorship of Computer Engineering
Technische Universität Chemnitz
Chemnitz, Germany
omar.elsayed@s2021.tu-chemnitz.de

Wolfram Hardt
Faculty of Computer Science,
Professorship of Computer Engineering
Technische Universität Chemnitz
Chemnitz, Germany
hardt@cs.tu-chemnitz.de

***Abstract*—In recent years, the pervasive integration of technology in various domains has opened up new avenues for cybersecurity threats and data breaches. The automotive industry, in particular, has experienced significant impacts from technological advancements, most notably with the advent of vehicle-to-everything (V2X) communication. Ensuring a secure framework for data exchange among vehicles has emerged as a crucial concern in the realm of automotive cybersecurity. This manuscript presents a comprehensive examination of a novel hybrid-encryption-based secure data exchange system, accompanied by a proposed implementation for an automated emergency reporting system in the event of a car accident.**

Keywords—hybrid encryption, automotive cybersecurity, V2X, MQTT, data access control

I. Introduction

The growing reliance on technology has rendered our digital data increasingly susceptible to cyber-attacks. This vulnerability extends to the automotive industry, which has witnessed numerous prominent incidents in recent years. For instance, in 2022, Nissan North America fell victim to a data breach [1], while in 2015, hackers successfully commandeered a car's steering wheel while it was in motion on a highway [2]. These occurrences not only imperil customers' personal data but also jeopardize their physical safety. To address these challenges, the automotive industry has adopted enhanced security measures, such as hybrid encryption protocols, vehicle-to-everything (V2X) communication protocols [3], message queuing telemetry transport (MQTT), and data access control [4]. These measures have demonstrated effectiveness in safeguarding vehicles against cybersecurity threats and shielding users from identity theft, fraud, and other malicious activities. It is noteworthy that such attacks not only compromise digital personal data but also endanger the physical well-being of drivers, underscoring the criticality and significance of cybersecurity. This has resulted in an increased interest in the security field. Figure 1 provides a categorization of automotive cyberattacks in 2020 and 2021, indicating a higher prevalence of communication channel threats and vehicle data threats compared to other types of threats.

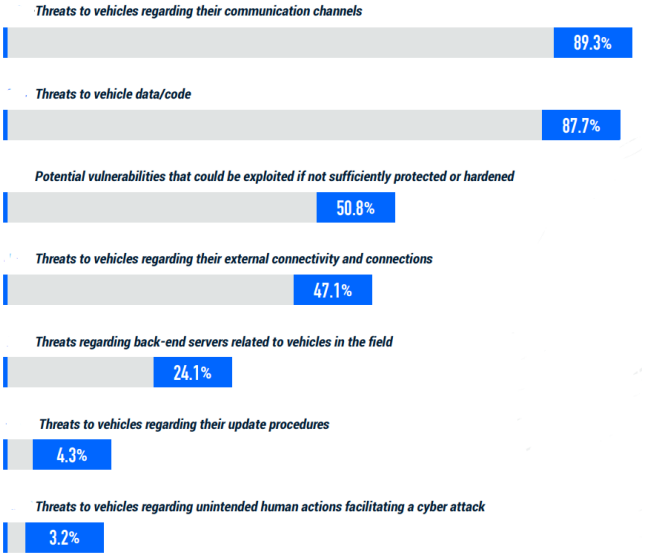

Figure 1. 2020-2021 Cyber Incidents Categorized [5]

Alternative approaches to securing vehicle communication include the utilization of blockchain technology for data authentication and security [6]. Additionally, employing blockchain-as-a-service for highly secure data transmission and storage can be considered. Furthermore, the integration of artificial intelligence (AI) algorithms for the detection and prevention of malicious network activity can enhance the security of vehicle communication. Moreover, secure multiparty computation (SMCs) can be employed to securely process and store data, thereby offering supplementary protection against malicious

attacks. Lastly, leveraging distributed ledgers, such as the Hyperledger Fabric, to maintain an immutable record of all transactions can further fortify the security of vehicle communication.

II. CONCEPT

In our architectural design, the vehicle and ambulance serve as network nodes that can establish a connection through an intermediary component referred to as the broker. This broker utilizes the Message Queuing Telemetry Transport protocol (MQTT) over Secure Socket Layer (TLS) to facilitate secure message exchange and filtering. Consequently, each node must be designated as one of the following:

- **Publisher:** This node is responsible for transmitting data based on predefined circumstances derived from the diagnostic module in the Electronic Control Unit (ECU).
- **Subscriber:** This node is configured to actively await data from a specific publisher.
- **Publisher/Subscriber:** This type of node possesses the capability to both send and receive data throughout the system's life cycle.

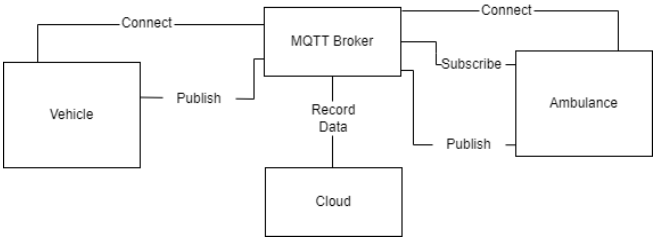

Figure 1. System Overview

Figure 2 shows the system's communication nodes connected to a broker, and the role of each node, whether it is a publisher, subscriber, or both. With the vehicle as publisher and the ambulance as publisher/subscriber.

MQTT assumes a pivotal role as the fourth node in the system, complementing the sender, receiver, and cloud components. It operates as a routing point within the architecture, facilitating seamless communication and data exchange across the network infrastructure. By leveraging the Vehicle-to-Everything (V2X) network, contributing to the seamless integration of vehicular systems. The utilization of MQTT allows for real-time data transfer, event-driven interactions, and reliable message delivery. This architecture underscores the importance of MQTT in enabling effective and robust vehicle communication within the V2X ecosystem.

A. System Security

Important security objectives have to be considered to provide secure communication over a computer network.

Integrity: Transport Layer Security (TLS) is a cryptographic protocol that provides secure communication over the internet. It provides data integrity by encrypting the data passed between two systems using one or more encryption algorithms. TLS uses a hybrid encryption approach, in which it combines symmetric and asymmetric encryption algorithms to encrypt and decrypt data. Symmetric encryption algorithms use a single key to both encrypt and decrypt data, while asymmetric encryption algorithms use two different keys, one for encryption and one for decryption. TLS also implements digital signatures, message authentication codes (MACs), and hash functions to ensure that the data being transmitted is both authentic and unmodified.

Confidentiality: Cloud security is an immensely important issue, and organizations must ensure that all data stored in the Cloud is secure and only accessible by authorized personnel and entities. To ensure data security, organizations must employ mechanisms such as identity and access management (IAM) and Transport Layer Security (TLS).

IAM is a system of identity identification, authentication, authorization, and accountability, designed to grant or deny access to resources based on the identity of the user. IAM typically involves the use of usernames and passwords and can also include biometric authentication and two-factor authentication. IAM also includes the restriction of access to certain services, resources and applications to specific user groups.

TLS works by establishing an encrypted connection between two systems, and then encrypting the data sent between them. TLS uses public and private keys, allowing the two systems to authenticate each other and share a secret key. This key is then used to encrypt the data before being sent, ensuring confidentiality, and preventing malicious actors from accessing the data. Once the data is received, the receiver can use the shared secret key to decrypt the data. TLS helps to ensure data privacy and integrity and is especially important for the security of Cloud-based applications.

Authentication: The authentication process of a vehicle in cloud-based systems is essential to guarantee that the data is sent to the exact vehicle. To handle this, the proposed system suggests using the vehicle identification number (VIN) as a unique value that is sent automatically whenever the vehicle tries to send a request to the cloud. Additionally, to secure the data, the proposal recommends using Transport Layer Security (TLS) with Advanced Encryption Standard 256-bit (AES-256) and RSA for hybrid encryption. AES is a symmetric-key encryption algorithm with only one secret key, which makes it suitable for encrypting large amounts of data. However, it is vulnerable to brute-force attacks. RSA, on the other hand, is an asymmetric encryption algorithm with two keys, one public and one private, which offers more security than AES but is slower and more complex. By employing AES and RSA in a hybrid encryption process, the system can take advantage of the best of both encryption methods.

The proposed system benefits from utilizing Transport Layer Security (TLS) due to its combination of security and efficiency [7]. To achieve enhanced security, a hybrid encryption approach employing AES-256 and RSA is deemed effective [8]. AES (Advanced Encryption Standard) offers exceptional data encryption capabilities as a symmetric-key encryption algorithm, using a single secret key for all data blocks. This makes AES well-suited for

encrypting large volumes of data. However, its simplicity renders it vulnerable to brute-force attacks.

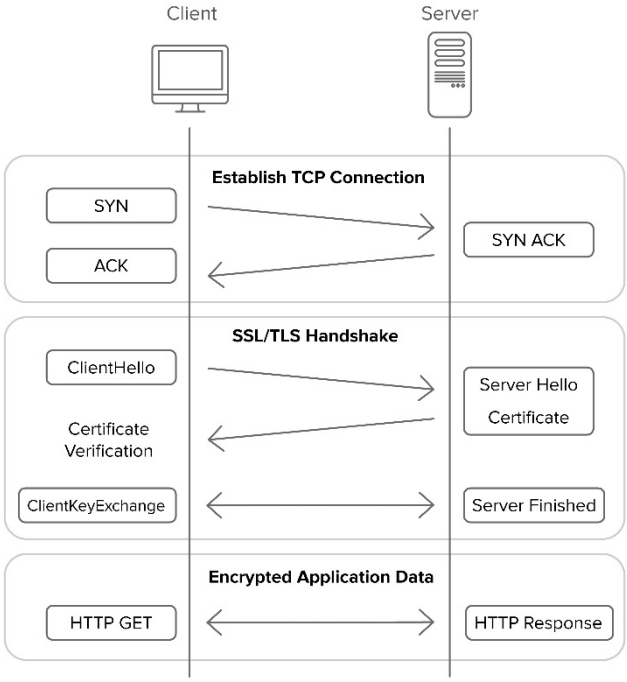

Figure 2. TLS Process Overview

In contrast, RSA is an asymmetric encryption algorithm that employs two distinct keys: a public key and a private key. This significantly enhances security compared to AES. However, RSA is less suitable for encrypting large amounts of data due to its resource-intensive nature, stemming from its heightened security measures.

In our approach, both encryption algorithms are utilized to leverage the respective advantages they offer. The hybrid encryption scheme operates as follows:

1) AES-256 shall encrypt the data with a generated key.
2) The AES key shall then be encrypted by the receiver's public key.
3) Both AES-encrypted data and RSA-encrypted key shall be sent together to the receiver.
4) The key shall be decrypted on the receiver's side using the receiver's private key.
5) The receiver then shall be able to use the decrypted AES key to decrypt the AES-encrypted data.

To achieve the authentication objective discussed earlier, the Vehicle Identification Number (VIN) serves as a unique value for authenticating the vehicle's identity. In order to prevent man-in-the-middle attacks, the Cloud stores the VINs of registered vehicles and verifies any requests originating from a vehicle. Since the VIN is a critical value, it must be securely and safely stored. Our system proposes the use of the Secure Hashing Algorithm 512-bit (SHA-512) to hash the VIN values on the cloud prior to storage. Hashing is an suitable technique for this purpose as it differs from encryption. It is an irreversible process, meaning that once a value is hashed, it cannot be restored to its original plain-text form. This characteristic ensures that the VINs remain secure, even in the event of a data breach in the Cloud. In terms of communication, all the hashed Vehicle Identification Numbers (VINs) transmitted during the authentication process are securely conveyed via an encrypted tunnel, established through the certified full-handshake procedure facilitated by the SSL/TLS protocol.

B. System Communication

In order to ensure system compatibility and affordability, the utilization of the MQTT protocol is imperative. MQTT, built upon the TCP transport protocol, is a lightweight protocol stack specifically designed for Internet of Things (IoT) devices. It is optimized to operate efficiently on limited, small-scale, and cost-effective devices. By employing MQTT, the system benefits from cost reduction and enhanced battery life, making it suitable for resource-constrained environments.

Moreover, MQTT security is segmented into three different levels, which are:

- **Network Level:** a secured network has to be connected to the broker. Accordingly, a Virtual Private Network (VPN) has been suggested to establish between the Cloud and the broker.
- **Transport Level:** in this layer, TLS has to be implemented. Therefore, an encrypted tunnel shall be created for the vehicle/ambulance and Cloud.
- **Application Level:** MQTT has to authenticate using VIN with Hashing mechanism, as discussed earlier in this paper.

Additionally, several encryption mechanisms have been distinguished to provide effective network throughput over the communication channel.

Publisher-to-Subscriber Encryption (P2S): In this mechanism, data shall be encrypted by the sender and decrypted by the receiver. This process ensures end-to-end encryption. In other words, unauthorized clients either attackers can access the data, because the data publisher and topic subscriber only know the decryption key and method as shown in figure 4.

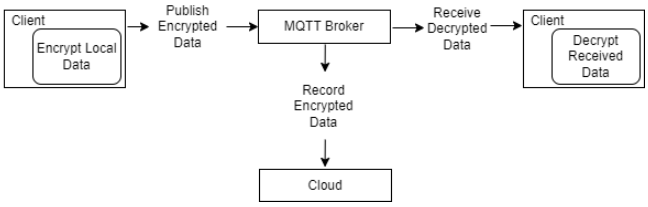

Figure 3. P2S Data Encryption

Publisher-to-Broker Encryption (P2B): In this method, data can be decrypted before reaching the receiver. This method can be helpful in the case of cloud data processing as shown in figure 5.

Furthermore, the implementation of our system necessitates the utilization of the aforementioned approaches in accordance with the project's proposed concept and activities.

One potential drawback of employing MQTT over TLS is the potential for overhead, as the introduction of security measures often entails increased CPU performance requirements and communication overhead. This overhead is primarily attributed to the repetitive TLS handshake,

particularly when MQTT client connections are short-lived. While the additional CPU usage incurred by TLS is typically insignificant for MQTT, it can pose challenges for resource-constrained devices that cannot handle the computational demands associated with intensive security protocols. To address this issue, Session Resumption is introduced as a solution to enhance TLS performance and enable its effective use with MQTT on low-end devices, thereby minimizing communication overhead [9].

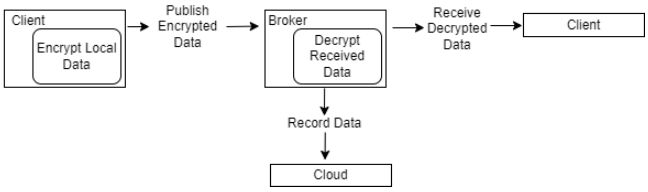

Figure 4. P2B Data Encryption

1) TLS Session Resumption

As mentioned above, TLS session resumption would be essential in case of low-end devices to avoid communication and performance overheads. It is basically a technique that allows the reuse of the already negotiated and handshaked TLS sessions when reconnecting to the server. As a result, the client and the server do not have to repeat the TLS handshake all over again. TLS session resumption basically has two mechanisms:

a) **Session Tickets:** In this mechanism, the secret state of the server is sent to the client in encrypted form with a secret key that is only known to the server. Then the client sends this ticket again back to server whenever it wants to reconnect. If the server was able to decrypt the ticket back to its original form, then the client is verified, and the session is resumed with the state included in the secret ticket.

b) **Session IDs:** In contrast, in this mechanism the server stores the secret state alongside of the Session ID, and when the client tries to reconnect again it provides the same Session ID, and then the session can be resumed again without having to re-initiate the TLS handshake process, as shown below in figure 6.

Our proposed system will be using HiveMQ for MQTT with session resumption by Session IDs as HiveMQ only supports this technique.

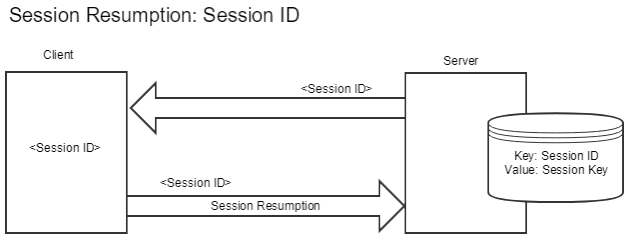

Figure 5. Session Resumption via Session ID

III. Conclusion and Future Work

A. Conclusion

In conclusion, the automotive industry's escalating reliance on technology has significantly heightened the susceptibility of digital data to cyber-attacks, as evidenced by a series of notable incidents in recent years. In response, industry has implemented various security measures to counter these threats. Hybrid encryption protocols, which leverage the simplicity and efficiency of symmetric ciphers to encrypt data of any size while enhancing security through the use of asymmetric ciphers to encrypt the symmetric key, have been adopted. Additionally, vehicle-to-everything (V2X) communication protocols, message queuing telemetry transport (MQTT), and data access control mechanisms have been employed to safeguard drivers against identity theft, fraud, and malicious activities without affecting the performance by any potential overhead in both communication and security. The gravity of these cyber-attacks and their potential harm to drivers have underscored the urgent need for enhanced cybersecurity measures. Consequently, the automotive industry continues to invest in the development of novel strategies to mitigate these threats. As illustrated in Figure 1, communication channel threats and vehicle data threats emerged as prominent categories of cyber-attacks within the automotive sector during the years 2020 and 2021. This observation emphasizes the ongoing necessity for robust security protocols within the industry. It is important to note that while significant efforts are being made to fortify automotive cybersecurity, the notion of a completely impervious system remains elusive. The concepts discussed herein represent initial iterations rather than finalized solutions employed in our project, acknowledging the evolving nature of cybersecurity challenges and the need for continuous adaptation.

B. Future Work

The concept was designed to be tested on our Automotive level test bench and demonstrator, which was built in cooperation with Automotive companies and their requirement as well. This concept is already being implemented and still in the initial stage. Afterwards, this concept will be tested in a real environment to achieve proof of work.

References

[1] "Data of 18.000 Nissan North America Clients Exposed by a Third-party Breach," Jan. 2023, section: Cybersecurity News. [Online]. Available: https://heimdalsecurity.com/blog/data-of-18-000-nissan-north-

[2] A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," Wired, section: tags. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] D. Ulybyshev, A. Oqab Alsalem, B. Bhargava, S. Savvides, G. Mani, and L. Ben Othmane, "Secure Data Communication in Autonomous V2X Systems," in 2018 IEEE International Congress on Internet of Things (ICIOT), Jul. 2018, pp. 156–163. K. Elissa, "Title of paper if known," unpublished.

[4] F. B. Setiawan and Magfirawaty, "Securing Data Communication Through MQTT Protocol with AES-256 Encryption Algorithm CBC Mode on ESP32-Based Smart Homes," in 2021 International

Conference on Computer System, Information Technology, and Electrical Engineering (COSITE), Oct. 2021, pp. 166–170

[5] "2022 Global Automotive Cybersecurity Report." [Online]. Available: https://upstream.auto/2022report

[6] J. Noh, Y. Kwon, J. Son, and S. Cho, "Blockchain-based one-time authentication for secure v2x communication against insiders and authority compromise attacks," IEEE Internet of Things Journal, vol. 10, no. 7, pp. 6235–6248, 2023

[7] A. Satapathy and J. Livingston, "A comprehensive survey on ssl/ tls and their vulnerabilities," International Journal of Computer Applications, vol. 153, pp. 31–38, 11 2016

[8] Q. Zhang, "An overview and analysis of hybrid encryption: The combination of symmetric encryption and asymmetric encryption," in 2021 2nd International Conference on Computing and Data Science (CDS), 2021, pp. 616–622

[9] T. H. Team, "TLS/SSL - MQTT Security Fundamentals," May 2015. [Online]. Available: https://www.hivemq.com/blog/mqtt-security-fundamentals-tls-ssl/