The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)
ISSN: 2602-3199

The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 2024

Volume 27, Pages 108-121

IConTech 2024: International Conference on Technology

Enhancing Connected Vehicle Security: Innovations in Two-Factor Authentication

Huseyin Karacali
TTTech Auto Turkey

Efecan Cebel
TTTech Auto Turkey

Nevzat Donum
TTTech Auto Turkey

Abstract: The automotive sector is undergoing profound changes with the advancement of technology, and connected vehicles represent one of the most notable examples. These vehicles, equipped with internet connectivity and communication capabilities with other devices, are becoming increasingly widespread. Consequently, they accumulate substantial amounts of data concerning drivers and their environments. However, this connectivity also brings about significant security concerns, particularly regarding the privacy and security of the metadata stored in these vehicles. Metadata encompasses diverse information about user activities, habits, location data, and personal preferences, making it an appealing target for potential attackers. Therefore, safeguarding the security of metadata in connected vehicles stands out as a primary concern for manufacturers. This study aims to surpass the two-factor authentication (2FA) systems developed to protect the metadata stored in connected vehicles. The system comprises two components: the Central Security Unit (CSU) and the AutoGuard (AG) mobile application. Integrated with the Remote Keyless Entry System (RKES), CSU initiates the 2FA process when the driver approaches the vehicle. Upon entering the second authentication factor (biometric, pattern, PIN code), successful authentication unlocks the vehicle doors via RKES, while failure prompts notification to the driver. To advance the 2FA system, a Bluetooth Low Energy (BLE)-based communication system has been integrated between CSU and AG. This integration enhances communication between the two, making it more secure and energy efficient. Furthermore, it enables data exchange without the need for a network connection, ensuring a seamless user experience. These innovative communication features transcend the 2FA system by rendering communication between CSU and AG more reliable and flexible. Additionally, by integrating the phone's location into the authentication system, AG functionality can enhance the accuracy of the 2FA system, potentially using the phone's location as an additional authentication factor.

Keywords: Metadata, Two-factor authentication, Connected vehicles, Vehicle security, Metadata, Bluetooth low energy

Introduction

In today's era, the automotive industry is progressively becoming more complex and dynamic. Technological advancements are fundamentally altering the expectations and needs of both drivers and passengers, thereby continuously incentivizing industrial actors to seek innovative solutions. At the core of this transformation lies the integration of digitization and connected devices, epitomized by the "connected vehicle" technology.The concept of connected vehicles represents an evolutionary leap from the traditional notion of automobiles, achieved through the amalgamation of advanced technologies such as inter-vehicle communication, cloud computing, artificial intelligence, and smart sensors. This technology aims to enhance the daily lives of drivers

and passengers by rendering them safer, more efficient, and more enjoyable. Vehicles are no longer mere modes of transportation but have evolved into intelligent devices.

These intelligent systems enable vehicles to perceive their surroundings and gather various data points, encompassing factors like traffic conditions, road status, weather conditions, and the locations of other vehicles. This information is analyzed and utilized in real-time to provide drivers with safer and more efficient driving experiences.However, the adoption and implementation of this innovative technology entail certain challenges. Concerns regarding security, data privacy, infrastructure compatibility, and regulatory compliance may hinder or delay the widespread adoption of connected vehicles. Therefore, it is imperative for industrial stakeholders to collaborate and develop solutions to overcome these challenges.

Connected vehicles represent one of the most significant advancements in today's automotive technology landscape. These vehicles continuously generate a wide range of data through various sensors, cameras, GPS, and other data collection devices. This data encompasses various parameters of the vehicle, including its position, speed, fuel consumption, engine performance, environmental conditions, and passenger behavior. The data accumulated in a vehicle due to connected functionalities typically constitutes metadata. Metadata essentially serves as a summary of information related to other data. For instance, the speed and location of a vehicle constitute fundamental information that forms the metadata of the vehicle. This metadata enables drivers and manufacturers to monitor vehicle performance, enhance safety measures, and plan for future journeys.An important aspect of metadata is its capacity to enhance the data collection and analysis capabilities of vehicles. These data can be utilized to evaluate vehicle performance, identify maintenance requirements, analyze driver behaviors, and even optimize traffic flow. Technologies such as big data analytics, artificial intelligence, and machine learning facilitate in-depth analysis of this metadata, enabling drivers and industrial stakeholders to make better decisions.

The privacy of metadata has become an increasingly significant concern in today's data-driven world. Smart vehicles like connected vehicles continuously generate a vast array of data through various sensors and communication technologies. This data encompasses various parameters of the vehicles, including their location, speed, travel route, fuel consumption, engine performance, and driver behaviors. However, there is a significant concern regarding the collection and utilization of this data, specifically pertaining to data privacy and security. The large volume of data collected from vehicles may contain sensitive information about the private lives of drivers and passengers. For example, a vehicle's travel route could disclose a driver's home or workplace address. Similarly, vehicle speed and driver behaviors could lead to inferences about a driver's personal preferences or health status.

Therefore, the privacy of metadata is of critical importance for the safety and privacy of drivers and passengers. Unauthorized access to this data, its malicious use, or exposure to cyberattacks could have serious consequences. For instance, data breaches could result in identity theft, cyber harassment, or compromise physical security. Hence, during the development and implementation of technologies like connected vehicles, data privacy and security should be paramount. Vehicle manufacturers and technology providers should adopt measures such as robust encryption methods, secure data storage infrastructure, and access controls. Additionally, it is important to establish mechanisms that provide users with greater control over the data collection and sharing processes. In conclusion, the privacy of metadata is an important consideration in the development and implementation of smart vehicle technologies like connected vehicles. Preserving data privacy is a fundamental requirement for ensuring the safety and privacy of drivers and passengers. Efforts in this regard are critical for the sustainability of future technological advancements.

This study focuses on the protection of metadata and the vehicles themselves in connected vehicles. The research aims to go beyond a proposed two-factor authentication system designed to safeguard both the vehicle and the hosted metadata. The two-factor authentication system comprises a Central Security Unit (CSU) and a mobile application called AutoGuard (AG). The CSU is integrated with the Remote Keyless Entry System (RKES) of the vehicle. RKES is one of the security and access control systems used in modern automobiles. This system enables the vehicle owner to lock and unlock the vehicle from a certain distance without the need for a physical key. RKES typically operates using a set of technological features integrated into a key card or key fob (Analog Devices, n.d.). At its essence, RKES is comprised of an assortment of sensors and communication modules responsible for managing the vehicle's doors and locks. These sensors are designed to detect the presence of the key within a specified proximity to the vehicle. Utilizing wireless technologies such as RFID (Radio-Frequency Identification) or similar protocols, the key establishes communication with the system (Shafiullah et al., 2022b).

RKES provides drivers with both convenience and security, enabling them to interact with their vehicle without the need for a physical key. Furthermore, by allowing operations to be executed without direct physical contact with the key, RKES helps mitigate the risk of car theft (Kaspin, 2023b). This system is progressively emerging as a significant element of contemporary automotive technology. The initiation of the 2FA process takes place as the remote-control key approaches the vehicle, triggering the CSU, which subsequently activates the second authentication factor. AG prompts the driver to input a valid security method, such as biometric data, pattern recognition, or a PIN code. Upon successful second authentication, AG grants authorization to the CSU, facilitating the unlocking of the vehicle doors by the RKES. In instances where the 2FA process fails, the CSU promptly notifies the driver through the AG interface. Therefore, the primary objective of this system is to safeguard the metadata stored in authorized users' vehicles and the vehicles themselves from unauthorized intruders (Karacali et al., 2023). Expanding on this concept, the 2FA process functions as a robust security protocol triggered by the proximity of the remote-control key to the vehicle. This unique methodology strengthens security measures by implementing a dual-layer verification system. Upon activation by the remote-control key, the sophisticated CSU seamlessly integrates with the vehicle's RKES, coordinating a synchronized authentication process.

The AG mobile application, an essential element of this security framework, serves as the conduit for the second authentication factor. It engages the driver, requesting the input of a valid security method, which may include biometric data for heightened personal identification, pattern recognition for a custom user-defined pattern, or a PIN code for an additional numerical layer of security. This multi-faceted approach ensures a robust defense against unauthorized access, necessitating not only possession of the remote-control key but also a personalized and verified security input from the authorized driver (Karacali et al., 2023). Following the successful conclusion of the second authentication, AG provides the requisite authorization to the CSU. This crucial interaction facilitates the RKES in unlocking the vehicle doors, seamlessly merging the security and access control functionalities. In the unfortunate event of an unsuccessful 2FA process, the CSU, functioning as the guardian of security, promptly alerts the driver through the AG interface. This transparent and immediate notification system ensures that the driver remains informed regarding any potential security breaches (Karacali et al., 2023). In addition to the SMTP-based communication system, a Bluetooth Low Energy (BLE) based communication system has been integrated into the connected vehicles to further enhance communication and provide a comprehensive security solution. This integration aims to make in-vehicle communication more secure and efficient while also improving user experience.

The integrated BLE communication system optimizes data exchange between the CSU and the AG, thereby enhancing security measures. BLE is known for its low energy consumption, ensuring reliable communication while preserving the vehicle's battery life. Moreover, this communication system does not require network connectivity, allowing for data exchange without reliance on external networks. This enables seamless data exchange and enhances user experience without the need for network access. The BLE communication system strengthens the connection between the CSU and AG, making data exchange more reliable and flexible. While ensuring low energy consumption, the system maintains robust security protocols, ensuring communication security and data integrity among users. Additionally, by facilitating effective data exchange in connected vehicles, the BLE communication system enhances security measures. Therefore, the integration of the BLE-based communication system improves communication reliability and efficiency in connected vehicles.

Materials

Raspberry Pi 5

Raspberry Pi 5, developed by the Raspberry Pi Foundation, represents the latest addition to the Raspberry Pi family. This miniature computer is a preferred platform by a wide user base and is utilized in various projects. Raspberry Pi 5 offers high performance, low power consumption, and a cost-effective solution. Looking at the technical specifications, Raspberry Pi 5 features a quad-core 64-bit ARM Cortex-A72 processor running at 1.8 GHz, providing robust processing capabilities (Raspberry Pi 5, 2023). Additionally, the device boasts an impressive memory capacity. Equipped with 8 GB LPDDR4 RAM, Raspberry Pi 5 enables smooth multitasking. In terms of connectivity options, Raspberry Pi 5 offers a diverse range of choices. The device is equipped with a Gigabit Ethernet port, dual-band Wi-Fi (802.11ac), and Bluetooth 5.0. These features facilitate easy connection to wireless networks and reliable data communication. Raspberry Pi 5 is equipped with Bluetooth Low Energy (BLE) capability, enabling the device to provide wireless communication with low power consumption (Raspberry Pi 5, 2023). BLE is an energy-efficient communication protocol, preserving battery life while ensuring reliable connectivity over long distances. The BLE feature of Raspberry Pi 5 makes it

an ideal choice for various IoT (Internet of Things) applications. This feature allows Raspberry Pi 5 to interact with environmental sensors, smart home devices, and other BLE-enabled devices. Furthermore, the BLE feature of Raspberry Pi 5 facilitates seamless integration with mobile applications. This allows users to control Raspberry Pi 5 with other smart devices such as smartphones or tablets, enhancing the device's flexibility of use (Raspberry Pi 5, 2023). In this study, an upgrade in hardware has been made beyond the previous study, replacing the Raspberry Pi 3B+ with the Raspberry Pi 5 platform (Karacali et al., 2023).

Raspbian Operating System

Raspbian, an operating system based on Debian and tailored for Raspberry Pi microcomputers, stands out for its adaptability and efficiency. This technical assessment delves into the core features that make Raspbian a preferred option among Raspberry Pi enthusiasts and developers (Raspberry Pi, 2023). Leveraging Debian's robust foundation known for its resilience and stability, Raspbian provides a dependable framework conducive to customizations catering to the specific needs of Raspberry Pi users (Raspberry Pi, 2023). By building upon Debian's reliability and robustness, Raspbian creates a Linux distribution finely tuned for Raspberry Pi, ensuring a stable platform for tailored adjustments. Engineered with the resource constraints of Raspberry Pi in mind, Raspbian is finely optimized for minimal power consumption and maximal performance, enhancing user experience and system responsiveness. Leveraging Debian's package management system, Raspbian streamlines the installation, updating, and maintenance of software packages, with a vast software repository offering access to a wide array of applications (Raspberry Pi 5, 2023). The preference for Raspbian as the operating system for the CSU stems from its compatibility with the versatile capabilities of the Raspberry Pi 5. As a Debian-based system, Raspbian builds upon a sturdy foundation, guaranteeing reliability, stability, and a flexible environment. The CSU's primary role is to proficiently administer and enforce security protocols in connected vehicles. Raspbian's alignment with the Raspberry Pi's resource constraints optimizes energy efficiency and fortifies the CSU's efficacy. Moreover, the Debian package management system facilitates seamless software updates, swift resolution of security vulnerabilities, and access to an extensive software repository, thereby bolstering the CSU's functionality. In summary, Raspbian emerges as an optimal choice for enhancing the security of connected vehicles, blending reliability, performance, and customization prospects for the CSU.

PyQt

PyQt emerges as a potent toolset for crafting desktop applications using Python as the core programming language. Serving as Python bindings for Qt, a prevalent cross-platform framework for application and UI development, PyQt seamlessly blends Python's simplicity with Qt's extensive capabilities. This amalgamation equips developers with a versatile arsenal for crafting intricate graphical user interfaces. Given PyQt's status as a Python library, it harmonizes seamlessly with the project's reliance on Python as the primary programming language, ensuring a smooth development journey while leveraging Python's readability and adaptability (Python Wiki, n.d.). PyQt was selected as the framework for the CSU application's development owing to its abundant features and user-friendly nature.

RC522 RFID NFC Module

The RFID RC522 module is an affordable and high-performance RFID device operating at 13.56 MHz. Its primary purpose is to enable efficient and extensive utilization of RFID technology (Handson Technology, n.d.). Compliant with ISO/IEC 14443 Type A standards, the RC522 communicates seamlessly with cards adhering to these standards. Capable of both reading and writing RFID tags, the RC522 module finds practical applications in access control systems, asset tracking, and identity authentication scenarios. Utilizing the SPI (Serial Peripheral Interface) protocol, the module ensures rapid and reliable data transmission when communicating with the microcontroller (MACFOS, n.d.). In this study, the RC522 module has been integrated with the Raspberry Pi 5 to serve as a simulation tool for the remote key.

Android Studio

Android Studio serves as the primary integrated development environment (IDE) specifically crafted for Android app development (Google, 2018). This feature-rich toolset, curated by Google, offers an extensive array of resources to streamline the app creation process, blending efficiency, flexibility, and robust

functionality into one cohesive platform. Android Studio's interface is designed with user-friendliness in mind, ensuring seamless navigation and accessibility to a wide range of tools within an organized workspace to bolster developer productivity (Google, 2018).

Within Android Studio, developers benefit from a sophisticated code editor proficient in multiple programming languages, notably Java and Kotlin for Android development. These capabilities empower developers with efficient coding experiences, including features like code completion, syntax highlighting, and real-time error detection (Google, 2018). The AG application's development journey heavily relied on Android Studio as the designated IDE, chosen for its official status and comprehensive toolkit tailored for Android app development (Google, 2018). By utilizing Android Studio, developers ensure smooth integration with the latest Android SDKs, APIs, and platform updates, guaranteeing optimal performance and access to cutting-edge features provided by the Android operating system.

Java was selected as the programming language for the AG application due to its platform independence and widespread adoption in Android development circles (Google, 2018). Aligning with Java's "write once, run anywhere" philosophy, this decision aims to ensure that the AG application delivers a consistent user experience across various devices and operating systems. Leveraging the extensive support and libraries within the Java ecosystem simplifies the development process, enhancing the reliability and scalability of the AG application (Google, 2018).

In essence, the development of the AG application relied on Android Studio as the preferred IDE, harnessing its official endorsement and robust feature set for Android app development. The integration of Java as the programming language underscores the commitment to platform independence and leverages the widespread community support within the Android development realm, culminating in the creation of a powerful and user-friendly AG application poised to deliver consistent experiences across diverse platforms.

Firebase

Firebase, a platform for mobile and web app development developed by Google, offers developers a wide range of cloud-based services to streamline the development process and improve user experience. With the goal of expediting application development and providing efficient application management tools, Firebase provides a comprehensive suite of tools and services to support various stages of the development lifecycle (Firebase, 2019). Central to Firebase is its Realtime Database, which is built on a NoSQL foundation and allows for the real-time synchronization of application data. This feature enables users to receive instant updates, thereby enhancing the overall user experience (Firebase, 2019). Additionally, Firebase Authentication ensures the security of user logins by offering secure authentication methods through different identity providers, including email and social media accounts. In the AG mobile application, Firebase has been employed for the authentication process to verify authorized drivers.

Simple Mail Transfer Protocol (SMTP)

SMTP serves as a communication standard utilized to send electronic mail across different servers. Essentially, SMTP facilitates the transmission of messages between email servers by following a defined set of rules and commands (Lepilkina, 2020). It establishes a connection between two servers to relay email data, terminating the connection once the transmission process concludes. SMTP ensures the proper formatting and accurate interpretation of transmitted data. Control commands are utilized by the sending server to verify the successful delivery of messages. Error codes and messages are employed by SMTP to report any transmission errors encountered. The operational mechanism of SMTP revolves around establishing a connection between sender and recipient servers, with the sending server transmitting email data through a series of commands and receiving responses from the destination server. Various checks are performed by the sending server to guarantee the precise delivery of messages (AWS, n.d.). Despite its widespread usage, SMTP is generally considered insecure due to its reliance on transmitting messages in plain text format between servers, often lacking encryption (AWS, n.d.). To enhance security, additional measures like Transport Layer Security (TLS) are commonly implemented for secure email transmission. In the research, communication between the CSU and AG is facilitated using the SMTP protocol.

Bluetooth Low Energy (BLE)

BLE is a communication protocol that forms a subset within wireless communication technologies. Fundamentally, it prioritizes energy efficiency by providing low power consumption, making it a suitable option for devices powered by batteries. BLE is commonly used to fulfill short-range communication needs, particularly in small-sized devices (Bluetooth, n.d.). Technically, BLE operates within the 2.4 GHz frequency band and supports low data rates tailored to specific application domains, enabling short communication distances (Bluetooth, n.d.). This optimization aims to minimize energy consumption while optimizing communication range and speed. BLE finds applications across various devices such as cellular devices, smart wearable technologies, health monitoring devices, and other smart objects. For data exchange and inter-device interaction, BLE utilizes the Generic Attribute Profile (GATT) protocol (Bluetooth Low Energy | Connectivity, n.d.). This protocol enables BLE devices to define their services, attributes, and relationships, thereby providing a standardized approach for data transfer and communication between devices. One of the significant advantages of BLE is its ability to provide long battery life by operating in low power modes. This ensures that battery-powered devices remain active for extended periods while consuming minimal energy (Mocrii et al., 2018). Additionally, the fast connection establishment process and low latency facilitate quick and efficient communication between devices. BLE based communication system was used between the CSU and the AG.

Method

This section delineates the developmental procedures involved in crafting the 2FA system. The system comprises two primary elements, namely CSU and AG, as depicted in Figure 1.

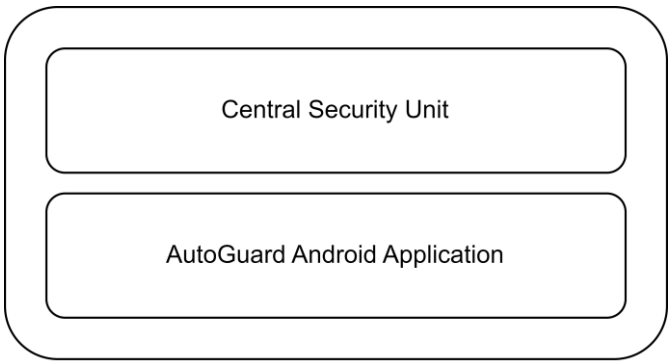

Figure 1. Two-factor authentication system main components

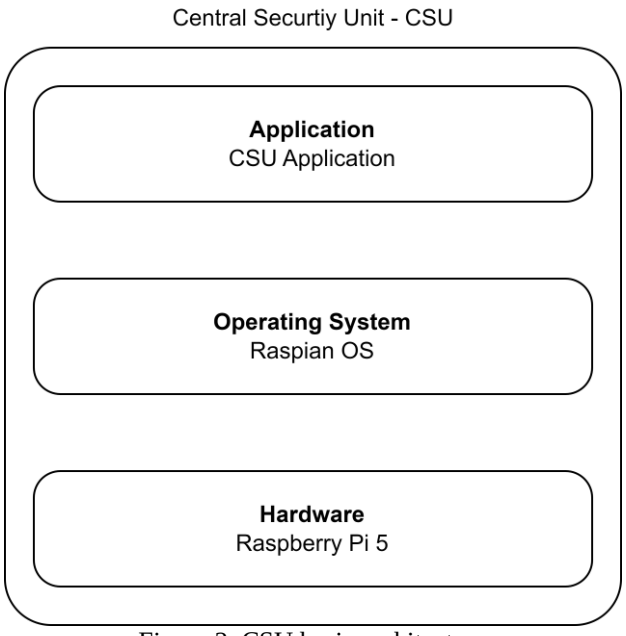

Figure 2. CSU basic architecture

CSU constitutes an embedded unit within the vehicle. Built upon the hardware foundation of the Raspberry Pi 5 platform, CSU operates on the Raspbian OS, initiating its boot process from an SD card. The architectural blueprint of CSU is illustrated in Figure 2. Development of the CSU application leverages PyQt within the Raspbian OS environment. This intricate setup underscores the robust integration of CSU within the vehicle infrastructure, ensuring seamless operation and compatibility with diverse hardware components.

CSU seamlessly integrates into the security framework of connected vehicles, serving as a vital component. The integration process entails a multi-step authentication procedure, starting with the initial verification via a physical key. The RKES system utilizes the physical key for initial authentication, detecting it through RFID or similar wireless technology upon proximity to the vehicle (Karacali et al., 2023). Once the remote key is successfully detected, RKES triggers CSU, initiating the first step of the verification process, as depicted in Figure 3.

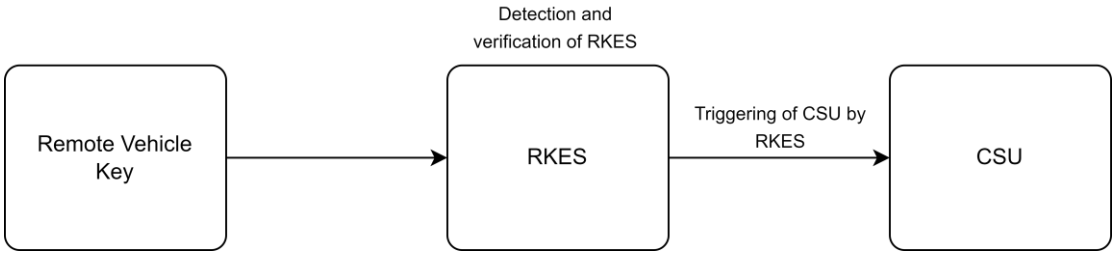

Figure 3. Remote vehicle key detection and triggering CSU

To simulate the process depicted in Figure 3, an RFID card was used instead of a remote key, with the RC522 RFID NFC module serving as the RFID reader integrated into the CSU hardware. This integration enabled smooth communication and accurate interpretation of RFID card signals for authentication initiation. The communication between the RC522 RFID NFC module occurs through the SPI protocol (Karacali et al., 2023). Once the hardware connections are established, the Raspbian operating system activates the SPI Protocol.

The CSU is integrated into a structure that performs the simulation of RKES. This structure involves the use of an RFID card to emulate an input provided to the vehicle's RKES system. By using the RFID card instead of a physical key, it mimics the functionality of a remote key detected by the RKES. Once triggered by the RKES, the CSU reads the RFID card and retrieves the identity information. The obtained identity information is then compared to the pre-defined authorized card identity. If the card's identity is successfully verified, this step is completed, and the first stage of the RKES authentication process is initiated (Karacali et al., 2023). Information regarding the success or failure of the authentication process is transmitted via SMTP and BLE. Therefore, the CSU initially checks internet connection and SMTP server connection to facilitate this communication.

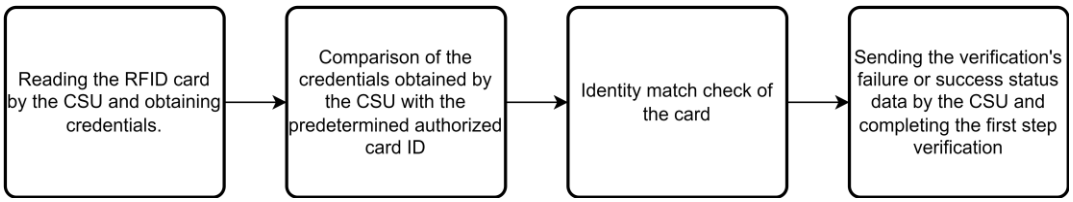

Figure 4. First authentication process block diagram

Following the completion of the initial verification step, the second stage is executed through the AG application. Developed using the Java programming language in Android Studio, the AG application requires authorized drivers to create a profile upon installation. During profile creation, various authentication methods, such as PIN, pattern schema, and biometric data (fingerprint and facial recognition), can be employed for password setting (Karacali et al., 2023). In the background, Firebase is utilized to ensure a secure authentication experience, allowing the vehicle to grant access exclusively to authorized users.

Firebase provides cloud-based services and tools for mobile and web app development. It securely manages user profiles and authentication for the AG app through Firebase Authentication. This service stores email addresses and passwords securely and supports various authentication methods. Firebase uses encryption to protect user credentials during transmission and storage, ensuring data confidentiality and integrity. Additionally, Firebase enables easy integration of biometric authentication, like fingerprint and facial recognition, in the AG app. Leveraging Firebase Authentication, the app ensures enhanced security and user experience with multiple

authentication options. In essence, Firebase strengthens the AG app's authentication system, ensuring secure and efficient user validation through various methods.

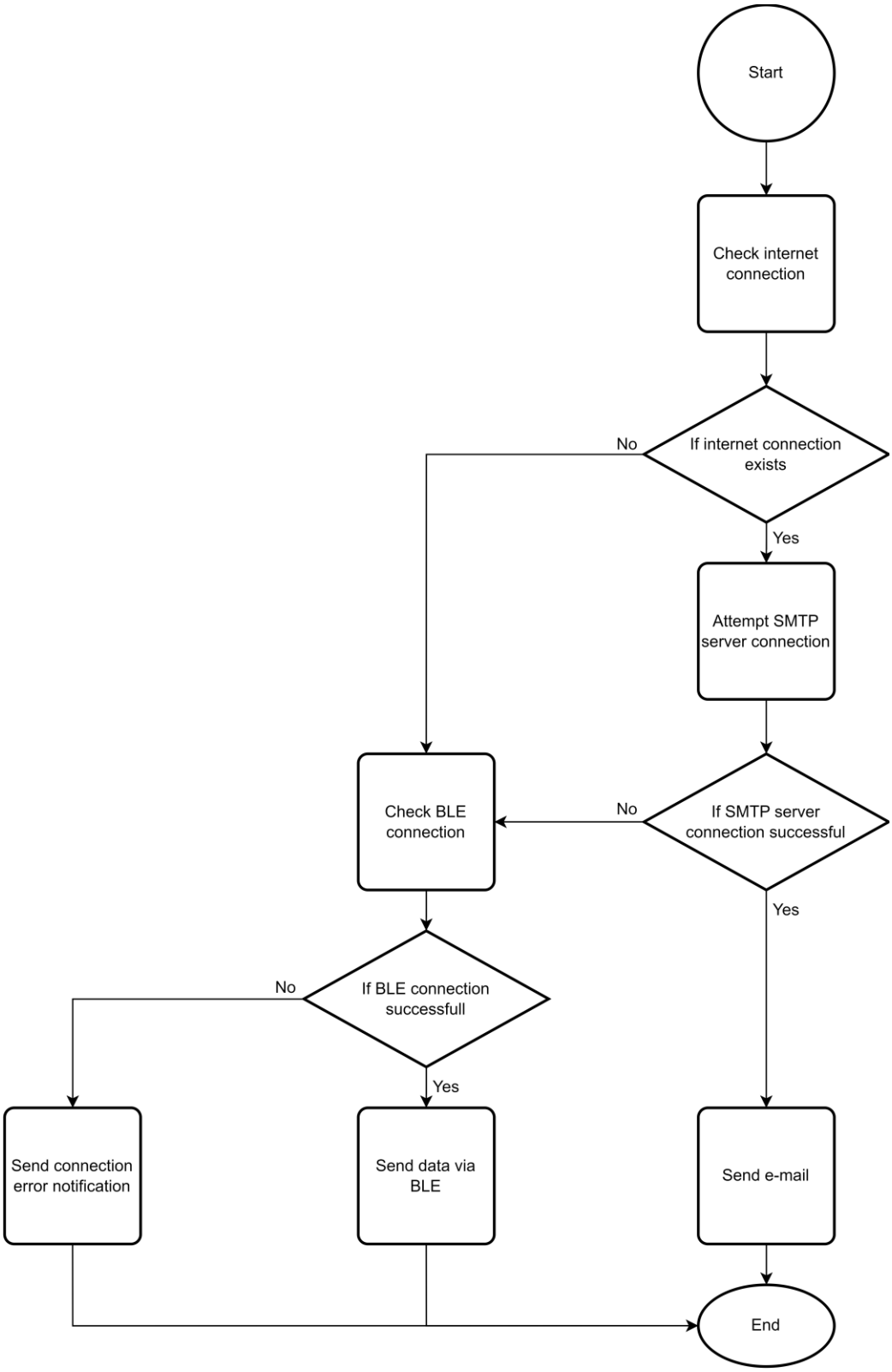

Figure 5. Basic connection control process

Upon successful completion of the profile creation process by the authorized driver, the AG application becomes operational. The registration interface of the AG application is depicted in Figure 6.

Figure 6. AG application registration form

In the case of an Internet connection CSU and AG communicate via SMTP. The AG application utilizes the Internet Message Access Protocol (IMAP) to receive emails sent by CSU. Retrieval of email content is accomplished through the Jsoup application. Subsequently, the extracted HTML content from the read email is parsed for further processing. To prevent application unresponsiveness during email reception, asynchronous programming with Java's CompletableFuture class is employed in the AG app. This ensures a responsive user interface by allowing multiple tasks to be managed simultaneously while waiting for email reception to complete.

In cases where the Internet connection is the culprit, CSU and AG communication is carried out via BLE. The registration procedure, leveraging the NFC capabilities of the phone, entails a multifaceted technical workflow designed to identify and synchronize with the MAC address of our vehicle, represented by the Raspberry Pi platform. This intricate process involves a series of protocol-specific operations to enable seamless communication between Bluetooth-enabled devices by initiating the establishment of an RFCOMM (Radio Frequency Communication) socket.

At its core, the process kicks off with the invocation of the "rfcomm" utility, a fundamental component of the Linux Bluetooth stack, tasked with managing RFCOMM channels. This utility is leveraged to initiate a communication session with the Bluetooth device, facilitating the negotiation of parameters and the establishment of a reliable data link. Subsequently, the registration process entails the transmission of initialization commands and parameters to the Bluetooth device, orchestrated through the RFCOMM channel. This includes configuring the Bluetooth interface of the Raspberry Pi to operate in a discoverable mode, enabling it to be detected and paired with the phone's NFC module. Upon successful establishment of the RFCOMM session and parameter negotiation, the next phase involves the exchange of authentication tokens and encryption keys between the phone and the Raspberry Pi. This step is critical for ensuring the integrity and confidentiality of the data exchanged during the registration process, mitigating potential security risks.

Furthermore, meticulous error handling mechanisms are incorporated throughout the process to detect and mitigate any anomalies or discrepancies encountered during the communication session. This includes robust error detection and correction algorithms to ensure reliable data transmission and seamless registration. In essence, the technical intricacies of the registration process underscore the meticulous orchestration of protocol-specific operations and communication protocols to seamlessly integrate the phone's NFC capabilities with the vehicle's Raspberry Pi platform, thereby facilitating a streamlined and efficient registration experience. In the CSU application, these operations are performed for data transfer over BLE.

In AG Java application BluetoothService module serves as the core component responsible for orchestrating all Bluetooth-related tasks within the system architecture. Primarily, its functionality revolves around the establishment and management of Bluetooth communication channels between the CSU and the paired mobile

device. Upon initialization, the BluetoothService initiates the creation of a Bluetooth socket, a pivotal interface facilitating bidirectional data exchange between the RPi and the mobile device. This socket remains receptive, awaiting signaling cues from the RPi to trigger subsequent actions. Upon receipt of a designated signal, typically denoted as 'True', the service promptly triggers a notification event on the mobile device, prompting user interaction.

Subsequently, user interaction with the notification triggers a seamless redirection to the designated BluetoothPassActivity page, where further actions, typically associated with authentication or data exchange, ensue. Central to the BluetoothService's operation is the establishment of a robust serial communication protocol between the RPi and the mobile device. This protocol ensures reliable and efficient data transmission, crucial for the integrity and responsiveness of the overall system. Additionally, the BluetoothService module incorporates a sophisticated mechanism for monitoring the mobile device's internet connectivity status. This feature enables the system to adapt its data transmission strategy dynamically based on the availability of internet access. In instances where the mobile device lacks internet connectivity, the BluetoothService seamlessly transitions to an alternative data transmission mode, utilizing the send_data function. The send_data function serves as a pivotal component within the BluetoothService, facilitating the transmission of data packets over the established Bluetooth connection. It encompasses a versatile set of functionalities, capable of handling diverse data transmission scenarios, including but not limited to the authentication process.

In essence, the BluetoothService module embodies the intricate interplay between hardware and software components, providing a robust foundation for seamless Bluetooth communication within the system architecture. After completing the verification step, the authorized driver receives a notification on their phone through the AG application. This notification prompts the user to proceed with the verification process by entering the application. Upon entering the AG application, the driver enters the password they have set, which is then authenticated by the application. Following successful verification of the password, the AG application sends a data packet to the CSU indicating the outcome of the verification process. This data packet is received and processed by the CSU. If the verification is successful, the RKES (Remote Keyless Entry System) is activated, allowing the driver to lock or unlock the vehicle. During this process, data communication between the AG application and the CSU is conducted either via SMTP or BLE. SMTP facilitates data transmission via email, while BLE enables wireless communication with low energy consumption. Both communication protocols ensure secure and reliable data transmission. The AG application provides the driver with a user interface displaying the status of the vehicle's lock. This interface allows the driver to see whether the vehicle's lock is open or closed. Figures 7 and 8 illustrate screen captures from the AG application showing the vehicle's lock status, providing the driver with information about the vehicle's security.

Figure 7. AG application vehicle lock status form

Figure 8. AG application vehicle unlock status form

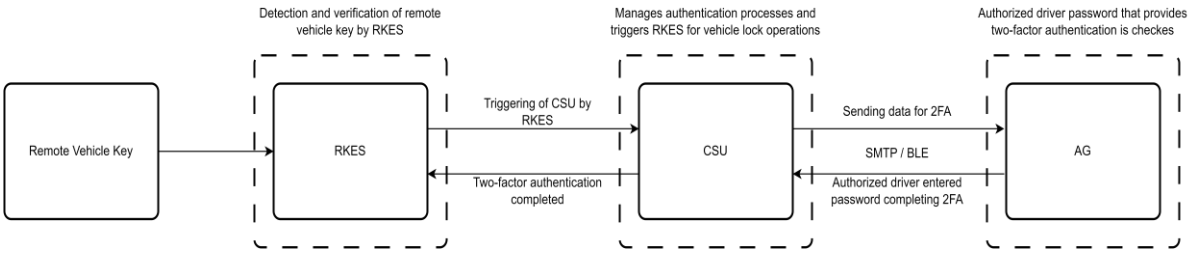

Figure 9. 2FA basic working principle block diagram

Results and Discussion

In the foreseeable future, there is an expected surge in the integration of connected vehicles into the automotive landscape. This surge is propelled by advancements in smart technologies, which are catalyzing the development of an array of connected features within the automotive sector. Internet-connected vehicles hold significant promise in augmenting safety, convenience, and operational efficiency by furnishing drivers with a diverse array of information and services at their fingertips. According to research findings, the sales of connected vehicles are forecasted to witness a substantial growth trajectory, surpassing 80 million units between 2017 and 2030 across key markets such as the United States, Europe, and China, as depicted in Figure 10 (Zaffiro & Marone, 2019).

The rapid increase in the adoption of connected vehicles heralds a significant transformation in the automotive sector. With the advancement of smart technologies, connected vehicles now have the potential to offer drivers a wide range of information and services beyond being mere modes of transportation. Communication between vehicles generates substantial data related to driver habits, environmental conditions, and vehicle performance. Particularly, with vehicles being connected to the internet, this data volume has further escalated.

The widespread adoption of connected vehicles results in a notable increase in the volume of data collected and processed. This data, spanning from driver habits to environmental conditions, underscores the growing importance of data management and security strategies in the automotive industry. This wealth of data plays a crucial role in driving the demand for advanced features such as advanced driver-assistance systems, autonomous vehicles, and service-based mobility, thereby shaping the future of automotive technologies.

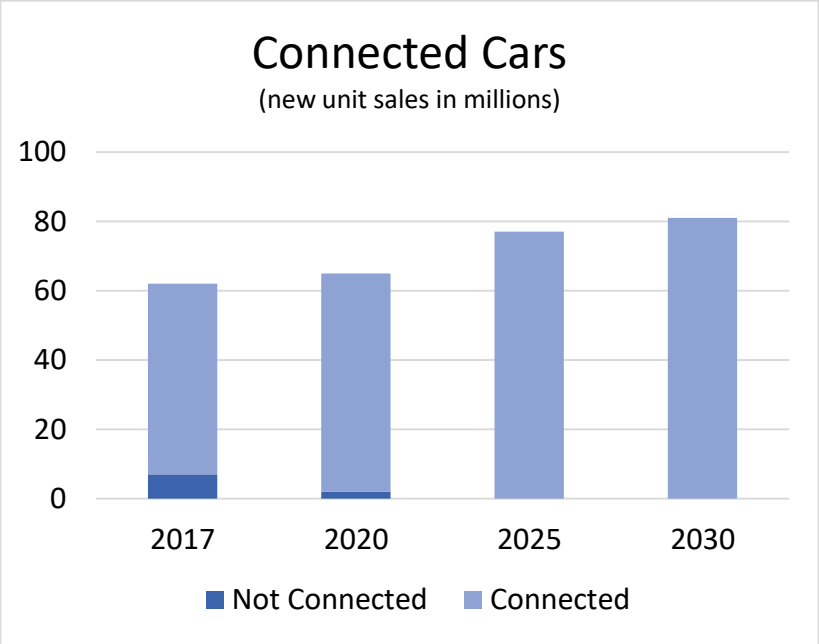

Figure 10. Connected cars sales forecast graphics

In this context, industry stakeholders need to develop strategies to effectively manage and securely utilize the growing data density. Issues such as data privacy, security, and compliance are of critical importance in the development and implementation of data-driven services in the automotive sector. Therefore, industry actors must meticulously work on data security policies and practices, developing strategies aligned with best practices in the field. This will not only ensure the security of existing customers but also support the development of future connected vehicle technologies.

In the contemporary landscape, the newly devised 2FA mechanism has introduced an additional layer of security within the domain of connected automotive systems. This innovative framework encompasses both the CSU and the corresponding mobile application known as AG, with a primary focus directed towards fortifying the protection of metadata. The core objective of this system revolves around bolstering the security infrastructure of connected vehicles, thereby thwarting any potential unauthorized access, courtesy of a robust secondary authentication mechanism coupled with the operational efficiency of a centralized security hub.

At its essence, this security framework is meticulously tailored to safeguard the intricate web of sensitive metadata housed within the interconnected automotive ecosystem. Employing a multifaceted approach, vehicles are fortified through an array of authentication methodologies tailored to the preferences of drivers. Biometric markers, intricate pattern recognition algorithms, and personalized PIN codes constitute the arsenal of protective measures skillfully deployed to deter any unauthorized entry attempts by individuals lacking proper authorization or ownership credentials.

The imperative nature of shielding this metadata cannot be overstated within the dynamic realm of cybersecurity threats, where the exponential surge in data volumes poses an imminent risk of perilous cyber incursions and breaches of individual privacy. As such, the comprehensive 2FA framework adopted by connected vehicles emerges as a formidable bulwark, ensuring the impregnable security of both drivers' and vehicle owners' data, thereby serving as a pivotal catalyst in fortifying the broader cybersecurity paradigm. The integration of BLE communication in the developed two-factor authentication (2FA) system for connected vehicles has yielded significant benefits and outcomes. By incorporating BLE into the communication framework between the CSU and the AG mobile application, several advantages have been realized.

Firstly, BLE-based communication has enhanced the security of data exchange between CSU and AG. BLE offers encryption capabilities, ensuring that transmitted data remains secure and protected from potential eavesdropping or interception by unauthorized parties. This heightened security is paramount in safeguarding the sensitive metadata stored in connected vehicles, addressing concerns regarding data privacy and integrity. Secondly, the integration of BLE has resulted in improved energy efficiency within the 2FA system. BLE technology is inherently designed to operate with minimal power consumption, optimizing energy usage and extending the battery life of devices such as smartphones used in conjunction with the AG application. This

energy-efficient communication mechanism ensures that the 2FA system remains operational for extended periods without significantly draining device batteries.

Moreover, BLE-based communication facilitates seamless data exchange between CSU and AG without the reliance on a network connection. This capability is particularly advantageous in scenarios where network connectivity may be limited or unavailable, such as remote or off-grid locations. By enabling offline communication, the 2FA system ensures uninterrupted functionality and maintains a seamless user experience regardless of network availability. Additionally, the integration of BLE communication enhances the reliability and flexibility of communication between CSU and AG. BLE technology offers robust connectivity even in congested or interference-prone environments, ensuring consistent and reliable data transmission between the two components of the 2FA system. This reliability enhances the overall performance and effectiveness of the system, contributing to its trustworthiness and usability.

In conclusion, the incorporation of BLE communication into the developed 2FA system for connected vehicles has yielded substantial benefits, including enhanced security, improved energy efficiency, offline functionality, and increased reliability. These advantages underscore the effectiveness and viability of BLE as a communication protocol in securing and managing metadata within connected automotive environments.

The 2FA system offers a reliable security solution not just for individuals but also for safeguarding corporate and commercial connected vehicles. Particularly useful in shared vehicle scenarios like rental fleets or corporate usage, it ensures only authorized drivers access vehicles, enhancing security during leasing and corporate usage. This benefits companies and rental firms by managing vehicles securely. Overall, the 2FA system enhances metadata security in connected vehicles, providing a robust defense against cyber threats and safeguarding valuable information and digital assets.

Conclusion

In the discussion section, a thorough assessment of the system's performance and potential improvements is provided. While the presented 2FA system effectively safeguards metadata in connected vehicles, future enhancements are essential to consider. Integrating AG features with location data emerges as a promising avenue for bolstering security. This integration could leverage real-time location information from the driver's phone to enhance authentication accuracy based on proximity. By utilizing location data, the system can more effectively discern the driver's presence near the vehicle, enhancing security measures. Furthermore, exploring novel authentication methods and encryption algorithms can further strengthen the system's resilience against potential attacks. These enhancements can elevate the security of connected vehicles and lay the groundwork for future improvements.

Scientific Ethics Declaration

The authors declare that the scientific ethical and legal responsibility of this article published in EPSTEM Journal belongs to the authors.

Acknowledgements or Notes

* This article was presented as an oral presentation at the International Conference on Technology (www.icontechno.net) held in Alanya/Turkey on May 02-05, 2024.

* We would like to extend our sincerest appreciation to Huseyin Karacali, the Software Architect, for his exceptional mentorship and inspiring influence. Moreover, we would like to acknowledge the invaluable assistance rendered by TTTech Auto Turkey throughout the developmental stages of this project.

References

Amazon Web Services. (n.d.). *What is SMTP? - SMTP server explained*. Retrieved from https://aws.amazon.com/what-is/smtp/

Analog Devices. (n.d.). *Remote keyless entry systems*. Retrieved fromwww.analog.com/en/resources/app-notes/remote-keyless-entry-systems-overview.html

Android Developer. (n.d.). *Android mobile app developer tools*. Retrieved from https://developer.android.com/

Android developers. (n.d.). *Bluetooth low energy*. Retrieved from https://developer.android.com/develop/connectivity/bluetooth/ble/ble-overview

Bluetooth® Technology website. (n.d.). *Bluetooth technology overview* Retrieved from https://www.bluetooth.com/learn-about-bluetooth/tech-overview/

Firebase. (n.d.). *Add firebase to your Android project firebase for Android*. (n.d.). Retrieved from https://firebase.google.com/docs/android/setup

Handson Technology. (n.d.). *Data specs RC522 RFID development kit*. Retrieved from https://www.handsontec.com/dataspecs/RC522.pdf

Karacali, H., Cebel, E., & Donum, N. (2023). Two-factor authentication system for connected vehicles In review of two-factor authentication system for connected vehicles (p.26). 3 *rd International Conference on Design, Research and Development.*

Kaspin, E. (2023, March 30). *Car keyless entry vs remote keyless entry: What's the difference?* Retrieved from https://vaistech.com/remote-keyless-entry-vs-keyless-entry-whats-the-difference/

Lepilkina, D. (2024, April 5). *SMTP basics: How it works and why it matters*. Retrieved from https://mailtrap.io/blog/smtp/

Macfos. (2023, October 21). *Buy RC522 RFID card reader module 1K3.56MHz online at Robu.in*. https://robu.in/product/rc522-rfid-card-reader-module-13-56mhz/

Mocrii, D., Chen, Y., & Musilek, P. (2018). IoT-based smart homes: A review of system architecture, software, communications, privacy and security. *Internet of Things*, *1*, 81-98.

Python Wiki. (n.d.). PyQT. Retrieved from https://wiki.python.org/moin/PyQt

Raspberry Pi 5. (2023). *Raspberry Pi 5 product.* https://datasheets.raspberrypi.com/rpi5/raspberry-pi-5-product-brief.pdf

Raspberry Pi. (2023). *Raspberry Pi documentation.* Retrieved from https://www.raspberrypi.com/documentation/computers/os.html

Shafiullah, M., Abido, M. A., & Al-Mohammed, A. (2022). *Utility practices on fault location* (pp. 347–396). Elsevier eBooks.

Zaffiro, G., & Marone, G. (2019). Smart mobility: New roles for Telcos in the emergence of electric and autonomous vehicles. In *2019 AEIT International Conference of Electrical and Electronic Technologies for Automotive (AEIT AUTOMOTIVE)* (pp. 1-5). IEEE.

Author Information

Huseyin Karacali
TTTech Auto Turkey

Efecan Cebel
TTTech Auto Turkey
Contact e-mail: efecan.cebel@tttech-auto.com

Nevzat Donum
TTTech Auto Turkey

To cite this article:

Karacali, H., Cebel, E., & Donum, N. (2024). Enhancing connected vehicle security: Innovations in two-factor authentication. *The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 27*, 108-121.