Research Article

Two-Factor Authentication System for Protecting Metadata and Connected Vehicles

Huseyin KARACALI[1*], Nevzat DONUM[2*], Efecan CEBEL[3*]

[1] TTTechAuto Turkey, Software Architect, Orcid ID: https://orcid.org/0000-0002-1433-4285, E-mail: huseyin.karacali@tttech-auto.com
[2] TTTechAuto Turkey, Embedded Software Engineer, Orcid ID: https://orcid.org/0000-0002-8293-8267, E-mail: nevzat.donum@tttech-auto.com
[3] TTTechAuto Turkey, Embedded Software Engineer, Orcid ID: https://orcid.org/0000-0002-2027-0257, E-mail: efecan.cebel@tttech-auto.com
[*] Correspondence: efecan.cebel@tttech-auto.com

Received: 11 September 2024
Revised: 12 May 2025
Accepted: 05 June 2025
Published: 27 June 2025

Reference: Karacalı, H., Donum, N., & Cebel, E. (2024). Two-factor authentication system for protecting metadata and connected vehicles. The European Journal of Research and Development, 5(1), 34-51.

Abstract

Connected vehicles are becoming increasingly common, and they store a significant amount of data about their drivers and their surroundings. This data is attractive to attackers, and there is a need for effective security measures to protect it. This study proposes a two-factor authentication (2FA) system to protect the metadata stored in connected vehicles and the vehicles themselves. The system consists of two main components: the Central Security Unit (CSU) and the AutoGuard (AG) mobile application. The CSU is integrated with the Remote Keyless Entry System (RKES), while the AG is installed on the authorized driver's phone. The 2FA process begins when the remote key is in proximity to the vehicle. This triggers the CSU, which then initiates the second authentication factor. The AG prompts the driver to enter a valid security method, such as a biometric, pattern, or PIN code. If the second authentication is successful, the AG authorizes the CSU and the vehicle doors are opened by the RKES. The driver is notified by CSU through AG if the 2FA process is unsuccessful. As a result, this system aims to protect the metadata stored in authorized users' vehicles and their vehicles from unauthorized invaders. Furthermore, it is possible to enhance the accuracy of the 2FA system by integrating the location of the phone with AG functionality into the authentication system.

Keywords: Metadata, Two-Factor Authentication, Connected Vehicles, Vehicle Security

1. Introduction

The increasingly prevalent connected vehicles are rapidly establishing themselves as fundamental components within the modern mobility ecosystem. These vehicles possess the capability to interact with each other and their surroundings through internet and communication technologies. Equipped with sensors, cameras, and other data collection tools, connected vehicles exert a significant impact on the safety, comfort, and efficiency of both drivers and passengers. Furthermore, they integrate into a wide spectrum of applications such as public transportation systems, traffic management, and smart city initiatives, laying the foundations for a smarter and more sustainable transportation infrastructure. In this context, connected vehicles emerge as a critical element in the future paradigms of mobility.

Longside the escalating prevalence of connected vehicles, a substantial accumulation of metadata emerges within these automobiles. The seamless integration of internet-based technologies and sophisticated sensor systems enhances the capacity of these vehicles to capture, process, and store diverse data related to their operations and environmental conditions.

Metadata, encompassing information such as driving patterns, vehicle diagnostics, and environmental conditions, transforms into a valuable asset within the framework of connected vehicles. The real-time exchange and storage of this metadata play a pivotal role in augmenting the functionality and responsiveness of these vehicles. Furthermore, the amassed data serves as a foundational element for developing sophisticated analyses, thereby contributing to the evolution of intelligent transportation systems.

The metadata, while encompassing the personal information of the driver, particularly sensitive data such as location information, forms a comprehensive dataset within connected vehicles. This extensive set of data goes beyond just the driving habits and vehicle diagnostics, including intricate details such as the driver's real-time location, travel routes, and parking locations.

The storage of the driver's location information within metadata brings forth a range of potential advantages. For instance, these data can be utilized to monitor traffic conditions, optimize travel routes, and enhance services like finding parking spaces. However, the sensitivity of this information necessitates the protection of drivers' privacy rights.

In this context, connected vehicles and the accumulated metadata should be addressed to include the driver's location information. Strong encryption methods, strict access controls, and data anonymization measures should be implemented during the collection and storage of this data. Thus, while safeguarding the privacy rights of drivers, the aim is also to contribute to the development of intelligent transportation systems through the effective utilization of this data. The security measures taken in this regard are fundamental requirements for connected vehicle technologies to gain societal trust and be used effectively.

This study focuses on safeguarding the metadata in connected vehicles and the vehicles themselves. The research proposes a two-factor authentication system with the aim of protecting the vehicle and the hosted metadata. The system consists of a Central Security Unit (CSU) and a mobile application named AutoGuard (AG). The CSU is integrated with the vehicle's Remote Keyless Entry System (RKES). RKES is one of the security and access control systems utilized in modern automobiles. This system provides the vehicle owner with the capability to lock and unlock the car from a specific distance without the need for a physical key. RKES typically operates by employing a set of technological features integrated into a key card or key fob [1].

At its core, RKES consists of an array of sensors and communication modules that control the doors and locks of the vehicle. These sensors detect the presence of the key within a certain proximity around the car. The key, usually communicating through a wireless technology such as RFID (Radio-Frequency Identification) or a similar protocol, establishes communication with the system [2].

RKES offers drivers both convenience and security by allowing them to interact with the vehicle without the use of a physical key. Moreover, the execution of these operations without physical contact with the key can mitigate the risk of car theft [3]. This system is increasingly becoming a prominent component of modern automotive technology.

The initiation of the 2FA process occurs when the remote control key approaches the vehicle. This subsequently triggers the CSU, which initiates the second authentication factor. AG prompts the driver to input a valid security method, such as biometric data, pattern recognition, or a PIN code. In the event of successful second authentication, AG grants authorization to the CSU, enabling the unlocking of the vehicle doors by the RKES. In cases where the 2FA process fails, the driver is promptly notified by the CSU through the AG interface. Consequently, the primary objective of this system is to protect the metadata stored in authorized users' vehicles and the vehicles themselves from unauthorized intruders.

Expanding upon this, 2FA process serves as a robust security protocol initiated upon the proximity of the remote control key to the vehicle. This distinctive approach enhances the protective measures by introducing a dual-layered verification mechanism. As the remote control key triggers the process, the sophisticated CSU seamlessly integrates with the vehicle's RKES, orchestrating a synchronized authentication workflow.

AG mobile application, an integral component of this security architecture, acts as the conduit for the second authentication factor. It engages the driver, soliciting the input of a valid security method, which could encompass biometric data for enhanced personal identification, pattern recognition for a tailored user-defined pattern, or a PIN code for a numerical layer of security. This multi-tiered approach ensures a robust defense against unauthorized access, requiring not only possession of the remote control key but also a personalized and validated security input from the authorized driver.

Upon successful completion of the second authentication, AG confers the necessary authorization to the CSU. This pivotal interaction grants permission for the RKES to unlock the vehicle doors, seamlessly integrating the security and access control mechanisms. In the unfortunate event of a failed 2FA process, the CSU, acting as the sentinel of security, promptly communicates the issue to the driver through the AG interface. This transparent and instantaneous notification mechanism keeps the driver informed about any potential security breach.

In essence, this meticulously designed system aligns its objectives with the safeguarding of metadata stored in authorized users' vehicles, fortifying the protective barriers against unauthorized entities. The synergy of technology, secure authentication protocols, and real-time communication channels underscores the comprehensive security paradigm embedded in this innovative 2FA system.

2. Materials

2.1. Raspberry Pi 3B+

The Raspberry Pi 3B+ is a microcomputer board developed by the Raspberry Pi Foundation, renowned for its widespread adoption among a diverse user base. Engineered to be utilized in various projects, it stands out for its functionality, cost-effectiveness, and extensive connectivity options. The Raspberry Pi 3B+ builds upon the features of its predecessors, aiming to enhance its capabilities for a range of applications [4].

The Raspberry Pi 3B+ boasts a quad-core ARM Cortex-A53 processor, each core operating at a speed of 1.4 GHz. This configuration ensures high performance across diverse computing tasks. With built-in support for 802.11ac Wi-Fi and Bluetooth 4.2, the device facilitates wireless communication. This feature enables wireless internet access and seamless interaction with other devices. Featuring 40 expandable GPIO pins, the Raspberry Pi 3B+ facilitates interaction with external sensors, motor drivers, and various other components. The inclusion of a Gigabit Ethernet port allows for swift data transmission, catering to applications requiring high-performance wired network connectivity [4].

The Raspberry Pi 3B+, chosen as the CSU for the 2FA system due to its versatile capabilities and robust performance, brings forth a secure, cost-effective, and widely adopted platform for safeguarding the metadata protection mechanism of connected vehicles. By selecting the Raspberry Pi 3B+ as the CSU, the 2FA system leverages the benefits of a reliable and extensively embraced platform. This strategic decision enhances the security and efficiency of the metadata protection mechanism, contributing to a secure and streamlined operation. The utilization of the Raspberry Pi 3B+ underscores the commitment to a system that is not only technologically robust but also aligns with the principles of cost-effectiveness and widespread acceptance, crucial in ensuring the widespread adoption and success of the 2FA system in protecting connected vehicle metadata.

2.2. Raspbian Operating System

Raspbian, a Debian-based operating system specifically designed for Raspberry Pi microcomputers, is recognized for its flexibility and efficiency. This technical review focuses on the key elements that make Raspbian an optimal choice for Raspberry Pi enthusiasts and developers. Raspbian is derived from Debian, a Linux distribution known for its durability and stability. This choice provides a reliable framework for customizations tailored to the unique requirements of the Raspberry Pi [5]. Raspbian builds upon the durability and stability of Debian, forming a Linux distribution tailored for Raspberry Pi. This foundation offers a reliable framework for customizations to meet the specific needs of Raspberry Pi. Designed with consideration for the resource limitations of Raspberry Pi, Raspbian is optimized for low power consumption and high performance. This optimization enhances the overall user experience and system responsiveness. Raspbian utilizes Debian's package management system, allowing users to easily install, update, and manage software packages. A vast software repository ensures access to a diverse range of applications. Raspbian employs Debian's package management system, providing users with easy installation, updating, and management of software packages. The extensive software repository guarantees access to a diverse range of applications [5].

The Raspbian operating system has been preferred for the CSU due to its compatibility with the versatile capabilities offered by the Raspberry Pi 3B+. Raspbian, being a Debian-based operating system, builds on a robust foundation, providing reliability, stability, and an adaptable framework. The primary task of the CSU is to effectively manage and implement security measures in connected vehicles. Raspbian aligns with the limited resources of the Raspberry Pi, optimizing energy efficiency and enhancing the CSU's power efficiency. Additionally, the Debian package management system facilitates easy software updates, swift resolution of security vulnerabilities, and access to a diverse array of tools through an extensive software repository, thereby augmenting the functionality of the CSU. In conclusion, the Raspbian operating system emerges as an ideal choice to reinforce the security of connected vehicles through its combination of reliability, performance, and customization opportunities for the CSU.

2.3. PyQt

PyQt stands out as a powerful framework for developing desktop applications with a Python programming language foundation. It is a set of Python bindings for Qt, a widely used cross-platform application and UI development framework. PyQt seamlessly combines Python's simplicity with Qt's robust features, offering developers a versatile toolkit for creating sophisticated graphical user interfaces. As PyQt is a Python library, it aligns well with the project's use of Python as the primary programming language. This integration allows for a seamless development experience, taking advantage of Python's readability and versatility [6].

In the development of the CSU application, PyQt was chosen as the framework due to its rich features and ease of use.

2.4. RC522 RFID NFC Module

RFID RC522 is a low-cost, high-performance 13.56 MHz RFID (Radio-Frequency Identification) module. This module is designed to facilitate the effective and extensive utilization of RFID technology [7]. Operating at a frequency of 13.56 MHz, the RC522 conforms to ISO/IEC 14443 Type A standards, allowing it to communicate with cards compliant with these standards. The RC522 possesses the capability to read and write RFID tags, making it particularly suitable for scenarios such as access control systems, asset tracking, and identity authentication applications. The module communicates with the microcontroller using the SPI (Serial Peripheral Interface) protocol, ensuring fast and reliable data transmission [8].

In the study, the RC522 has been integrated with the Raspberry Pi 3B+. This module has been utilized to simulate the remote key.

2.5. Android Studio

Android Studio is the official integrated development environment (IDE) designed for Android application development. This powerful tool offers a comprehensive set of features and resources to facilitate the application development process. Developed by Google, Android Studio is a choice that brings together efficiency, flexibility, and robust functionality for developers creating Android applications [9]. Android Studio boasts an intuitive and user-friendly interface that provides smooth navigation and access to various tools. The UI offers an organized workspace to enhance developer productivity.

The IDE includes a sophisticated code editor supporting various programming languages. Primarily focusing on Java and Kotlin for Android development, these features provide efficient coding experiences such as code completion, syntax highlighting, and real-time error checking [9].

The development process of the AG application involved the use of Android Studio, the official integrated development environment (IDE) for Android app development. Android Studio was chosen due to its status as the official IDE, offering a comprehensive set of features and resources to facilitate the development of Android applications [9]. Developing the AG application in Android Studio ensures seamless integration with the latest Android SDKs, APIs, and platform updates. This guarantees that the AG application remains optimized for performance and takes advantage of the latest features provided by the Android operating system [9].

The selection of Java as the programming language for the AG application is motivated by the need for platform independence and the widespread use of Java in Android development. Java's philosophy of "write once, run anywhere" aligns with the goal of ensuring that the AG application can run on various devices and operating systems, providing a consistent user experience across different platforms. The extensive support and libraries within the Java community simplify the development process of the AG application, contributing to its reliability.

In summary, the AG application was developed using Android Studio as the chosen IDE, leveraging its official status and robust features for Android development. The adoption of Java as the programming language ensures platform independence and benefits from the widespread use and support within the Android development community. This strategic combination aims to create a powerful and user-friendly AG application that can deliver a consistent experience across diverse platforms.

2.6. Firebase

Firebase is a mobile and web application development platform offered by Google, providing developers with a comprehensive range of cloud-based services. Firebase aims to expedite the application development process, enhance user experience, and assist developers in efficiently managing their applications. It offers a set of tools and services designed to cover various aspects of the development lifecycle [11].

At its core, Firebase incorporates a NoSQL-based Realtime Database, facilitating the real-time synchronization of application data. This enables users to witness instant updates, contributing to a seamless user experience [11]. Firebase Authentication ensures secure user logins through various identity providers, including email and social media accounts.

In the AG mobile application, Firebase has been utilized for the authentication process of authorized drivers.

2.7. Simple Mail Transfer Protocol (SMTP)

Simple Mail Transfer Protocol (SMTP) is a communication protocol utilized for the transmission of electronic mail. Essentially, SMTP facilitates the transfer of messages between email servers. This protocol encompasses a set of rules and commands that initiate the email sending process and relay it to the target email server [11]. A connection is established between two email servers, and when the email transmission process is completed, the connection is terminated. SMTP ensures that messages are correctly formatted and that the transmitted data is interpreted accurately. The sending server employs control commands to determine whether the message has been delivered correctly. SMTP uses error codes and messages to report errors occurring during transmission. The operational principle of SMTP relies on initiating a connection between two email servers, with the sending server transmitting email data to the destination email server through a series of commands and responses. The sending server conducts various checks to ensure the accurate delivery of the message [11].

SMTP is a widely used protocol for email transmission, but it is generally considered an insecure communication protocol. Messages are transmitted between the sending and receiving servers in a text-based format, and the data they contain is typically not encrypted [11]. Additional security layers, such as Transport Layer Security (TLS), are commonly employed for secure email transmission.

In the study, communication between CSU and AG is provided via SMTP protocol.

3. Method

This section describes the development processes of the 2FA system. The system consists of two main components, CSU and AG, as seen in Figure 1.

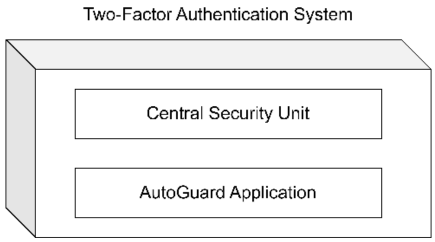

Figure 1: Two-Factor Authentication System Main Components

The CSU is a unit embedded within the vehicle. The hardware foundation of CSU is built upon the Raspberry Pi 3B+ platform. The CSU operates with the Raspbian OS, a 32-bit operating system, and its boot process is initiated from an SD card. The architecture of CSU is depicted in Figure 2. CSU application was developed with PyQt on Raspbian OS.

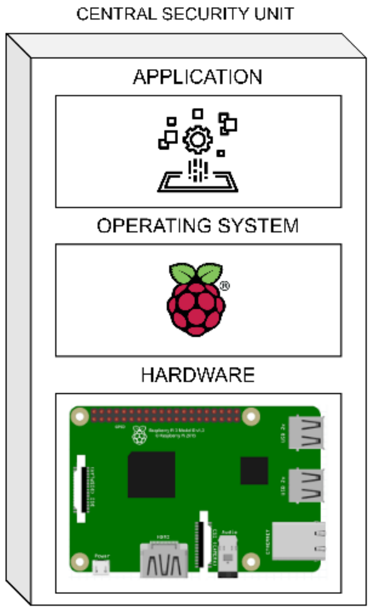

Figure 2: Central Security Unit Architecture

CSU seamlessly integrates with the RKES, forming a crucial component of the overall security architecture in connected vehicles. The integration process involves a multi-step authentication mechanism, with the initial verification relying on a physical key. The RKES system employs a physical key as the primary means of initial authentication. The Remote Key, equipped with RFID or a similar wireless technology, is detected by the RKES system when it comes into proximity with the vehicle. Upon successful detection of the remote key, the RKES system triggers the CSU and initiates the first step of the verification process. This process is shown in Figure 3.

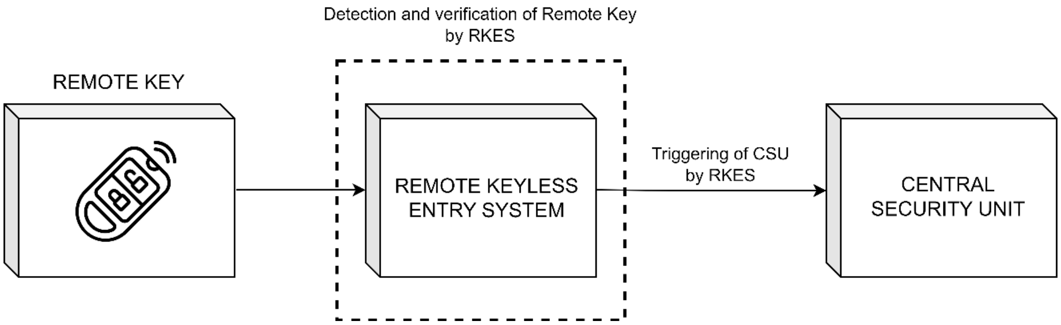
Detection and verification of Remote Key by RKES
REMOTE KEY
REMOTE KEYLESS ENTRY SYSTEM
Triggering of CSU by RKES
CENTRAL SECURITY UNIT

Figure 3: Remote Key Detection and Triggering CSU

An RFID card was used instead of a remote key to simulate the operation shown in Figure 3. RC522 RFID NFC module was used as the RFID reader. First, module connections were made to CSU. RC522 module is integrated into the CSU hardware. This integration involves precise connections and configurations to ensure seamless communication between the RFID module and the CSU. A powerful interface has been created that can accurately interpret RFID card signals and initiate the authentication process.

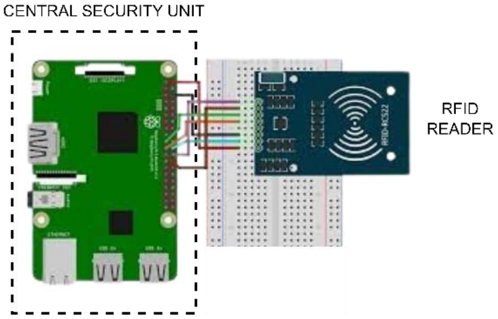

Figure 4: Connection of RFID Reader to CSU

RC522 RFID NFC module communicates with SPI protocol. After the hardware connections are completed, SPI Protocol is enabled from the Raspbian operating system.

CSU is integrated into a structure that performs the RKES simulation. This structure includes the use of an RFID card. By using the RFID card instead of a physical key, it simulates an input provided to the vehicle's RKES system. The RFID card is analogous to a remote key that is detected by the RKES. After being triggered by the RKES, the CSU reads the RFID card and obtains the identity information. The obtained identity information is compared to the pre-defined authorized card identity. If the card's identity is verified, this step is successfully completed and the first stage of the RKES authentication process is realized. The CSU has the ability to send email using a Python-based Simple Mail Transfer Protocol (SMTP) library. An email containing information about whether the authentication was successful or unsuccessful is sent to the AG application. All of these stages are shown in the flowchart in Figure 5.

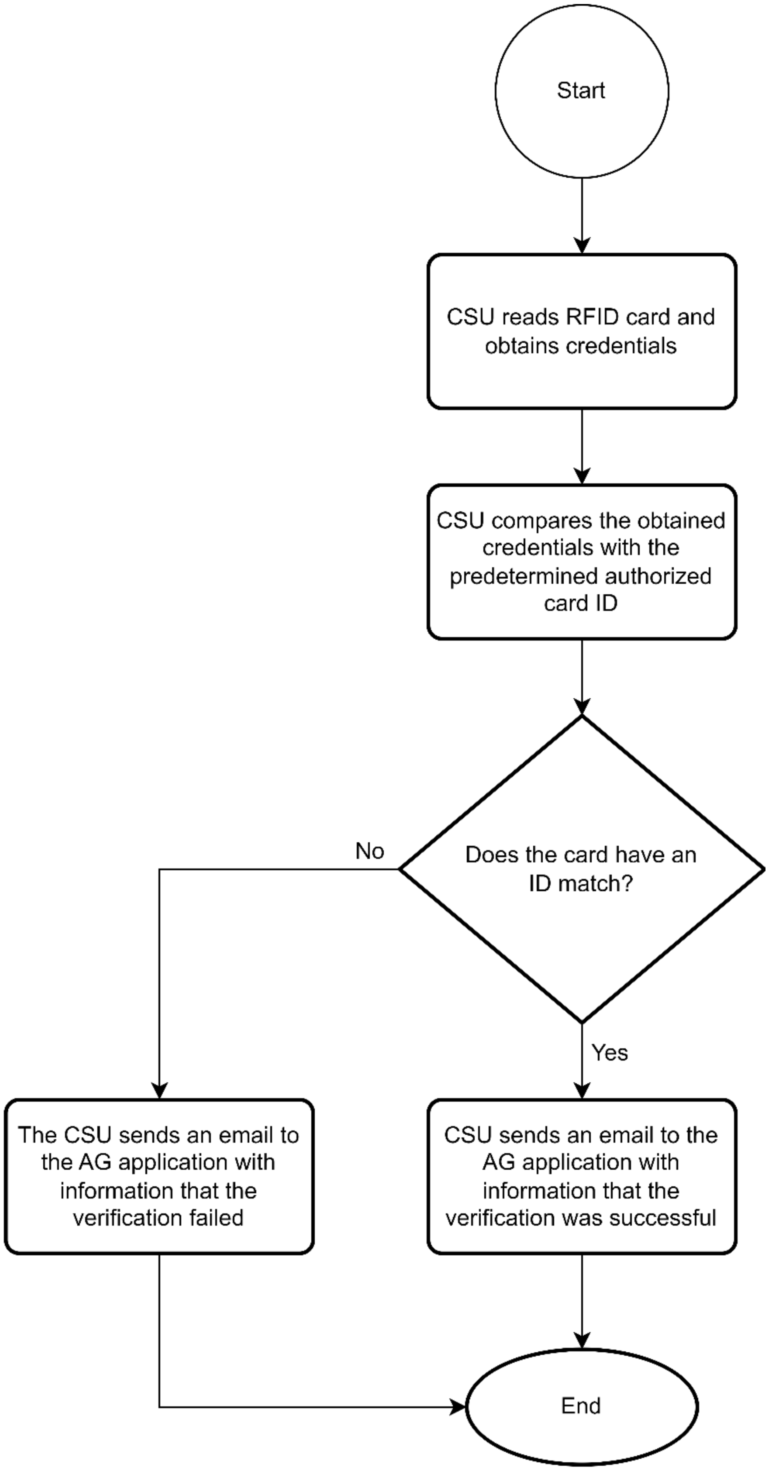
Start
CSU reads RFID card and obtains credentials
CSU compares the obtained credentials with the predetermined authorized card ID
Does the card have an ID match?
No
Yes
The CSU sends an email to the AG application with information that the verification failed
CSU sends an email to the AG application with information that the verification was successful
End

Figure 5: First Authentication Process

After completing the first authentication step, the second authentication step is carried out through the AG application. The AG application is developed using Java programming language in Android Studio. The authorized driver encounters the obligation to create a profile after installing the application on their Android device. To complete the profile creation process, the authorized driver must specify an email address and choose a unique password. During the password-setting stage, the driver can utilize various authentication methods such as PIN, pattern schema, and biometric data (fingerprint and facial recognition). In the background of the AG application, Firebase is used for the authentication process. Firebase serves as backend support to ensure a secure and seamless authentication experience. This mechanism enables the vehicle to grant access only to authorized users, enhancing the overall security and reliability levels.

Firebase operates as a comprehensive mobile and web application development platform, providing a range of cloud-based services and tools. In the context of the AG application's authentication process, Firebase plays a crucial role in securely managing user profiles and authentication credentials. Firebase Authentication, a part of the Firebase suite, offers a robust and scalable solution for verifying user identities.

When an authorized driver creates a profile on the AG application, Firebase Authentication securely stores the chosen email address and password. The platform supports various authentication methods, including email/password, phone number, and federated identity providers such as Google or Facebook. Firebase employs encryption protocols to safeguard user credentials during transmission and storage, ensuring the confidentiality and integrity of sensitive information.

Furthermore, Firebase facilitates the seamless integration of biometric authentication, such as fingerprint and facial recognition, into the AG application. Leveraging Firebase Authentication's capabilities, the AG app can provide a multi-layered security approach, enhancing the overall user experience by offering convenient yet highly secure authentication methods.

In summary, Firebase empowers the AG application with a robust authentication infrastructure, enabling it to validate user identities securely and efficiently through a variety of authentication mechanisms.

After the authorized driver successfully completes the profile creation process, the AG application becomes active. The registration form of the AG application is shown in Figure 6.

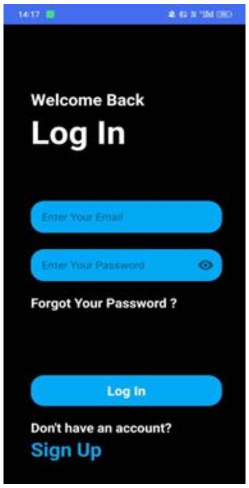

Figure 6: AG Registration Form

The communication between CSU and AG is facilitated through the SMTP. The AG application utilizes the Internet Message Access Protocol (IMAP) to receive emails sent by CSU. The retrieval of email content is achieved through the implementation of Jsoup. Subsequently, the HTML content extracted from the read email content is parsed for further processing.

Email reception is generally a time-consuming process, and this process can lead to unresponsiveness in the application by freezing the user interface. To prevent this negative situation and positively impact the user experience, asynchronous programming has been utilized in the AG application. Asynchronous programming allows the application to manage multiple tasks simultaneously and ensures that the user interface remains responsive. In this context, asynchronous programming methods have been implemented in the AG application using Java's CompletableFuture class. CompletableFuture is a class that represents a task to be completed in the future and is commonly used in Java applications to easily manage asynchronous processes. This class allows other tasks to proceed while waiting for the completion of the authorized driver's email reception process. Consequently, the user interface remains unfrozen, and the application stays responsive.

After the successful completion of the initial authentication step, once the email received from CSU to the AG application is parsed, the authorized driver receives a notification on their phone through the AG application. By clicking on the notification, the authorized driver enters the application. After entering the application, the driver enters their password, which is then verified. Upon successful verification of the password, the AG application sends an email to CSU. The received email is checked by CSU, and upon verification, RKES is triggered, putting the vehicle's locks in an unlocked state. The vehicle's lock statuses can be seen in the AG application. Figure 7 and Figure 8 show the appearance of the vehicle's lock status in the AG application.

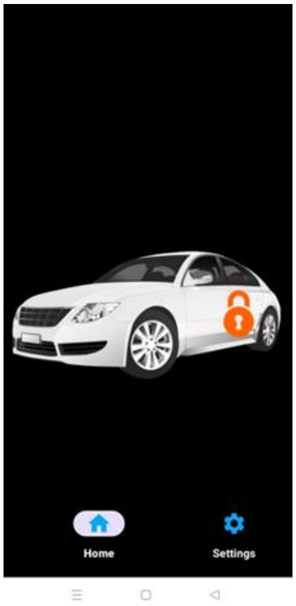

Figure 7: AG Application Vehicle Lock Status

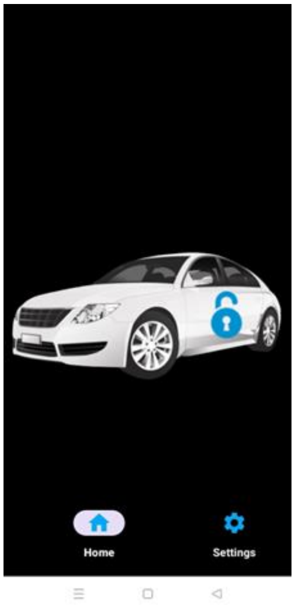

Figure 8: AG Application Vehicle Unlock Status

The block diagram showing the general working principle of the 2FA system is shown in Figure 9 below.

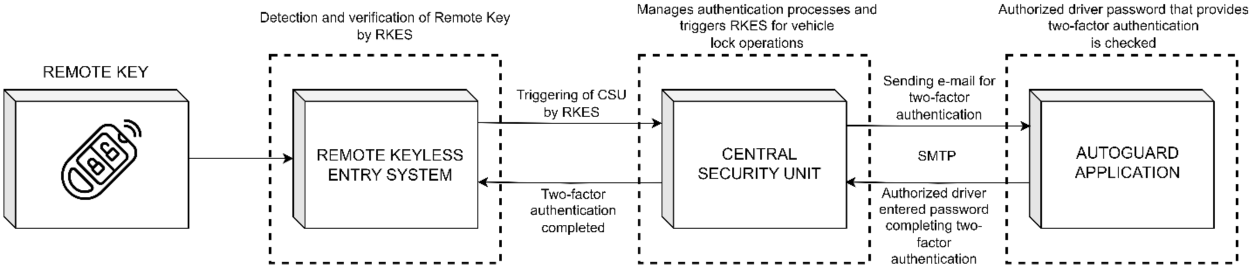
Detection and verification of Remote Key by RKES
Manages authentication processes and triggers RKES for vehicle lock operations
Authorized driver password that provides two-factor authentication is checked
REMOTE KEY
Triggering of CSU by RKES
Sending e-mail for two-factor authentication
REMOTE KEYLESS ENTRY SYSTEM
CENTRAL SECURITY UNIT
SMTP
AUTOGUARD APPLICATION
Two-factor authentication completed
Authorized driver entered password completing two-factor authentication

Figure 9: 2FA System General Working Principle

4. Results

In the coming years, a rapid increase in the adoption of connected vehicles is anticipated as advancements in smart technologies drive the development of various connected features in the automotive sector. In this context, internet-connected vehicles have the potential to enhance safety, comfort, and efficiency by providing drivers with a wide range of information and services. Research indicates that connected vehicle sales are projected to exceed 80 million from 2017 to 2030 in the United States, Europe, and China, as illustrated in Figure 10 [12].

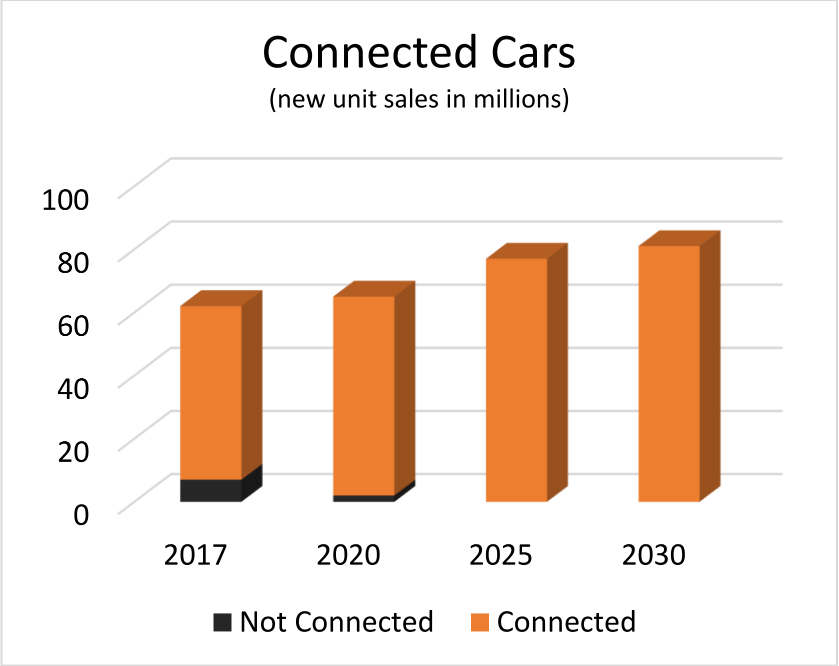

Figure 10: Connected Cars Sales Forecast Chart

This surge in adoption implies a substantial rise in the volume of metadata generated by connected vehicles. The communication between vehicles generates significant data related to driver habits and vehicle performance. Consequently, the proliferation of connected vehicles leads to an increase in metadata, underscoring the growing importance of data management and security strategies in the automotive industry. This abundance of data will play a pivotal role in driving demand for advanced features such as advanced driver-assistance systems, autonomous vehicles, and service-based mobility, further transforming the automotive industry. In this context, industry stakeholders should focus on developing strategies to manage the growing data density and securely leverage this data for continued advancements.

In this context, the developed 2FA system has introduced a new security layer in connected vehicles. This system encompasses the CSU and the AG mobile application, focusing particularly on metadata protection. The system aims to enhance the security of connected vehicles against unauthorized access through a robust second authentication factor and an effective central security unit.

This security layer targets the protection of sensitive metadata stored in connected vehicles. Vehicles are safeguarded through the preferred authentication methods of the drivers. Security measures such as biometric data, pattern recognition, and PIN codes are successfully utilized to prevent unauthorized access to vehicles by individuals who are not the owners or authorized users.

Protecting this metadata is of vital importance in the rapidly evolving landscape of cybersecurity threats. The increasing volume of metadata can potentially lead to dangerous cyber-attacks and breaches of personal privacy. Therefore, this 2FA system in connected vehicles keeps drivers' and vehicle owners' data secure, further enhancing cybersecurity.

2FA system is an effective solution not only for individuals but also for ensuring the security of connected vehicles intended for corporate and commercial purposes. Particularly in scenarios involving shared vehicle usage, such as rental car fleets or corporate vehicles, the 2FA system provides effective protection against unauthorized usage. The system implements a strong second authentication factor to ensure that vehicles are only used by authorized drivers. This strengthens security in leasing processes and corporate vehicle usage, prevents unauthorized vehicle usage, and preserves corporate assets. This is especially beneficial for companies and vehicle rental firms in managing their vehicles more securely and efficiently.

In conclusion, the Two-Factor Authentication system presented in this study provides an effective solution for enhancing the security of metadata in connected vehicles. By offering a more robust defense layer against cybersecurity threats, the system increases the security of valuable information stored in connected vehicles and protects the digital assets of drivers.

5. Discussion and Conclusion

In the discussion section of this study, a detailed evaluation of the system's performance and applicability has been conducted. The presented 2FA system successfully achieves its goal of protecting the metadata stored in connected vehicles. However, it is crucial to consider the potential areas for future development of the system.

One of the prospective areas for future development in this study is the integration of AG functionality with location data to provide a more comprehensive security layer. This integration could enhance the 2FA process by utilizing real-time location information from the driver's phone. Specifically, the driver's presence or absence in a particular location can become a significant criterion in security authentication.

The advantages that this integration could offer include the ability to more accurately determine whether the driver is physically near the vehicle. For instance, in situations where the driver's phone is not in proximity to the vehicle, the 2FA process can be enforced more rigorously, effectively preventing potential attackers from attempting remote identity authentication.

Additionally, exploring new authentication factors or methods to add more security measures and reduce potential attack vectors is another avenue for future development. For example, considering increased use of biometric data for securing the driver's phone or implementing more complex encryption algorithms for phone security could be contemplated. These additional measures can fortify the 2FA system, minimizing potential security vulnerabilities.

By integrating AG functionality with location data, the 2FA system used in connected vehicles could potentially elevate its security level and provide a robust foundation for future enhancements.

6. Acknowledge

We express our appreciation to Huseyin Karacali, the Software Architect, for his adept guidance and inspirational leadership. Furthermore, we recognize the invaluable support extended by TTTech Auto Turkey during the project's evolution.

References

[1] “Remote Keyless Entry Systems Overview | Analog Devices.” https://www.analog.com/en/app-notes/remote-keyless-entry-systems-overview.html.

[2] “Remote Terminal Unit - an overview | ScienceDirect Topics.” https://www.sciencedirect.com/topics/engineering/remote-terminal-unit.

[3] “Car Keyless Entry vs Remote Keyless Entry: What.” https://vaistech.com/remote-keyless-entry-vs-keyless-entry-whats-the-difference/.

[4] “Raspberry Pi 3 Model B+.” https://datasheets.raspberrypi.com/rpi3/raspberry-pi-3-b-plus-product-brief.pdf.

[5] “Raspberry Pi OS – Raspberry Pi.” https://www.raspberrypi.com/software/.

[6] “PyQt - Python Wiki.” https://wiki.python.org/moin/PyQt.

[7] “RC522 RFID Module Pinout, Features, Specs & How to Use It.” https://components101.com/wireless/rc522-rfid-module.

[8] “Buy RC522 RFID Card Reader Module 13.56MHz Online at Robu.in.” https://robu.in/product/rc522-rfid-card-reader-module-13-56mhz/.

[9] “Android Developers: Android Mobile App Developer Tools.” https://developer.android.com/

[10] “Add Firebase to your Android project | Firebase for Android.” https://firebase.google.com/docs/android/setup

[11] “What is the Simple Mail Transfer Protocol (SMTP)? | Cloudflare.” https://www.cloudflare.com/learning/email-security/what-is-smtp/

[12] G. Zaffiro and G. Marone, “Smart Mobility: new roles for Telcos in the emergence of electric and autonomous vehicles,” *2019 AEIT International Conference of Electrical and Electronic Technologies for Automotive (AEIT AUTOMOTIVE)*, Jul. 2019, doi: 10.23919/eeta.2019.8804575.