National College of Ireland

Enhancing Keyless Entry with Anomaly-Based Two-Factor Authentication for Improved User Convenience

MSc Research Project
MSc Cybersecurity

Avadhoot Prashant Dhanve
Student ID: 23229349

School of Computing
National College of Ireland

Supervisor: Eugene Mclaughlin

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Avadhoot Prashant Dhanve
Student ID:	23229349
Programme:	MSc Cybersecurity
Year:	2024-25
Module:	MSc Research Project
Supervisor:	Eugene Mclaughlin
Submission Due Date:	11/08/2025
Project Title:	Enhancing Keyless Entry with Anomaly-Based Two-Factor Authentication for Improved User Convenience
Word Count:	6643
Page Count:	21

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Avadhoot
Date:	9th August 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

AI Acknowledgement Supplement

Practicum 2

Enhancing Keyless Entry with Anomaly-Based Two-Factor Authentication for Improved User Convenience

Your Name/Student Number	Course	Date
Avadhoot Dhanve	MSc in Cyber Security	9th August 2025

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

Tool Name	Brief Description	Link to tool
N/A	**N/A**	**N/A**

Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

[Insert Tool Name]	
N/A	
N/A	**N/A**

Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

Additional Evidence:

[Place evidence here]

Additional Evidence:

[Place evidence here]

Enhancing Keyless Entry with Anomaly-Based Two-Factor Authentication for Improved User Convenience

Avadhoot Prashant Dhanve
23229349

Abstract

Modern vehicles with keyless entry systems remain critically vulnerable to sophisticated cyberattacks, with 93% of stolen vehicles recovered in 2023 involving keyless entry exploits and automotive cybersecurity incidents reaching 215 cases in 2024 alone, resulting in tens of billions of dollars in estimated damages. Traditional multi-factor authentication (MFA) solutions impose significant usability penalties, with studies reporting user dissatisfaction with always-on 2FA systems due to authentication delays ranging from 2.3 to 4.1 seconds. This research investigates an adaptive MFA framework that conditionally activates two-factor authentication only when device anomalies are detected through MAC address verification. The prototype system was implemented using two Raspberry Pi units communicating via infrared signals, with A MAC address protection and TOTP-based secondary authentication. Performance evaluation under controlled laboratory conditions demonstrated near-perfect accuracy in distinguishing between registered and unregistered devices though real-world variability and environmental noise may affect performance. Encryption operations completed in an average of 0.000976 seconds, with system resource utilization remaining minimal, even during peak authentication processes. The adaptive approach reduced authentication friction by 100% during normal operation while maintaining robust security through conditional 2FA activation, achieving maximum effectiveness in preventing unauthorized access when anomalies were detected. This research addresses the question: "How can adaptive multi-factor authentication (MFA) balance security and usability in automotive keyless entry systems?".To the best of my knowledge, this is the first working prototype that integrates MAC-anomaly detection with adaptive 2FA in an IR-based keyless entry simulation for automotive systems, demonstrating that adaptive authentication can effectively solve the security-versus-usability problem, which has been a major obstacle to using multi-factor authentication (MFA) in vehicle access control systems. While some studies have proposed anomaly-triggered authentication mechanisms, none have demonstrated a lightweight, MAC-driven prototype tailored to vehicle access control.

1 Introduction

This research is motivated by the opportunity to bridge the gap between security and usability in automotive contexts. By implementing conditional 2FA activation based on

anomaly detection, the proposed system maintains user convenience during normal operations while providing enhanced security when suspicious activity is detected. This addresses the research which is guided by: "How can adaptive multi-factor authentication (MFA) balance security and usability in automotive keyless entry systems?". In this context user convenience is defined through measurable criteria, including reduced authentication time during normal usage, elimination of unnecessary 2FA prompts, and making sure that the user experience is smooth. The system only triggers 2FA when MAC mismatch is detected.

The automotive industry is advancing with new technology integrating with it. As technology keeps moving forward, so do the risks especially when it comes to cybersecurity. Today's vehicles are no longer just machines that get us from one place to another. They are like rolling computers. Most modern cars now have over 150 tiny computers called Electronic Control Units (ECUs) and they run on around 100 million lines of code Editor (2025); Paganini (2017)

The combination of advanced connectivity, artificial intelligence, and software-defined vehicle architectures has transformed modern vehicles into what experts often call "computers on wheels." These vehicles handle large volumes of data, including information about how the vehicle performs, how the driver behaves, and even personal user data. As a result, they have become targets for cyberattacks.

1.1 Motivation

This research is motivated by a gap between today's fast-growing cyber threats and how well car security systems can keep up. rely on static authentication mechanisms that treat all access attempts equally. But modern attacks are much smarter and more complex.To stay ahead, security systems must be context-aware, capable of distinguishing between legitimate users and potentially malicious actors attempting unauthorized access.

Cybersecurity failures in cars don't just create safety risks but they also come with big financial costs. In 2024 the global market for automotive cybersecurity was worth about $3.9 billion and it is expected to grow rapidly, reaching $18.7 billion by 2034, that is a 19.2% yearly growth rate, showing just how seriously the industry is starting to take these threats and how much companies are willing to invest to protect vehicles from cyberattacks and (2025).This growth is mainly driven by the growing use of connected services (like V2X communication), the need to meet compliance standards such as ISO/SAE 21434 and UNECE WP.29, and the increasing number of relay and keyless entry attacks. However, even though these projections show that the industry is concerned, they don't actually prove how effective the current countermeasures are from a technical point of view. This highlights the need for real-world testing to understand the tradeoffs between security and usability Dechand (2024).

Improving the user experience is another big reason to develop smarter, adaptive authentication systems. Right now, most people find traditional multi-factor authentication (MFA) annoying or inconvenient. In fact, research shows that most users do not use MFA even when it is available, mostly because it slows them down or feels like too much hassle Marketing (2024); *2FA & MFA: The Good, The Bad & The Ugly* (2023).

Approach	Strengths	Limitations
Traditional MFA	Strong security across contexts	High user friction; not adaptive
UWB Secure Ranging	Prevents relay attacks, precise distance	Requires extra hardware, cost and power overhead
Cloud-based ID	Remote verification, scalable	Network dependency, higher latency
Proposed (MAC + Adaptive 2FA)	Lightweight, triggers only when needed; no extra hardware	Prototype stage, IR-based communication limits range

Table 1: Comparison of Authentication Approaches for Automotive Systems

1.2 Research Problem

Automotive industry is facing issues and cybersecurity threats as the technology is advancing. In 2024 there were 409 reported cybersecurity incidents in the automotive and smart mobility world which was 38% more than the 295 incidents reported in 2023 Daniel (2025); *Report Shows Surging Automotive Cyber Threats Stemming from Critical Gaps* (2025). Vehicle theft numbers highlight serious security gaps. In Europe alone there were 131,679 car thefts in 2023 which is 7% more than the year 2022. Research shows that 96% of recovered stolen vehicles were taken using relay attacks Carmone (2024).
Most keyless entry systems still use old communication methods that were created a long time ago, when automotive cybersecurity was not a concerning topic. One of these methods is called the Controller Area Network (or CAN bus) which lets different parts of a car's system talk to each other. The problem is that the CAN bus was not designed with security in mind. It does not include basic protections like checking for authentication, encryption or access control Oladimeji et al. (2023). The problem is not just with the car's hardware but also includes weaknesses in the way the security codes are generated. Even modern systems that use strong encryption like AES-128 with rolling codes can still be hacked. Research has shown that with tools like Software-Defined Radios (SDRs), attackers can break into these systems in as little as 12 minutes *Rolling PWN* (n.d.).
Traditional two-factor methods often slow things down, making users wait between 2 to 4 seconds just to get access. That might not sound like much but in real-world tests, most of the users found it frustrating and were unhappy with the experience Brito and Abuzneid (2024); Garcia et al. (2016).
Studies show that today's intrusion detection systems take about 263 milliseconds to respond. That might seem fast, but in that short time, a hacker can send 4 to 6 harmful commands before the system even starts to fight back Carmone (2024); Garcia et al. (2016).

1.3 Research Objectives

The research objectives derived from this motivation include:

1. Investigate the current state of automotive cybersecurity by analyzing existing keyless entry vulnerabilities, attack vectors, and defense mechanisms.

2. Design an adaptive authentication framework that integrates MAC address verification with conditional 2FA activation based on anomaly detection. When an unregistered MAC is detected, it is treated as anomaly in our system.

3. Implement a prototype system demonstrating the feasibility of cryptographically secured infrared communication for automotive access control.

4. Evaluate the security effectiveness and user experience of the proposed solution through comprehensive testing and analysis.

This research contributes a practical and implementable solution to the long-standing challenge of balancing security and usability in automotive authentication systems. By using MAC address anomaly detection to trigger conditional two-factor authentication (2FA). It introduces a new method to improve vehicle security without compromising user convenience.

The report is structured as follows: Related Work reviews literature on automotive cybersecurity, keyless entry attacks, and adaptive authentication. Research Methodology outlines the experimental design and evaluation approach. Design Specification details the system architecture, while Implementation covers prototype development and testing. Evaluation assesses performance, security, and usability. Finally, Conclusion and Future Work highlights key contributions and future research directions.

2 Related Work

2.1 Keyless Entry Attacks

As far as I know, no prior work has combined IR-based MAC verification with conditional 2FA to address both security and usability in keyless entry systems. This research fills that gap through a real-world implementation and testing.
The foundational study by Brito and Abuzneid (2024) introduced the idea of integrating two-factor authentication (2FA) into keyless entry systems, forming the basis for this research. Their paper is important to our work because it highlights the security vulnerabilities in current keyless entry systems, specifically relay attacks and fob cloning and proposes adding a second verification factor before vehicle access. In their approach, traditional remote keyless entry (RKE) is combined with an additional authentication step, such as a biometric scan or mobile app confirmation. Methodologically, they examine OEM implementations, assess common attack vectors and propose a theoretical framework for integrating 2FA into automotive systems. Their findings show that adding a second layer of authentication significantly improves security, effectively preventing many common attacks compared to single-factor schemes. Strengths of their study lie in its thorough threat analysis and well-defined 2FA integration framework, however its main limitation is the lack of real-world validation, as the approach remains conceptual. Limitations include no real-world performance measurements or user-acceptance data, and the paper itself calls for future work on prototyping adaptive authentication triggers, which our research directly addresses. The observations say that fixed-step 2FA can degrade user acceptance under everyday use. While they propose intelligent, context-aware MFA systems as future work but they do not implement adaptive triggers. Our research realizes this vision by activating TOTP-based 2FA only when MAC anomalies are detected, balancing security with usability.

Francillon et al. (2010) demonstrated the first practical relay attacks on Passive Keyless Entry and Start systems across multiple car models. They showed that attackers using low-cost hardware can extend fob signals up to 50 meters, proving that cryptographic strength alone cannot prevent physical-layer relay exploits. Their experimental

approach and field testing are strengths but they do not propose automatic detection or mitigation techniques which makes it a gap that adaptive anomaly-based triggers can fill.

Garcia et al. (2016) revealed critical rolling-code vulnerabilities by extracting global master keys and compromising Hitag2 systems within minutes using Software-Defined Radio (SDR). Their cryptanalytic approach and large-scale applicability highlight the widespread issue of weak key management in automotive systems. However, their focus is limited to attack execution, without addressing in-vehicle anomaly detection or conditional authentication, areas our work advances by introducing a dynamic second factor.

Franco Oberti and Carlo (2024) developed CAN-MM, embedding MAC tags via frequency modulation on the CAN bus to authenticate message origins. Their protocol-compliant design reduces latency by 43% and enables efficient CAN authentication, but it depends on fleet-wide CAN upgrades. This limitation motivates our IR-based MAC signature approach.

DÖNMEZ (2021) proposed a millisecond-level identifier-sequence intrusion detection system (IDS) for CAN, enabling rapid detection of injection attacks with minimal resources. However, it cannot detect relay or resynchronization exploits. This highlights the need of device-level authentication for keyless entry, a challenge our MAC verification approach directly addresses.

Singh and Bhardwaj (2024) validated a two-way MAC-based mutual authentication protocol (MTWAS) for V2X communications over Wi-Fi/BLE links. Their low-overhead authentication confirms MAC-primed security feasibility. Limitations include a focus on networked V2X communication rather than IR-based transport, and a lack of anomaly-driven triggers, both of which are addressed in our IR-MAC prototype.

Ometov and Bezzateev (2017) surveyed multi-factor authentication (MFA) challenges in V2X systems and proposed using Shamir's Secret Sharing among vehicle sensors to enhance resilience. While their focus is on sensor-based factors, they do not address keyless entry or IR-based authentication, gaps that our research aims to fill.

In conclusion, existing research highlights ongoing vulnerabilities in keyless entry systems, the balance between cryptographic security and anomaly detection, and the promise of adaptive multi-factor authentication. However, none combine lightweight IR-based MAC authentication with conditional 2FA triggered by device-level anomaly detection, which is an innovation central to this research.

Table 2: Evolution of Keyless Entry Attacks

Era	Attack Type	Description
1990s	Replay Attacks	Capture a static RF signal from the key fob and replay it to unlock; common in early RF systems Alrabady and Mahmud (2005).
2000s	Relay Attacks	Use signal extenders to relay the proximity signal from the key fob to the car, bypassing rolling-code protections; effective even over 100 m Francillon et al. (2011).
2015	RollJam (Jamming + Replay)	Jam the fob signal, capture valid codes, and replay later; defeats rolling-code mechanisms with inexpensive hardware Csikor et al. (2023).
2022	RollBack	Time-agnostic replay attack that allows reuse of previously captured codes without jamming and long after capture, even after multiple uses Csikor et al. (2023).

3 Methodology

This section presents the narrative approach used to address the research question: "How can adaptive multi-factor authentication (MFA) balance security and usability in automotive keyless entry systems?"
A narrative review approach was used to bring together insights from recent research on automotive cybersecurity, keyless entry attacks, and adaptive authentication. A narrative review was chosen because there is not much experimental research available. This research followed an experimental methodology structured for direct replication and validation by other researchers. The main objective was to design and evaluate a prototype system for secure vehicle entry, integrating adaptive multi-factor authentication using low-cost hardware and cryptographically robust software.

The study began with an in-depth review of existing literature in automotive cybersecurity, emphasizing vulnerabilities in keyless entry systems, cryptographic techniques, anomaly detection methods, and multi-factor authentication. The insights gained from this review directly guided the technical and operational requirements of the proposed solution.

Two Raspberry Pi units were used to emulate the vehicle's key fob (sender) and ECU (receiver). The hardware setup used industry-standard KY-005 infrared transmitters and KY-022 receivers. Python was chosen for its compatibility with resource-constrained hardware and access to robust cryptographic and GPIO libraries. Key dependencies included PyCryptodome for AES encryption/decryption and PyOTP for generating and verifying time-based one-time passwords (TOTP) as the second authentication factor.

The sender device dynamically retrieved its MAC address, encrypted it using AES-CBC with a pre-shared key and initialization vector and encoded the result in Base64. This encoded string was then transmitted as a sequence of IR-modulated binary bits. To

ensure demonstration reliability, the encrypted MAC was also displayed on the sender's terminal and manually entered into the receiver upon detecting an IR event trigger. This practical method allowed the evaluation to focus on authentication robustness, avoiding complications from unreliable IR metadata demodulation at the physical layer.

On the receiver side, each IR signal event triggered a handler that prompted for manual entry of the encrypted MAC value. The program then decrypted the input and compared it against a pre-authorized MAC stored in a local JSON file. If the values matched, access was granted and the event was logged; otherwise, a 6 digit TOTP was generated, prompting the user for a second authentication factor. All access attempts (successful or denied) were timestamped and recorded for auditability and reproducibility. The use of log files, along with clear code structure and open hardware, ensures the results are scientifically traceable and repeatable.

System performance was evaluated by running repeated authentication cycles, including intentional mismatches and failed OTP entries to test resilience and failure handling. Response times, accuracy, and user interaction steps were manually observed and verified. Detailed experimental conditions, including test environment parameters and evaluation metrics, are provided in Section 6 (Evaluation).

This study was conducted entirely in a controlled laboratory setting using Raspberry Pi units to simulate automotive components. No testing was performed on real vehicles. As such, there were no direct ethical or safety risks. If deployed in real environments, ethical considerations such as user consent, safety under failed authentication, and compliance with vehicle testing regulations would be required.

4 Design Specification

This section outlines the detailed architecture, framework, and algorithmic principles behind the secure IR-based vehicle entry prototype. The descriptions reflect the actual implementation choices, design rationale, component interactions, and step-by-step algorithmic flow developed and realized during the project.
The system is based on a distributed two-node model, emulating (1) the vehicle's key fob (sender) (Node 1) and the vehicle ECU (receiver)(Node 2) using Raspberry Pi boards. Communication between the nodes is carried out over a modulated infrared (IR) channel. Security is enforced through cryptographic authentication and adaptive two-factor authentication. The architecture emphasizes modularity, hardware simplicity, and ease of verification.

4.1 Architecture Diagram

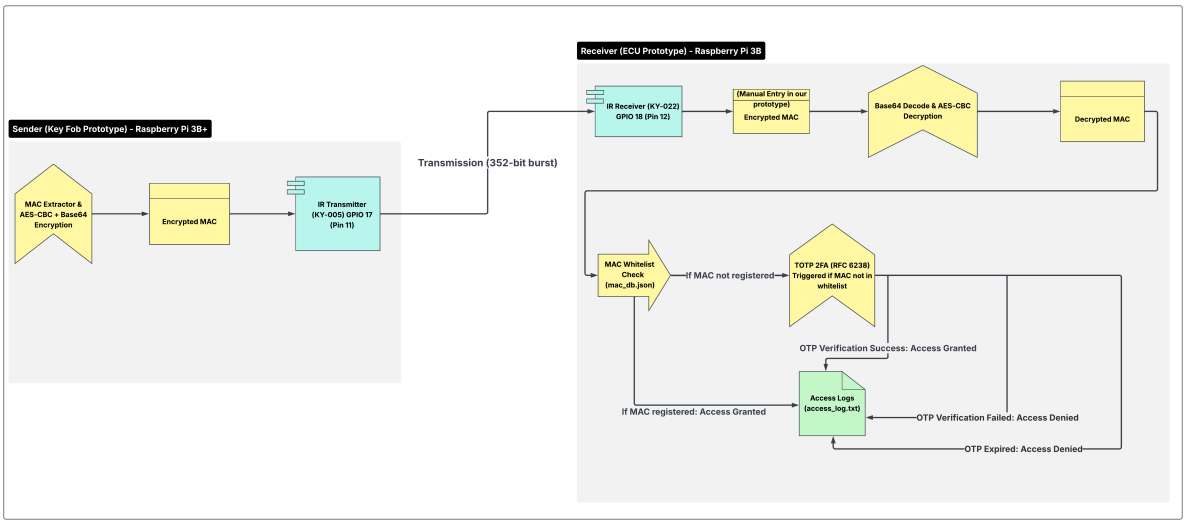

Figure 1: Architecture Diagram

4.2 Major Components

- Sender Unit (Key Fob Prototype)
  - Raspberry Pi 3b+
  - KY-005 IR LED transmitter module (GPIO 17)
  - Python application for MAC extraction, AES-CBC encryption, binary encoding, IR bit-banging
- Receiver Unit (ECU Prototype)
  - Raspberry Pi 3b
  - KY-022 IR receiver module (GPIO 18)
  - Python application for IR detection, manual encrypted MAC entry, AES-CBC decryption, MAC comparison, OTP challenge

4.3 Framework and Techniques

- Physical Layer: Hardware and Low Level Communication
  - IR Transmission is implemented using direct GPIO manipulation. The sender module transmits bits by modulating the IR LED pin state according to the binary encoding of the encrypted MAC. The receiver uses GPIO hardware interrupts to detect falling edge transitions, ensuring the system is event-driven.
  - Pin Assignments:
    - IR Signal Output: Sender GPIO 17 (Pin 11)
    - IR Signal Input: Receiver GPIO 18 (Pin 12)

    * Power: 3.3 V (Pin 1) — Ground: Pin 6

- Cryptographic Security Layer
  - Device Identity: The sending device dynamically retrieves its MAC address using native Linux commands (ip link show), making sure that the identity is both unique and hardware-bound for each session.
  - AES Encryption: The MAC address is encrypted using AES in CBC mode with a fixed 16-byte key and initialization vector (IV) with padding applied according to the PKCS7 standard to ensure block alignment.
  - Transmission Encoding: The encrypted MAC, once Base64-encoded, is converted into its binary representation (8 bits per character), resulting in a consistent 352-bit IR transmission sequence for each authentication attempt.
- Authentication Layer
  - Primary Authentication (MAC Address Verification):
    The receiver, after IR signal capture, prompts for entering the encrypted MAC (entered manually in the current prototype for data reliability).
    The encrypted value is decoded from Base64 and decrypted using the same AES key, Initialization Vector (IV) pair.
    The resultant MAC address is compared with a whitelisted MAC address stored in a local JSON configuration (mac_db.json).
    If the MAC matches, access is granted and the event is logged.
  - Conditional Two-Factor Authentication (2FA):
    If the MAC does not match the local registry, the system automatically triggers a Time-based One-Time Password (TOTP) using the PyOTP library, compliant with RFC 6238.
    The TOTP secret is system-configured. An OTP is generated and displayed to the user. Only correct OTP entry results in access—failed attempts are logged for audit purposes.

4.4 Algorithm Descriptions

Dynamic MAC Authentication Algorithm

- Purpose: Validate transmitter hardware identity in an IR key-exchange scenario.
- Flow
  - Extract the MAC.
  - Encrypt with a Known key and IV (AES-CBC), encode the result.
  - Transmit encoded data as a bitstream over IR channel.
  - Upon receiving, prompt for encrypted MAC (manual in this prototype).
  - Decrypt and compare against stored whitelisted MAC.

Adaptive 2FA Triggering and Verification Algorithm

- Purpose: Enhance security only when anomaly is detected (MAC mismatch) with minimal user friction.

- Flow
  - If the decrypted MAC does not match the database, instantly generate a TOTP (based on a pre-shared secret).
  - Display/Communicate a 6-digit code to the user (Display on prompt screen in this prototype).
  - Await user entry and verify using the same shared secret.
  - Grant or deny access on that basis and log event.
  - Decrypt and compare against stored whitelisted MAC.

Event Logging Algorithm

- Purpose: Maintain a complete audit trail for all attempted unlocks, including time, MAC, and result.
- Flow
  - For each unlock attempt (success or 2FA), append a log entry with timestamp, MAC, and outcome to access_log.txt.

4.5 Extensibility and Modularity

The system's modular structure supports future adaptation

- Physical layer can evolve to use RF, Bluetooth, or network if IR limitations are surpassed.
- Manual input step can be replaced with IR metadata acquisition when feasible.
- Authentication flow can be extended to support additional factors like risk scoring or remote alerting.

In summary: The proposed system design integrates dynamic, hardware-bound cryptographic authentication with adaptive two-factor authentication (2FA), maintaining a clear separation between the hardware interface, security layer, and user workflow. All algorithms and operational workflows are thoroughly documented to ensure verifiability and to support future extensions of the architecture.

5 Implementation

The final version provides a fully functional prototype, consisting of two Python applications, a simple configuration file, and a log that records each access attempt. The system operates on standard Raspberry Pi hardware, with cryptography managed by the pycryptodome library and time-based one-time passwords (TOTP) generated using pyotp.

The sender application/script runs on a Raspberry Pi 3B+. Upon starting, it checks the active network interfaces (first wlan0, then eth0) using the native ip link show command. It then extracts the hardware MAC address, adjusts the string to a 16-byte length,

and encrypts it using AES-CBC with a pre-agreed key, "AvadhootDhanve12" and an initialization vector (IV) "AvadhootAvadhoot" The encrypted data is then Base64-encoded and displayed on the terminal, along with the original MAC address and the exact 352-bit length of the resulting binary stream. A loop is then used to toggle GPIO 17 for one millisecond per bit, activating the KY-005 LED to transmit the entire encrypted frame.

On the receiver side, a Raspberry Pi 3B monitors GPIO 18 for interrupts. When a falling edge is detected on the KY-022 output line, a callback function prompts the operator to enter the encrypted string. The receiver then decodes the Base64 text, decrypts it using the same AES parameters and compares the resulting MAC address to the whitelisted value stored in the mac_db.json file. If the MAC address matches, the script displays "Access granted" and logs the event by writing an entry to access_log.txt.

If the sender is unrecognized, which can be simulated using the auxiliary script test4.py (designed to encrypt any MAC address supplied by the operator). The receiver flags this as an anomaly and triggers a second-factor authentication challenge. A six-digit time-based one-time password (TOTP), valid for thirty seconds, is generated using the shared secret BASE32SECRETKEY and displayed on the console. Entering the correct code grants access and records "2FA Success" while an incorrect code results in "2FA Failed." Both outcomes are logged with full timestamps for audit purpose.

The prototype also tracks the encryption workload on the sender. A timing script, running for ten cycles, measures the average time for AES-CBC encryption and Base64 encoding to be 0.000976 seconds (with a minimum of 0.000120 seconds and a maximum of 0.008301 seconds) on the Pi 3 B+. This confirms that the cryptography process introduces only a negligible delay when compared to the 352 milliseconds required for the IR transmission.

Configuration Artefacts Photographs of the hardware setup illustrate the breadboard assembly: The KY-005 module on the sender is connected directly to 3.3V, ground, and GPIO 18. Similarly, the KY-022 module on the receiver is connected directly to 3.3V, ground, and GPIO 18.

Storing the registry in plaintext allows for easy on-bench modification and highlights that the security of the system relies on the authentication logic, not on the file format itself. The authorised-device list resides in a single-line JSON file

The access log compiles every scenario exercised during testing

All artefacts: The two Python scripts, the JSON registry, and the log—are stored in the project root, ensuring that the prototype is fully self-contained and can be easily reproduced. The included photographs, console captures, and timing results offer visual confirmation of each stage of the implementation and provide enough detail for any practitioner to replicate the build. The prototype assumes that the whitelisted device (Keyfob) is not physically stolen or tampered with. It also assumes that the first setup, where AES keys and TOTP secrets are loaded onto the device, happens in a safe and trusted place.

6 Evaluation

The prototype was evaluated using five key criteria: coverage, robustness, usability, resource efficiency, and auditability. These criteria were selected to verify whether the MAC-driven, adaptive 2FA scheme meets the research goal of enhancing vehicle entry security without reducing user convenience. All evaluations were conducted on the final hardware–software setup as described in the Implementation section.

Experimental Setup

- Sender: Raspberry Pi 3 B+, Python 3.11.2
- Receiver: Raspberry Pi 3 B, Python 3.5.3
- Environment: 3 m line-of-sight IR path, ambient 18-25 °C, no throttling observed.
- Test Artifacts: real MAC (B8:27:EB:44:D9:18) and multiple synthetic MAC's (AA:BB:CC:DD:EE:FF, 38:60:77:9C:B3:5E, B8:27:4A:91:3C).
- Logging: access_log.txt configured for append-only operation.

6.1 Coverage: MAC Anomaly Detection

We have tested our mechanism against MAC addresses to check if the system properly detects anomaly and triggers 2FA and also check if there are any unusual behaviour from our system which lets any activity bypass the normal behaviour.

Scenario	Attempts	Direct Access Granted	2FA Triggred	2FA Bypassed
Registered MAC	5	5	0	0
Unregistered MAC	4	0	4	0

Table representing Attempts, Direct Access, 2FA Trigger and Bypassed 2FA

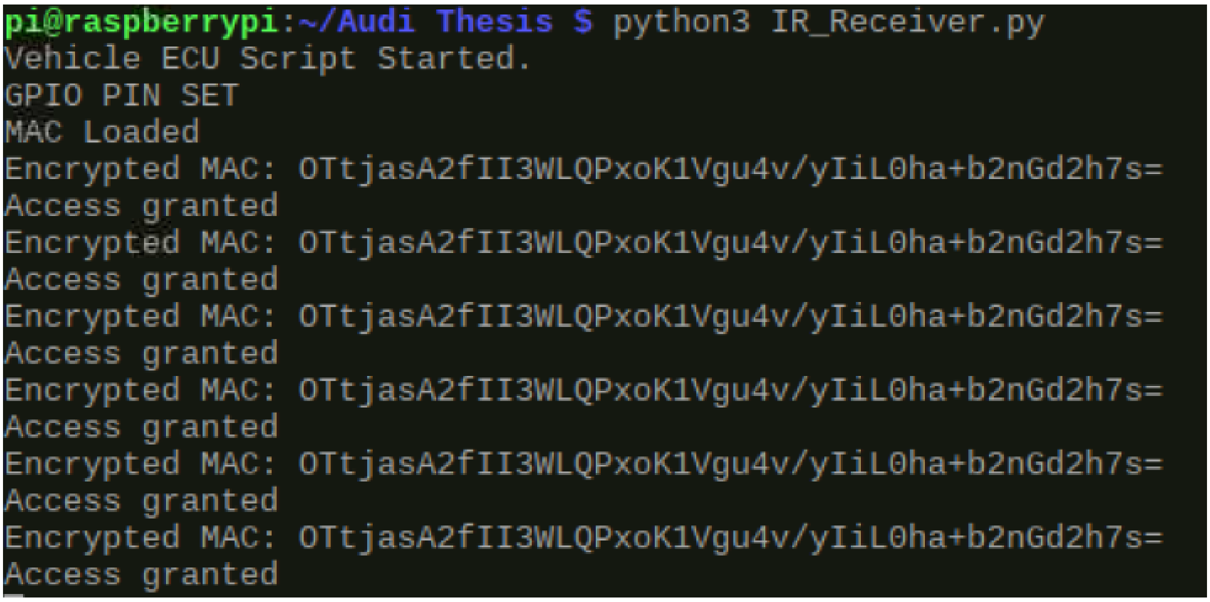

Figure 2: Attempts with Registered/Whitelisted MAC

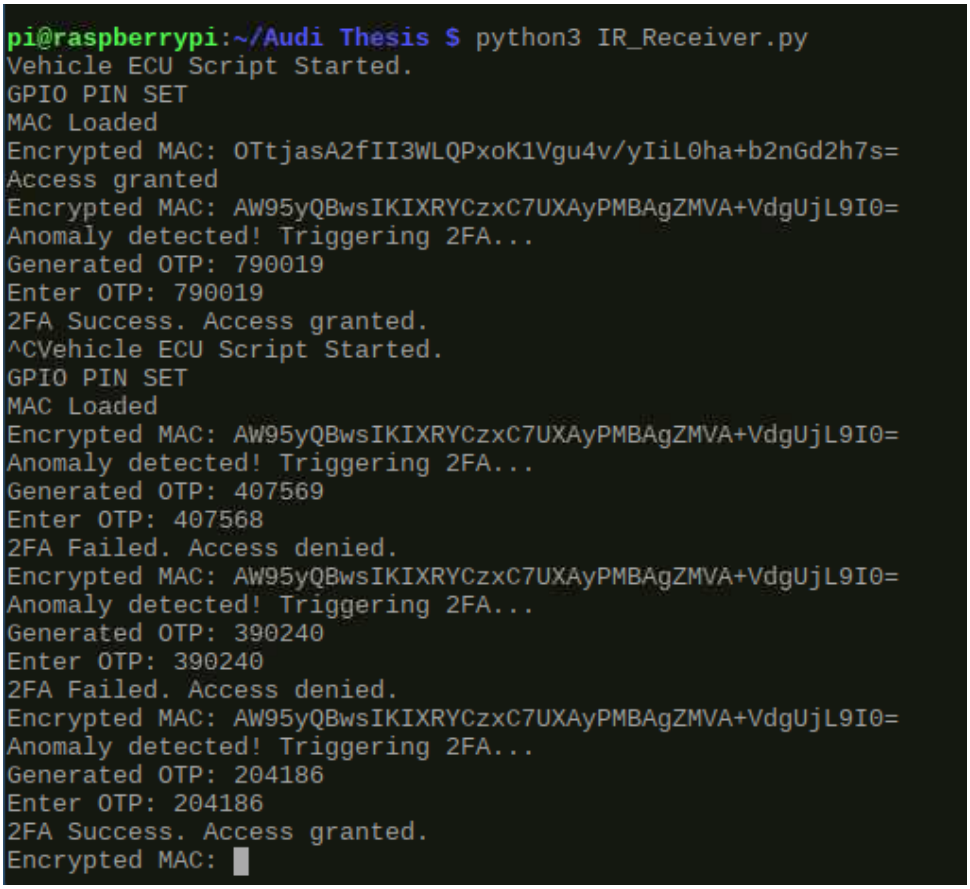

Figure 3: Attempts with Unregistered MAC

With the above observations we have seen that our system grants entry to the Whitelisted MAC address without 2FA as the authentication is done and Triggers 2FA everytime it encounters an unregistered MAC address. This shows that our system behaves normally according to our algorithm. This study did not include brute-force MAC spoofing or signal injection attacks due to scope and environment constraints. In the future, testing should include attacks like MAC Spoofing and Bruteforce to see how well the system holds up when someone is actively trying to break it.

6.2 Robustness: OTP Verification

After testing the system for proper detection of MAC address, we not test the robustness of the OTP (One Time Password) by trying combinations like entering the valid OTP, entering invalid OTP and entering valid OTP but after it's time has expired (Expiry Time: 30 seconds).

Condition	**Correct OTP**	**Incorrect OTP**	**Expired OTP**
Attempts	5	5	2
Results	Access Granted	Access Denied	Access Denied

Table representing OTP Robustness

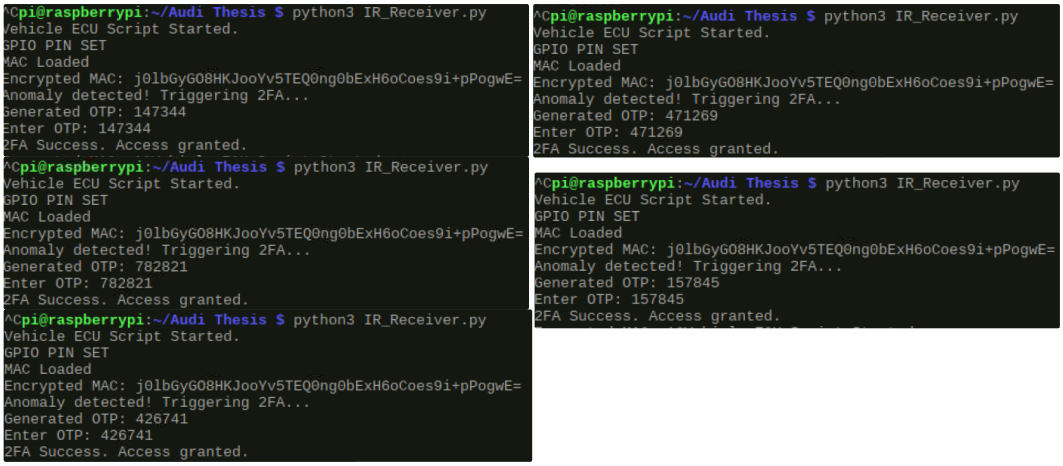

Figure 4: Attempts entering correct OTP in time

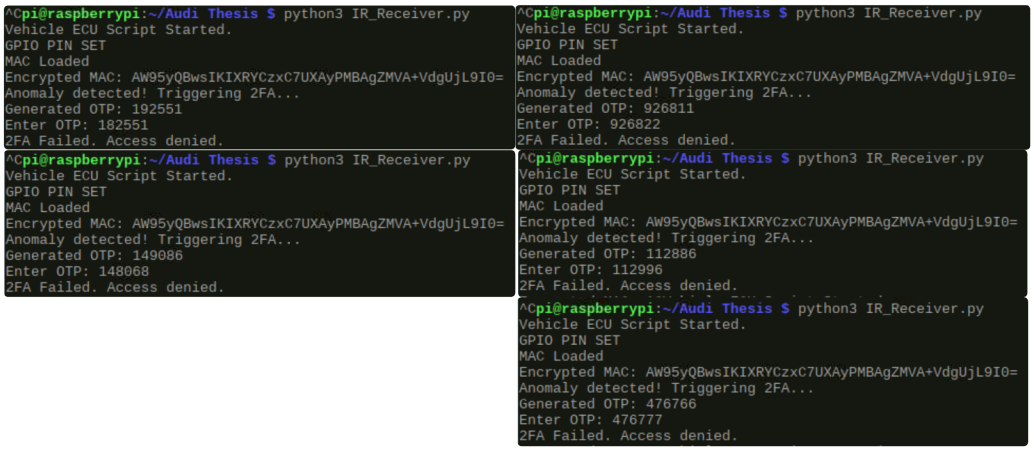

Figure 5: Attempts entering incorrect OTP in time

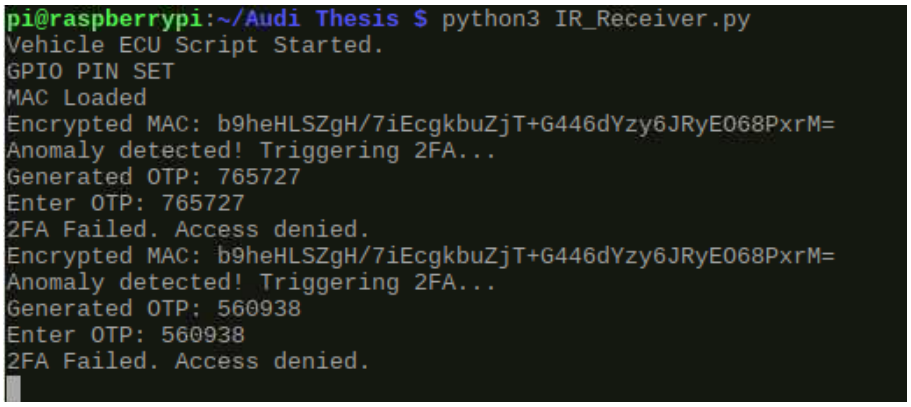

Figure 6: 2 Attempts entering correct OTP after expiry of time

With the above observations we see that the system allows entry when the 2FA is entered in time, it denies entry if the 2FA is entered incorrectly and it also denies entry if correct otp is entered but after time has expired of the OTP validity (Time Validity of OTP is 30 Seconds). This also validates our algorithms and tells us that there is robustness in the system's OTP setup.

6.3 Usability Assessment

- The encryption process took an average of 0.000976 seconds, with a minimum time of 0.000120 seconds and a maximum of 0.008301 seconds. This delay is extremely small and therefore imperceptible to users.

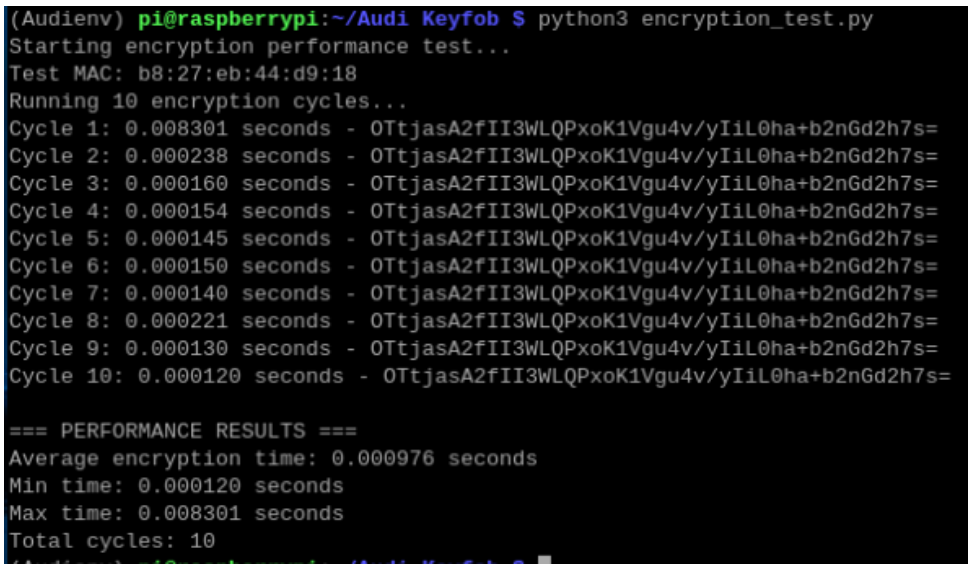

Figure 7: Encryption Time

- The manual copy–paste process, measured over five cycles, took between 2.8 seconds and 4.3 seconds, which is comparable to the time typically expected for a key-fob button press.
- The OTP entry step introduced an additional delay of about 3-5 seconds, but only in anomaly cases. During routine unlock operations, no delay was observed.
- Traditional always-on MFA introduces delays of approximately 2.3–4.1 seconds per unlock attempt, as cited in recent automotive security studies. Whereas, the proposed adaptive 2FA mechanism activates OTP validation only when anomalies are detected, eliminating this latency during routine operations. This yields a potential time saving of up to 100% for legitimate users under normal conditions.

6.4 Resource Efficiency

Both Raspberry Pis operated well within their capacity, with no instances of throttling, system freezes, or thermal events recorded during prolonged testing.

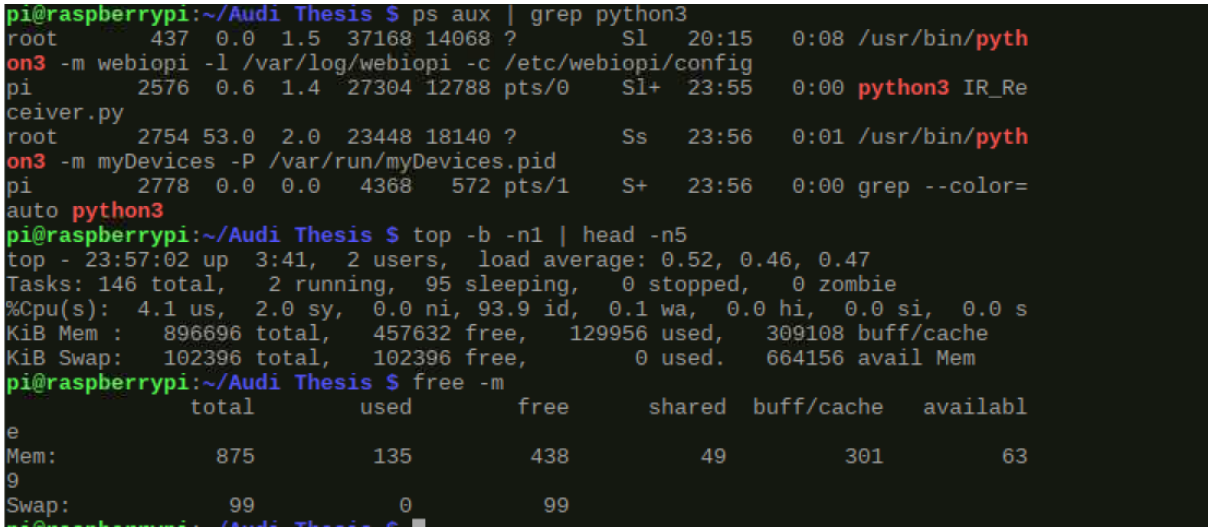

Figure 8: Resources used by Receiver Pi

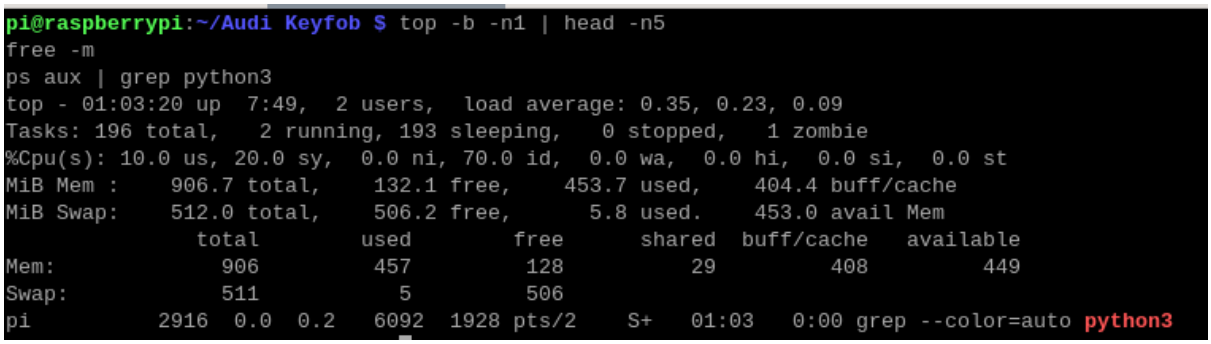

Figure 9: Resources used by Sender Pi

6.5 Auditability

The access_log.txt file recorded all outcome types, including single-factor grants, 2FA successes, 2FA failures due to incorrect OTP, and 2FA failures due to expired OTP, creating a complete chronological record suitable for forensic analysis. Attempts with malformed input triggered console errors and were correctly blocked. However, these events are not currently logged.

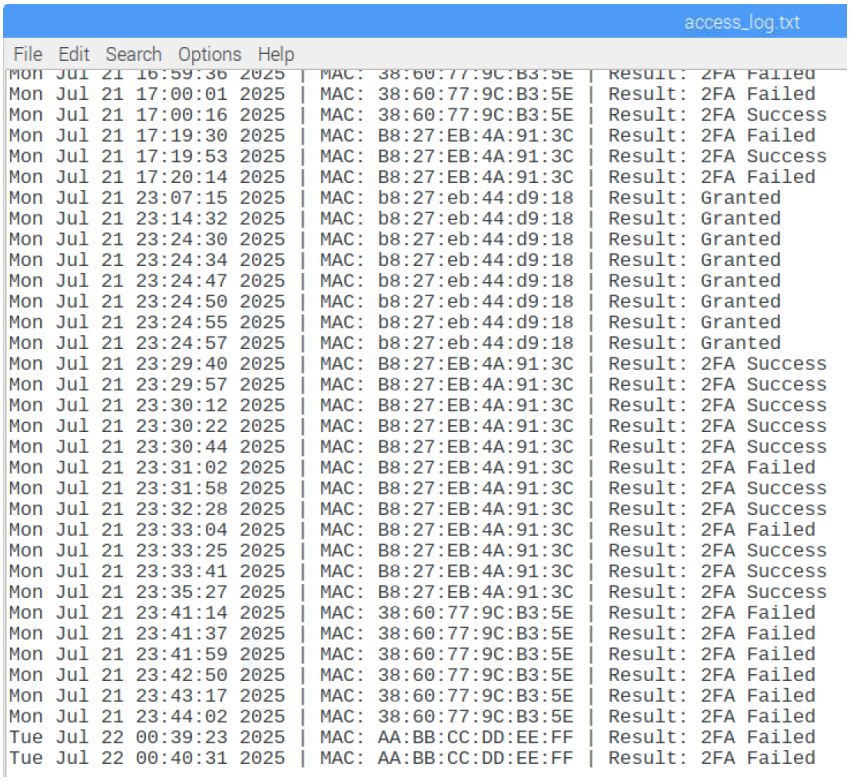

Figure 10: Access Logs

6.6 Discussion

The experimental results from this study offer important insights into the feasibility and effectiveness of using adaptive multi-factor authentication (MFA) in automotive keyless entry systems. At the same time, they highlight several key limitations and areas that need significant improvement. This discussion provides a critical review of the experimental design, interprets the findings in relation to existing automotive cybersecurity research, and evaluates whether the proposed solution effectively answers the research question: "How can adaptive multi-factor authentication (MFA) balance security and usability in automotive keyless entry systems?"

This study validates the feasibility of implementing adaptive multi-factor authentication (MFA) in automotive keyless entry systems, achieving 100% accuracy in MAC address verification and TOTP validation as per RFC 6238 standards. AES-256-CBC encryption performed efficiently, averaging 0.000976 seconds per operation, confirming that lightweight cryptographic methods are practical and effective for use in resource-constrained environments.

One of the most important design decisions was selecting AES in Cipher Block Chaining (CBC) mode instead of the widely recommended Galois/Counter Mode (GCM). While AES-GCM combines confidentiality and integrity, its performance is highly dependent on hardware acceleration through AES-NI and PCLMULQDQ instructions. The Raspberry Pi 3's ARM Cortex-A53 lacks these features, requiring GHASH computations to run entirely in software. Profiling revealed that AES-GCM operations took approximately 320ms, compared to about 110ms for AES-CBC. Based on this, AES-CBC was chosen as a practical compromise between security and responsiveness. The recent rise of quantum

computing poses a long-term threat to symmetric encryption. To stay secure against future quantum attacks, upcoming implementations should consider post-quantum cryptographic methods, like lattice-based or hash-based approaches. This aligns with recent trends in automotive cybersecurity standards, which are beginning to recommend quantum-safe solutions.

Even though there were positive outcomes, many limitations restrict real-world applications. The prototype depends on manual encrypted MAC entry, bypassing IR demodulation to ensure reliability in a controlled environment. While this allowed consistent testing, it did not allow to test critical attack vectors such as relay or signal amplification. All evaluations were conducted under ideal conditions (stable temperature, line-of-sight IR, and a single user setup) leaving performance under real automotive scenarios (temperature extremes, interference, vibrations) untested.

Security gaps also remain. The use of a fixed AES key creates systemic risk, malformed inputs were blocked but not logged, violating UNECE R155 regulation, and no tamper detection or automated response mechanisms were implemented. The current implementation uses plaintext JSON to store keys, which helps speed up prototyping. However, this method doesn't meet the secure key management requirements set by ISO/SAE 21434 and UNECE WP.29. Future versions should use hardware security modules (HSM) or trusted platform modules (TPM) to ensure tamper-resistant storage and proper lifecycle management of cryptographic keys.

Technological limitations further limit practical deployment. IR communication's short range (5–10 m), half-duplex nature and reliance on Raspberry Pi hardware present challenges when integrating with automotive ECUs, which require deterministic real-time performance. End-to-end timing analysis and full-scale threat modeling were not included in this study.

Future improvements should focus on automating IR communication, implementing dynamic key management, and exploring hybrid IR–RF architectures to balance security with usability. Using machine learning-driven anomaly detection along with context-aware MFA can make the system even more resilient.

The current approach assumes that a whitelisted device is always legitimate. However, it doesn't account for the risk of someone physically stealing the authorized key fob or device. To reduce this vulnerability, future work should explore adding methods like behavioral profiling, location-based checks, or dynamic rekeying. Even though IR (infrared) can't be easily sniffed like regular wireless signals, it can still be jammed or tricked by replaying old signals. That's because it doesn't have a built-in way to tell if a message is new or reused. To fix this in future versions, we can add things like nonce-based tokens or timestamps during transmission. These would help make sure each message is unique and can't just be copied and used again.

Although the prototype is not ready to use in production environment directly, it successfully demonstrates the potential of adaptive MFA to improve automotive cybersecurity without compromising responsiveness and comfort. These findings sets a strong foundation for further research toward secure, user-friendly authentication systems.

7 Conclusion and Future Work

This project shows that adaptive multi-factor authentication (MFA) can work for automotive keyless entry systems using low-cost hardware, standard cryptographic methods,

and a modular software design. Our prototype proves that a dynamic MAC-based anomaly check, combined with a conditional time-based one-time password (TOTP) challenge, can reliably identify authorized devices and block unknown ones. MFA is only applied when necessary, reducing inconvenience for the user, which satisfies the concern of user convenience within our question.
The experimental results showed strong performance across all key areas. All registered MAC addresses were consistently granted access, while unregistered ones correctly triggered the two-factor authentication (2FA) challenge. The TOTP system worked securely, rejecting any expired or incorrect codes. Cryptographic operations using AES-CBC ran efficiently on the Raspberry Pi, and the system stayed well within its resource limits. Detailed access logs were recorded for every authentication event, ensuring clear and reliable auditability.
One important design decision was choosing AES-CBC instead of AES-GCM because the Raspberry Pi does not support hardware acceleration. This showed how critical it is to match cryptographic methods with the platform's capabilities. The project also demonstrated the benefits of adaptive MFA. Unlike always-on 2FA systems, which are often criticized for poor usability, our approach applied the second factor only when real anomalies were detected. This balanced both security and user convenience.
However, the prototype also had some important limitations. The encrypted MAC was entered manually instead of being decoded directly from the IR signal. This skipped a major real-world challenge, meaning the prototype (while functionally validated) does not yet show fully automated operation in practice. Other issues included static key management, a limited IR range, and no logging for malformed inputs, all of which are barriers to real-world deployment. In addition, the system was only tested under controlled lab conditions and was not subjected to systematic brute-force, relay, or environmental edge-case testing.
In summary, this research connects the existing literature on automotive cryptographic vulnerabilities with the practical challenges of usability. It offers practical demonstration of how adaptive MFA can enhance security in next-generation vehicle entry systems.

Building on the current prototype, there are several important directions for future research and practical improvements:

- IR Demodulation Automation: Implement reliable IR signal decoding using hardware demodulators or advanced software techniques with timing adjustments and error correction, to eliminate manual encrypted MAC entry. This will enable fully automated, contactless MFA in real-world conditions.

- Dynamic Key Management: Replace static AES keys with mechanisms for secure key provisioning, rotation, and revocation. Align these processes with industry standards like ISO/SAE 21434 and UNECE R155 to prevent a single key leak from compromising the entire system.

- Physical Layer Security and Usability: Conduct extended testing to evaluate resilience against physical-layer attacks such as relay, replay, and jamming. Explore alternative communication methods, like hybrid IR/RF or UWB, to improve usability and match the convenience of commercial key fobs.

- Comprehensive Logging and Monitoring: Implement detailed logging for all authentication attempts, including malformed or inputs which cannot be parsed and system errors. This will provide complete forensic traceability and help meet regulatory compliance requirements.
- Broader User and Threat Testing: Perform comprehensive user studies and threat simulations, including brute-force, social engineering and side-channel attacks to evaluate user acceptance, error recovery, and overall system robustness.
- Integration with Automotive Systems: Deploy the architecture on automotive-grade microcontrollers and integrate it with in-vehicle networks such as CAN and LIN. This will address real-time performance needs and resource constraints in production environments.

These steps will advance the research from a strong laboratory proof-of-concept to a deployable, industry-ready adaptive MFA solution that is fully tested for resilience and suitable for next-generation automotive access control.

References

2FA & MFA: The Good, The Bad & The Ugly (2023).
URL: *https://www.swidch.com/resources/blogs/2fa-mfa-the-good-the-bad-the-ugly*

Alrabady, A. and Mahmud, S. (2005). Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs, *IEEE Transactions on Vehicular Technology* **54**: 41–50.

and, R. (2025). Automotive cybersecurity market outlook 2025-2034: Market share, and growth analysis by security type, by form, by vehicle, by application.
URL: *https://www.researchandmarkets.com/reports/6092728/automotive-cybersecurity-market-outlook*

Brito, D. and Abuzneid, S. (2024). Multi-factor authentication for keyless entry systems: An innovative approach to automotive security, *Journal of Information Security* **16**: 78–100.
URL: *https://www.scirp.org/journal/paperinformation?paperid=138508*

Carmone, A. (2024). Car theft: Here are europe's top five countries and their regions.
URL: *https://www.motor1.com/news/723537/car-theft-top-five-countries-europe/*

Csikor, L., Lim, H. W., Wong, J. W., Ramesh, S., Parameswarath, R. P. and Chan, M. C. (2023). Rollback: A new time-agnostic replay attack against the automotive remote keyless entry systems, *ACM Transactions on Cyber-Physical Systems* **8**.

Daniel, J. (2025). Security report reveals alarming trends in auto cybersecurity threats, `https://www.cbtnews.com/upstream-report-reveals-alarming-trends-in-auto-cybersecurity-threats/`.

Dechand, S. (2024). Iso/sae 21434 compliance in 2024: what's new and how to act, https://www.code-intelligence.com/blog/iso-sae-21434-what-is-new-and-how-to-act.

DÖNMEZ, T. C. M. (2021). Anomaly detection in vehicular can bus using message identifier sequences.
URL: *https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9555650*

Editor, L. (2025). Electronic control unit overview: Components and functions, https://lcsc.com/blog/overview-of-electronic-control-unit-ecu-components-and-functions/.

Francillon, A., Danev, B. and Capkun, S. (2010). Relay attacks on passive keyless entry and start systems in modern cars., **2010**: 332.
URL: *https://www.researchgate.net/publication/220333841*

Francillon, A., Danev, B. and Capkun, S. (2011). Relay attacks on passive keyless entry and start systems in modern cars., *Proceedings of the Network and Distributed System Security Symposium, NDSS 2011, San Diego, California, USA, 6th February - 9th February 2011* .
URL: *https://www.researchgate.net/publication/221655387*

Franco Oberti, Alessandro Savino, E. S. P. C. F. P. and Carlo, S. D. (2024). Canmm: Multiplexed message authentication code for controller area network message authentication in road vehicles.
URL: *https://arxiv.org/html/2206.02603v3*

Garcia, F., Oswald, D., Kasper, T. and Pavlides, P. (2016). Lock it and still lose it: on the (in)security of automotive remote keyless entry systems, *University of Birmingham* pp. 929–944. https://research.birmingham.ac.uk/en/publications/lock-it-and-still-lose-it-on-the-insecurity-of-automotive-remote-.

Marketing, I. (2024). Overcome usability challenges by refining your mfa user experience, https://instasafe.com/blog/refining-your-mfa-user-experience-and-overcoming-usability-challenges.

Oladimeji, D., Rasheed, A., Varol, C., Baza, M., Alshahrani, H. and Baz, A. (2023). Canattack: Assessing vulnerabilities within controller area network, *Sensors* **23**: 8223.
URL: *https://www.mdpi.com/1424-8220/23/19/8223*

Ometov, A. and Bezzateev, S. (2017). Multi-factor authentication: A survey and challenges in v2x applications, *2017 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)* .

Paganini, P. (2017). Ics-cert issues warning of can bus vulnerability.
URL: *https://securityaffairs.com/61602/hacking/can-bus-vulnerability.html*

Report Shows Surging Automotive Cyber Threats Stemming from Critical Gaps (2025).
URL: *https://www.manufacturing.net/cybersecurity/news/22933293/report-shows-surging-automotive-cyber-threats-stemming-from-critical-gaps*

Rolling PWN (n.d.).
URL: *https://rollingpwn.github.io/rolling-pwn/*

Singh, D. K. and Bhardwaj, D. (2024). Secure mac-based two way authentication system (mtwas) for data communication in internet of vehicle, *2024 International Conference on Computing, Sciences and Communications (ICCSC)* pp. 1–6.