

Configuration Manual

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:	2024-2025
Module:	MSc Research Project
Supervisor:	Eugene McLaughlin
Submission Due Date:	11/08/2025
Project Title:	Configuration Manual
Word Count:	590
Page Count:	4

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):	

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

Avadhoot Prashant Dhanve
23229349

1 Introduction

This manual documents every hardware item, software component and configuration step used to build and demonstrate the prototype “secure key-fob” system: Two Raspberry Pis exchange an AES-encrypted MAC address over an infrared (IR) link. If the receiver recognises the MAC, it unlocks immediately; otherwise it demands a TOTP second factor.

Because the classroom prototype cannot yet capture IR metadata reliably, the encrypted string is written to a shared file that the receiver reads automatically. The code is written in Python for both the Car ECU that is the “Receiver” and the Key Fob that is the “Sender”.

2 Hardware and Software Specifications

2.1 Hardware Specifications

Following are the hardware specifications:

- CPU: 13th Gen Intel(R) Core(TM) i7-13700HX
- Memory: 16 GB Ram DDR4
- Storage: 1TB SSD, 8 GB SanDisk Micro SD Card, 32 GB Sandisk Micro SD Card
- Controller Board: Raspberry Pi 3b, Raspberry Pi 3b+
- IR Receiver: KY-022
- IR Transmitter: KY-005
- 2x Breadboard
- 6x Jumper wires: Male to Female
- Router: THREE 5G Hub ZTE MC801A
- 2x Micro-USB Cables

2.2 Software Specifications

Following are the software specifications:

- Windows 11 PRO 24H2 64-bit Operating system
- RealVNC Viewer 7.13.1
- Nmap 7.97
- Raspbian GNU/Linux 9 Operating System
- Debian GNU/Linux 12 (bookworm) Operating System
- Python 3.5.3, Python 3.11.2
- Python Libraries: pycryptodome 3.20.0, pycryptodome 3.23.0 pyotp 2.6.0, pigpio 1.38, RPi.GPIO 0.7.1 (*PyCryptodome — PyCryptodome 3.160b1 documentation*; n.d.; *PyOTP - The Python One-Time Password Library — PyOTP documentation*; n.d.; *What is the official Raspberry Pi library for accessing GPIO ports ? - Raspberry Pi Forums*; 2022)

3 Configuration Details

3.1 Installing Python Libraries

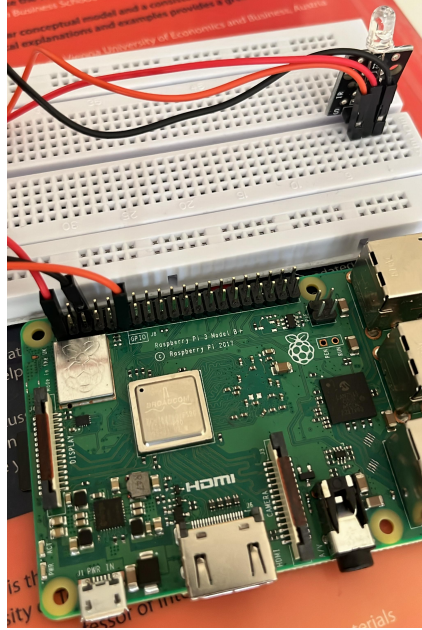
Install the Python libraries using the following commands:

- `sudo apt-get update`
- `sudo apt-get install pigpio python3-pigpio python3-crypto python3-pyotp`

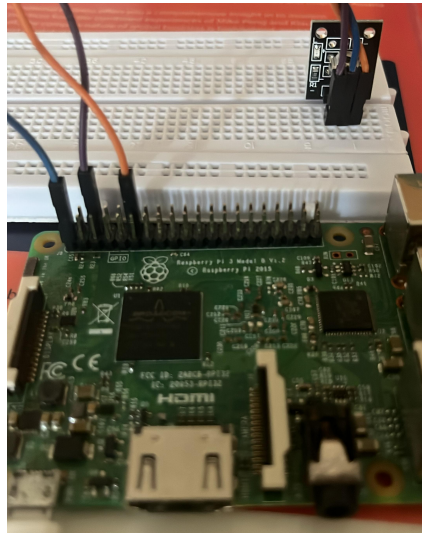
3.2 Configuration for Emulated Car ECU "Receiver" and Emulated Key Fob "Transmitter"

Signal	Receiver (Raspberry Pi 3b)	Transmitter (Raspberry Pi 3b+)
Signal	Connect to Pin 12 (GPIO 18)	Connect to PIN 11 (GPIO17)
VCC	Connect to Pin 1 (3.3v output)	Connect to Pin 1 (3.3v output)
Ground	Connect to Pin 6 (Ground)	Connect to Pin 6 (Ground)

Table 1: Table representing physical pin connections



Raspberry Pi 3b+ (Sender Connections)



Raspberry Pi 3b (Receiver Connections)

(*Raspberry Pi hardware - Raspberry Pi Documentation*; 2024)

3.3 Runtime Sequence

- Sender Pi
 - Reads the MAC of the Hardware via ip link show.
 - Encrypts with AES-CBC - Base64.
 - Transmits the same string as a 352-bit IR burst.
 - Displays the output, showing both the dynamically grabbed MAC address and the encrypted MAC address
- Receiver Pi

- When there is a signal received, that is when the signal goes from HIGH (1) to LOW (0), ir-callback function is called.
- Paste the Encrypted value of the MAC address received from the Sender output.
- Decrypts and compares the MAC with the whitelisted/stored MAC in mac-db.json file.
- If there is a match, then a successful unlock.
- If the MAC does not match, then 6-digit OTP is sent to verifies user entry.
- Logs every attempt to access-log.txt.

4 Conclusion

This configuration manual provides complete documentation for implementing a secure IR-based vehicle entry system prototype using Raspberry Pi hardware. The system successfully demonstrates encrypted communication, device authentication, and two-factor authentication capabilities while maintaining user satisfaction of not having to enter the second factor authentication every time they enter the car.

References

PyCryptodome — PyCryptodome 3.16.0b1 documentation (n.d.).

URL: <https://www.pycryptodome.org/src/introduction>

PyOTP - The Python One-Time Password Library — PyOTP documentation (n.d.).

URL: <https://pyauth.github.io/pyotp/>

Raspberry Pi hardware - Raspberry Pi Documentation (2024). <https://www.raspberrypi.com/documentation/computers/raspberry-pi.html#gpio>.

What is the official Raspberry Pi library for accessing GPIO ports ? - Raspberry Pi Forums (2022).

URL: <https://forums.raspberrypi.com/viewtopic.php?t=376663>