COM6017M:
IOT ASSESSMENT

Student ID: 220049861

Contents

Introduction and Problem Definition:

The rapid growth of the Internet of Things (IoT) has revolutionised the way devices interact and communicate, enabling more efficient and secure solutions across various domains. Access control is one of the critical areas where IoT technology can enhance security, improve efficiency, and provide real-time monitoring capabilities. Traditional access control systems often operate in isolation, lacking integration with modern IoT platforms for data analytics and remote monitoring.

This project aims to address these challenges by developing an IoT-enabled RFID-based access control system. This system will integrate an RFID scanner, an Arduino, a Raspberry Pi, and a cloud platform to provide a secure, real-time solution for managing access to restricted areas.

Problem Definition:

Effective access control is vital to ensuring security in various settings, including offices, schools, and industrial facilities. However, many existing systems are:

- Standalone: Lacking connectivity to analyse data and remotely monitor access attempts.
- Static: Offering limited or no adaptability to changes to users or security needs.
- Data-deficient: Provide no mechanism for real-time logging or analytics.

These limitations could pose security risks or operational inefficiencies. This project addresses these challenges by integrating IoT technologies into an RFID based access control system. The solution will offer the following features:

- Real-time Monitoring: Logs RFID scans and displays data on a cloud-based dashboard.
- Access Decisions: Validates scanned RFID UIDs against a database to allow or deny access.
- Data Insights: Provide visualisations of the logged data via ThingSpeak.

Project Requirements:

Hardware:

The hardware components required for the implementation of this IoT project include:

- Raspberry Pi:
  - Serves as the central data processing unit, managing data from the Arduino, integrating with the database and providing a connection to the cloud.
- Arduino Nano with MFRC522 RFID Module:
  - The RFID module reads the data on any presented RFID tag and sends the data to the Arduino, which in turn passes the data to the Raspberry Pi.
- Relay Module:
  - Controls the door locking system based on the access decisions.
- LEDs:
  - Provide a visual indication to the user.
- Power Supply:
  - To provide a stable supply of power to the components.
- Jumper wires and breadboard:
  - Allows each component to be connected.

Software:

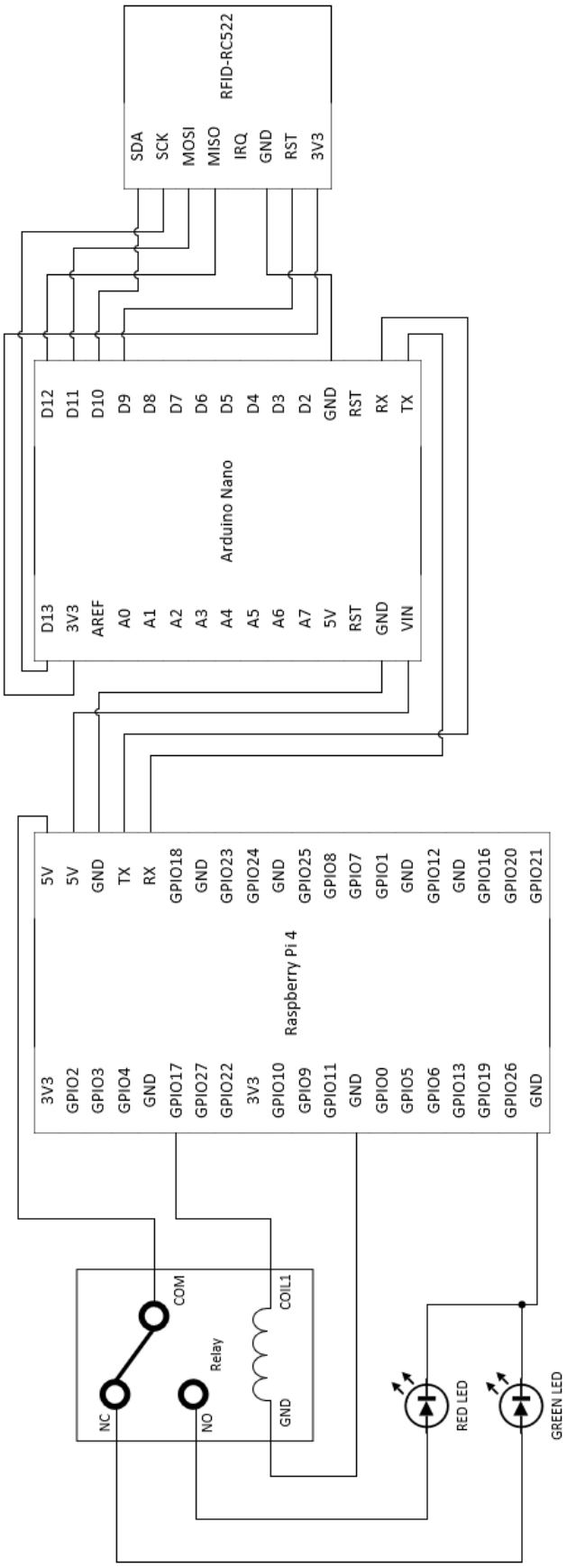
- Arduino IDE:
  - Allows the programming of the Arduino and provides a serial monitor.
- Python:
  - For processing the data on the Raspberry Pi.

- SQLite3:
    - Allows python to connect to an SQL database.
- ThingSpeak API:
    - Provides the cloud-based connection.

Cloud Services:

- ThingSpeak Channel
    - For this project other cloud services were considered such as AWS, and Azure. However, due to the costs and complexity of integrating these services it was decided against using these for the prototype.

Circuit Design:



Project Testing:

Testing Overview:

Testing was conducted to ensure that the functionality and reliability of the IoT based RFID access control system was satisfactory to meet the requirements of the problem set out. The testing focused on verifying hardware connections, software functionality and system performance under various scenarios.

Testing Plan:

Hardware Testing:

- Objective: Verify hardware components function as intended.
- Steps:
    - Confirm RFID reader can correctly read UIDs.
    - Ensure the relay can be controlled from the Pi.
    - Check the LEDs light up at the appropriate time.
    - Ensure a stable power supply to all components.
- Expected Outcome: All hardware works as intended.
- Actual Outcome: As expected.

Software Testing:

- Objective: Ensure software logic accurately processes the UIDs and integrates with the database and cloud platform.
- Steps:
    - Test UID parsing and database validation with valid and invalid UIDs.
    - Confirm the data logging in the SQLite3 database.
    - Confirm the data logging in the cloud platform.
- Expected Outcome: Reliable software performance and data logging.
- Actual Outcome: As expected.

Integration Testing:

- Objective: Ensure hardware and software work together correctly.
- Steps:
    - Perform end to end tests by scanning RFID cards with both valid and invalid UIDs.
    - Monitor relay activation for valid UIDs and ensure no activation for invalid UIDs.
    - Check real-time data upload on ThingSpeak.
- Expected Outcome: Full interaction between the software and hardware.
- Actual Outcome: As expected.

Failsafe Testing:

- Objective: Ensure the system fails safe if the software were to crash.
- Steps:
    - Stop the python code from running on the Pi and ensure the relay drops to the NC (Normally Closed) Position and the door unlocks to prevent people becoming trapped.
- Expected Outcome: LEDs change from red to green to show door unlocked status.
- Actual Outcome: As expected.

Results:

The testing phase concluded the following:

- Reliable hardware integration and connectivity.
- Successful database validation and secure logging of access attempts.
- Real-time updated to ThingSpeak for monitoring.

Data Analytics

Data Analysis and Visualisation:

Data collected from this IoT-based access control system is displayed on the ThingSpeak platform. Currently there are four different visualisation that the ThingSpeak channel is set up to provide.

1. Grid Data Log: This visualisation shows the timestamp of the data, UID and its status in a grid text format to show a basic log. (Appendix Figure E)
2. Status Pie Chart: This visualisation shows the frequency of valid and invalid scans in a pie chart, along with a text count for the frequency number. (Appendix Figure F)
3. UID Frequency: This visualisation shows the frequency of valid and invalid scans for each UID. (Appendix Figure G)
4. Status of UID over time: This visualisation shows the status of each UID scan against the date in the timestamp with colour coded spots – green for valid, and red for invalid attempts. (Appendix Figure H)

These visualisations are set up, so system administrators can track each logged attempt and clearly identify which RFID cards are being used based on their UID. This further allows them to identify and analyse the number of access attempts that were valid, and invalid, which can allow them to identify unauthorised access attempts therefore increasing security.

Legal and Ethical Evaluation:

Legal Considerations:

Data Privacy Compliance:

- This system complies with the General Data Protection Regulation (GDPR) requirements by ensuring that all UID data is anonymised before storing or transmitting it to the external platform ThingSpeak. Personal identifiers are not logged, ensuring compliance with minimisation principles.
- End-users will be informed about the purpose of data collection, its retention period, and their rights to access or request deletion of their data.

Data Encryption:

- Data transmissions on this system between the Arduino, Raspberry Pi and ThingSpeak are done in plain text, and are not encrypted. This is due to the anonymity of the data, therefore there is no risk of personal data being captured by unauthorised personnel. If, however, personal data was to be transmitted over this system, then data encryption techniques could be easily implemented to ensure compliance is still met with GDPR and the safeguarding of personal data.

Data Retention and Deletion Policies:

For the purposes of this artefact being designed as a prototype and only being used in a closed testing process there has been no implementation of a data retention and deletion policy. However, if this project were to make use of open testing or to be used by another external person or organisation, a data retention and deletion policy would be implemented. This policy would clearly outline how the data is stored, how long it is retained within the system and how and when the data is deleted. This would be to ensure all stakeholders are clearly informed on how data is processed to reassure that all legal obligations are met.

Legal Accountability:

System administrators are responsible for ensuring data handling complies with applicable laws and regulations. Any changes to the system must undergo a thorough legal review to ensure continued compliance with the regulations. Furthermore, a data controller should also be appointed if any personal data is to be stored within the system.

Ethical Considerations:

Transparency to Users:

This system notifies system administrators of access attempts and logs, this should be made clear to all end users ensuring that they understand the purpose and scope of the data collection and logging process.

Fairness and Non-Discrimination:

This system operates on a non-discriminatory bases, validating UIDs solely on pre-established permissions without bias or favouritism. This ensures that there is fair usage for all end users.

User Accountability:

Access logs maintain accountability, tracking access attempts with timestamps. This ensures that system actions can be audited to resolve disputes or investigate misuse.

Minimisation of Surveillance:

This system only collects the data necessary to manage access control effectively. Features that may invade user privacy, such as extensive monitoring or location tracking are intentionally excluded.

Inclusion and Accessibility:

This system is designed to support all users, included those with disabilities. By using RFID UIDs, it is possible to assign a wide range of RFID cards to this system varying from small RFID key tags, RFID ‘credit card’ style cards or by using larger RFID enabled devices such as mobile phones.

Security by Design:

Ethical responsibility extents to ensuring the system is robust against cyberattacks, reducing potential harm caused by unauthorised access to physical or digital assets. By ensuring that all transmitted data is anonymous, there is no potential for personal data to be extracted.

Potential Ethical Challenges:

Misuse of Data:

System administrators must ensure that access logs are used strictly for legitimate purposes and are not for unauthorised monitoring of individuals.

Unauthorised Access Attempts:

Ethical considerations included balancing the system’s ability to detect unauthorised access while respecting the privacy of legitimate users.

Bias in Database Configuration:

Care must be taken to prevent inadvertent bias in the UID database, such as omitting certain users.

Conclusion:

The development of the IoT-enabled RFID access control system successfully demonstrates the integration of hardware, software, and cloud-based solutions to enhance security and provide real-time monitoring capabilities. By utilising technologies such as the Raspberry Pi, Arduino, RFID modules and ThingSpeak, the system offers a scalable and efficient approach to managing access control in various environments.

Key achievements of this project include:

- Seamless data processing and storage using SQLite3 and ThingSpeak for real-time insights.
- Comprehensive testing and analytics, ensuring reliability, performance, and usability under different conditions.

This project also considers the ethical implications of data collection, emphasising transparency, accessibility, and user privacy. Future enhancements could focus on adding more accessibility features such as auditory feedback for visually impaired users, integrating mobile notifications, advanced data analytics, and improved data encryption standards. The potential to adapt this solution to larger-scale applications, such as multi-level, or multi-site access, highlights its versatility and practicality.

In conclusion, this project demonstrates the power and potential of IoT in transforming traditional systems into connected, intelligent solutions. By addressing both technical and ethical considerations, it sets a foundation for future innovations in access control and IoT-enabled systems.

Source Code:

The source code is available from multiple locations for ease of access, each source provides the same file set.

GitHub:

https://github.com/OKirkby/COM6017M-IoT-Assessment

OneDrive:

https://1drv.ms/f/s!AqLM3gL5AHiYgaxba4v8esspeK1c4Q?e=AvYxvR

ThingSpeak Channel:

The ThingSpeak channel has been made public so the graphs and data can be viewed.

https://thingspeak.mathworks.com/channels/2747437

Demonstration Video:

YouTube:

https://youtu.be/Rt_Ppzrom7k

OneDrive:

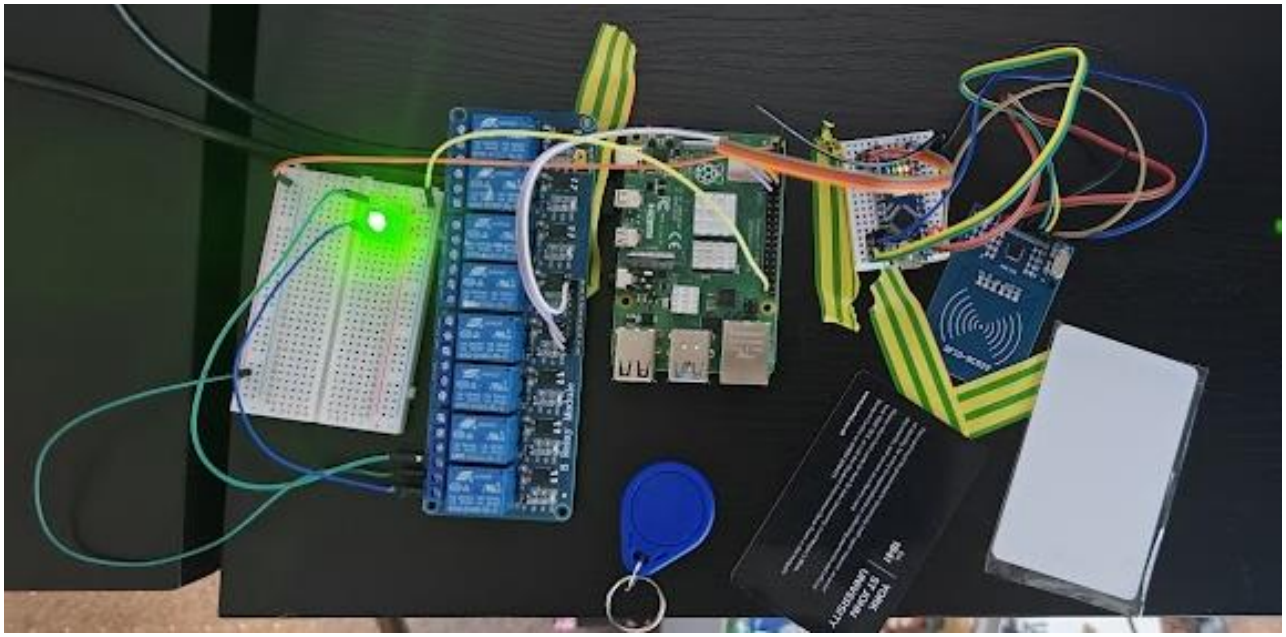
https://1drv.ms/v/s!AqLM3gL5AHiYgbBx_3XTxmZ17deUuw?e=rZIDxN

References:

1. European Union (2018) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu (Accessed 3 January 2025).
2. UK Government (2018) Data Protection Act 2018. Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents (Accessed 3 January 2025).
3. MathWorks (n.d) ThingSpeak API Documentation. Available at: https://thingspeak.com/docs (Accessed 18 December 2024).

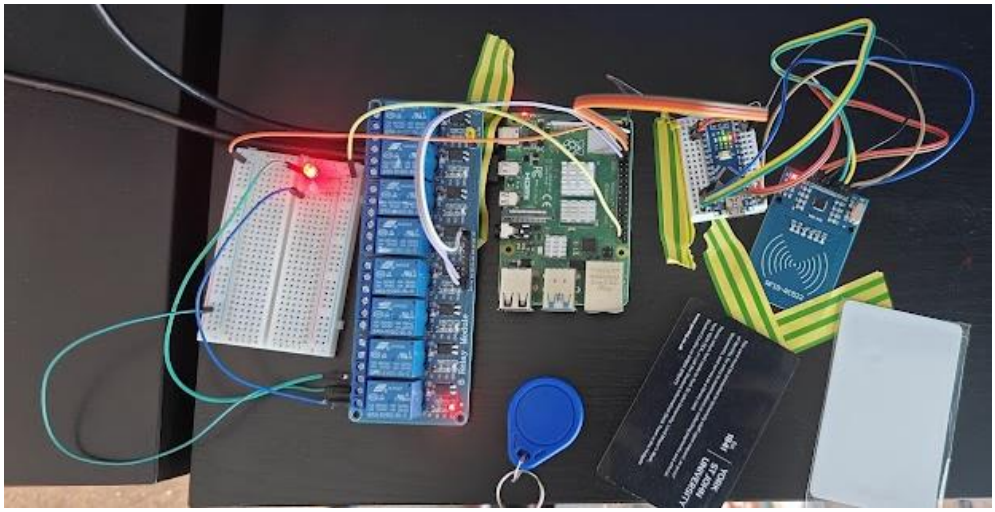
Appendix:

Figure A:



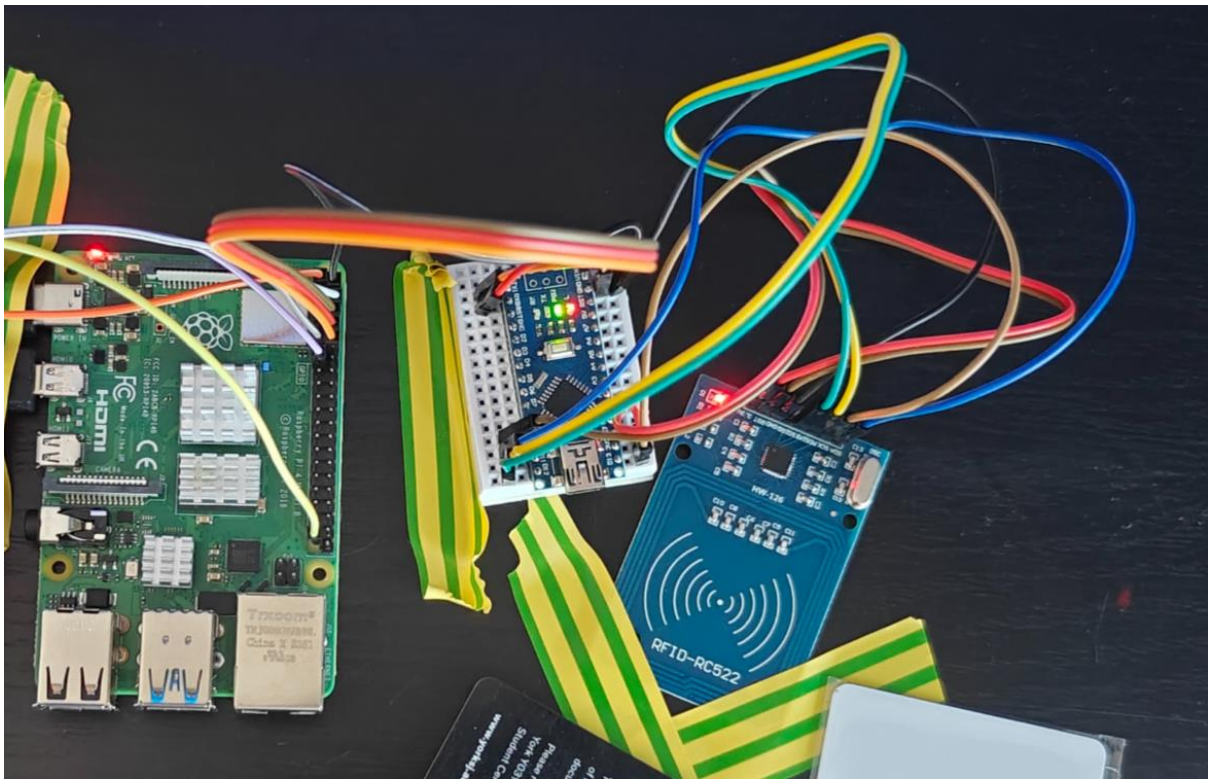
Door access relay in the unlocked state after a valid RFID card is scanned.

Figure B:



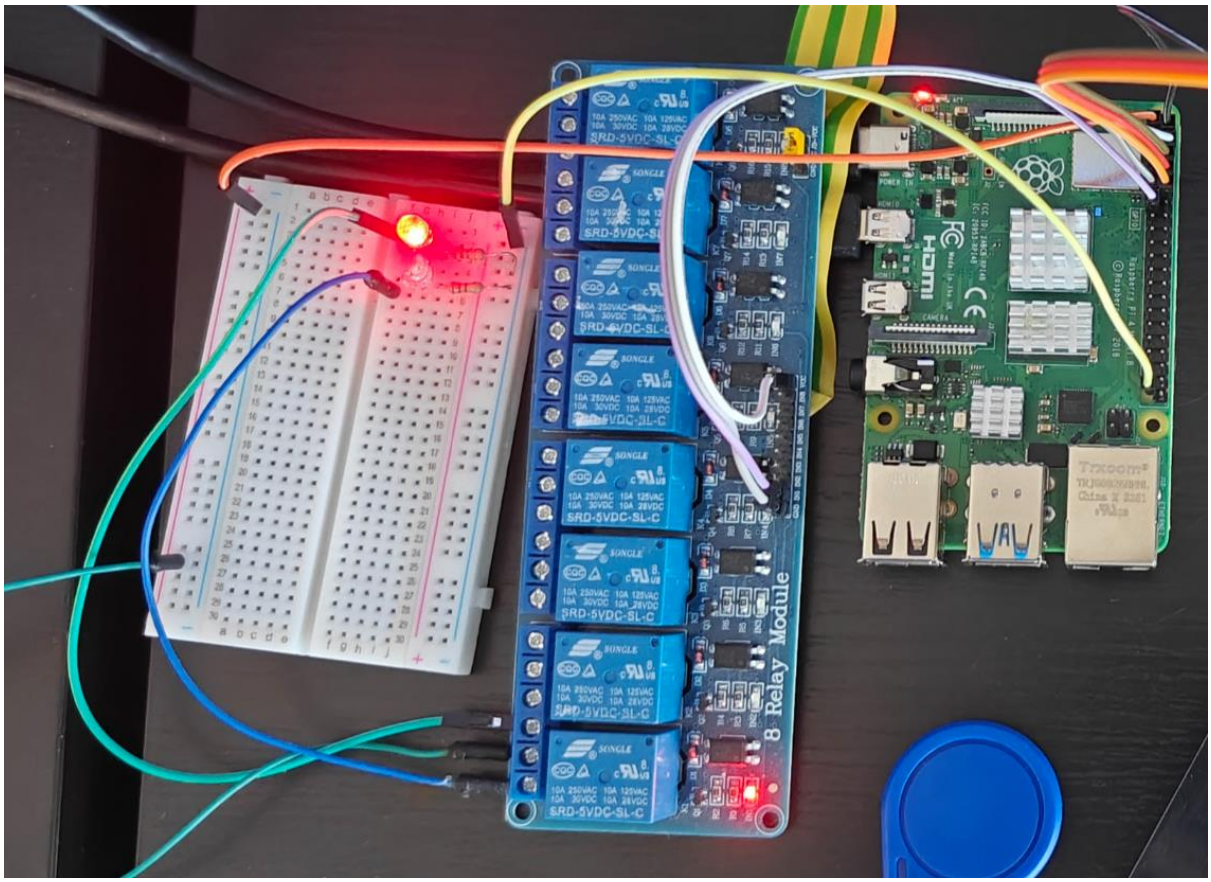
Door access relay in the locked state.

Figure C:



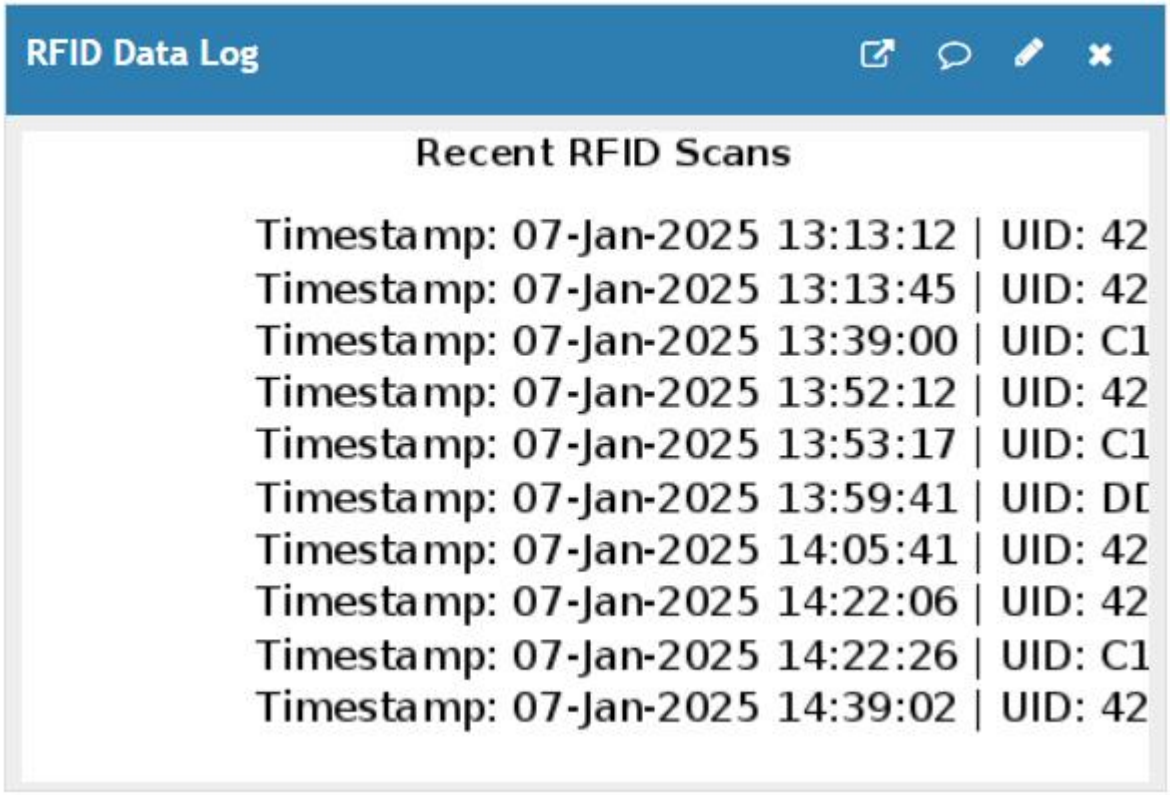
A close-up of the Raspberry Pi > Arduino > RFID connections.

Figure D:



A close-up of the of the Raspberry Pi > Relay Module connections.

Figure E:



Recent RFID Scans

Timestamp: 07-Jan-2025 13:13:12 | UID: 42F92C03 | Status: Valid

Timestamp: 07-Jan-2025 13:13:45 | UID: 42F92C03 | Status: Valid

Timestamp: 07-Jan-2025 13:39:00 | UID: C160B002 | Status: Valid

Timestamp: 07-Jan-2025 13:52:12 | UID: 42F92C03 | Status: Valid

Timestamp: 07-Jan-2025 13:53:17 | UID: C160B002 | Status: Valid

Timestamp: 07-Jan-2025 13:59:41 | UID: DDFF6975 | Status: Invalid

Timestamp: 07-Jan-2025 14:05:41 | UID: 42F92C03 | Status: Valid

Timestamp: 07-Jan-2025 14:22:06 | UID: 42F92C03 | Status: Valid

Timestamp: 07-Jan-2025 14:22:26 | UID: C160B002 | Status: Valid

Timestamp: 07-Jan-2025 14:39:02 | UID: 42F92C03 | Status: Valid

Figure F:

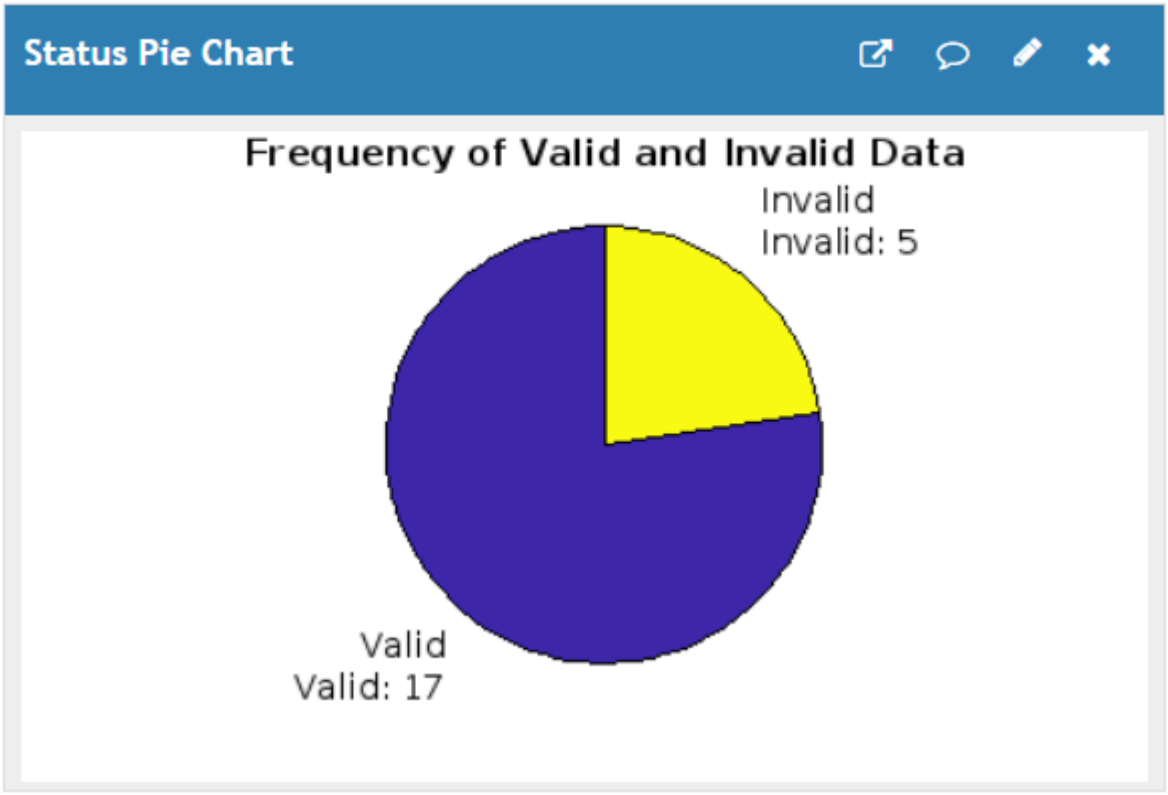


Figure G:

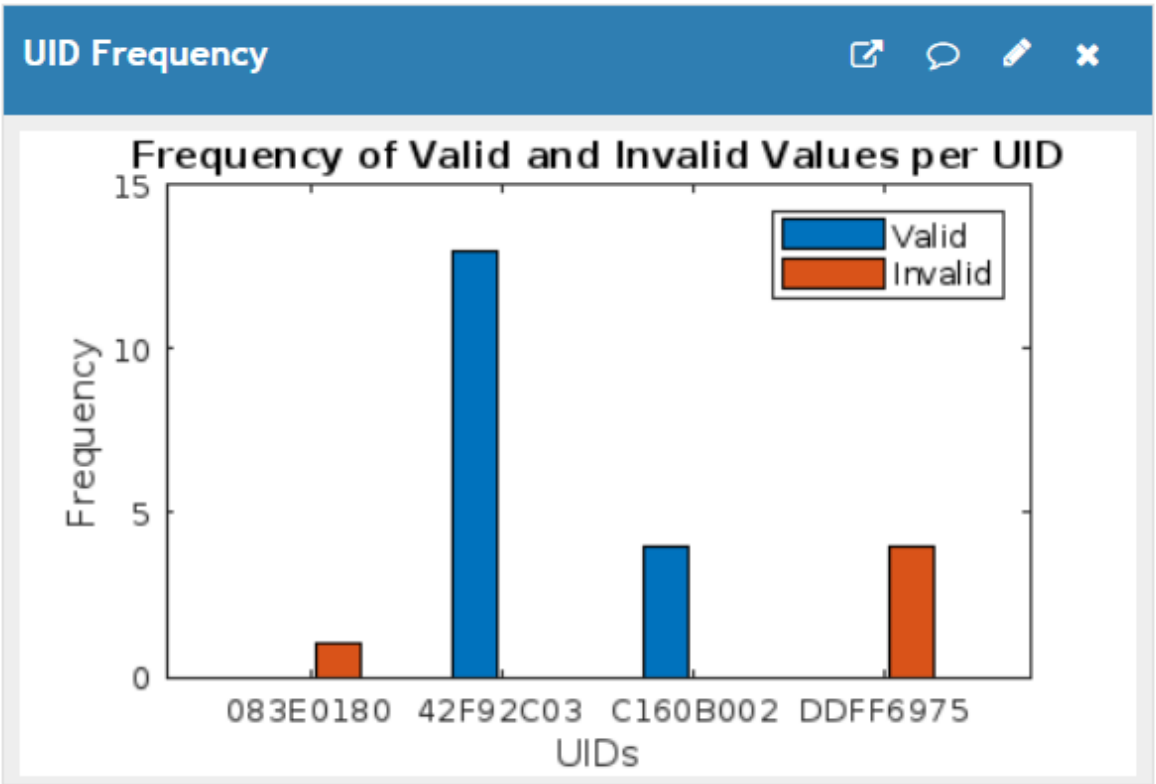
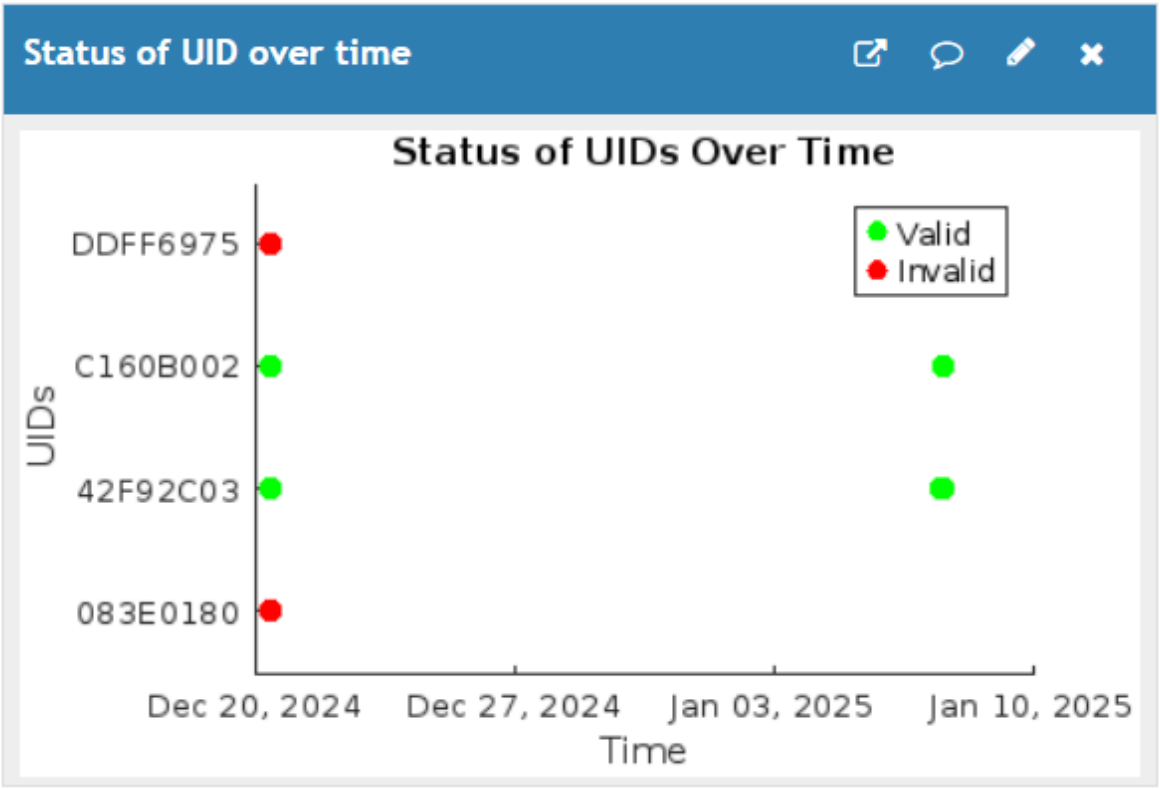


Figure H:


Status of UID over time
Status of UIDs Over Time
Valid
Invalid
DDFF6975
C160B002
42F92C03
083E0180
UIDs
Dec 20, 2024
Dec 27, 2024
Jan 03, 2025
Jan 10, 2025
Time