School of Computer Science
Faculty of Science and Engineeing

University Of Nottingham

Malaysia

UG FINAL YEAR DISSERTATION REPORT

- Well-Rounded IoT-based Home Security System -

Student's name : Yeoh Zi Song

Student Number : 20306220

Supervisor Name : Chew Sze Ker

Year : 2024

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF BACHELOR OF SCIENCE IN COMPUTER SCIENCE WITH ARTIFICIAL INTELLIGENCE (HONS)

THE UNIVERSITY OF NOTTINGHAM

- Well-Rounded IoT-based Home Security System -

Submitted in May 2024, in partial fulfilment of the conditions of the award of the degrees B.Sc.

- Yeoh Zi Song -

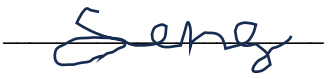
School of Computer Science

Faculty of Science and Engineering

University of Nottingham

Malaysia

I hereby declare that this dissertation is all my own work, except as indicated in the text:

Signature 

Date __2__/__05__/___2024___

Abstract

Despite advances in home security technology, burglaries continue to occur worldwide with alarming ease. Burglars operate with impunity, evading traditional security measures such as sirens, alarms, and surveillance cameras. Compounding the issue, existing affordable home security systems often lack real-time notification capabilities, leaving homeowners unaware of intrusions until it's too late. In response to this pressing need, this project aims to develop a comprehensive IoT-based home security system. By integrating cutting-edge security measures and equipment, our system seeks to thwart burglary attempts effectively. Moreover, we propose the implementation of a lockdown mechanism to confine intruders within a designated area, preventing their escape and enhancing the safety of homeowners and their property. Through this innovative approach, we aspire to provide homeowners with a robust and proactive defense against burglaries, ensuring peace of mind and safeguarding their homes and loved ones.

Table of Contents

1.0 Introduction

In the modern days, home security systems play an important role in securing our assets within our houses. However, without continuous development in home security systems, the risk of burglaries will still happen throughout the world. Hence, it is important for everyone to recognize the need for innovation in home security systems to ensure the safety and security of our homes.

Rich celebrity houses in the United States (US) have their houses break in easily and causing them to lose very high value of assets. United States (US) that owns one of the top home security technologies in the world reports to have 899,781 burglary cases in 2021 (Ruby Home, n.d.) which indicates a higher crime rate among the world. Therefore, burglary crimes are hard to solve nowadays due to there are few or no local eyewitnesses, and the surveillance camera technology is inadequate, helping burglars to cover themselves with masks and caps to avoid closed-circuit television (CCTV) around the world.

Statistics (Department of Statistics Malaysia, n.d.) have shown that the crime rates of house break-in & theft are 16,497 in 2019 and 14,040 in 2020 which is average around 38 to 45 cases of burglary would happen in a day throughout Malaysia even some with the home security technology out there. Alarm systems at houses, condominiums or staying in gated & guarded areas do not secure your houses from burglars 100%.

According to (Chitnis et al., 2016), one of the fastest and evolving cities in India, Pune happens to have 1200 cases of home burglaries in year 2015 alone, with only 240 cases being solved which indicates that only 20% of the burglaries have been caught. The burglaries resulted in property losses totaling 157.2 million rupees, with only 20 million rupees worth of valuables recovered so far. These burglaries occur more frequently in the suburban regions of Pune, but incidents are also happening within the city center.

Therefore, it is an urge to utilize and develop new technology to come up with a better solution to ensure houses being safe from burglars, or at least can have them detained or enclosed in an area to delay them until the authorities arrive.

Therefore, in the swiftly evolving realm of home security, incorporating state-of-the-art technologies is crucial to enhancing the safeguarding of our homes. One such transformative technology is using the landscape of Internet of Things (IoT) technology, which represents a network of interconnected devices that communicate and exchange data seamlessly. In the context of home security, IoT involves the incorporation of smart devices and sensors that can be interconnected to create an intelligent and responsive and convenient home security system. These devices can include smart home devices like smart cameras, motion sensors, facial recognition readers, and environmental sensors. What sets IoT apart is its ability to enable these devices to communicate with each other and with users, providing convenience, real-time insights and facilitating remote monitoring at anytime and anywhere for the users. For instance, IoT-enabled security systems can send instant alerts to homeowners' smartphones, allowing them to respond promptly to any potential security threats. Embracing IoT in home security not only enhances the effectiveness of traditional security measures but also opens the door to innovative solutions that can adapt to evolving threats and challenges in the realm of residential security. As we explore the transformative potential of IoT, it becomes clear that this technology has the capacity to redefine and elevate the standards of safety and security within our homes.

2.0 Aim

The aim of this project is to come up with a well-rounded IoT-based home security system with a lock down system to lock down burglars that broken in at an enclosed area. The home security system will be equipped with motion sensor, camera and others for security measures and a lock down system to lock the burglars.

3.0 Objectives

1. To implement a comprehensive home security system that ensures the safety of houses.
2. To implement a secure lock down system to delay the burglars' time until authorities arrive.

4.0 Significant of project

1. Implementing the home security system that can ensure the safety of houses.
2. Achieve the lock down system to lock the burglars and wait for authorities to arrive.
3. Providing convenience for users through remote view and control of household.

5.0 Motivation

Home security has a long history that reflects an evolving response to the persistent challenge of safeguarding residential spaces. Historically, basic security measures such as locks and alarms have been the primary means of defense against unauthorized intrusions, but the security level was very low as keys for locks could be copied and alarms only serve the purpose to buzz loudly in hope to scare the burglars away. As societal complexities or cases of false alarms happen, and criminal tactics advanced, so did the need for better security solutions. The emergence of closed-circuit television systems marked a significant leap forward, allowing homeowners to monitor their properties remotely. However, as technology progressed, burglars adapted by wearing a cap or walking through the blind spots of CCTV to avoid being captured on footage, hence there is a need for continuous innovation in home security.

Therefore, the technology of smart door lock which requires password, fingerprint, or even biometric recognition was developed and having it cooperating with the CCTV, the home security level rises as burglars will have a harder time to make their way into houses. But still, burglars were able to fake fingerprints of the household owners by obtaining it easily or observing the owners while they key in their passcodes to enter their house.

Recent research papers highlight the difficulty in solving burglary cases, with perpetrators escaping most of the time before authorities can arrest them. While modern forensic tools like fingerprinting and DNA analysis offer potential leads to seek for suspects, but their high costs limit widespread adoption, particularly in regions such as Malaysia. This disparity underscores the importance of preventative measures that homeowners can employ in their home to halt burglaries in progress or from running off to delay time for authorities to arrive.

The motivation for this project is deeply rooted in global burglary statistics and the challenges law enforcement faces in tracking and apprehending criminals swiftly. By exploring existing work on the Internet of Things and its application in home security, we seek to contribute to the ongoing evolution of residential protection, addressing the persistent need for effective and accessible solutions.

6.0 Literature Review

From the past of having keys to open door, setting up alarms in case of intruders, installing CCTV to monitor the household by users and implementing smart door lock for a higher security verification purpose, the burglaries rate is still high around the world. Therefore, a lot of researchers have conducted research regarding home security by using IoT systems as a technology development for higher house security level. The IoT systems serve the purpose of convenience at their best by ensuring household safety through providing household owners to spectate real time insights of their house and remotely control the house at anytime and anywhere by utilizing the technology of IoT to issue commands and have the sensors to interact with each other and act upon it. Therefore, the existing research proposed does not punish burglars from breaking into the house, whereby if they manage to break in, they steal and then leave despite the alarm buzzing loudly or before the authorities can arrive; and if they don't manage to break in, they just leave empty handed with no guilt or punishment held onto them. The IoT systems should be further utilized to aid the police in arresting the burglars despite whether they manage or does not manage to break in, as the police are having a hard time to catch burglars right now in the real world even with high pixel footage of surveillance camera because finding the burglar itself is an impossible thing among almost 8 billion people in the world. Hence, the technology of utilizing IoT should be implemented by delaying the burglars from breaking out after stealing until the police arrive and catch them easily.

According to (Taryudi et al., 2018), in their study on an IoT-based integrated home security and monitoring system, they have developed a home security and a monitoring system that incorporates the function of detecting lights opening, presence of rain. The research used RFID as the first layer of security and numerical PIN as the second layer of security. PIR sensor is used to detect movements from intruders and sends notifications to user by using a Catalex YX5300 MP3 Player. This research uses low cost to ensure the security of the house, but without having surveillance camera to observe real-time movements of the visitors and capturing images, the household users will have no idea regarding who is entering the house.

According to (Osman et al., 2002), the research project was conducted by using PIR Motion Sensor to detect movements from human and send the notifications and image to user by using Telegram Bot. The input from PIR Motion Sensor is processed by the microcontroller Raspberry PI WH to deduce whether is there an intruder and send the notifications to Telegram Bot. The Telegram Bot was used to receive notifications and send commands for the sensor device to act remotely. The GPS module is used in this research to pinpoint the house's geographical location and send it back to the user, but this is useless as it should be sent directly to the house security guards and police to notify them about a break in.

According to (Hussein & Al mansoori, 2017), his research project was done by using Raspberry pi 3, camera pi, keypads, and a database to store the snaps and guest-id of guests. The system used face recognition technology by using Fisher method to compare the image with the existing images in database. If a matching face is found, the door opens, if no owner will be notified about it and decide the appropriate action. The camera pi acts as a surveillance purpose to capture image of guests, Raspberry pi 3 acts as the control module for the actions to be taken which includes sending SMS message to owner and also the actions of communicating with the database for registering newcomers or comparing images; the keypad lets the guest to key in their guest-id and enter the door if it is correct. This system provides convenience to existing guest users as they can key-in their existing guest-ids for future entries along with their snapped images sent to owner to notify them

about "ACCESS DOOR REQUEST". It also helps to register newcomers' images into the database and provide them with a new guest-id for future entries.

According to (JosephNg et al., 2023), in one of their research project, they uses NFC Card Emulation by emulating the physical NFC cards or tags into their mobile phones. This is done by using Arduino Uno as the microcontroller board to incorporate all the programming and equipment parts, MFRC 522 NFC/RFID Module as the NFC Reader, Relay Module to provide a higher or lower voltage level for the input and output terminals, and a solenoid lock that has anti-theft and shockproof construction to lock or unlock the door. This research aims to eliminate the physical NFC cards to provide convenience and comfortable contactless experience with the NFC reader due to the COVID-19 pandemic at the time the project was conducted. The hotel guests were able to experience a high-level innovation operation by having their mobile phone to act as the physical NFC card or tag and this reduces the guest's effort when opening the door.

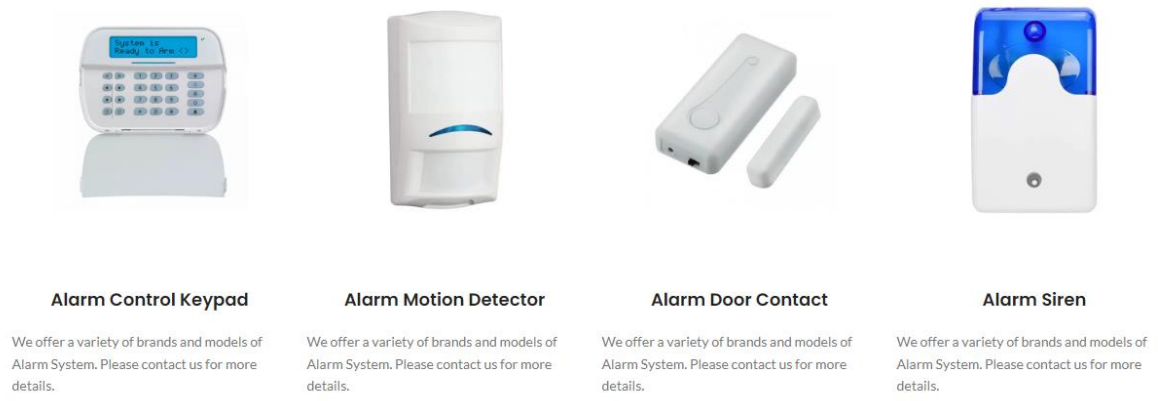
For the first security measure, according to (Khabarlak & Koriashkina, 2020), they had developed a "upside-down" control scheme, whereby the phone is acted as a NFC reader to scan NFC tags that are placed near the door. The administrator will bring a device for the programming to take place on the passive NFC tags to store information about which unique gate number and the gate location it is located at, the API to launch program instantly for both Apple and Android. This type of data is formatted as NDEF (NFC Data Exchange Format). A server is being used to handle all the data and the information of employees. Employees will only have to use their phone which has a built-in NFC chip and scan the passive NFC tags and an application would be launched and they must take a photo of themselves as a biometric matching in the database of the server. In this research, the researchers have made use of the built-in NFC chip of mobile phones despite different operating systems which restrict the NFC chip functionalities to third-party developers. This has made it more convenient, cheaper, and easy to implement as third-party developers do not have to worry about the developer capabilities of different operating systems.

According to (Pierce, 2019), with the emerging technology of smart home that uses the landscape of IoT technologies, there has been many types of affluent and tech-savy demographics—to novel modes of interaction and smart functionality smart home security cameras been introduced to the consumers. These newly developed smart home security cameras push the boundaries of conventional definitions of home security and offer security against the old and new threats to the home. By all means, it offers new vulnerabilities to the most private and intimate interior space of users to track and surveillance around their home. Some of the big companies like Google and Amazon have developed their own smart home security camera. Google's Nest Cam implements artificial intelligence (AI) for facial recognition, analyzing human anatomy and behavior, and any environmental activity. Google's Nest Cam will be able to detect any unfamiliar faces or uncommon senses activity and notify users to alert them regarding the happenings in their home. Besides that, there has been emerging technology of using big data and analytics for any predictive criminal activities. The use of big data will make real-time facial-recognition software that links with existing surveillance cameras to massive biometric database to automatically identify people with open warrants.

Apart from the research and prototypes that have been mentioned above, there have been few home security systems that are offered to customers in the current market. One of them being Huntaway Security Singapore.

According to Huntaway Security Singapore (n.d.), they offer a Burglar Alarm System that has the features of Alarm Control Keypad, Alarm Motion Detector, Alarm Door Contact and Alarm Siren. This

system generates loud noises and flashing lights and sends alerts to authorized parties whenever there is a breach of a sensor or motion detector. Besides that, Huntaway Security Singapore still offers a Home Door Access service whereby the technology of the access system is advanced technology that should be utilized and equipped by every household. A notable product series would be the Series Facial Recognition Reader whereby it equips different types of security access which are fingerprint reader, facial recognition, and card terminal. These different types of security access can be utilized depending on the user. The Series Facial Recognition Reader also offers advanced time attendance software which notifies the user regarding the entry of user with live stream camera and time attendance. Users can remotely control the security access around the world with the provided application. Regrettably, the presence of multiple security access points for home doors means that burglars would only need to compromise one of these access points to gain entry, potentially undermining the overall security of the property. This vulnerability highlights the importance of comprehensive security measures that address potential weak points in the system. Burglars can enter the household and steal some easily seen worthy items and escape easily even if there's loud sirens and flashing lights. Considering these factors, users should carefully evaluate the advantages and disadvantages of installing both the Burglar Alarm System and Home Door Access service, opting for only the necessary features while eliminating any redundant ones. This strategic approach is essential to mitigate the risk of burglars exploiting vulnerabilities and gaining unauthorized access to the household, ensuring robust security measures tailored to specific needs.



Huntaway Security Singapore's Burglar Alarm System

Another home security company that is currently in the Malaysia market is SECOM Smart Malaysia. According to SECOM Smart Malaysia (n.d.), they provide two packages of home security system, one of the notable one is named SECOM Smart CP155+. The SECOM Smart CP155+ package includes sensors and detectors like smoke detector, motion detector, acoustic glass break sensor, shock sensor and door contact sensor. The sensors have enhanced the security level of household by installing in every possible path of entry to the house with stress-free installation which indicates no cable-laying or wall-hacking required which prevents any unnecessary mess. Whereby motion detector detects any sense of motion, acoustic glass break sensor detects a smash or breaking window by utilizing a microphone to recognize the acoustic patterns of smashing and breaking windows. The shock sensor detects any force entry of windows or doors, door contact sensor monitors the opening and closing

of doors to alert any use of irregular activities. The smoke detector just acts as a fire prevention as it is implemented with the latest Optical Chamber technology to detect potentially harmful smoke particles. The packaged home security system also includes a surveillance system inside and outside of the house as well. The indoor surveillance camera can be customized with battery pack to allow back up power in case of power failure providing complete uninterrupted surveillance at high camera level quality. The indoor surveillance camera also requires internet connection with the online cloud storage to record and store high quality recording camera footage that is out of any hacker's reach. The outdoor surveillance camera provides cloud services to record and store high-quality recordings of camera footage too. It also comes with heightened motion detection to detect potential intruders. The outdoor surveillance camera also equips a two-way audio with a built-in microphone and speaker to remotely communicate and listen through mobile application, making remotely real-time monitoring a dream come true. Included in the comprehensive home security package are several essential accessories designed to enhance safety and convenience. These include a user-friendly wireless keypad for easy and quick access to their security system, a physical panic button for instant emergency response, an outdoor visible and audible siren to deter intruders, an intelligent alarm reporter for seamless communication between devices and the control panel, and a physical keyfob enabling remote arming and disarming from anywhere within your property.

According to SECOM Smart Malaysia (n.d.), they set the standard for top-tier protection with its cutting-edge surveillance system seamlessly integrated with secure cloud storage. Featuring advanced motion detection capabilities, it distinguishes genuine threats from innocuous disturbances, sparing users from needless interruptions. Gone are the days of incessantly checking phones for false alarms triggered by stray animals or objects. Additionally, SECOM Smart Malaysia prioritizes inclusivity with screen reader support, ensuring visually impaired individuals can stay informed about their home's activities. Furthermore, our commitment to seamless operation minimizes downtime during installation, upgrades, or maintenance, guaranteeing uninterrupted security for your household.

According to SECOM Smart Malaysia (n.d.), they offer comprehensive support to its users, including 24/7 central monitoring services and professional installation assistance. With dedicated professionals available round-the-clock, users can rest assured knowing that their safety is constantly monitored. Utilizing state-of-the-art wide-angle cameras and high-resolution imagery, potential threats are swiftly identified. Upon detection of any unauthorized activity, the vigilant monitoring team is promptly alerted through advanced motion sensors. They then take immediate action by informing both the user and the appropriate authorities. This proactive approach ensures rapid response to any security concerns, providing peace of mind to users year-round. The central monitoring service and installation support seamlessly integrate with chosen security packages, encompassing alarm sensors and surveillance cameras, to offer a complete security solution.

SECOM Smart Malaysia's SECOM Smart CP155+ Package

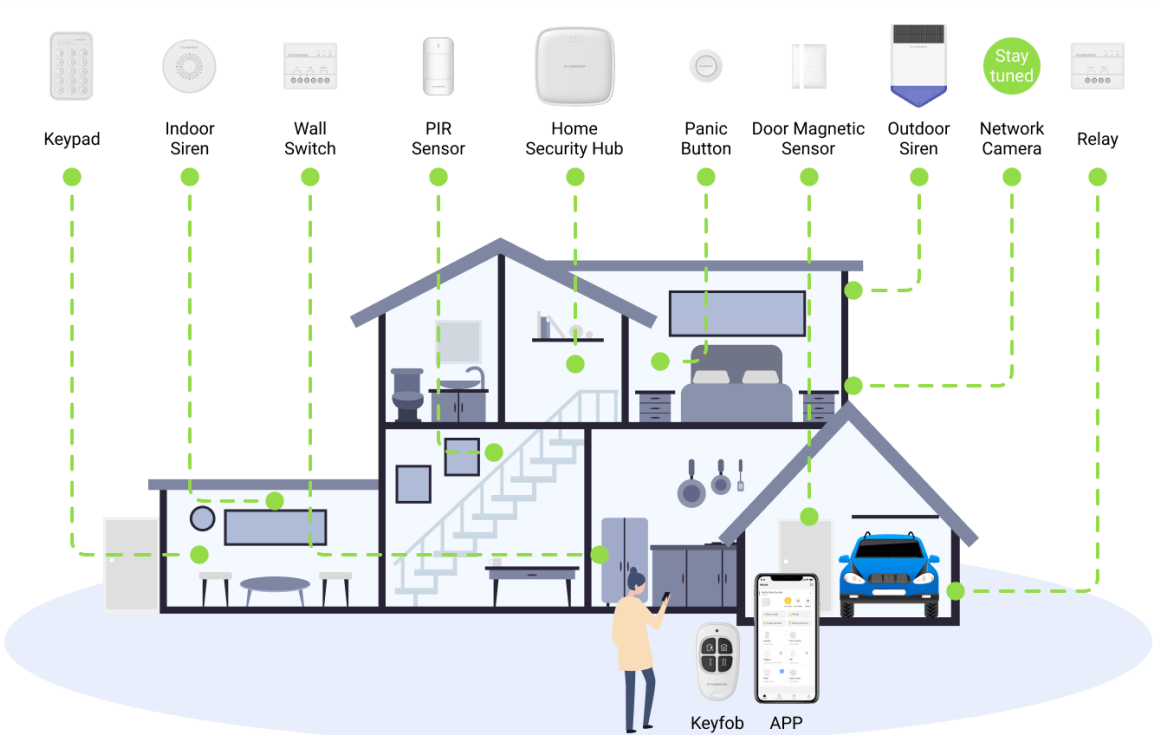
Together, with these components and services, they can form a robust security framework, ensuring comprehensive protection for users' homes and loved ones while offering unparalleled convenience and peace of mind. SECOM Smart Malaysia introduces a cutting-edge home security system package, which combines traditional security methods with state-of-the-art technology. One notable advancement is the integration of keyfobs, allowing users to wirelessly operate auto-gates with ease. While this integration elevates security standards through various sensor types, the reliance on physical keyfobs and panic buttons presents a limitation. These devices are only operable within the confines of the housing area, lacking remote accessibility. Despite this inconvenience, the overall security level is undeniably heightened, showcasing SECOM's commitment to modernizing and enhancing residential safety measures.

There has been a global and remarkable security company providing home security system in the United Kingdom, Europe and Netherlands named Roombanker. According to (RoomBanker, n.d.), Roombanker has designed a specific home security system for every type of housing, therefore the convenience and suitability are at the top level of it. The common equipment in all the types of home security system are intrusion detection and indoor environment safety and comfort. The intrusion detection includes pir sensor, door magnetic sensor, sirens, panic button, relays, wall switch, keypad and a keyfob. This intrusion detection offers all compassing protection during day and night as it is equipped with a wide range of sensors at the windows, doors, rooms, and areas where intrusions often occur for confident security. Besides that, it is easy to install and maintain as it has little to no wires. The application that Roombanker has provided is a fully remote control with only a tap, one-click for the intrusion detection to arm or disarm, anytime and anywhere. The application will also inform the users with real-time videos for visual verification which avoids the waste of manpower to check out the household, time and money caused by false alarm. Roombanker enhances convenience through the integration of IoT principles, utilizing relays to safeguard against overvoltage and monitor electricity consumption, complemented by wall switches for remote configuration via the mobile application, enabling users to effortlessly toggle or deactivate the switches with a simple click within the application interface. A special feature of Roombanker's home security system is it incorporates three types of wireless technology in all the equipment, which are Zigbee, Bluetooth and RBF.

According to (RoomBanker, n.d.), the RBF technology provides Two-way wireless communication that has vast coverage, lower power consumption, frequency hopping spread spectrum technology, AES-CCM data encryption, omni-directional antenna, automatic signal adjustment, listen before talk mechanism. The RBF technology is built upon Sub-1GHz spectrum and leveraged advanced FSK/DSSS modulation technology which provides wireless communication with an impressive vast coverage up to 3500 meters. The RBF protocol employs AES-CCM data encryption in conjunction with FHSS, rendering the intrusion attempts of attackers futile in terms of interference, signal interception, and replication. With the omni-directional antenna, the signal strength is balanced and can traverse strongly in all directions, resisting signal loss that is caused by obstacles in the transmission path effortlessly. All RBF devices require just two AA batteries for a standby lifespan of up to 2 years which significantly reduces maintenance frequency. The frequency hopping spread spectrum technology is being utilized as anti-jamming whenever the RBF devices meet continuous interference from an intruder that uses the signal illegally within the same frequency range. Devices with RBF technology can adjust the transmission power based on signal strength automatically, to lower the power consumption, extending the battery life of devices and hence reducing the frequency of battery replacement. The listen-before-talk mechanism integrated into devices with RBF technology engages when multiple events are triggered simultaneously; each peripheral activates this mechanism to ascertain if the current channel is occupied, subsequently either switching to an alternate frequency or awaiting channel availability before transmitting the signal, thereby averting channel congestion and potential data loss. The implementation of RBF technology has significantly bolstered security measures, effectively safeguarding against unauthorized tampering with surveillance footage and thwarting attempts at equipment interference by intruders. Moreover, the system ensures robust signal transmission across expansive areas up to 3500 meters, facilitated by automatic signal adjustment mechanisms, thereby reducing power consumption and prolonging battery life, ultimately resulting in fewer instances of battery replacement and uninterrupted operational efficiency with the listen before talk mechanism. While Roombanker's home security system boasts numerous benefits, there are also several drawbacks worth considering. Firstly, the reliance on wireless technology, including Zigbee, Bluetooth, and RBF, may introduce vulnerabilities to potential hacking or interference, despite the encryption measures in place. Additionally, the complexity of integrating multiple wireless protocols could potentially lead to compatibility issues or system malfunctions, especially with the need for automatic signal adjustment and frequency hopping spread spectrum technology. Moreover, while the system offers vast coverage of up to 3500 meters, obstacles in the transmission path could possibly still result in signal loss or degradation, compromising the effectiveness of the security measures in certain environments. Furthermore, although the listen-before-talk mechanism helps prevent channel congestion and data loss, it may also introduce delays in signal transmission, impacting the system's responsiveness in critical situations. Overall, while Roombanker's RBF technology enhances security and convenience in many aspects, it's essential for users to weigh these advantages against the potential limitations and vulnerabilities inherent in such advanced systems.

The equipment employed by various companies and prototypes mentioned above share a common objective: to bolster security measures and thwart potential burglaries. However, in the ever-evolving landscape of security threats, modern-day burglars exhibit a relentless pursuit of exploiting vulnerabilities across all types of home security systems available in the market. Gone are the days of brute force entries; today's intruders are adept at circumventing sophisticated measures, from bypassing biometric fingerprint scanners to executing swift thefts and eluding detection even in the presence of sirens and surveillance cameras. Consequently, it is imperative for users to have

contingency plans in place to respond effectively when they become aware of a breach in their home security.



Roombanker's Intrusion Detection

Companies	Huntaway Security Singapore	SECOM Smart Malaysia	Roombanker
Equipment	Burglar Alarm System	Smart CP155+ Package	Intrusion Detection
Motion sensors	Alert authorities when any breach of sensor or motion	Wide and special implementations of Window and shock sensors	Wide range of sensors attached everywhere
Uniqueness	Facial Recognition Reader offers time attendance and notification system	Outdoor surveillance camera offers two-way audio communication and motion sensor	Devices with RBF Technology
Types of control remotely	Remote Mobile Application	Remote Mobile Application	Remote Mobile Application
Security accessories included	Motion sensor, camera, etc	Motion sensor, camera, etc	Motion sensor, camera, etc
Methods of notifying user	Notification system	24/7 Central Monitoring Service	Notification system
Inconvenient	Inconvenient due to control keypad needs to be manually controlled	Inconvenient physical keyfob and panic button can only be used in housing area	Inconvenient physical keyfob and panic button can only be used in housing area
Vulnerability	Multiple access points	Vulnerability to potential hackers	Vulnerability to potential hackers

Therefore, this project uses some of the ideas and hardware mentioned above to implement a well-rounded IoT based home security system which gives the burglars a harder time to break in the house and a remote lockdown system to keep broke in burglars enclosed in an area, delaying their time until the authorities arrive.

7.0 System Design

7.1 Methodology

To build home security based on IoT technology, multiple security measures will be implemented. The security measure is implemented with the use of NFC technology, users will have to scan their MIFARE tag and have the tag ID match against the NFC reader, if it matches then access will be to the first door will be allowed. The tag ID will be preset in the NFC reader.

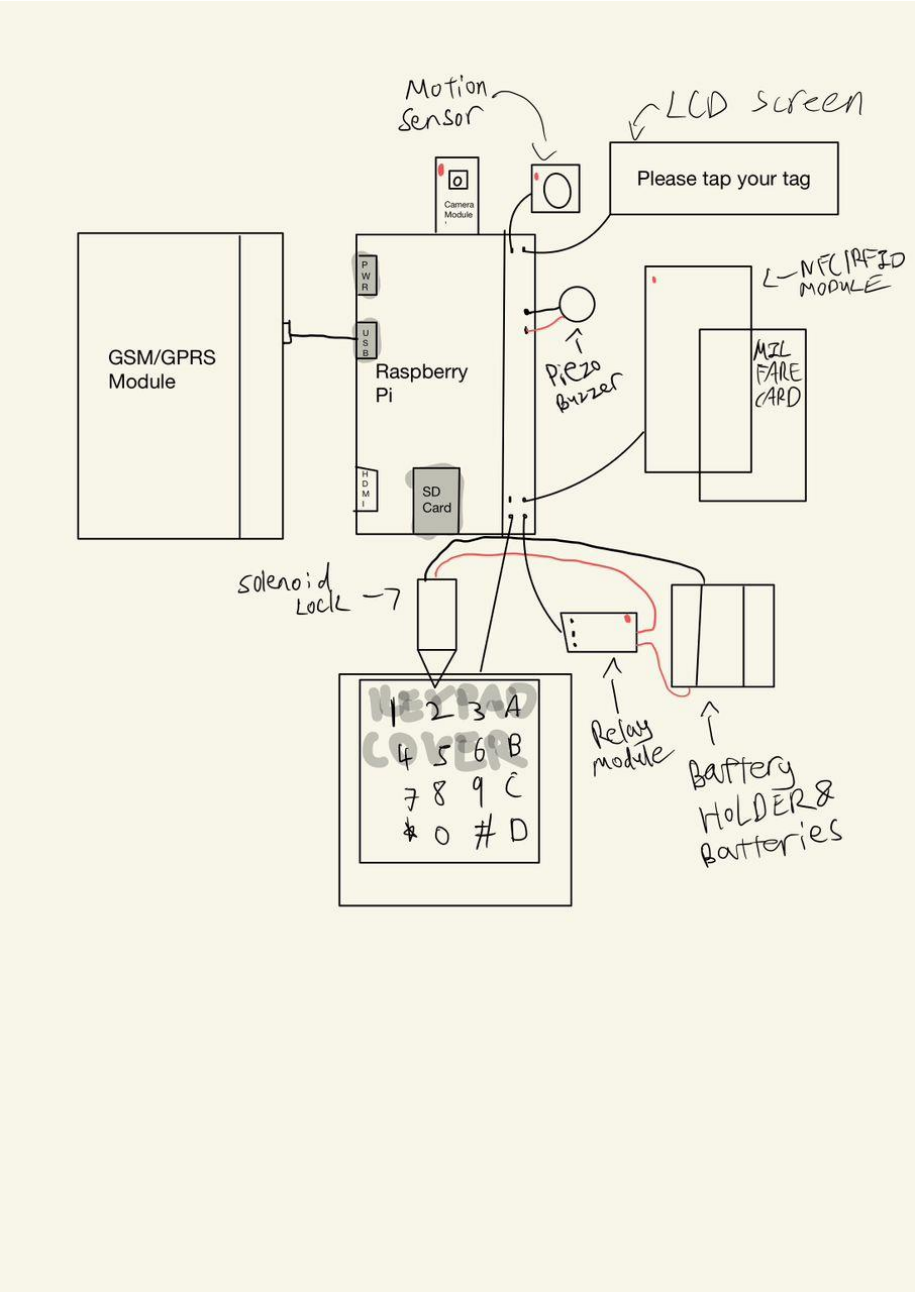
The second security measure employs a password key mechanism with a limit of three attempts. After three unsuccessful attempts, an automatic lock down will be initiated. To physically secure the password entry, the solenoid door lock pushes the hard lid down and covers the keypad, to prevent direct contact between the burglar and the keypad.

The lock down can be activated remotely by the house owner at any time or location by using the blynk app, or it will automatically be triggered after three failed password attempts. Furthermore, motion sensor will only be activated after successful entry from the first door. By triggering the motion sensor, it will detect any motion and if there are, the camera module of raspberry pi will be activated as well to capture live camera footage for few seconds. The camera footage will then be attached into an email and sent to the users as a notification system to alert them about it.

In the event of a lock down, a siren by piezo buzzer is triggered to alert nearby neighbors to be aware of it.

The blynk app utilizes internet connectivity for the users to issue commands remotely around the world. Hence, the lock down system is managed by users controlling through blynk app which informs the microcontroller to perform or remove the lock down. This provides users with the capability to issue or remove lock downs at their discretion and control the on and off the alarm.

7.2 Model Diagram



With the model diagram above, there would be 4 scenarios happening.

The first scenario

1. User scans NFC/RFID tag and enters first door.
2. Motion sensor detects motion and trigger camera module to capture recordings.
3. Email is sent to the user with recording attached.
4. User locks the first door by scanning the NFC/RFID tag again.
5. User enters keypad password.
6. User enters house.

The second scenario

1. Intruder scans incorrect NFC/RFID tag.
2. Intruder cannot enter the first door.

The third scenario

1. Intruder scans correct NFC/RFID tag.
2. Motion sensor detects motion and trigger camera module to capture recordings.
3. Email is sent to the user with recording attached.
4. Intruder keys in three times wrong keypad password.
5. Lock Down is automatically issued.

The fourth scenario

1. Intruder scans correct NFC/RFID tag.
2. Motion sensor detects motion and trigger camera module to capture recordings.
3. Email is sent to the user with recording attached.
4. Lock Down is issued by user.

7.3 Hardware

Raspberry Pi 2.0 Zero 2 WCH Basic Kit is used as the microcontroller board to incorporate the programming and connect to all the other electronic modules to perform the programmed actions. This module acts as the central system where it performs all the programmed actions based on the invasion of intruder or inputs from the user. A relay module is connected to the microcontroller board to provide higher or lower levels of voltage to the solenoid lock to perform the pushing action.

GSM/GPRS module is used as the communication model with the user's mobile phone as it would be used to receive input for the microcontroller to perform according to specific inputs with specific key words in the user's text messages by SMS by specifying specific keywords.

Keypad and PN532 NFC/RFID Module Kit which includes ISO 14443A/MIFARE tag, are used for the multi-layered security system of the doors. MIFARE tag will be used to register it's ID tag as desired into the PN532 NFC/RFID Module Kit and use for reading ID tag for future entry of the door. Keypad acts as the input of password from user and is connected to the programmed microcontroller board as well to achieve the 3 attempts for password key-in. The LCD Screen has the main purpose to display results when the MILFARE tag scans the NFC/RFID module.

Anti-theft and shockproof construction Solenoid Door Lock is used as the push and pull "spring" of the keypad cover when the lock down is triggered or removed. It is connected to the programmed microcontroller board to receive inputs from the users to determine whether to push or pull the keypad cover.

5MP Camera Board for Raspberry PI is used to capture the images of visitors and send it to the users through email by connecting to the programmed microcontroller board. PIR sensor Module is used to detect the motion of visitors and if it does detect, triggers the Camera Board for Raspberry PI to capture images.

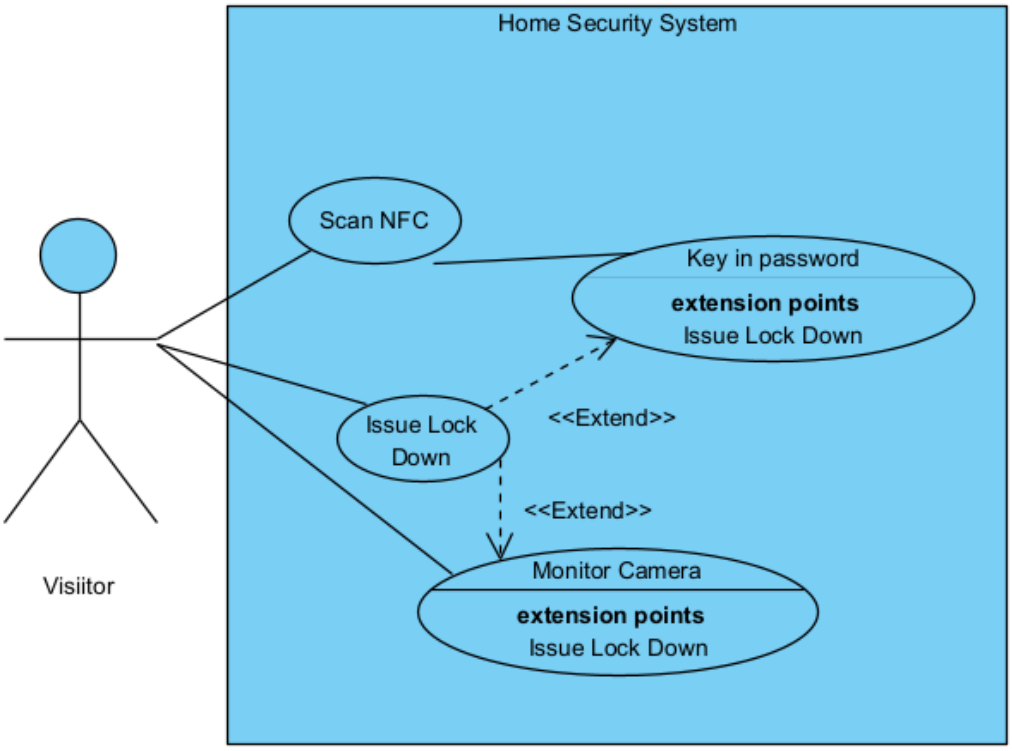
Piezo Buzzer is used as an alarm siren by connecting to the programmed microcontroller board buzzes together with the lock down mechanism.

With all components connecting to the microcontroller board, the lcd screen should display the preset words and users can scan the NFC/RFID module with their preset Tag ID. Then, the motion sensor will detect motion and trigger the camera module to capture recording. The captured recording will be sent as an email to the user. Keypad password could only then be keyed in next and if reaches three times of failure, lock down will be issued automatically or can be issued and removed manually by user remotely by controlling through the blynk app. These are drafted and shown in the Model diagram.

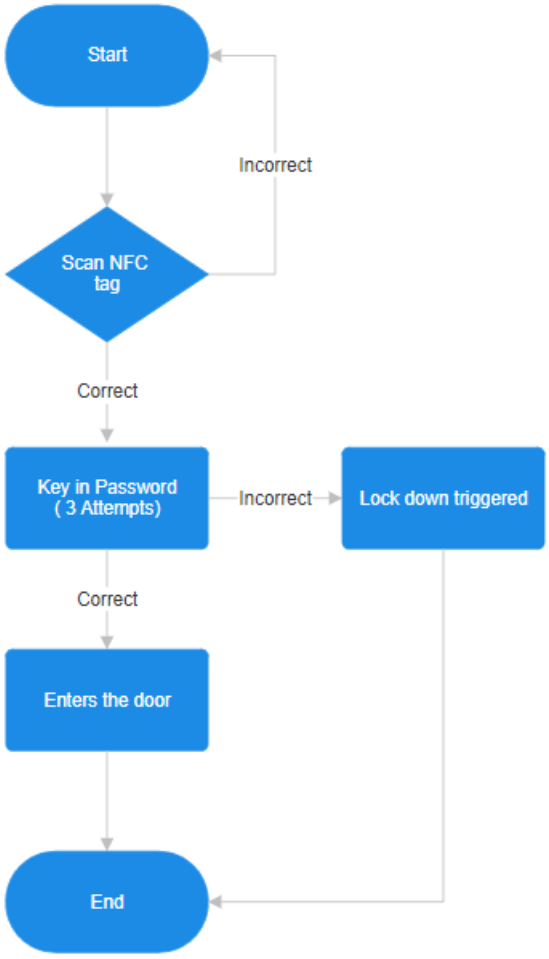
7.4 Software

An open-source app called Blynk app (Anitha, 2017) is the central system to control the commands and send inputs to the microcontroller board from anywhere to perform certain actions. The app provides user to control the lock down remotely from anywhere in the world.

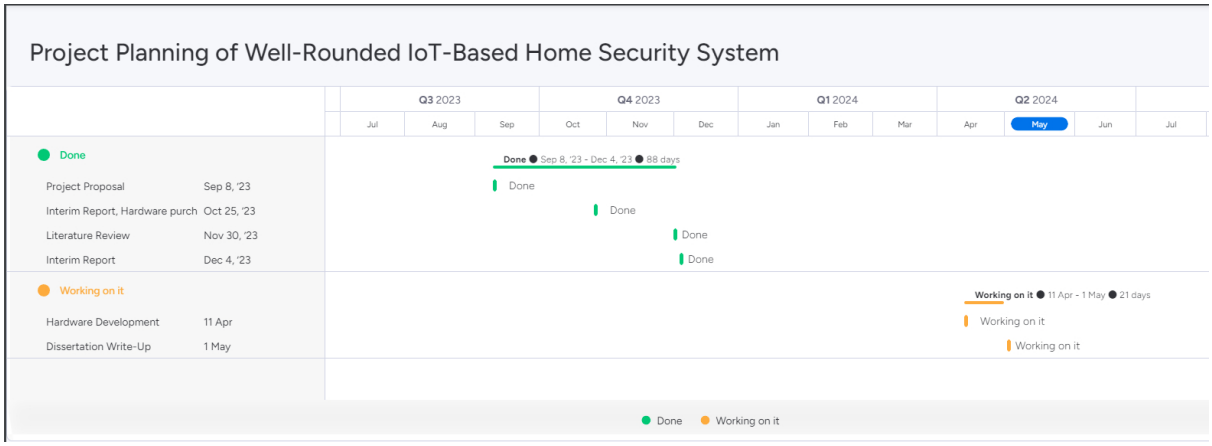
7.5 Use Case Diagram



7.6 Flowchart



8.0 Project Plan



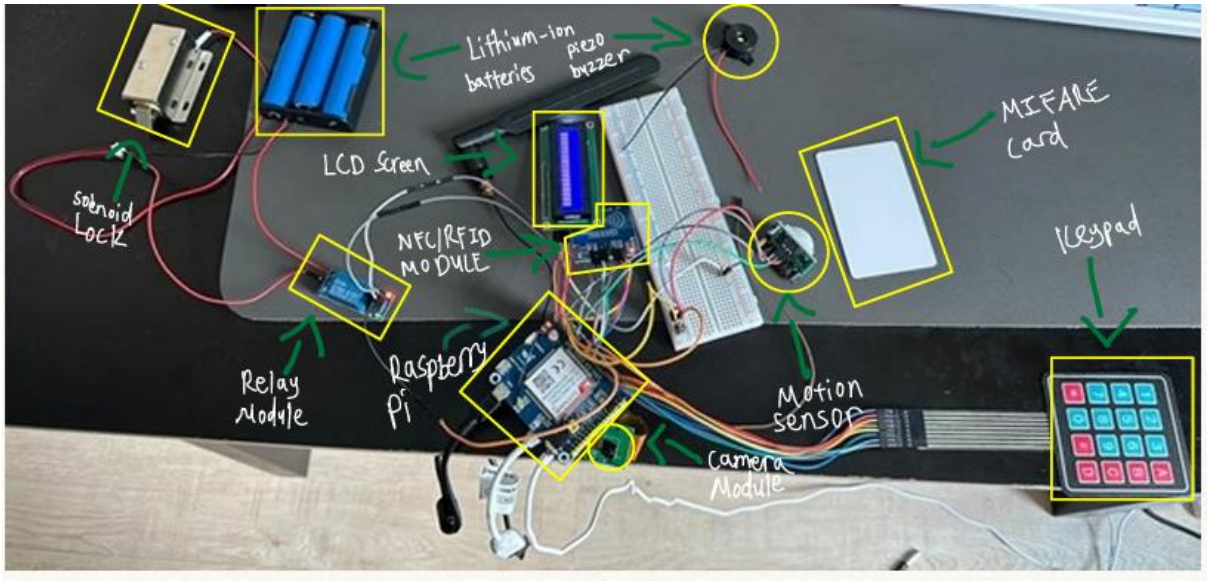
The Gantt chart above is designed by using Monday. The Gantt chart consists of the following phases. With phase 1 being submitting the project proposal, which is already done, and approval was granted. Upon the approval of the project proposal, phase 2 begins with writing off the Interim Report which includes introduction, objectives, aim, and literatures review meanwhile surveying the hardware to make early purchases. After the completion of phase 2, begins phase 3 of completing the literature review by going through articles, papers and weblinks to obtain useful information and write it into the interim report. With the completion of phase 3, finishing off the interim report was in the next phase which is phase 4. After phase 4 is finished, Hardware development had the most time in phase 5 as it is the most crucial part in the Well-Rounded IoT-Based Home Security System project. Phase 4 is planned to finish on the 11th of April 2024. If phase 4 manages to finish on time, it will go to the final phase which is dissertation write-up.

Various planning frameworks exist for computer science projects, with popular options including the waterfall model and the scrum framework. While the scrum framework is favored for its flexibility and adaptability, thanks to its iterative sprints lasting two to four weeks, it wasn't chosen for this project. This decision stemmed from the project's initial documentation being paramount, particularly as the completion of the interim report precedes hardware development. The project's tasks, as outlined in the Gantt chart, are interdependent; without completing one phase, progression to the next is impossible. Given these considerations, comprehensive planning and documentation are imperative.

Thus, the traditional waterfall model was selected for project planning, characterized by its five sequential phases with assigned tasks. In this model, each phase must be finalized before transitioning to the next, ensuring a methodical and linear progression. Additionally, the varying complexity of tasks across phases necessitates different timeframes for completion. A notable aspect of the waterfall model is its emphasis on upfront documentation and planning, with minimal changes allowed before entering the development or implementation phase.

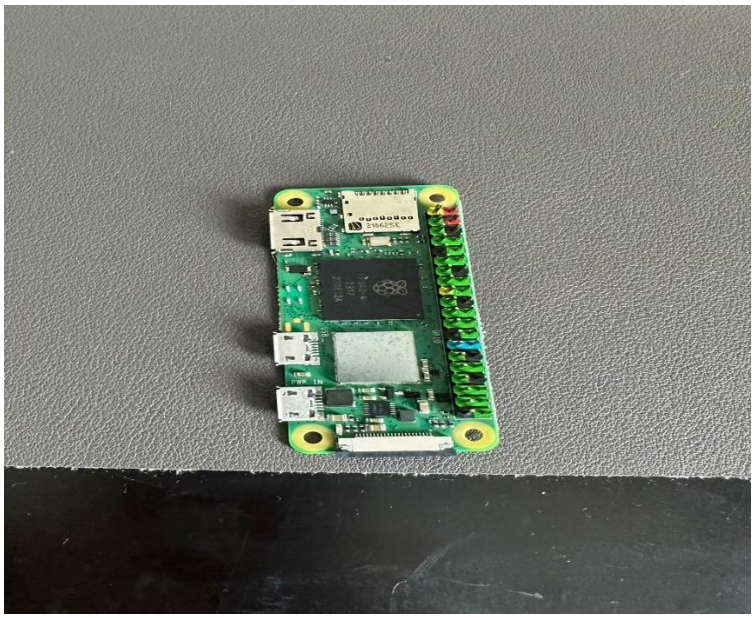
While the waterfall model offers a clear and stable roadmap for developmental projects, it can be less accommodating of immediate changes or uncertainties arising mid-project. Despite this limitation, the waterfall model aligns with the requirements of the Well-Rounded IoT-Based Home Security project. The structured roadmap facilitated necessary hardware purchases and development, with minimal alterations during the project's lifecycle.

9.0 Implementation



From the picture above, the Raspberry Pi Zero 2 is paired below with the GSM/GPRS module. The keypad module, motion sensor, relay module, solenoid lock, Lithium-Ion batteries, LCD screen, NFC/RFID module and Raspberry Pi Camera are being connected to the Raspberry Pi through GPIO pins with some extensions on the breed board.

9.1 Raspberry Pi Zero 2 With Color Head (WCH) Module



Above the physical product of the Raspberry Pi Zero 2 that is used as the microcontroller of the whole project. Below is the method of setting up the Raspberry Pi Zero 2 for further implementation of other electronic components.

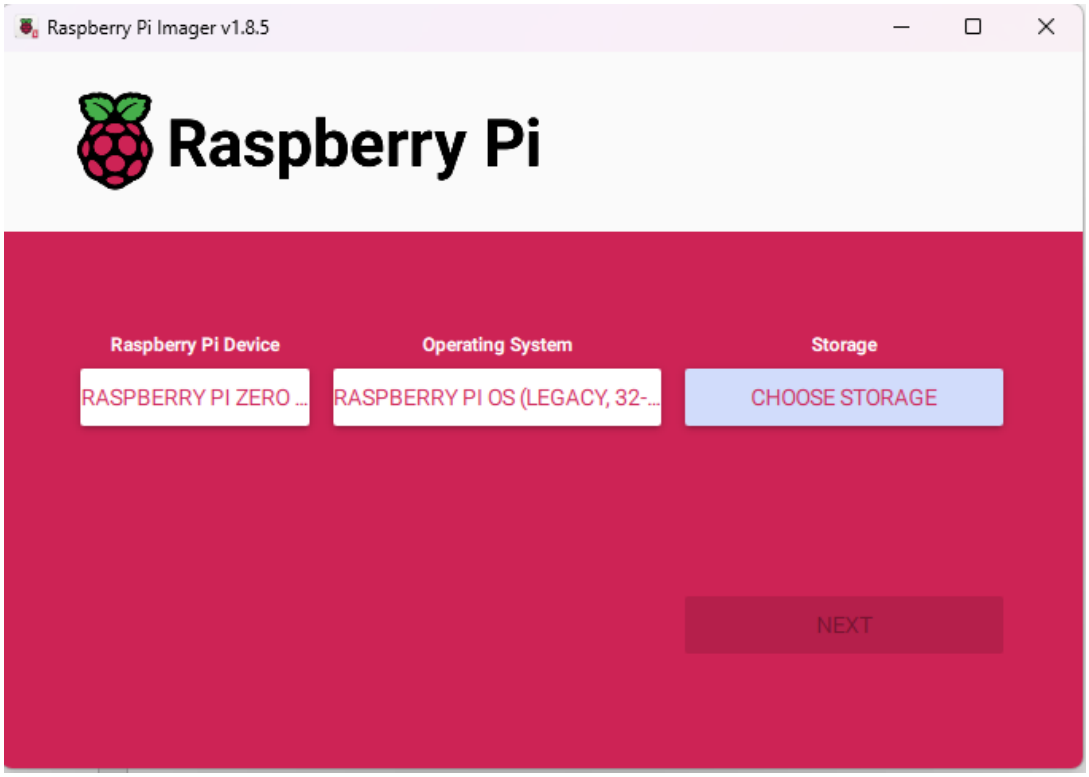
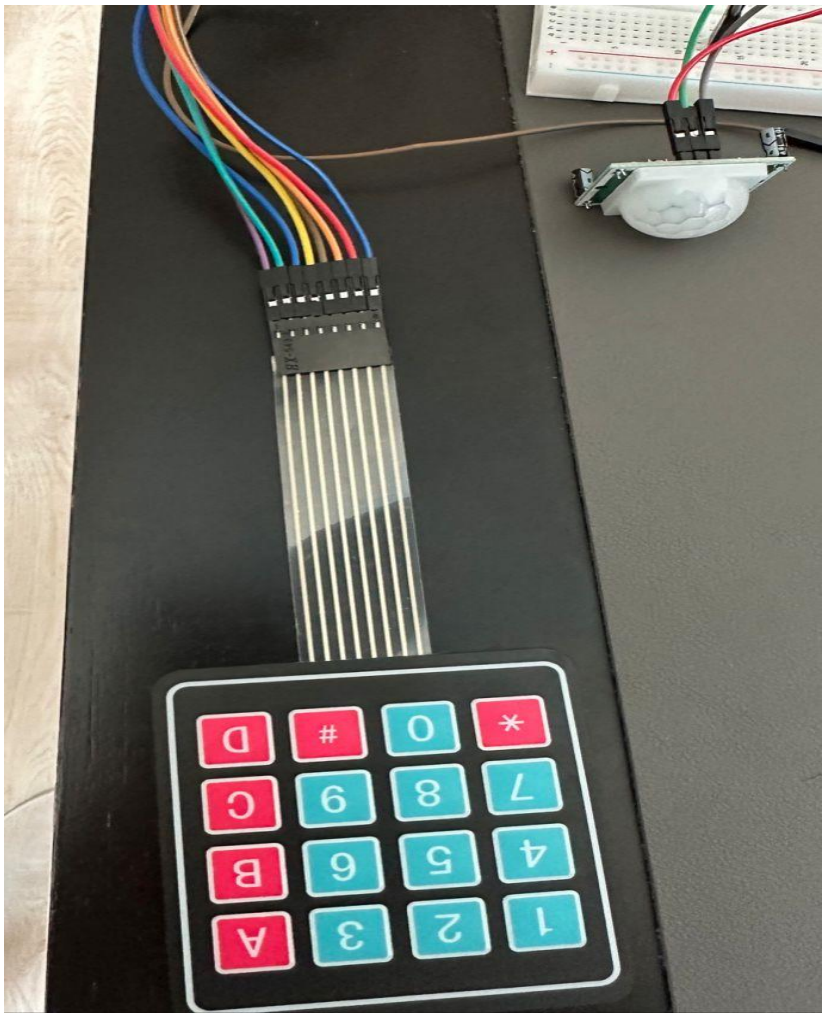


Figure 1

The setup of Raspberry Pi Zero 2 starts by inserting an SD Card written by an app called Raspberry Pi Imager shown in Figure 1. By choosing the correct Raspberry Pi Device, Operating System desire and Storage of the SD Card, it then writes the Operating System into the SD Card. After that, inserting into the Raspberry Pi Zero 2 and having it connected to the power plug, the Raspberry Pi Zero 2 powers up; by plugging a HDMI cable connecting to a monitor and the Raspberry Pi Zero 2, the display is shown.

9.2 Keypad



Picture above is the physical product of the keypad. Below are the figures attached along with the methods of implementing the keypad.

```
MATRIX = [[1, 2, 3, 'A'],
          [4, 5, 6, 'B'],
          [7, 8, 9, 'C'],
          ['*', 0, '#', 'D']]

COL = [26, 19, 13, 6]
ROW = [21, 20, 16, 12]
```

Figure 1.1

The keypad is being setup by connecting it to the GPIO pins of 31,32,33,35,36,37,38 and 40. With the range of 31 to 35 being the column array and 36 to 40 being the row array shown in Figure 1.1.

```
# Secret Code
secret_code = [1, 'A', 2, 'B']  # Secret code is 12AB
```

Figure 1.2

The string is then matched with the pre-set password which is shown in Figure 1.2 to see if it matches. If it matches, the access is granted, and the terminal will show “Secret code matched!”, if it does not match it will display “Secret code does not match!” in the terminal.

```
while time.time() - start_time < timeout and not code_entered:
    for j in range(4):
        GPIO.output(COL[j], 0)

        for i in range(4):
            if GPIO.input(ROW[i]) == 0:
                input_buffer.append(MATRIX[i][j])
                print(MATRIX[i][j])
                while GPIO.input(ROW[i]) == 0:
                    pass
                time.sleep(0.3)

        GPIO.output(COL[j], 1)
```

Figure 1.3

The pressed keys are then appended to a string which is the secret code to the 2nd door shown in Figure 1.3. The keypad is later coded by using a while loop to scan which keys gives an output of 1 which indicates the key being pressed and a time.sleep() to prevent the keys being tapped twice in a short period of time, avoiding unintended keywords.

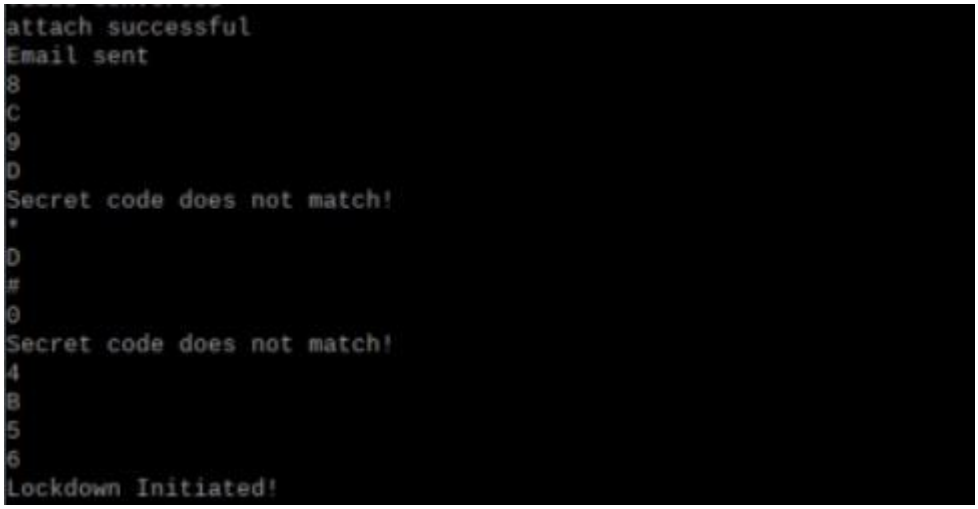
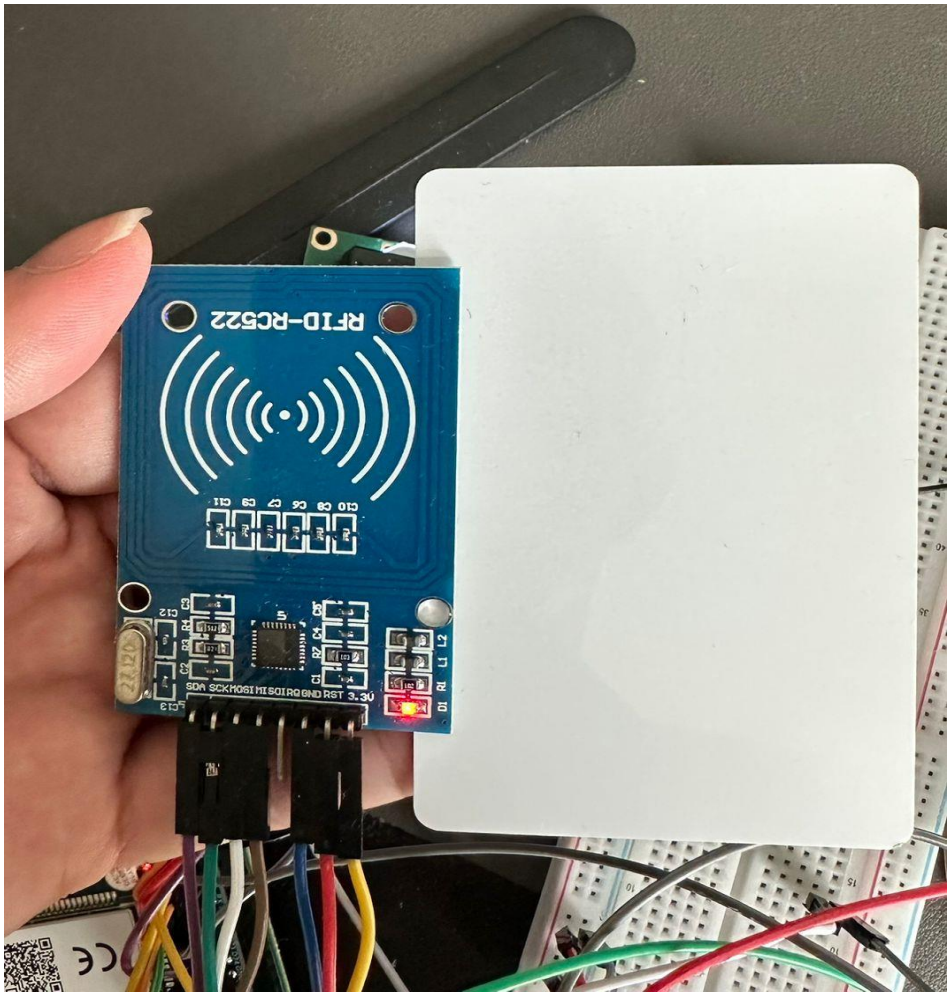


Figure 1.4

An attempt up to 3 tries can be made until whereby all the attempts are finished, the lock down will be initiated instantly and automatically and displaying “Lockdown Initiataed!” in the terminal shown in Figure 1.4.

9.3 NFC/RFID Module



The NFC/RFID module comes with pre-soldered pins; therefore, the soldering pins action was not needed. The NFC/RFID module is being setup by connecting the pins to the GPIO pins of 19 to 24 along with a 3V3 power GPIO pin 1. The setup of the NFC/RFID module started by installing some libraries like spidev and mfrc522 in the raspberrypi terminal.

```
try:
        print("Now place your Tag to scan")
        lcd.lcd_display_string("Place your Tag",1,1)
        scan.write("Tag ID")
        id,Tag = scan.read()
        print("Your Tag ID is : " + str(id))
        lcd.lcd_clear()
        lcd.lcd_display_string("Tag ID",1,5)
        lcd.lcd_display_string(str(id),2,1)
```

Figure 2.1

The method of retrieving the tag ID involved utilizing the scan.read() function and prompting the user with the message "Place your Tag" on the LCD screen. It can be observed from Figure 2.1 above.

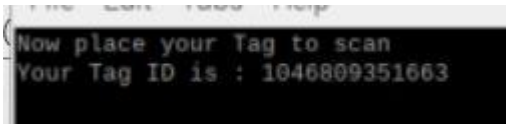


Figure 2.2

After the MIFARE card was being scanned onto the NFC/RFID module it displays “Your Tag ID is : ,shown in Figure 2.1 above.

```
id, Tag = read.read()

id = str(id)

if id == Tag_ID:
```

Figure 2.3

The tag ID is then copied and pasted into another python file which consists of the NFC/RFID module read function to allow access for the 1st door. It uses a read.read() function shown in Figure 2.3 to read the tag ID of the MIFARE card and makes it into a string to compare with the pre-registered tag ID, if it matches then access is granted and it will display “Successful Door is opened”. If the MIFARE card is scanned again after displaying “Successful Door is opened”, it will display “Successful Door is locked”.

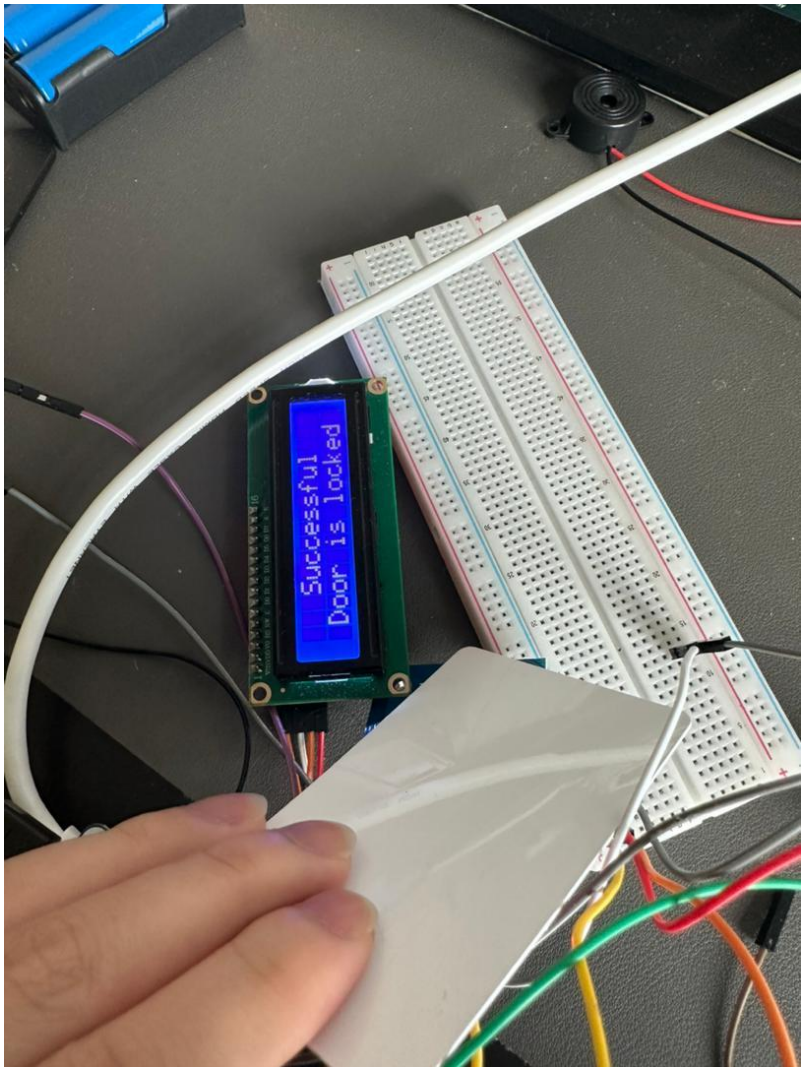


Figure 2.4

If the tag is scanned to lock the door it displays “Successful Door is locked” on the LCD screen. It can be observed from Figure 2.4 above.

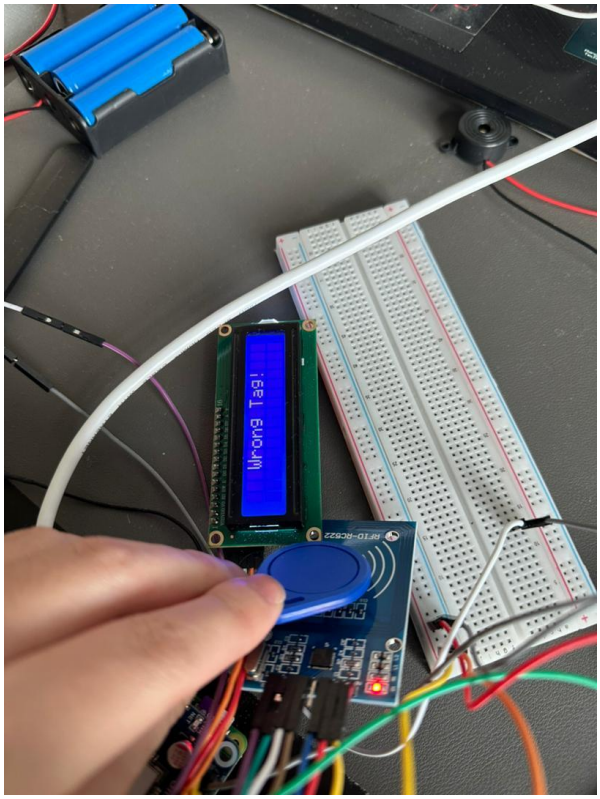


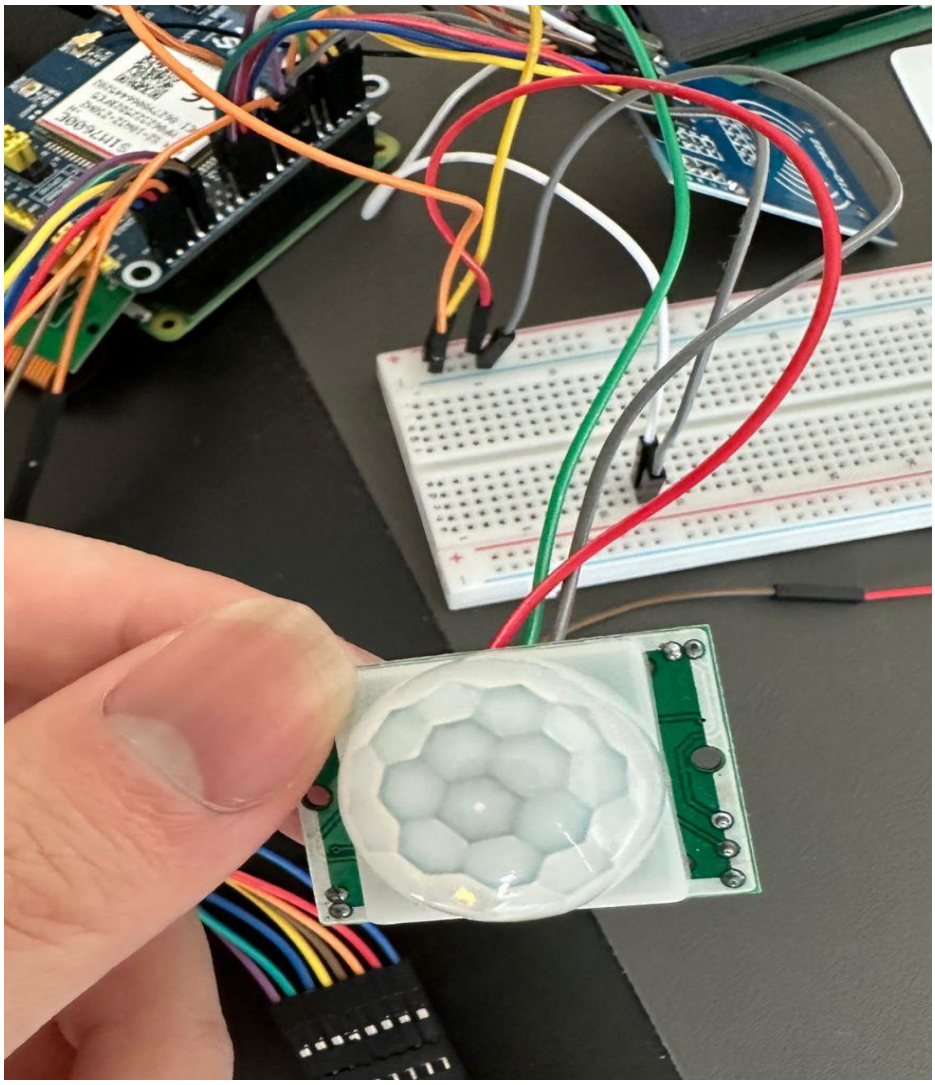
Figure 2.5

If Wrong Tag is scanned, it displays “Wrong Tag” on the LCD screen. It can be observed from Figure 2.5 above.

Figure 2.6

If the tag is scanned for opening the door it displays “Successful Door is open” on the LCD screen. It can be observed from Figure 2.6 above.

9.4 Motion Sensor



The motion sensor is set up by connecting to the GPIO 4,6 and 7. The motion sensor will only be triggered if the entry for the first door is successful.

```
if pir.motion_detected:
    print("Motion Detected")

    camera.resolution = (640, 480)
    camera.rotation = 180
    camera.start_recording('alert_video.h264')
    camera.wait_recording(5)
    camera.stop_recording()
```

Figure 3.1

The motion sensor is coded by importing the library of MotionSensor, and with pir.motion_detected, it detects any motion and if triggers the camera module to start recording shown in Figure 3.1

9.5 Camera Module

The camera module is connected by the cable ribbon and locked with the connector on the raspberry pi. The set up of the camera module is along with the notifications sent through email. The camera module is implemented to trigger when the motion sensor detects for any motion.

A new gmail account was created named raspberrypi031402@gmail.com. This email is used to send email to the user with attached photos or recording captured by the camera module.

The python script imports libraries from picamera import PiCamera , import time import datetime. The camera module is triggered to capture recording of intruder whenever pir.motion_detected from the motion sensor returns true indicating that someone is detected.

```
from_email_addr = 'raspberrypi031402@gmail.com'
from_email_password = 'wbdp hlhr qpwz dpmq'
to_email_addr = 'songzs758@gmail.com'
```

Figure 4.1

The email account is pre-set in the python script, with the sender's email address and password and the receiver's email address shown in Figure 4.1.

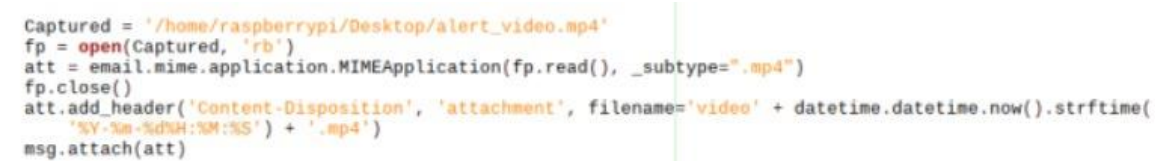


Figure 4.2

The python script of the notification is set up along with the camera module. It imports libraries from email.mime.image import MIMEImage , from email.mime.multipart import MIMEMultipart and import smtplib. By executing the python script, it will then log into the sender's email account with server.login(from_email_addr, from_email_password) and send it to the receiver's email address with server.sendmail(from_email_addr, msg.as_string()). It can be observed from Figure 4.2 and proceeds on with the method in Figure 4.3 below.

Figure 4.3

By connecting to the SMTP server and establishing the TLS communication protocol to encrypt the created message attaching with the captured recording which is converted from h246 to a mp4 file that is playable in mobile phones shown in Figure 4.3 above.

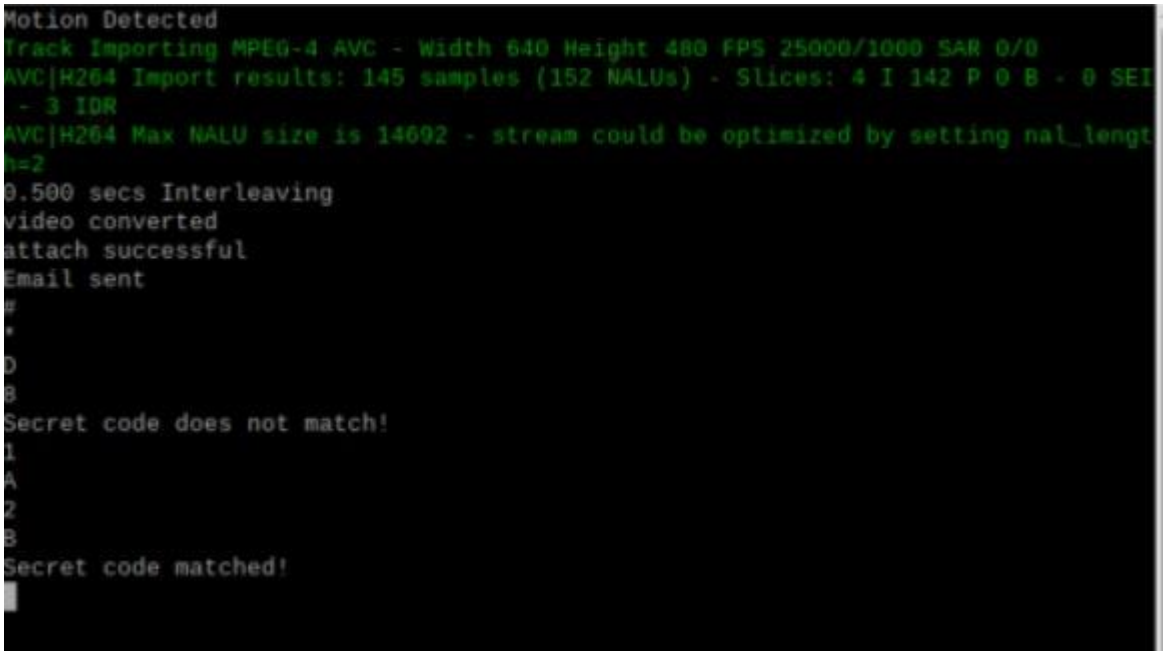


Figure 4.4

Figures 4.4 above shows the success of conversion from h246 to mp4 file and the camera recording attached and sent to personal use of email.

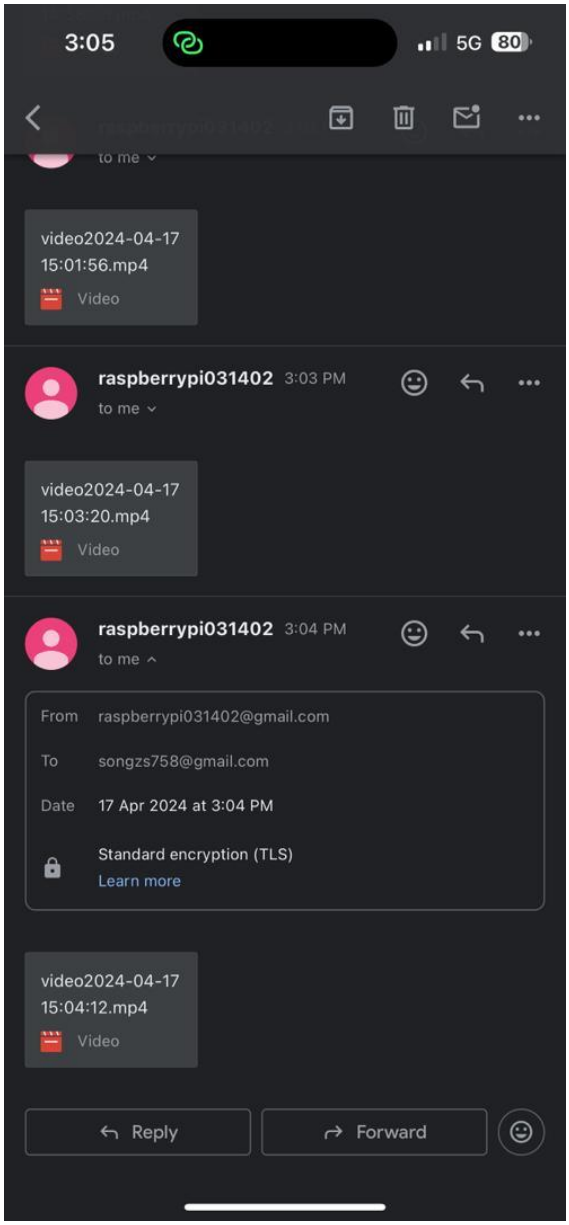
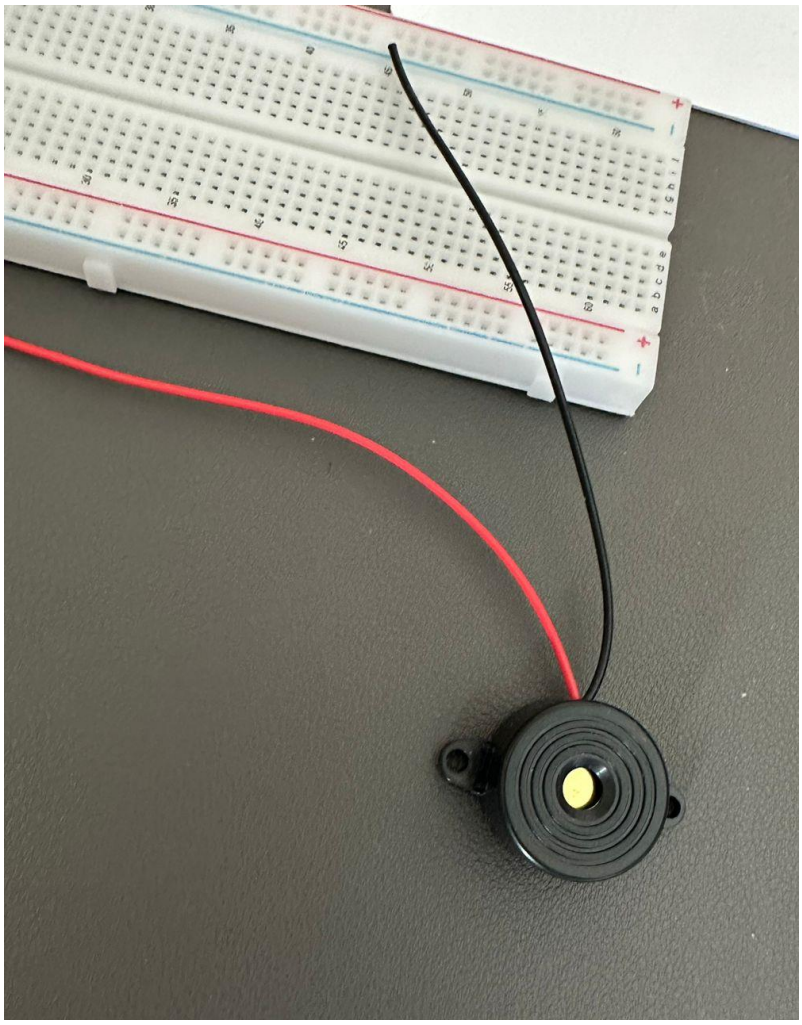


Figure 4.5

Figure 4.5 above shows the success of receiving email from raspberrypi031402@gmail.com with the recorded mp4 camera footage file attached along.

9.6 Piezo Buzzer

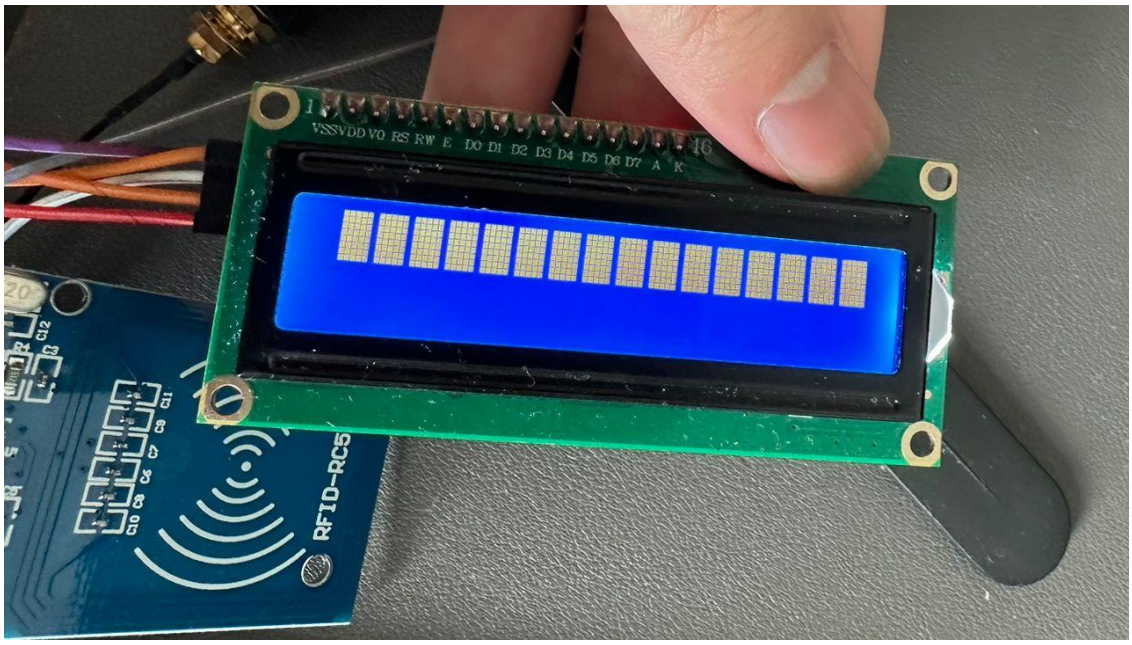


```
lockdown_initiated = True
print("Lockdown Initiated!")
GPIO.output(RELAY_PIN, 1)
GPIO.output(piezo, 1)
time.sleep(2)
```

Figure 5

Piezo Buzzer is connected to GPIO 23 and GND. It is then coded by setting up the GPIO pins and sirens whenever it is triggered by outputting the voltage to 1 and 0 which causes the siren to stop shown in Figure 5. The piezo buzzer is set to buzz whenever lock down is initiated.

9.7 Liquid Crystal Display Module (LCD Screen)




```
  lcd.lcd_clear()
  lcd.lcd_display_string("Place your Tag", 1, 1)
```

Figure 6.1

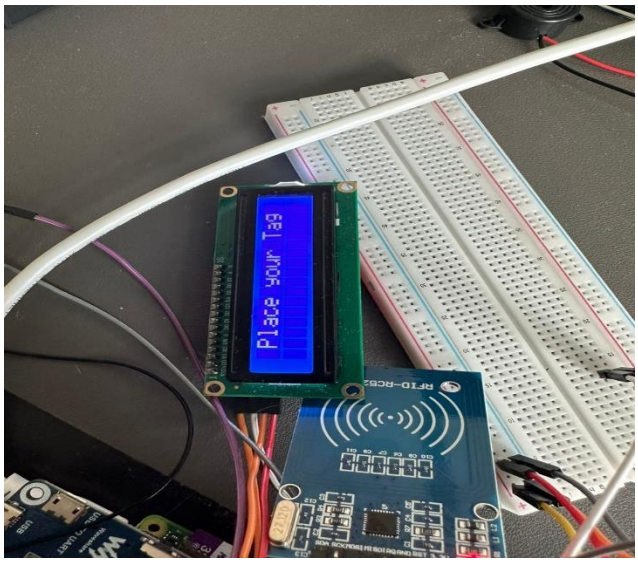
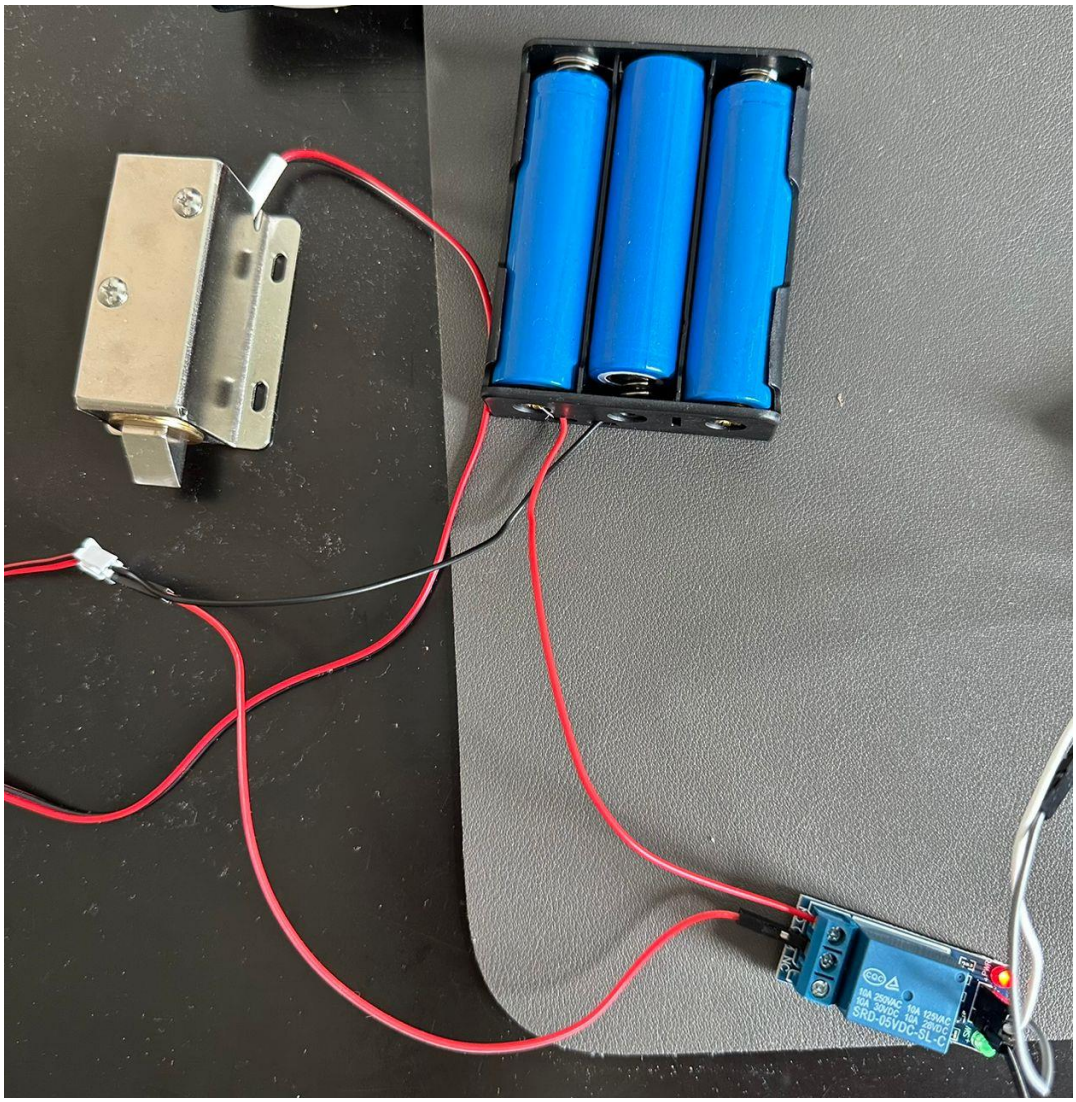


Figure 6.2

The LCD Screen connects to GPIO 3,5,9 and 2 which is a 5V power pin. The method of displaying the result is by importing the library of I2C_LCD_driver and using a lcd.lcd_display_string(“ “,) which the numbers being row and column. Afterwards a lcd.lcd_clear() is used to clear the current results

displayed. The LCD Screen will display “Place your Tag” whenever the script is executed. Those mentioned above are all shown In Figure 6.1 and Figure 6.2.

9.8 Solenoid Lock, Relay Module and Lithium-Ion Batteries



The solenoid lock is connected to three Lithium-ion batteries and relay module to supply sufficient current. The solenoid lock's positive wire connects to the relay module to the COMMON input of the relay module and the negative is connected by the negative wire of the batteries. The batteries' positive wire is connected to the Normally Open input of the relay module so that the solenoid lock will be open by default when the script is executed. The relay module is then connected to GPIO 17,18 and 20.

```
if len(input_buffer) >= len(secret_code):
    if input_buffer[-len(secret_code):] == secret_code:
        print("Secret code matched!")
        code_entered = True
        break
    else:
        if a == 2:
            lockdown_initiated = True
            print("Lockdown Initiated!")
            GPIO.output(RELAY_PIN, 1)
            GPIO.output(piezo, 1)
            time.sleep(2)
            break

        else:
            a += 1
            print("Secret code does not match!")
            input_buffer = []
```

Figure 7

The solenoid lock is coded by setting up the GPIO pins and acts as the lock down mechanism. It will be triggered whenever the three attempts of password are finished and failed or triggered remotely by the user controlling with Blynk app. The implementation method is shown in Figure 7.

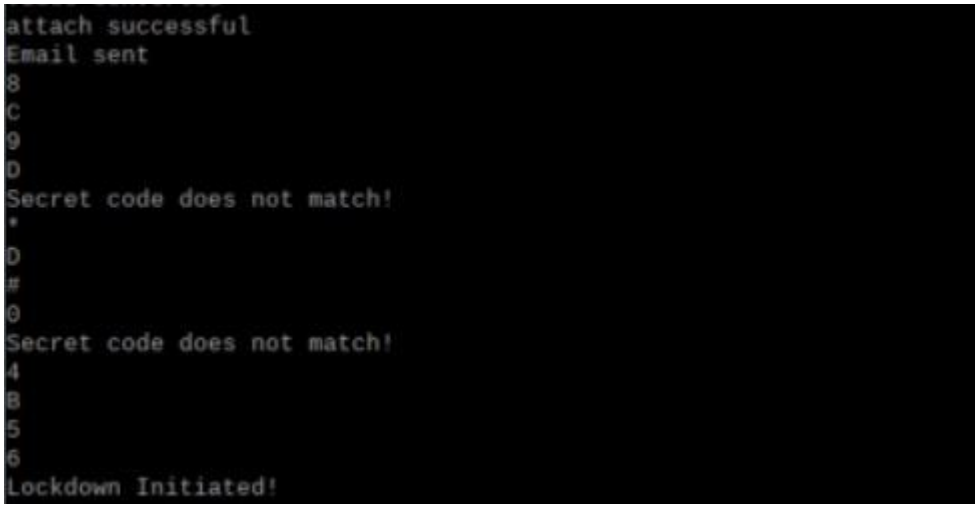


Figure 7.1

Figure 7.1 above shows the lockdown being initiated when three attempts of password are finished and failed.

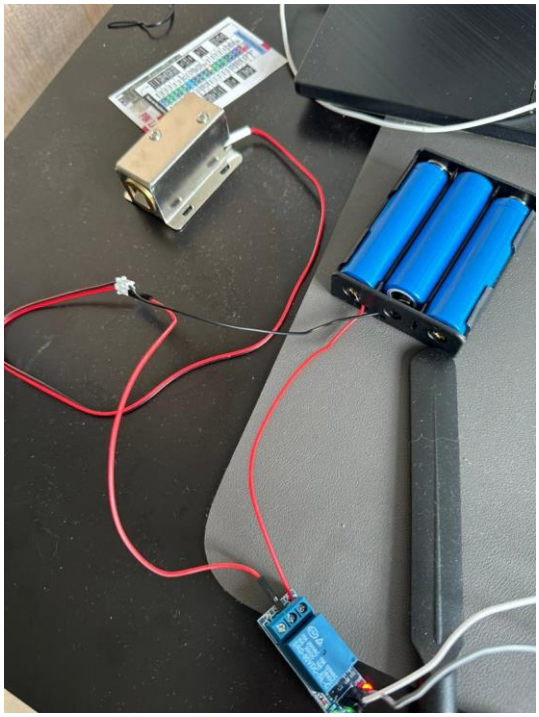


Figure 7.2

The initial state of the solenoid lock which is closed can be observed from Figure 7.2

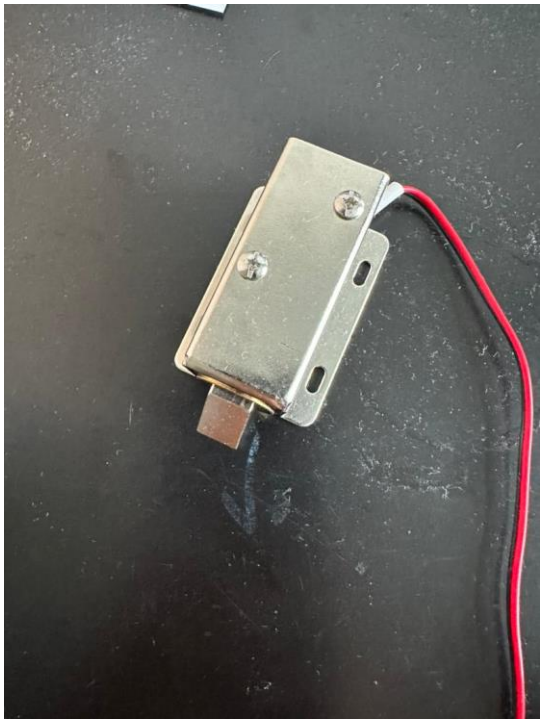


Figure 7.3

The state of success lock down which is opened can be observed from Figure 7.3.

9.9 Blynk App

The Blynk app was utilized to control the lock down system remotely. Blynk was being set up by creating an account and logging in on the website. After that, the mobile phone downloads the blynk app and logs into the same account being created previously on the website to control the lockdown remotely.

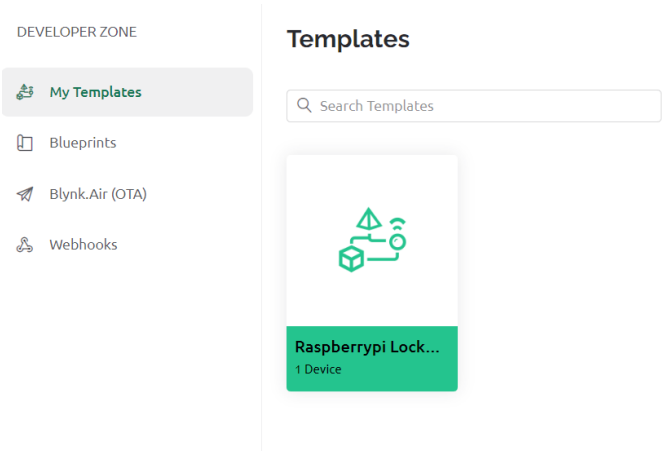


Figure 8.1

A new template named Raspberrypi Lockdown was created and shown in Figure 8.1 to employ device in it.

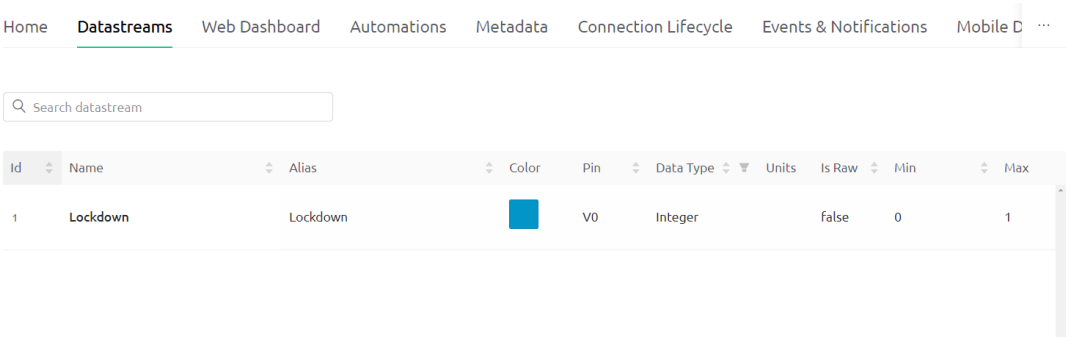


Figure 8.2

A new device is then created and named Lockdown by setting up the virtual pin number, types of connection and hardware module and is shown in Figure 8.2 above.

```
# Blynk authentication token
BLYNK_AUTH = 'UIFGFZl6zERAEufRqDqUtsVa7UH_2tQq'

# Initialize Blynk
blynk = BlynkLib.Blynk(BLYNK_AUTH)
```

Figure 8.3

It is further on coded into the raspberrypi with the methods of connecting to the blynk app with the authentication token gotten from creating the device previously in the template shown in Figure 8.3.

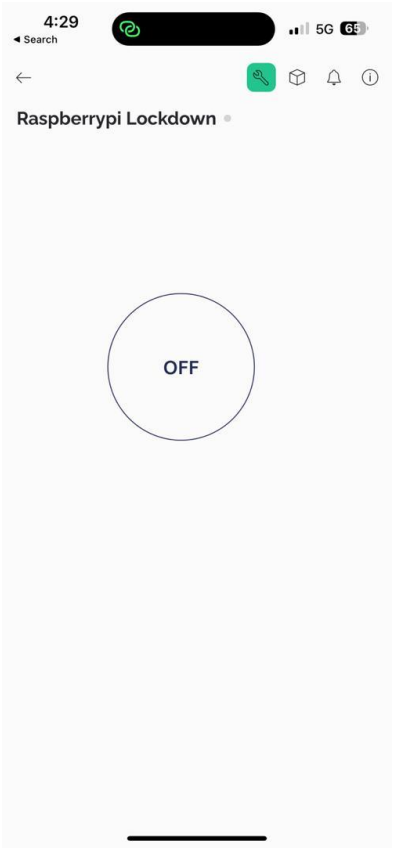


Figure 8.4

With the success of connection to the blynk app displaying in the terminal, users can control the lock down with the interface shown in Figure 8.4. Upon pressing the button and receiving confirmation through the "on" status, signifying the successful initiation of the lockdown via the Blynk app, the terminal will concurrently display "Lockdown Initiated." Conversely, if the button is pressed again, displaying "off" to indicate the deactivation of the lockdown, the terminal will show "Lockdown Removed.

```
# Lockdown control through V0 virtual pin
@blynk.on("V0")
def v0_write_handler(value):
#    global led_switch
    if int(value[0]) is not 0:
        GPIO.output(23, GPIO.HIGH)
        GPIO.output(18, GPIO.HIGH)
        print('Lockdown Initiated')
    else:
        GPIO.output(23, GPIO.LOW)
        GPIO.output(18, GPIO.LOW)
        print('Lockdown Removed')
```

Figure 8.5

Figure 8.5 above shows that the device's virtual pin which is V0 in the template was used to set up for the connection by implementing onto the GPIO input of solenoid and piezo buzzer for turning on and off for the lock down system.

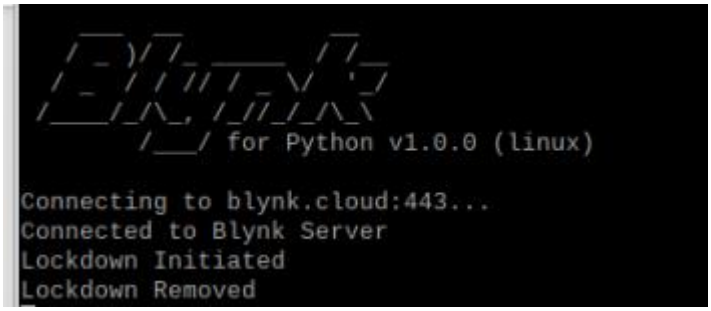


Figure 8.6

Figure 8.6 above shows the success of connecting to Blynk server and the success of initiating and removing the lock down.

10.0 Conclusion

10.1 Results and Discussion

In the beginning, the project planning provided extra time for the hardware development phase as it is expected that it will require more time to develop and run tests for the hardware and software of the project. Towards the end of the project, the phases of tasks were completed successfully within the period provided as planned in the first place.

Moving on will be discussing the choices of hardware and microcontrollers used. The choices of hardware were quite good as it succeeds in making it affordable and achieving the objectives mentioned above as well. Choosing raspberry pi was a good choice but it was not the best choice as there are a few microcontrollers in the market that aim to perform better in IoT-based projects like ESP32 and Arduino microcontrollers.

The results can be summarized as follows: The security measures of both doors were functioning in good condition as they were able to detect the false and correct tag ID and password to decide the grant of access. After successful entry of the first door by tapping the tag ID to the NFC/RFID module, it triggers the motion sensor to detect any motion. Upon the successful of motion detected, it then triggers the raspberry pi camera module to turn on and captures 5 seconds of recording footage of the intruder and the recording footage was attached in an email naming “INTRUDER ALERT!” and sent to the user by email. The keypad was implemented with the success of pressing and keying in the secret code that was pre-set during the implementation. Upon three failed attempts of keying the secret code, the lock down will be initiated immediately, the piezo buzzes functions well to lock the keypad to avoid any direct contact from the intruder. The solenoid lock was malfunctioning due to overheating from previous experiments and attempts causing the internal hardware to be broken, hence it will not function as expected in future usage. By the success of implementing the Blynk app, users can initialize or remove the lock down whenever they want remotely around the world as long as there is internet connection. Overall, these results demonstrate the achievement of the objectives outlined, including successful burglary prevention through comprehensive security measures, an effective notification system, and motion detection implementation. Despite minor hardware issues with the solenoid lock, the lockdown system proved successful against broke in burglars, accompanied by the effective buzzing of the piezo siren. Additionally, the convenience of remotely controlling the lockdown via the Blynk app was added to the overall success of the security system.

```
def blynk():
    import blynk


def main_program():
    RELAY_PIN = 18
    piezo = 23

    GPIO.setwarnings(False)
    GPIO.setmode(GPIO.BCM)

    MATRIX = [[1, 2, 3, 'A'],
              [4, 5, 6, 'B'],
              [7, 8, 9, 'C'],
              ['*', 0, '#', 'D']]

    COL = [26, 19, 13, 5]
    ROW = [21, 20, 16, 12]
```

Figure 9.1 shows that the main program of the home security system and the program of blynk app which is imported from blynk.py script are defined in two different functions in the main script.

```
main_thread = threading.Thread(target=main_program)
main_thread.start()

main_thread = threading.Thread(target=blynk)
main_thread.start()
```

Figure 9.2 The two functions defined above are being run concurrently with threading.

10.2 Limitations

Although this prototype is low cost and easy to implement, there are a wide range of limitations to it. One of them being it can only be applied to condominiums and apartments as landed houses have the risk of burglars entering the house through windows or other entries which this prototype does not cover. People can only receive notifications and control the lock down remotely if they only have internet connection, without internet connection they will not be notified if intruders are trying to invade their house. People will also have to be alert for any incoming emails from the home security system to be notified of people entering their house. Another limitation would be that it must be plugged into the socket to provide electricity for the prototype to work, if a blackout happens, the prototype will be shut down and everything will not function. Hardware limitations also persists such as solenoid lock will be too hot after turning on for more than 20 minutes; there are few suggestions to cooling down the solenoid lock, one of them being installing a cooling fan near the solenoid to enhance heat dissipation.

10.3 Future Enhancements

In the evolving landscape of home security, future advancements hold the promise of even greater protection through the integration of cutting-edge technologies. Emerging methods such as fingerprint or biometric authentication systems and remote security access control systems are poised to redefine the paradigm of safeguarding our homes. Additionally, one innovative solution on the horizon is the utilization of emulation card technology, which capitalizes on the IoT concept of convenience. This technology transforms users' ubiquitous mobile phones into emulated cards, each containing a unique tag ID utilized for scanning NFC/RFID modules. By eliminating the need for physical card tags, this approach streamlines entry processes and enhances user convenience.

Moreover, the adoption of emulation card technology represents a significant leap forward in household security. Leveraging the widespread presence of mobile phones, individuals are empowered to carry their access credentials seamlessly and remain constantly vigilant. This integration not only simplifies access procedures but also fortifies overall security measures.

Furthermore, by combining these advanced security measures with IoT principles, the potential for remote access control becomes increasingly tangible. Through interconnected systems, homeowners can wield unprecedented control over their security infrastructure, granting or denying entry privileges with unparalleled ease and efficiency. This convergence of innovative technologies heralds a future where home security is not only robust and comprehensive but also seamlessly integrated into our everyday lives, ensuring peace of mind and convenience for all.

Besides that, adding an auto trigger report of the attempt of burglary can be sent to the nearest police station or security guard of condominium with the domestic address. Offering real-time live camera footage enables users to remotely monitor their homes, ensuring their safety and security with continuous vigilance. Delivering timely and personalized notifications to users upon activation of the lockdown mechanism or identification of a new facial profile by the facial recognition system or other biometric authentication system.

Implementing cryptographic technology and network protocols can significantly bolster home security measures. Utilizing secure communication protocols, such as TLS (Transport Layer Security), ensures encrypted data exchange among devices within the home security system, effectively thwarting unauthorized access attempts. Additionally, employing wireless encryption standards like WPA3 (Wi-Fi Protected Access 3) for Wi-Fi networks enhances security by safeguarding wireless

communication channels between devices, thus preventing potential hackers from eavesdropping, or gaining unauthorized access.

The concepts or ideas mentioned above could be integrated into the current prototype in future, enhancing household security, and offering increased convenience to users through IoT-based principles which matches with the objective and title of this project.

10.4 Reflection

A few things could be done better for this prototype to increase the security level and provide more convenience for people to acknowledge the convenience of IoT-Based projects. Commencing this project earlier would have been advantageous, particularly considering that towards its conclusion, several components exhibited malfunctioning. The necessity to prioritize repurchasing hardware like more Lithium-ion batteries to provide higher power supply for the solenoid lock emerged as one of the primary obstacles hindering the project's progression. Other than that, the utilization of the GSM/GPRS module for sending geographical locations to authorities for immediate response and implementation of telecommunications would be better as it requires no internet connection. With limited time remaining and lack of knowledge onto hardware components, the GSM/GPRS module was having failures in implementing it as the SMS mode could not be established due to conflicts with the serial input when it is compiled with the main script together, but it was executed perfectly when the python script of the GSM/GPRS module was ran individually. Besides that, it was inconvenient to implement the function sending geographical locations to authorities and calling the authorities to come over, as it imposes the risk of false alerts and troublesome for them.

10.5 To Conclude

In actuality, this home security system would be affordable for people to implement it in their condominium or apartment unit and abandon the traditional home security method. This home security system is well implemented and consists of the following.

- NFC/RFID access
- Keypad access
- Motion detection
- Camera Recording and notification
- Lock Down system

This low-cost home security system based on Raspberry pi zero 2 system and with the help of other components makes security more impeccable and convenient as it provides remote access. This technology will surely lower the percentage of burglaries crime happening. The implementation of hardware requirements may not be up to mark, but it is the fundamental idea of how an all-rounded home security system should be.

In conclusion, the proposed home security system offers an affordable and comprehensive solution for safeguarding condominiums and apartments, surpassing traditional methods with its multifaceted approach. Incorporating features such as NFC/RFID access, keypad entry, motion detection, camera recording, and a lockdown system, this innovative system, anchored by Raspberry Pi Zero 2 technology, not only enhances security but also facilitates remote monitoring and control. Authorities will finally have their hands on the burglars that broke into houses with the prototype implementation as it locks them in an enclosed area and awaits justice to be served. Citizens will no longer be afraid of false alarm or home being broke in by burglars anymore as they are able to receive notifications, notifying them any intruders invading their homes and further on taking the action of locking down them to prevent them from keying in the passcode and holding them in an enclosed area.

Acknowledging the potential for refinement in hardware implementation, it's essential to recognize that the essence of a comprehensive home security system is embodied in this concept. By effectively deterring potential burglars and enabling swift apprehension through its prototype deployment, this technology holds the promise of significantly reducing burglary rates. Furthermore, by empowering citizens with real-time notifications and robust security measures, it fosters a pervasive sense of safety and confidence, thereby alleviating concerns about intrusions and false alarms. As the efficacy of this system becomes increasingly apparent and the probability of apprehending criminals rises, it stands poised to fundamentally alter societal perceptions and behaviors. The prospect of burglars witnessing their peers apprehended due to this advanced home security system is likely to erode their confidence in committing such crimes, ultimately leading to a tangible decrease in overall crime rates.

11.0 References

Anitha, A. (2017). Home security system using internet of things. *IOP Conference Series: Materials Science and Engineering*, *263*(4), 1–12. https://doi.org/10.1088/1757-899X/263/4/042026

Burglary Statistics: What You Need to Know. RubyHome. Retrieved November 18, 2023, from https://www.rubyhome.com/blog/burglarystats/#:~:text=The%20U.S.%20burglary%20rate%20is,the%20offender%20knows%20the%20victim

Chitnis, S., Deshpande, N., & Shaligram, A. (2016). An Investigative Study for Smart Home Security: Issues, Challenges and Countermeasures. *Wireless Sensor Network*, *08*(04), 61–68. https://doi.org/10.4236/wsn.2016.84006

Department of Statistics Malaysia. (n.d.). Crime statistics publication 2021. Department of Statistics Malaysia. Retrieved from https://www.dosm.gov.my/portal-main/releasecontent/crime-statistics-publication-2021

Huntaway Security Singapore. (n.d.). Retrieved December 18, 2023, from https://huntaway.com.sg/solution/burglar-alarm-system/

Hussein, N. A., & Al Mansoori, I. (2017). Smart Door System for Home Security Using Raspberry pi3. 2017 International Conference on Computer and Applications, ICCA 2017, 395–399. https://doi.org/10.1109/COMAPP.2017.8079785

JosephNg, P. S., BrandonChan, P. Sen, & Phan, K. Y. (2023). Implementation of Smart NFC Door Access System for Hotel Room. Applied System Innovation, 6(4). https://doi.org/10.3390/asi6040067

Khabarlak, K. S., & Koriashkina, L. S. (2020). Mobile Access Control System Based on Rfid Tags and Facial Information. Bulletin of National Technical University "KhPI". Series: System Analysis, Control and Information Technologies, 0(2 (4)), 69–74. https://doi.org/10.20998/2079-0023.2020.02.12

Osman, M. N., Haika, M., Ismail, F., Sedek, K. A., & Othman, N. A. (2022). A Low-Cost Home Security Notification System Using IoT and Telegram Bot : A Design and Implementation. 7(2), 327–337. https://doi.org/10.24191/jcrinn.v7i2.325

Pierce, J. (2019). Smart home security cameras and shifting lines of creepiness a design-led inquiry. Conference on Human Factors in Computing Systems - Proceedings, 1–14. https://doi.org/10.1145/3290605.3300275

Roombanker. (n.d.). Retrieved December 10, 2023, from https://www.roombanker.com/solution/intrusion-detection/

SECOM Smart Malaysia. (n.d.). Retrieved December 14, 2023, from https://www.secomsmart.com.my/offers/home-security/?gad_source=1&gclid=Cj0KCQjw_qexBhCoARIsAFgBlet0WeeKexnJ_vyJOXp6S6-Naun2dXdOBF2sXPCPnbeSbFzHXYB_3TwaAomEEALw_wcB

Taryudi, Adriano, D. B., & Ciptoning Budi, W. A. (2018). Iot-based Integrated Home Security and Monitoring System. *Journal of Physics: Conference Series*, *1140*(1), 1–8. https://doi.org/10.1088/1742-6596/1140/1/012006