# 1.0 Introduction

## 1.1 Problem Statement

The project aims to develop a smart door system featured with presence detection, entry authentication and other basic functionalities as described in Section 1.2. Additional functionalities are added to improve the user-friendliness and practicality of the system.

## 1.2 Objectives

The objective of Activity 1 is to design a system to detect the presence of objects near to a physical door. The owner should be notified of the object movement through a video sent through Telegram.

The objective of Activity 2 is to design a machine learning algorithm for human movement classification in front of the door with the highest accuracy and lowest inference time. The movement info should also be updated to Telegram regularly.

The objective of Activity 3 is to feature the system with temperature and humidity measurements capability. The measurements should be used as environment info facilitating the users to understand the presence's movements better and should be updated regularly to Telegram.

The objective of Activity 4 is to implement a physical door lock.

The objective of Activity 5 is to implement an encryption and decryption method that can provide strong security, reliability, and efficiency.

The objective of Activity 6 is to include additional features to the door system so that it is more user-friendly and practical.

# 2.0 Literature Review

Theft, robbery, and breaching incidents that result in losses and damages to private and public properties in and around our surroundings are topics we hear about in the news much too often nowadays. Although the reports of property crime have declined substantially during the recent COVID-19 pandemic [1], cases like burglary and theft still appear notorious worldwide. For instance, in Malaysia, house break-in and theft decreased only by 14.9% in 2020 to 14,040 instances, compared to 16,497 cases in 2019, whereas other reports like vehicle theft have a higher decrease rate (30.1%) [2]. As a result, there is an urgent need to boost the strength of housing security and surveillance systems in order to provide optimum security. In the past, security methods included standard door locks with locks and keys, chain locks, and safe vaults with double locks. As time passed, many of these old-school security systems became less effective, thus resulting in the development of smart locking systems namely smart doors for higher security performance. With the prevalence of Internet of Things (IoT) as a means for influencing the internet and communication technologies, many IoT-based smart door systems are constantly on the rise [3], [4], [5].

Many recent smart door systems are combined with top notch IoT technology, each with their own unique sets of applications and features. M. Shanthini et al. proposed and designed a smart door by utilizing the low power requirements of Bluetooth and Arduino UNO, which is paired to the internet to ensure data storage in the cloud [4]. With user data stored in the cloud, the smart door possesses the ability to grant access to authorised users. For security purposes, any failed breach will send a message to the owner. Similarly, S. Kavde et al. also devised a smart door that utilises Bluetooth technology and microcontrollers, in addition to a database for storing visitor information [6]. Moreover, this smart door design includes a virtual key that is generated for third party access, serving as an encryption key for extra security measures. Still, it is acknowledged that these smart door designs that involve database systems tend to have the limitation of constantly maintaining and updating said database. On the other hand, a particular smart door design opts for remote accessibility, serving as an alternative to database systems [7]. When a user presses a switch at the door, the owner will be notified about their arrival via local network, and thus the visitor's live identity is streamed on the owner's phone. Based on the owner's willingness, the owner can open the door remotely for the visitor. However, it is sometimes stated that the owner is unable to recognize the person's face due to background issues.

Several smart doors revolve its design mainly around their locking systems. One paper proposed a RFID based security system for its smart door due to its easy identification and reliability [8]. When a RFID card is swiped and identified,

the door will be unlocked depending on if the card is within the list of authorized UIDs. However, anyone will have access to the door if the RFID card is stolen. To mitigate this, some smart door designs added some extra layers of security for authentication purposes. S. A. Prity et al. proposed an additional password input after a RFID tag is read successfully [9]. If a wrong tag is scanned, then an alert will be sent to the owner's phone. Depending on the level for a secure door lock system, more security layers can be added. For instance, one smart door design was designed for the use of critical zones, in which its design utilises multi-factor authentication [10]. The user needs to verify with RFID access, followed by a one-time-password (OTP) verification. A cloud database stores data of encryption keys encoded in symmetric block encryption techniques, and the system is governed by an Android application. More complex locking systems include the need for biometric sensors such as a fingerprint-based lock framework and face recognition [11], [12]. Still, it is acknowledged that a more complex locking system will lead to lower cost efficiency, thus the level of security has to be defined.

On the other hand, some smart doors thrive on the market based on some additional features besides their locking systems. One design has utilised Quick Response (QR) technology to implement a data logging system for the purposes of tracking ingoing and outgoing activities, such as classroom attendance [13]. Furthermore, another design proposed the survivability of the system during a power outage, in which the lock contains a USB connection that can be connected with a power bank to activate the lock system when the main power supply fails [14]. Lastly, one design utilised different sensors for the detection of various emergency events, namely temperature, gas leakage, burglary, fire and other environmental conditions, which are all frequently recorded to monitor the activity on the spot [15]. Actions will be taken corresponding to each emergency event, such as releasing water if fire is detected.

Thus, the proposal of a novel smart door system is discussed in this report. Some of the above-mentioned elements are combined in this system to yield an efficient smart door system with optimum security and various functionality.

# 3.0 Methodology

## 3.1 Activities 1 and 4: IoT Sensor, Network, and Door Lock System

The distance between the system and object is measured using a HC-SR04 Ultrasonic Sensor (U/S) continuously with a time interval of 0.2s to improve the responsiveness of the system. Once the distance between the nearest object and the U/S is detected to be smaller than 30cm, a 5-second video is recorded using PiCamera and sent to Telegram to notify the owner about the presence of the object. Concurrently, a panel is launched. There are 4 options on the panel. The first option is to gain access to the door through an activated radio-frequency identification (RFID) card; the second option is to activate an RFID card for new bla accounts (this feature will be further explained in Section 3.4.1); the third option is to ring a doorbell, which is demonstrated by the lighting up of a red light-emitting diode (LED), and the last option is to gain access to the door through a username and a 6-digit one-time password (OTP). If the RFID has been activated and is in the database, or if the username is in the database and the OTP is correct, access to the smart door is granted. Furthermore, to reduce the power consumption of the user panel, the panel will automatically turn off after a 90-second idle time.

The door lock system uses a normally actuated solenoid door lock, where the solenoid is normally in the extended position. If access to the smart door is granted, the solenoid retracts, and the door unlocks. After 3 seconds, the solenoid automatically extends, and the door relocks automatically.

## 3.2 Activities 2 and 3: Machine Learning System and Temperature and Humidity

### 3.2.1 Activity 2

Similar to Activity 1, the distance between the system and object is measured using a HC-SR04 Ultrasonic Sensor (U/S). There are **6 classes of movement data to be collected**: near stationary (<50cm), far stationary (50 to 100cm), no object (>100cm), forward / come from the side, backward / leave to the side, and pass by. The first 3 classes are static while the last 3 classes are dynamic. As the international building code determines that the minimum corridor width is 111.8cm [16], 100cm is used as the boundary to distinguish between far stationary object and no object to ensure the corridor wall in front of a door would not be considered as a far stationary object. This activity has 3 main coding procedures: **data collection**, **model training**, and **real-time movement classification and Telegram update**.

#### 3.2.1.1 Data Collection

To ensure the dataset is large enough to represent the general pattern of data distribution for each class, 100 samples of data are collected for each class, total **600 samples**. Each sample has 30 distance instances collected at a period of around 0.25s so each sample represents a movement roughly within a 7.25s timeframe.

#### 3.2.1.2 Model Training

To exploit the static and dynamic distinguishment between the classes, a **divide and conquer-based two-stage multilevel perceptron (DnC_MLP)** [17] as shown in Fig. 2 (classify movement (DnC_MLP)) and Table I is used. The first stage is a MLP for binary classification (MLP2) between static and dynamic classes. If a movement is predicted as static, it will then be classified as one of the 3 static classes by thresholding its average distance (th_sta). If a movement is predicted as dynamic, it will then be classified to one of the 3 dynamic classes using a 3-class MLP (MLP_dyn). In short, the DnC_MLP model is built with a binary MLP (MLP2), a 3-class MLP (MLP_dyn), and a simple thresholding algorithm (th_sta). The trained models are saved and will be used for real-time classification.

#### 3.2.1.3 Real-time Movement Classification and Telegram Update

The trained models are loaded and used for **real-time classification** with same time interval as the data collection. For **regular Telegram updates**, the movement info is updated every 8 hours. There is an additional feature of **abnormal event detection** which is positive if there is object detected more than 5/6 of the past 15 minutes in front of the door. Telegram message showing movement info of the last 15 minutes will be sent immediately upon abnormal event detected.

Table I
Configurations of MLP2 and MLP_dyn.

| | # hidden layers | # neurons per layer | Activations | Optimizer | L2 regularization factor | Initial learning rate |
|---|---|---|---|---|---|---|
| MLP2 | 6 | 200 | ReLU | Adam | 0.0001 | 0.0001 |
| MLP_dyn | 9 | 100 | | | 0.003 | |
| Note: [ represents the number of. ReLU is rectified linear unit. Adam optimizer speeds up training [18]. L2 regularization reduces overfitting [19]. | | | | | | |

### 3.2.2 Activity 3

The **temperature** and **humidity** are measured using a DHT22 Digital Temperature & Humidity Sensor Module (DHT22). This two info are then used to compute the **dew point** based on which an **environment status comment** is given. In addition, the temperature and humidity measurements are used for **weather** determination. Only these two features are insufficient to determine the weather using conventional methods [20]. Therefore, a supervised machine learning model is used.

Due to time and environment constraints, an online weather dataset of Israeli, an Asian country, is used for model training. There are 3 classes of weather: sky is clear, clouds, and rain. The dataset has 36000 weather data equally distributed across the 3 classes. After performance comparison between different supervised models, a Classification and Regression Trees (CARTS) model with entropy as split quality criterion is trained and saved for real-time weather determination. All five environment info are updated to Telegram along with movement info from Activity 2 for regular updates and abnormal event detection.

## 3.3 Activity 5: Security – Encryption and Decryption

Advanced Encryption Standard (AES) is used as the encryption and decryption method due to its strong security, mathematical soundness, resilience to all known attacks, fast encryption speed, and compatibility with a wide range of hardware and software. The general structure of AES is shown in Fig. 3 (right). The method starts with an Add round key stage, then 9 rounds of four stages, and finally a tenth round of three stages. These are the four stages:

i. Substitute bytes: Using an S-box which is a table that uses a 16*16 matrix of byte values (as shown in Appendix A), each byte in the state array is substituted. The matrix is made up of all conceivable permutations of an 8-bit sequence (256), and each byte in the matrix is mapped to a new byte. This information is then utilised to update the state matrix.

ii. Shift rows: Shift rows is basically a simple rearrangement, namely the first row of state remains unchanged, the second row is circularly moved 1 byte to the left, the both the third and fourth row are circularly moved 2 bytes to the left.
iii. Mix columns: Essentially a substitution, this stage uses GF arithmetic (28), in which a separate operation is performed on each column. Each byte in a column is translated into a new value that is a function of each of the column's four bytes. The subsequent matrix multiplication on state will reveal the transition. The sum of each row and column's individual elements makes up the product matrix's individual elements.
iv. Add round key: Using Rijndael's key scheduling, a subkey is created from the main key for each round. Overall, the 128 bits of state and the 128 bits of the round key are bitwise XORed in this stage. The interaction between the four bytes of the state column and the single word of the round key is considered as a column wise operation.

The 'Mix columns' stage is simply skipped in the tenth round.

A block cipher like AES is only suited for the safe cryptographic transformation (encryption or decryption) of a single fixed-length group of bits known as a block. Thus, a mode of operation is needed to specify how to securely transform quantities of data greater than a block by repeatedly applying a cipher's single-block operation. Here, two modes of operation are implemented: electronic codebook (ECB) and cipher block chaining (CBC). ECB is the rawest mode of operation, in which the message is segmented into blocks, and each block is encrypted and decrypted independently. This introduces a lack of diffusion; thus, data patterns are not hidden well. Hence, ECB is suitable for encrypting small messages. On the other hand, in CBC mode, each plaintext block is XORed with the previous ciphertext block before encryption. Each ciphertext block is thus dependent on all plaintext blocks, eliminating the lack of diffusion issue. An initialization vector must be used in the first block to make each message unique. This makes CBC suitable for encrypting large messages. The flowchart operations for ECB and CBC are shown in Fig. 3 (left).

In the smart door system, encryption is performed on the OTP message and the database to ensure the security of data transmission, reception, and storage in the smart door system.

## 3.4 Activity 6: Additional features

### 3.4.1 Database management and door access system

There are 3 types of accounts in the database, which are admin, user, and visitor accounts. First, **admin** account owners have the highest level of access. This includes access to the database management system through username and password with OTP authentication. Admin account owners also have access to the smart door through both RFID card and username with OTP authentication. Second, **user** account owners have moderate level of access. They have unlimited access to the smart door through username with OTP authentication. Third, **visitor** account owners have the lowest level of access to the smart door system. They are only granted access to the smart door for a specified duration only. Outside that time range, their accounts will be frozen, and they cannot access the smart door. Visitor accounts are mainly for one-time visitors who would like to visit the protected premise, or occasionally authorized personnel such as cleaners or babysitters who should have access to the protected premise for fixed time intervals only. Only admin account holders can specify the time range for visitor access.

In the database management system, after inputting the correct username and password, and successfully performing OTP authentication, **admin** account holders can perform the following functionalities. **First**, admins can view all existing accounts in the database. **Second**, admins can add new accounts to the smart door lock system. The accounts can be either admin, user, or visitor accounts. For new admin accounts, the corresponding RFID card needs to be activated at the door RFID card reader before the RFID card can be used to unlock the smart door. **Third**, admins can unfreeze (or enable) accounts. For visitors, a time range when the account is enabled need to be specified, while for admins and users, the time range is not specified. This feature is crucial to ensure that any account which has been unintentionally disabled can be enabled back so that the person can access the door successfully. **Lastly**, admins can freeze (or disable) accounts. This feature replaces the remove account feature so that all accounts that have been created can be stored forever for record purposes. Removing account is also not feasible as the admin or owner of the smart door may not be able to gain access to the door forever if hackers gain unauthorized access to the database and remove the account forever. Therefore, the account disabling feature is introduced so that admins can forcefully disable accounts that are inactive and will not be in use anymore.

### 3.4.2 Account Disabling for Security

Besides admins forcefully disabling accounts that will be inactive, account disabling is automatically reinforced if the password or OTP has been input wrongly for 15 consecutive times. This feature is added to make brute force attack not possible for the database management and smart door access system. If an account has been disabled, only admin account holders can enable the account to restore the account back to its active state (if the admin account has not been disabled). A Telegram notification message is also sent to the owner to notify the disabling of the account.

### 3.4.3 Panel Freezing

If a wrong password or wrong OTP has been entered several consecutive times, the screen or panel freezes before the person can attempt a new password or OTP. Table *II* below shows the screen or panel freezing time for several wrong password or wrong OTP entries.

Table II
Panel Freezing Time for Wrong Password or OTP

| **Wrong number of password entries (consecutive)** | **Panel freezing time (mins)** | **Wrong number of OTP entries (consecutive)** | **Panel freezing time (mins)** |
|---|---|---|---|
| More than 5 times | 1 | More than 5 times | 3 [21] |
| More than 9 times | 3 | More than 10 times | 3 [21] |
| More than 12 times | 10 | 15 times | 3 + account disabled |
| More than 14 times | 30 | | |
| 15 times | 30 + account disabled | | |

### 3.4.4 Resend OTP

To prevent network latency issues from impacting the process of sending and receiving OTPs, a request to send a new OTP can be made. This feature is implemented at both the door opening panel and the database management admin login page.

### 3.4.5 Strong Password Checker

For admin accounts, a strong password needs to be created upon new account creation. The password strength is checked for the following criteria [22]:

- The password needs to be between 6 to 20 characters.
- The password needs to have at least one uppercase letter, one lowercase letter, one number and one special character.
- The password cannot have 3 consecutive repeating characters (e.g., '…@@@…') .

### 3.4.6 System Integration

In this smart door system, 3 Raspberry Pi (raspi) microcontrollers are used to increase the responsiveness of the system at a tradeoff of increased installation cost. The first (main) raspi is used to track the proximity of the nearest object, launch the panel to access the smart door, and perform database management. This raspi is used to execute the main functionalities and act as an access point to send messages to the edge devices (second and third raspi) for communication purposes. The second raspi is used to record a 5-second video upon object detection within 30cm proximity from the U/S installed on the first raspi. The use of this second raspi is important to reduce the polling latency of the smart door system so that the smart door can be accessed without needing to wait until the end of video recording. The third raspi is used for movement, temperature, and humidity tracking for Activity 2 and 3. After performing system integration with the 3 raspi units, the whole smart door system can be controlled using the main raspi and communication between raspi. Communication between raspi is established using the MQ Telemetry Transport (MQTT) protocol. Relevant python scripts are executed when a message is received at the respective edge devices.

## 3.5 Flowcharts

### 3.5.1 Activities 1 and 4: IoT Sensor, Network, and Door Lock System

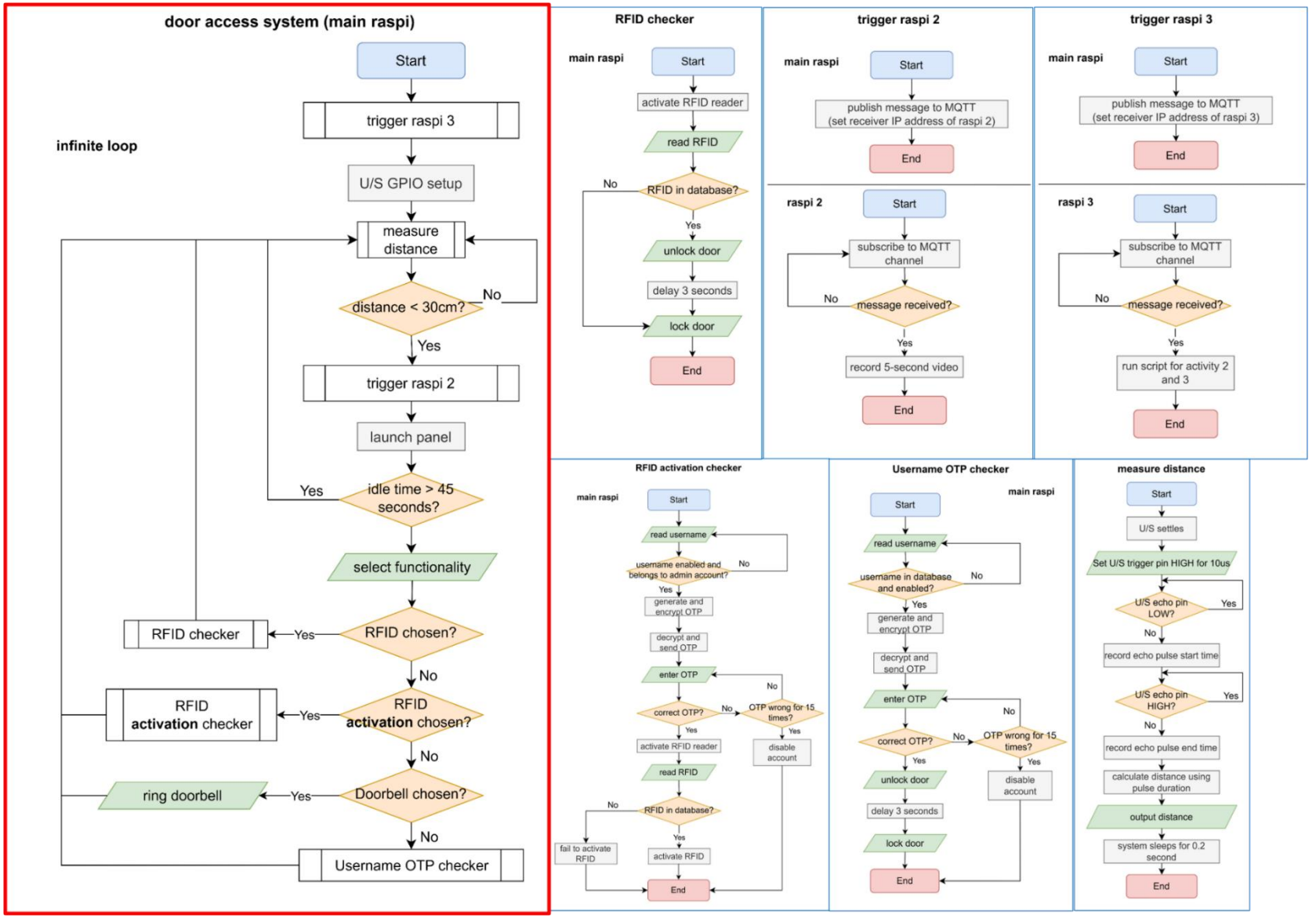


Fig. 1. Main flowchart (left in red frame) and subprocess flowcharts (right in blue frames) for Activities 1 and 4.

### 3.5.2 Activities 2 and 3: Machine Learning System and Temperature and Humidity

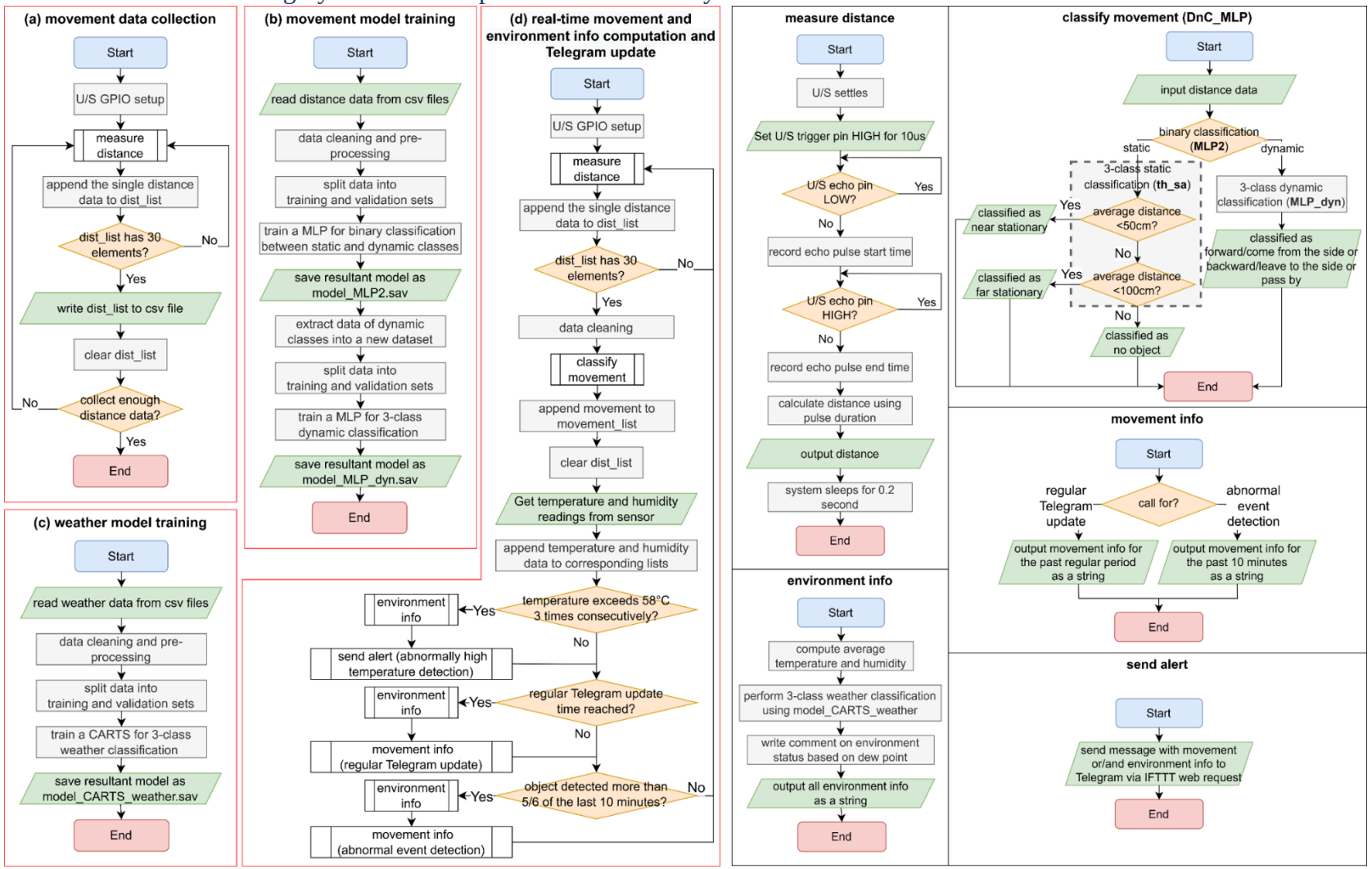


Fig. 2. Left in red frames: the 4 main Python files for Activities 2 and 3. Preliminary work: (a), (b), and (c). System execution file: (d). Right in black frames: Subprocesses or functions associated.

### 3.5.3 Activity 5: Security – Encryption and Decryption

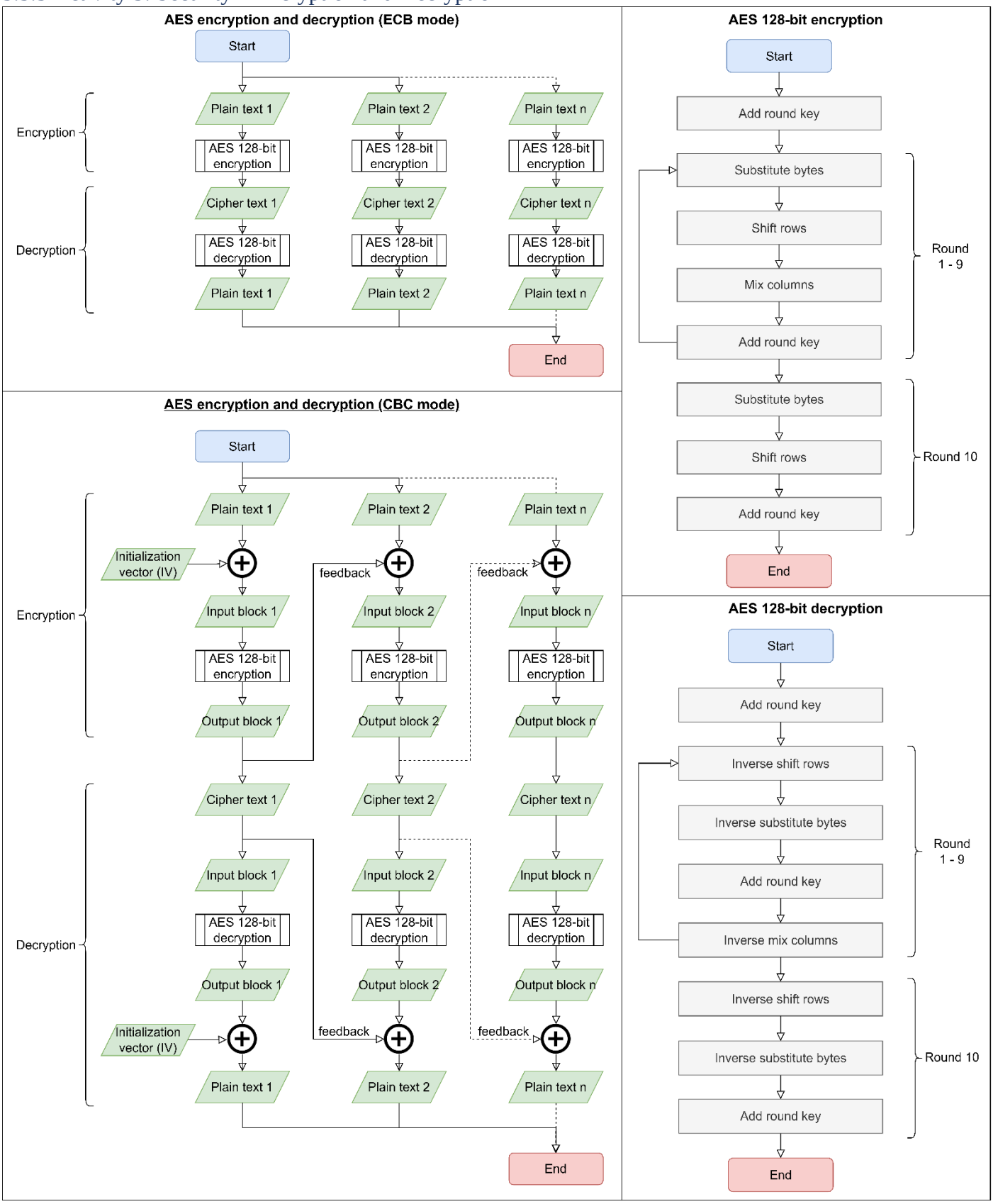


Fig. *3*. Main processes (left) and subprocesses (right) for Activity 5.

### 3.5.4 Activity 6: Additional Features

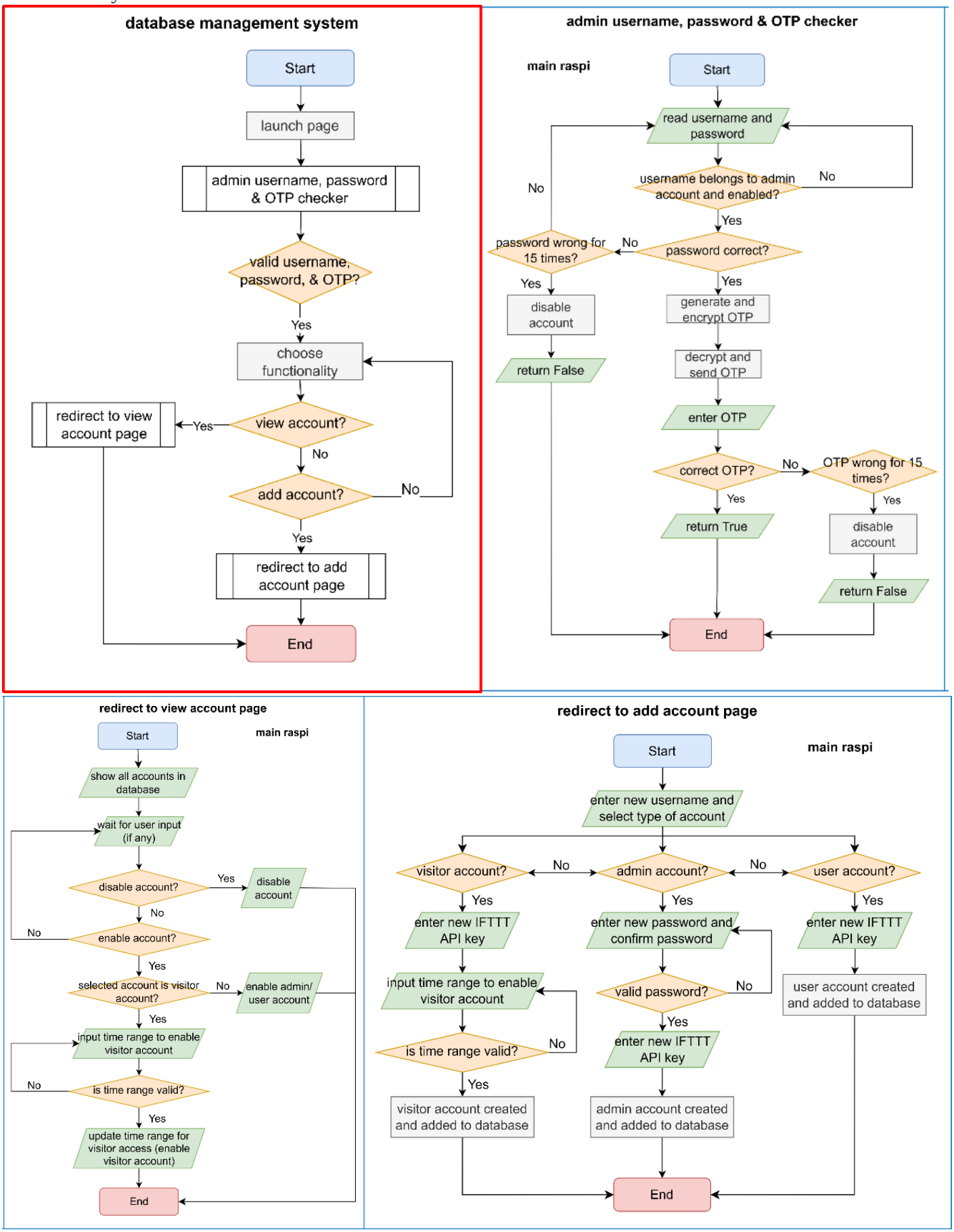


Fig. 4. Main flowchart (top left in red frame) and subprocess flowcharts (in blue frame) for Activity 6.

# 4.0 Results and Analysis

## 4.1 Activities 1, 4 and 5

The lab demonstration showed the successful implementation of this activity. As illustrated in the lab demonstration, once the presence of an object is detected by the U/S, a 5-second video is recorded by the PiCamera and sent to Telegram successfully. At the same time, the user panel is launched for the person to choose a mode to gain access to the door. As shown in Fig. 6, there are several functionalities that can be chosen by the user. Fig. 6 shows a successful door unlocking using username and OTP, which is the basic functionality of the smart door. Fig. 8 shows a successful door unlocking using RFID, an improved functionality of the smart door. The unlocking and locking motion of the solenoid lock has been demonstrated during the lab session. When attempting to gain access to the smart door system, the OTP was encrypted before sending to the person trying to gain access to the smart door system. The encryption process and the decrypted OTP in Telegram is shown in Fig. 7. Besides encrypting OTP, the database is also encrypted, and the encrypted database is shown in Fig. *18*, Appendix A.

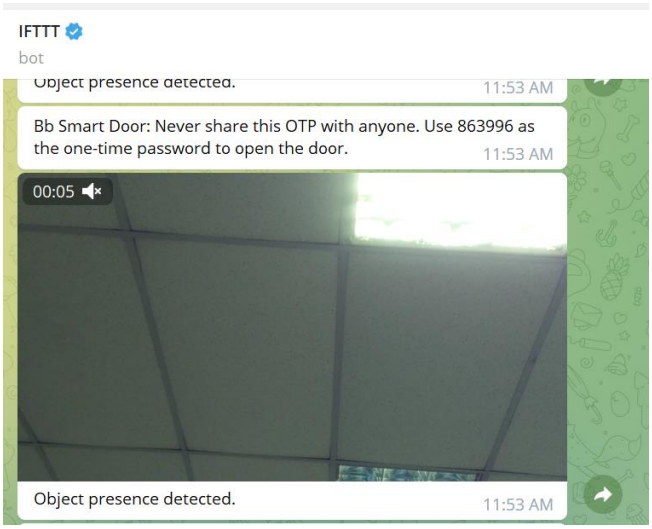


Fig. 5. Telegram receives an OTP for door unlocking upon correct username entered and a 5-second video recorded upon presence detected.


Fig. 6. A successful door unlocking using username and OTP.


Fig. 7. Demonstration of OTP encryption in user interface and OTP decryption in Telegram.


Fig. 8. A successful door unlocking using RFID.

## 4.2 Activities 2 and 3: Machine Learning System and Temperature and Humidity

### 4.2.1 Model Performance

The accuracies of the models are shown in Table III. The movement model DnC_MLP has a very high validation accuracy of 0.9591 showing its high capability of predicting the movement accurately. On the other hand, the weather model CARTS has a low validation accuracy of 0.5769 as there are only 2 features (temperature and weather) which are insufficient for weather determination. The accuracy can be improved by using additional different sensors to collect additional info such as air pressure, wind speed, and precipitation [22].

Table III
Model Accuracies.

| Accuracy | Movement | | | | Weather |
|---|---|---|---|---|---|
| | MLP2 | th_sta | MLP_dyn | DnC_MLP | CARTS |
| Validation | 0.9714 | 0.9954 | 0.9792 | 0.9591 | 0.5769 |
| Training | 0.9936 | - | 0.9859 | 0.9796 | 0.9474 |

### 4.2.2 Telegram Message

For demonstration purposes, the periods of both the abnormal event detection and the regular Telegram update are set as 2 minutes. The resultant Telegram messages are shown in Fig. *9*.

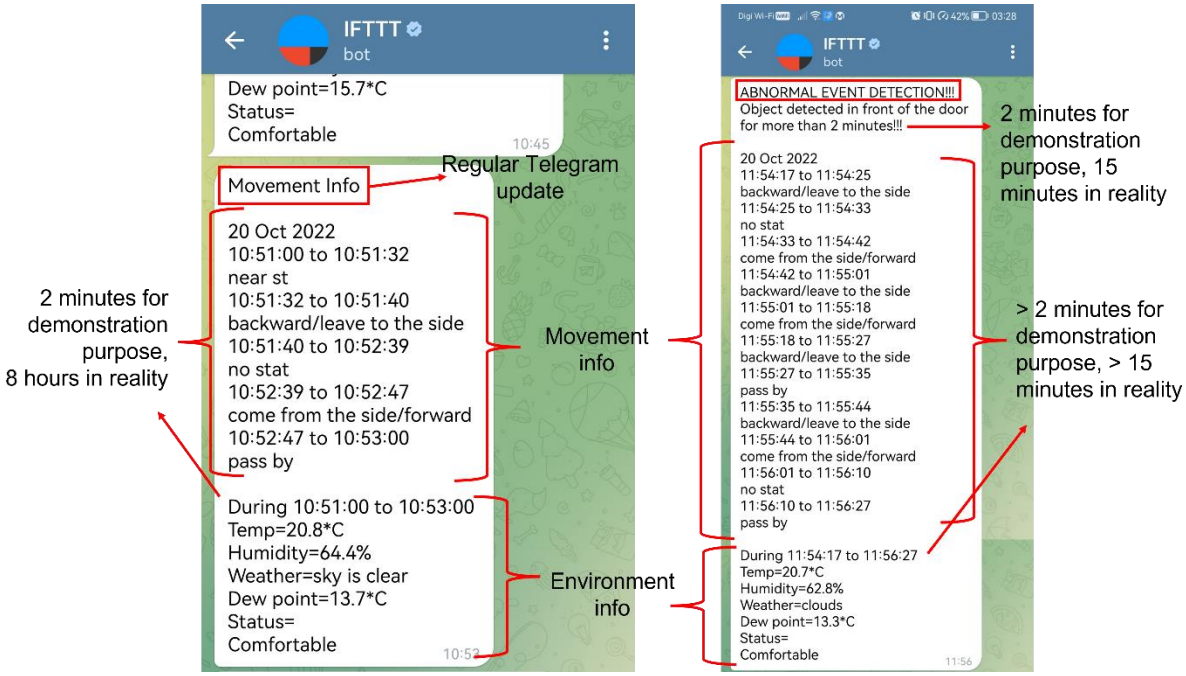


Fig. 9. Movement and environment info for regular Telegram update (left) and abnormal event detection (right).

Both events have movement info, i.e., movement with time, and environment info, i.e., 1) temperature, 2) humidity, 3) weather, 4) dew point, and 5) environment status comment in the message. The only difference is the normal movement info spans 8 hours while the abnormal event detection info spans the period of more than 15 minutes (first detection of object right before 15 minutes ago until current time).

## 4.3 Activity 6: Additional Features

### 4.3.1 Database management and door access system

The user interface for the database management system is shown in Fig. 10. The successful entering of an admin username, password, and OTP allows the admin account owner to access the database management system. Fig. 11 shows the user interface for successful account additions for different types of accounts (admin, user, and visitor). For visitor accounts, the time range at which the account is enabled (unlocked) must be a future time. Moving on, Fig. 12 shows the user interface to view all available accounts in the database. Every time the "View Accounts" option is clicked, the system refreshes and the latest account status (enabled/unlocked or disabled/locked) will be displayed as shown in Fig. 12. Once the time is within the specified time range to allow visitor access, the visitor account is automatically enabled/unlocked.

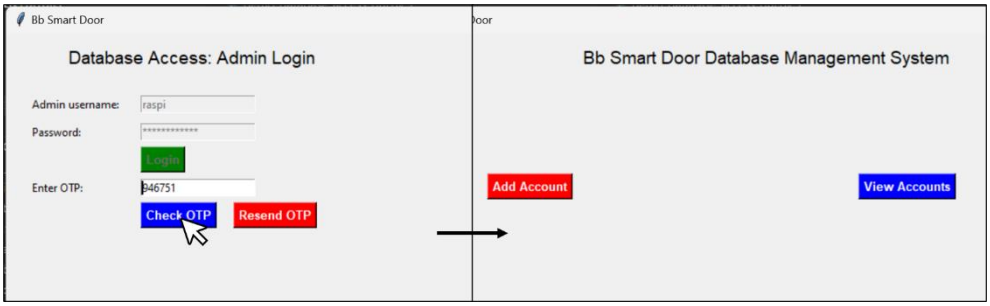


Fig. 10. User interface for database management system.

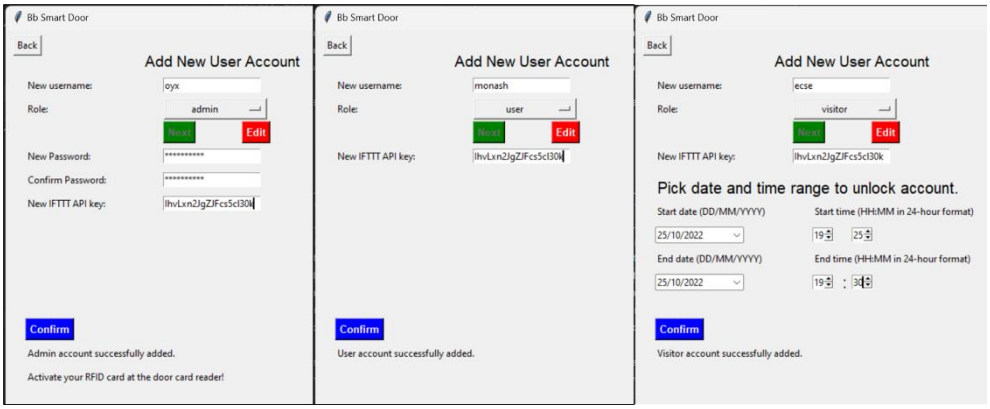


Fig. 11. User interface for successful account additions for admin, user, and visitor respectively (left to right).

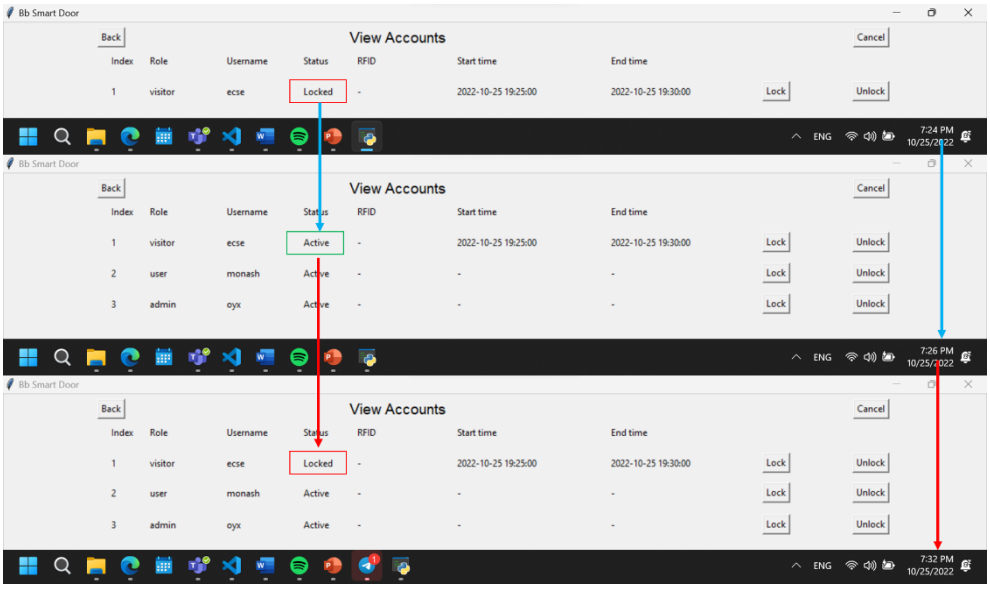


Fig. 12. Viewing account user interface. Visitor account status is refreshed depending on the current time and specified time range.

For new admin accounts, the corresponding RFID card needs to be activated at the door card reader. The activation process is shown in Fig. 13.

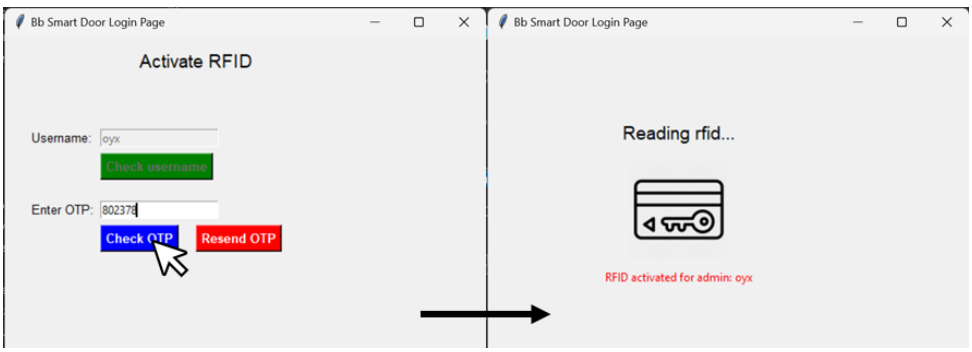


Fig. 13. Activating RFID user interface.

### 4.3.2 Account Disabling for Security

If the password or OTP entry is wrong for 15 consecutive times, the account will be disabled until permission is granted again by an admin account holder. The results are shown in Fig. 14. A notification is also sent to the owner to notify that the account is locked, as shown in Fig. 15.

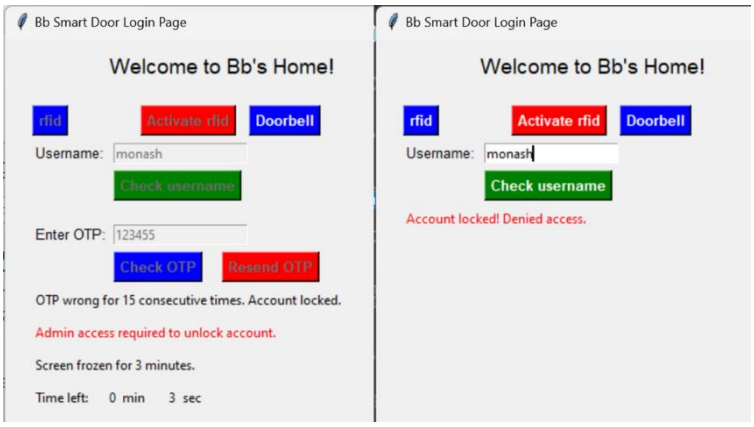


Fig. 14. Account disabled/locked due to security reasons.

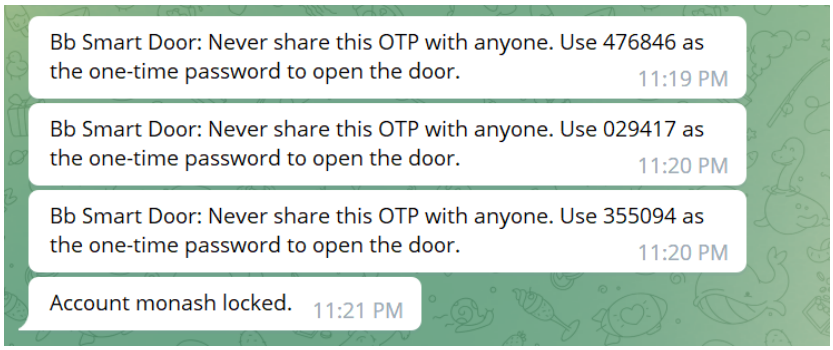


Fig. 15. Telegram notification to owner that account is locked.

### 4.3.3 Panel Freezing

For consecutive wrong attempts, the panel is frozen before a new password or OTP attempt can be made. An example of panel freezing for consecutive wrong OTP attempts is shown in Fig. 16.

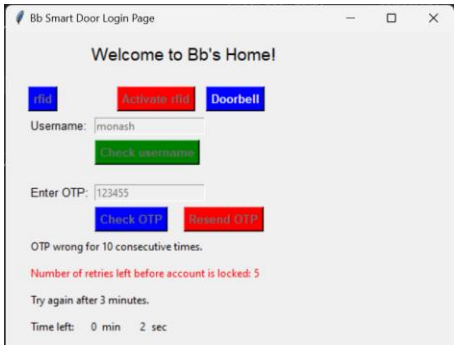


Fig. 16. user interface freezing due to consecutive wrong OTPs.

### 4.3.4 Resend OTP

Buttons to request for a new OTP to be resent have been successfully implemented as shown in Fig. 18. Once clicked, a new OTP will be generated and sent to Telegram, as shown in Fig. 19, Appendix A.

### 4.3.5 Strong Password Checker

The implementation of a strong password checker has been achieved. If the new password set does not meet the password strength requirements, an error message will be displayed, as shown in Fig. 20, Appendix A.

### 4.3.6 System Integration

The demonstration of overall system integration has been performed during the lab session. The system can be switched on by pressing only 1 button.

# 5.0 Feasibility Evaluation with Cost Benefit Analysis

Old-school security systems have become less effective, thus smart doors are necessary to automate the entering and exiting process, in addition with higher security measures. The scope of smart door designs is within IoT systems, in which various designs come with their own advantages like accessibility and pricing. Assumptions made towards the feasibility evaluation are as follows.

- Estimated an average of 30 seconds to enter the designed smart door
- The raspberry pi will remain idle when no one is using the smart door
- Costs are calculated for 1 year and 5 years
- Assumed that smart door will require an average of 1 maintenance per year

Alternative courses of actions (COAs) are defined as follows. It is noted that all COAs will have the implementation of Activities 1-5, thus the COAs will only showcase their main additional features.

1) System A has a database management and door access system, which include RFID cards and OTP authentication. Hierarchies are defined for different levels of access. This promotes flexible accessibility with moderate computation time and moderate usage of IoT devices.
2) System B has a facial recognition feature, thus a more secure system due to biometric authentication but requires high computation time and moderate usage of IoT devices.
3) System C has a fingerprint sensor feature, thus a more secure system due to biometric authentication but requires moderate computation time and high usage of IoT devices.

The cost estimate for each COA is shown in Table IV. Details of the calculations of cost and benefit for each COA can be referred in Appendix B for 1 year and Appendix C for 5 years. The quantifiable and non-quantifiable benefits of each COA are shown in

Table *V*.

Table IV
Cost Estimate for Each COA

| | | 1 year (RM) | 5 years (RM) |
|---|---|---|---|
| COA 1: System A | Cost (RM) | 3,127.50 | 3,541.90 |
| | Benefit (RM) | 5,200.00 | 26,000.00 |
| | **Total Net Return (RM)** | **2,072.50** | **22,458.10** |
| COA 2: System B | Cost (RM) | 3,127.50 | 3,541.90 |
| | Benefit (RM) | 5,200.00 | 26,000.00 |
| | **Total Net Return (RM)** | **2,072.50** | **22,458.10** |
| COA 3: System C | Cost (RM) | 3,277.50 | 3,691.90 |
| | Benefit (RM) | 5,200.00 | 26,000.00 |
| | **Total Net Return (RM)** | **1,922.50** | **22,308.10** |

Table V
Quantifiable and Non-Quantifiable Benefits of Each COA

| **Course of Action, COA** | COA 1: System A | COA 2: System B | COA 3: System C |
|---|---|---|---|
| **Quantifiable (Total Net Return)**<br>1 year<br>5 years | <br>RM 2,072.50<br>RM 22,458.10 | <br>RM 2,072.50<br>RM 22,458.10 | <br>RM 1,922.50<br>RM 22,308.10 |
| **Non-quantifiable** | • Flexible accessibility<br>• Moderate computation time<br>• Moderate usage of IoT devices | • More secure<br>• High computation time<br>• Moderate usage of IoT devices | • More secure<br>• Moderate computation time<br>• High usage of IoT devices |

Among the three COAs that were proposed, System A is chosen as it is the most feasible among the alternative choices in designing the features for the smart door. In terms of quantifiable costs, System A has the highest total net return rate. Still, it is acknowledged that all the systems will use similar hardware and thus quantifiable costs will be roughly similar. However, System A still wins in terms of non-quantifiable costs, as it can yield a more efficient system by having a moderate computation time and moderate usage of IoT devices. Although, System B and C offer a more secure authentication system, the security of System A is strong regardless due to the use of RFID cards and OTP authentication, paired with strong AES encryption from Activity 5. In addition, the functionality of database management and hierarchical users in System A results in the accessibility of the smart door to be more flexible and user-friendly to consumers.

# 6.0 Conclusion, Future Work and References

## 6.1 Conclusion

The smart door system is deemed complete by realizing the following improved basic features: 1) entry authentication using OTP and RFID, 2) presence detection which notifies users via Telegram video, 3) movement classification and abnormal event detection realized by machine learning, 4) provision of multiple environment info, 5) encryption of database and OTP, and 6) actual locking and unlocking demonstrated using a solenoid. The system is further equipped with additional features to improve user-friendliness and practicality: 1) database management and door access system which supports the backend of the system and opens different level of system control and access to different roles, 2) improved security realized via account disabling, panel freezing, OTP resend, and strong password checker, and 3) system integration, i.e., the system can be switched on by merely clicking one button.

## 6.2 Future Work

The system largely makes use of polling to integrate all functionalities. Polling has an advantage of relatively simpler coding and a disadvantage of relatively high latency. While most functionalities are done in a real-time manner, the latency aggravated by polling is reduced by using 3 Raspberry Pi's which incurs higher cost and energy consumption. Therefore, the system can have the cost and energy cut by using interrupt instead of polling that allows the number of Raspberry Pi to be reduced. Besides, two U/S are used for Activities 1 and 2 separately. By integrating the code of the two activities, the number of U/S can be reduced to one to reduce cost and energy consumption. A personal computer (PC) software and a phone application (app) can be developed to implement the database management and door access control system, which is demonstrated by GUIs in this project, to improve product readiness for sales. A fingerprint sensor can be included to enable authentication via fingerprint which is one of the popular features in today's smart doors. Powering the system using batteries instead of line power should be introduced since consumers may prefer either method for powering.

## 6.3 References


[1] United Nations Office on Drugs and Crime. "Crime and Homicide During COVID-19 Lockdown Is Only Short-Lived." https://www.unodc.org/unodc/en/frontpage/2020/December/unodc-research-reveals-drop-in-reported-property-crime-and-homicide-during-covid-19-lockdown-is-only-short-lived.html (accessed Oct. 20, 2022).

[2] Department of Statistics Malaysia. (2021). Crime Statistics Publication 2021. [Online] Available: https://www.dosm.gov.my/v1/index.php?r=column/cthemeByCat&cat=455&bul_id=eHE0eGZWSmNROG1BbHR2TzFvZzZxQT09&menu_id=U3VPMldoYUxzVzFaYmNkWXZteGduZz09

[3] S. Shetty, S. Shetty, V. Vishwakarma, and S. Patil, "Review Paper on Door Lock Security Systems," in 2020 International Conference on Convergence to Digital World - Quo Vadis (ICCDW), 18-20 Feb. 2020 2020, pp. 1-4, doi: 10.1109/ICCDW45521.2020.9318636.

[4] M. Shanthini, G. Vidya, and R. Arun, "IoT Enhanced Smart Door Locking System," in 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), 20-22 Aug. 2020 2020, pp. 92-96, doi: 10.1109/ICSSIT48917.2020.9214288.

[5] M. Pavelić, Z. Lončarić, M. Vuković, and M. Kušek, "Internet of Things Cyber Security: Smart Door Lock System," in 2018 International Conference on Smart Systems and Technologies (SST), 10-12 Oct. 2018 2018, pp. 227-232, doi: 10.1109/SST.2018.8564647.

[6] S. Kavde, R. Kavde, S. Bodare, and G. Bhagat, "Smart digital door lock system using Bluetooth technology," in 2017 International Conference on Information Communication and Embedded Systems (ICICES), 23-24 Feb. 2017 2017, pp. 1-4, doi: 10.1109/ICICES.2017.8070788.

[7] S. R. Pinjala and S. Gupta, "Remotely Accessible Smart Lock Security System with Essential Features," in 2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), 21-23 March 2019 2019, pp. 44-47, doi: 10.1109/WiSPNET45539.2019.9032715.

[8] M. S. Z. M. Zabidi et al., "IoT RFID Lock Door Security System," J. Phys.: Conf. Ser, vol. 2312, no. 1, p. 012092, 2022, doi: 10.1088/1742-6596/2312/1/012092.

[9] S. A. Prity, J. Afrose, and M. M. Hasan, "RFID Based Smart Door Lock Security System," American Journal of Sciences and Engineering Research E-ISSN-2348-703X, vol. 4, no. 3, 2021.

[10] M. Mathew and R. S. Divya, "Super secure door lock system for critical zones," in 2017 International Conference on Networks & Advances in Computational Technologies (NetACT), 20-22 July 2017 2017, pp. 242-245, doi: 10.1109/NETACT.2017.8076773.

[11] K. A. Patil, N. Vittalkar, P. Hiremath, and M. A. Murthy, "Smart door locking system using IoT," International Research Journal on EngTechnol (IRJET), pp. 3090-3094, 2020.

[12] R. B. C, S. Joy, A. S. Bale, A. S. Naidu, N. V, and S. N. V, "Advanced Computing in IoT for Door Lock Automation," in 2022 International Conference on Electronics and Renewable Systems (ICEARS), 16-18 March 2022 2022, pp. 565-569, doi: 10.1109/ICEARS53579.2022.9752140.

[13] A. F. M. Fauzi, N. N. Mohamed, H. Hashim, and M. A. Saleh, "Development of Web-Based Smart Security Door Using QR Code System," in 2020 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS), 20-20 June 2020, pp. 13-17, doi: 10.1109/I2CACIS49202.2020.9140200.

[14] Y. C. Yu, "A practical digital door lock for smart home," in 2018 IEEE International Conference on Consumer Electronics (ICCE), 12-14 Jan. 2018 2018, pp. 1-2, doi: 10.1109/ICCE.2018.8326305.

[15] Y. T. Park, P. Sthapit, and J. Y. Pyun, "Smart digital door lock for the home automation," in TENCON 2009 - 2009 IEEE Region 10 Conference, 23-26 Jan. 2009 2009, pp. 1-6, doi: 10.1109/TENCON.2009.5396038.

[16] International Code Council, International Building Code 2018, ser. International Building Code. International Code Council, Incorporated, 2017. [Online]. Available: https://books.google.com.my/books?id=IxS8zQEACAAJ

[17] H. Cho and S. M. Yoon, "Divide and conquer-based 1D CNN human activity recognition using test data sharpening," Sensors, vol. 18, no. 4, 2018. [Online]. Available: https://www.mdpi.com/1424-8220/18/4/1055

[18] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," arXiv preprint arXiv:1412.6980, 2014.

[19] A. Y. Ng, "Feature selection, L1 vs. L2 regularization, and rotational invariance," in Proceedings of the Twenty-First International Conference on Machine Learning, ser. ICML '04. New York, NY, USA: Association for Computing Machinery, 2004, p. 78. [Online]. Available: https://doi.org/10.1145/1015330.1015435

[20] National Geographic. "Weather." education.nationalgeographic.org. Accessed: Oct. 25, 2022. [Online]. Available: https://education.nationalgeographic.org/resource/weather

[21] Samsung SDS. SHS-G517 User Manual. (2018). Accessed: Oct. 25, 2022. [Online]. Available: https://www.samsungdigitallife.com/wp-content/uploads/samsungddldata/manual/DDL/SHS-G517_Manual.pdf

[22] Tutorials Point. “Strong Password Checker in Python.” Tutorialspoint.com. https://www.tutorialspoint.com/strong-password-checker-in-python (accessed Oct. 25, 2022).

[23] "Unit: ECE4810 Toolbox Loan Form 2022 - Form 1 - Main Toolbox." https://docs.google.com/forms/d/e/1FAIpQLScM9ZKCXLBhz8f1wIWLSX_n5QWtrmUyqiWkmnTmVpkh8LqIvg/viewform (accessed Oct. 20, 2022).

[24] Cytron. "Raspberry Pi 8MP Camera Module V2.1." https://my.cytron.io/p-raspberry-pi-8mp-camera-module-v2?r=1&gclid=CjwKCAjwwL6aBhBlEiwADycBIFlQuWrFtkPAgdFUfUGt26cVqpKLKJffzGAywuh7Lus_vVWhYt0bHBoCH3UQAvD_BwE (accessed Oct. 20, 2022).

[25] I. Kaur, G. S. Narula, R. Wason, V. Jain, and A. Baliyan, "Neuro fuzzy—COCOMO II model for software cost estimation," International Journal of Information Technology, vol. 10, no. 2, pp. 181-187, 2018, doi: 10.1007/s41870-018-0083-6.

[26] B. W. Boehm, Software cost estimation with Cocomo II. Upper Saddle River, NJ: Upper Saddle River, NJ : Prentice Hall, 2000.

[27] PayScale. "Average Software Programmer Salary in Malaysia." https://www.payscale.com/research/MY/Job=Software_Programmer/Salary (accessed Oct. 20, 2022).

[28] B. Mehl. "Access Control Systems Cost: Installation and Price per Door." https://www.getkisi.com/blog/breakdown-of-access-control-system-installation-costs (accessed Oct. 20, 2022).

[29] A. Bate. "Thermal testing Raspberry Pi 4." https://www.raspberrypi.com/news/thermal-testing-raspberry-pi-4/ (accessed Oct. 20, 2022).

[30] Department of Statistics Malaysia. (2022). Launching of report on the key findings population and housing census of Malaysia 2020. [Online] Available: https://www.dosm.gov.my/v1/index.php?r=column/cthemeByCat&cat=117&bul_id=akliVWdIa2g3Y2VubTVSMkxmYXp1UT09&menu_id=L0pheU43NWJwRWVSZklWdzQ4TlhUUT09

[31] "Forecast your electricity bill." https://myelectricitybill.my/bill_calculator_domestic.html (accessed Oct. 20, 2022).

[32] S. Ishak, "The costs of crime to the society in Malaysia," International Journal of Business, Economics and Law, vol. 11, no. 3, pp. 13-18, 2016. [Online]. Available: https://www.ijbel.com/wp-content/uploads/2017/01/ECON-136.pdf.

[33] Lazada. "Xiaomi Redmi Note 11 Pro 5G (8GB RAM + 128GB ROM) Original Smartphone 1 Year Warranty With Xiaomi Malaysia." https://www.lazada.com.my/products/xiaomi-redmi-note-11-pro-5g-8gb-ram-128gb-rom-original-smartphone-1-year-warranty-with-xiaomi-malaysia-i3062609967-s15251553615.html?exlaz=d_1:mm_150050845_51350205_2010350205::12:15210038057!133416790750!!!pla-293946777986!c!293946777986!15251553615!582857236&gclid=Cj0KCQjwkt6aBhDKARIsAAyeLJ1DNFOoIFguuj-bRSmjg4SUZEbwUWui1yT7AvVCUM4lxGoQcHU4xSYaAlfWEALw_wcB (accessed Oct. 20, 2022).

# 7.0 Reflective Summary

## 7.1 Reflective summary – Oh Yong Xin

In this project, I was mainly responsible for activity 1, 4, 6, and the integration of all activities together to form one complete smart door system. For activity 1, after discussion within the team, we decided to use 2 Raspberry Pi (raspi) microcontrollers to improve responsiveness of the system. I researched on various methods to implement communication between raspi, and finally programmed a simple code to implement this functionality. In this activity, I also integrated the RFID system to make the smart door system more user friendly. For activity 4, I read the project manual and successfully integrated the solenoid door lock to the smart door system, allowing a realistic prototype of door unlocking and locking to be demonstrated. For activity 6, after reading multiple existing smart door datasheets, watching YouTube videos on existing smart door locks, and considering the team's capabilities and time constraints, we decided to focus on smart door security features to make the smart door system more realistic, as security is of the highest priority for a smart door lock system. As the member in charge of implementing the additional features, I read several websites and watched a few tutorials on how to implement the security features decided within the team into the smart door system. After one week of continuous effort, activities 1, 4, and 6 were successfully implemented individually.

For the complete system integration, I communicated consistently with other team members to understand their progress on the project so that I have a rough idea on how to integrate all activities together as one complete smart door system. Yuen Yee was responsible for activities 2 and 3, which focused on movement tracking, as well as temperature and humidity sensing. Improvements on the basic functionalities were also implemented by her, which include hazard (fire) detection, weather monitoring, and abnormal movement alerts. The activities allocated to her mainly focus on developing machine learning algorithms to classify object motion and weather conditions, and her activities. Meanwhile, Seng Chee was allocated activity 5, which is on encryption and decryption. He performed extensive research on existing encryption algorithms. After a team discussion, we decided to use the Advanced Encryption Standard (AES) algorithm with cipher block chaining as an enhanced feature of the encryption algorithm. He successfully implemented the encryption and decryption algorithm before passing this encryption algorithm to me for the integration of this algorithm into the smart door system. After all team members have successfully completed their tasks, which was on Week 12 Tuesday, I performed the overall system integration by coding the communication between the 3 raspi used and integrated Seng Chee's code to perform encryption on the database and OTP generated.

For the report, I am responsible for writing the methodology and results for activities 1, 4, and 6. Yuen Yee is allocated the introduction, methodology and results for activities 2 and 3 and conclusion. Seng Chee is allocated the literature review, feasibility analysis and methodology and results for activity 5.

Throughout this project, communication between members was done using WhatsApp and Zoom. Whenever a team member faced any issues, the team would either meet physically on campus to solve any issues related to programming or meet virtually via Zoom to discuss any ideas that come to mind. The communication within the team was productive and all team members participated actively. Besides physical and virtual meetings, after I have completed some small tasks in the lab, I would also report my progress in the WhatsApp group to keep the team informed on the project progress so far, especially since I was responsible for system integration. In my opinion, there was no problem in communicating within the team especially when seeking help among members for this project.

All members were fully committed in this project. The team also compromised among each other, especially when distributing the workload among members. Since I spent a lot of time writing code for system integration, I am allocated less parts for the report, while Seng Chee is allocated more sections for the report as his part on coding is less. All in all, it was a great pleasure working in this team, and we successfully implemented the smart door system despite being deprived of one team member. This owes to the great cooperation within the team, excellent commitment of individual members, and efficient communication through physical and virtual means.

## 7.2 Reflective summary – Chong Seng Chee

During the progression of the project, it is acknowledged that the project was broad and challenging due to the need of merging numerous functionalities into a single smart door system. The project also expects additional functionalities that serve as the main distinction among other groups, which resulted in the difficulty of the project to be quite hard. In addition to the shortage of one team member, this makes the project even more demanding. However, our team managed to distribute our responsibilities and complete the project with the best of our abilities. The responsibilities of each team member are as follows:

1. Yong Xin: Given her excellent programming capabilities, she is given the task to implement Activity 1 (IoT sensor and network system), 4 (Security door lock) and 6 (Additional features). For Activity 1, she is tasked with implementing the door lock system with the provided components. For Activity 4, she extends Activity 1 to connect with the relay and solenoid door lock. For Activity 6, she integrates the door lock system with a database management system which serves as the main additional functionality of our proposed smart door system.
2. Yuen Yee: Due to her former experiences in machine learning, she is tasked with implementing Activity 2 (Machine learning system) and 3 (Temperature and humidity). For Activity 2, She is tasked with designing a machine learning algorithm which can classify the movement in front of the door. For activity 3, she is tasked with implementing a temperature and humidity sensor which can provide an environmental status comment via a supervised machine learning model.
3. Seng Chee: The remaining activities are thus tasked by me, which are Activity 5 (Encryption and decryption) as well as performing the literature review and feasibility evaluation with cost benefit analysis which would be used in the project report. For Activity 5, I was tasked with implementing a strong encryption and decryption algorithm, namely the AES algorithm. For the literature review, smart doors on the market are reviewed for reference for our smart door features. This ultimately leads into the feasibility evaluation to choose the best feature.

As our project advances, we found out that effective team communication is essential to ensure everyone is constantly making progress of their given responsibilities. Given that our time and resources are limited, our team also discovered the strong advantage of working as a group. Thus, frequent team discussions are held on Zoom as well as face-to-face meetings to help each other keep track of our progress as well as provide updates about our latest development. Furthermore, a WhatsApp group is also created among team members so that we can reach out to each other outside of our team discussions. Thus, during the times when our project is at its peak, team sessions are organized in the lab so that we can all combine and integrate our individual tasks into a full-fledged smart door system.

Commitments by each team member are also shown throughout the project duration. For instance, during the planning stages of our smart door system, it is found that everyone has their own point of view and ideas, thus resulting in a brainstorming session in which we each shared our own sets of ideas to reach the best idea for our project. During the process, we challenged each other's notions about what would and would not work. We could also see how modifying a design influenced its performance. During the implementation stages of the project, each of us have also made strong time commitments to ensure our proposed design can be fully realized. For instance, during the mid-semester break, our team would still agree to meet up and continue our project developments in campus, as we all unanimously come to an agreement that this would be the best outcomes towards successfully implementing our smart door system. When any of our team members have any doubts or questions, other team members would try their best to provide any guidance with the best of their abilities. If the question or issue persists, then we would collectively ask for guidance or help from the lecturer as a team.

Overall, it was a fulfilling experience for working in this team, as we successfully implemented a smart door system within our capabilities. This is all attributable to the strong cooperation and outstanding coordination of the team, which I am thankful for.

## 7.3 Reflective summary – Mah Yuen Yee

For this project, I am mainly responsible for activities 2 and 3. Activity 2 was realized by data collection, model training, and real-time execution of movement classification and Telegram updates. Slightly more than 3 full days were used for data collection and model training. At first I collected only 50 samples for each of the 8 classes: pass by, near stationary, far stationary, no object, forward, backward, come from the side, and leave to the side. The model training failed miserably with the data available having a validation accuracy of around 50%. After examining the dataset and the confusion matrix, I realized that the data collected for forward and come from the side are very similar to each other. The same goes to backward and leave to the side. Therefore, I combined the four classes into two classes, improving the validation accuracy to around 60%. The resultant training accuracy is around the same as the validation accuracy even if the model complexity increased, showing the insufficiency of data from which, the model cannot learn a comprehensive pattern of data distribution.

After discussion with my teammates regarding the model performance and the time constraints of the project, we decided I should collect more data. I thus collected more data, totaling 100 samples for each class for model training, resulting in a validation accuracy of around 80%. After some research, thinking, and study, I realized that the static and dynamic distinguishment of the data can be exploited by using a model known as divide and conquer. The validation accuracy improved to more than 95% through this approach. Different supervised models were tried for each phase of model training. MLP was found to be the most effective model compared to all other machine learning models available in sklearn (excluding other deep learning models such as Convolutional Neural Network (CNN) which is not considered due to the difficulty of installing a deep learning library such as Pytorch into Raspberyy Pi.) The real-time execution of movement classification and Telegram updates require an intensive cycle of coding, testing and debugging. Almost 2 full days were used for the purpose and the addition of abnormal event detection feature. ¼ of the 2 days were spent on polishing all the features to ensure the Telegram message has accurate time and corresponding movement shown the way the team agreed to.

For activity 3, the coding needed for temperature and humidity measurement is easy. The dew point and environment status computation are a reuse of laboratory work. The hardest part of this activity goes to model training for weather determination although its difficulty can hardly be same as activity 2. Due to time constraints, I decided to use an online weather dataset instead of collecting data myself using sensor available after a discussion with my teammates. A few hours were spent to find a suitable dataset: 1) hourly data, 2) both temperature and humidity data are inside, 3) weather description is inside, and 4) from an Asian country. I tried to use a combination of data from US and Israeli which resulted in a very low validation accuracy of 40%. Even the large dataset of 36000 samples which fulfills all the requirements only results in a validation accuracy of no more than 60%. In addition, it is interesting that CARTS performs better than MLP for weather determination. This should be due to the low number of features (only 2 which are temperature and humidity) input to the model. The entire activity was finished in slightly more than 1.5 full days including the code integration into the code for activity 2.

For this report, all the sections related to activities 2 and 3 were done by me, in addition to the small sections of conclusion and future work. I did most but not all parts of report formatting.

Yong Xin is mainly responsible for all other activities besides activity 5. She spent more time and effort than me for coding and completing the activities for demonstration. She also initialized meetings with all members whenever she needed our opinion for system design and met any difficulties or confusion when doing the project. For any stage she completed she showed us the results and asked for our opinion on any improvement needed. Overall, she is the most contributing member in the team for this project. For the report, she did all parts she responsible for coding and designing.

Seng Chee is mainly responsible for activity 5 (both coding and report), literature review and cost benefit analysis. He did a great deal of research for all the parts he is responsible for. Similar to Yong Xin, whenever he needed any opinion from us for system design or met any difficulties when doing the project, he initialized meetings with us for discussion. For any stage he completed he showed us the results and asked for our opinion on any improvement needed. Overall, he is the member who really paid a lot of time and effort to study and research knowledge inside and outside of the lecture content to complete his parts.

Overall, I am satisfied with this team and this project. I do not think this project could be done any better with only the 3 of us. We have tried our best and I am really grateful for the team and the achievement. We have tried to improve the features more and more under the high workload and time constraints we had.

# 8.0 Appendices

## 8.1 Appendix A: S-box substitution values for the byte (hexadecimal format)

| | x0 | x1 | x2 | x3 | x4 | x5 | x6 | x7 | x8 | x9 | xa | xb | xc | xd | xe | xf |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0x | 63 | 7c | 77 | 7b | f2 | 6b | 6f | c5 | 30 | 01 | 67 | 2b | fe | d7 | ab | 76 |
| 1x | ca | 82 | c9 | 7d | fa | 59 | 47 | f0 | ad | d4 | a2 | af | 9c | a4 | 72 | c0 |
| 2x | b7 | fd | 93 | 26 | 36 | 3f | f7 | cc | 34 | a5 | e5 | f1 | 71 | d8 | 31 | 15 |
| 3x | 04 | c7 | 23 | c3 | 18 | 96 | 05 | 9a | 07 | 12 | 80 | e2 | eb | 27 | b2 | 75 |
| 4x | 09 | 83 | 2c | 1a | 1b | 6e | 5a | a0 | 52 | 3b | d6 | b3 | 29 | e3 | 2f | 84 |
| 5x | 53 | d1 | 00 | ed | 20 | fc | b1 | 5b | 6a | cb | be | 39 | 4a | 4c | 58 | cf |
| 6x | d0 | ef | aa | fb | 43 | 4d | 33 | 85 | 45 | f9 | 02 | 7f | 50 | 3c | 9f | a8 |
| 7x | 51 | a3 | 40 | 8f | 92 | 9d | 38 | f5 | bc | b6 | da | 21 | 10 | ff | f3 | d2 |
| 8x | cd | 0c | 13 | ec | 5f | 97 | 44 | 17 | c4 | a7 | 7e | 3d | 64 | 5d | 19 | 73 |
| 9x | 60 | 81 | 4f | dc | 22 | 2a | 90 | 88 | 46 | ee | b8 | 14 | de | 5e | 0b | db |
| ax | e0 | 32 | 3a | 0a | 49 | 06 | 24 | 5c | c2 | d3 | ac | 62 | 91 | 95 | e4 | 79 |
| bx | e7 | c8 | 37 | 6d | 8d | d5 | 4e | a9 | 6c | 56 | f4 | ea | 65 | 7a | ae | 08 |
| cx | ba | 78 | 25 | 2e | 1c | a6 | b4 | c6 | e8 | dd | 74 | 1f | 4b | bd | 8b | 8a |
| dx | 70 | 3e | b5 | 66 | 48 | 03 | f6 | 0e | 61 | 35 | 57 | b9 | 86 | c1 | 1d | 9e |
| ex | e1 | f8 | 98 | 11 | 69 | d9 | 8e | 94 | 9b | 1e | 87 | e9 | ce | 55 | 28 | df |
| fx | 8c | a1 | 89 | 0d | bf | e6 | 42 | 68 | 41 | 99 | 2d | 0f | b0 | 54 | bb | 16 |

Fig. 17. S-box substitution values for the byte (hexadecimal format)

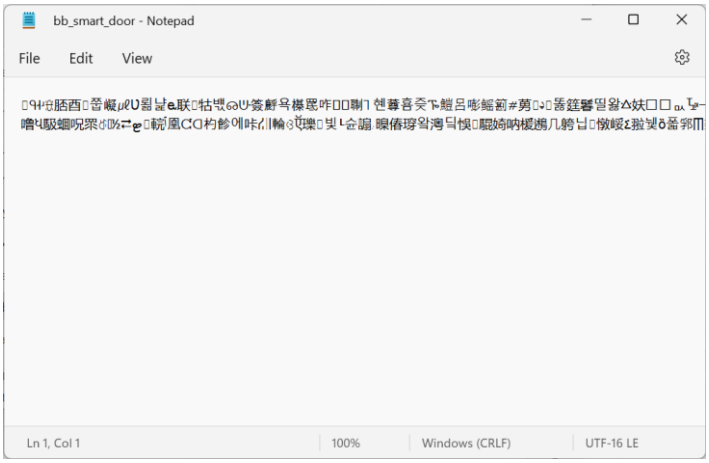


Fig. 18. Encrypted database

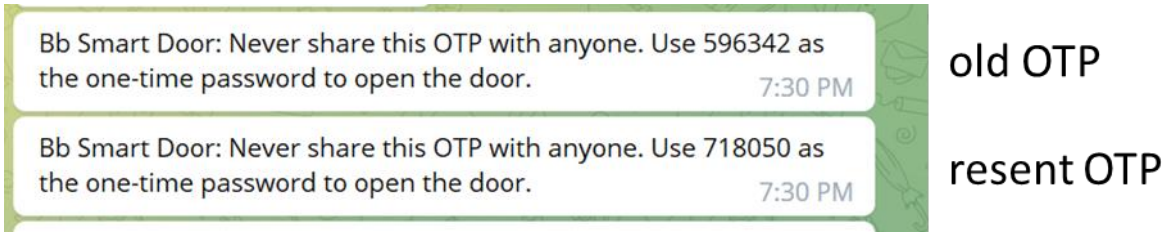


Fig. 19. Resending OTP.

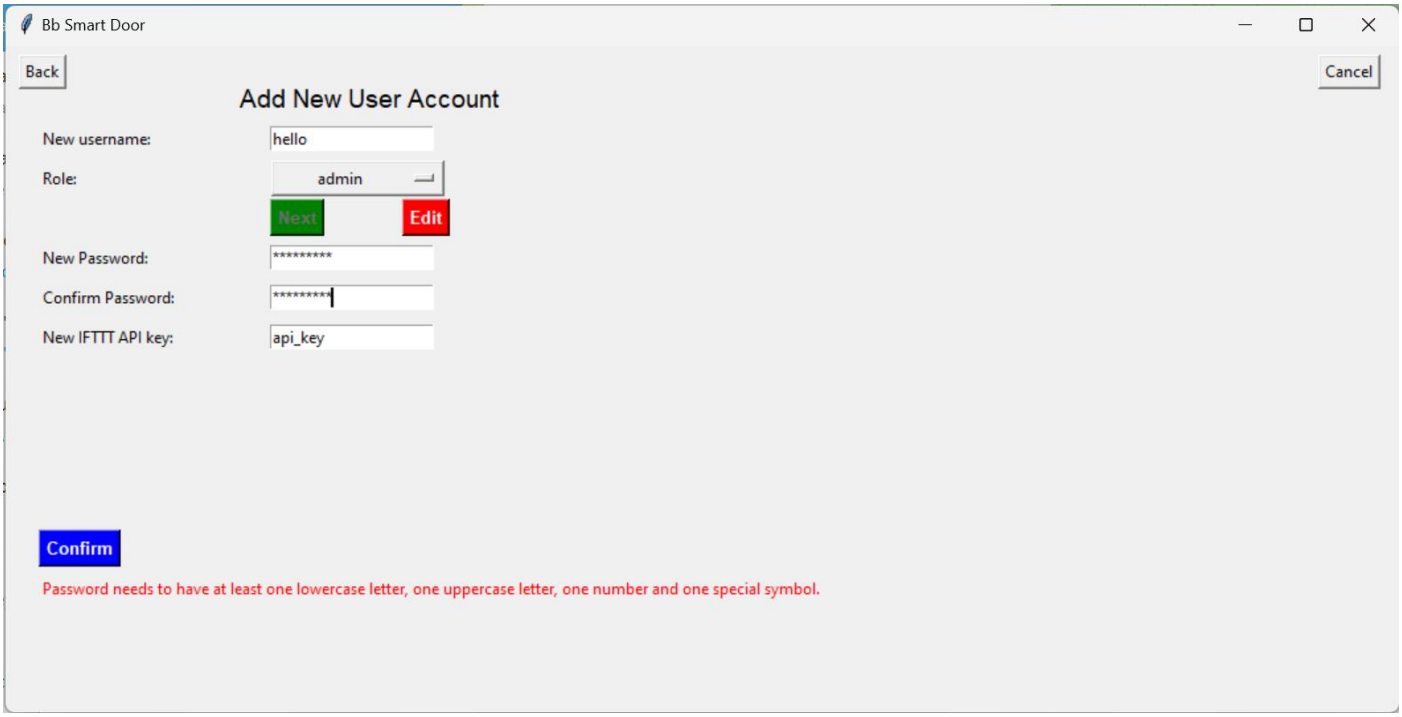


Fig. 20. Error message for weak password.

## 8.2 Appendix B: Detailed calculation of cost and benefit for each COA (1 year)

It is noted that COA 1 (System A) and COA 2 (System B) have the same cost and benefit calculations, thus both these COAs are calculated in a single table.

| Solution | Item | Unit amount (RM) | No. of years | Amount via years (RM) | Total amount (RM) | Comments/References |
|---|---|---|---|---|---|---|
| **COA 1 & 2** | **Costs** | | | | | |
| **System A & B** | Project Kit components (x3) - One time | 402.90 | 1 | 402.90 | | Costs provided by ECE4810 Toolbox Loan Form 2022, [23] |
| | RaspPi Kit (x3) - One time | 1,296.00 | 1 | 1,296.00 | | Costs provided by ECE4810 Toolbox Loan Form 2022, [23] |
| | Additional component - PiCamera (x1) - One time | 125.00 | 1 | 125.00 | | Cost found on Cytron Marketplace, [24] |
| | Development cost - One time | 1,200.00 | 1 | 1,200.00 | | Project is equivalent to work of 1 professional software programmer based on the Constructive Cost Model (COCOMO) [25], [26]. Since project used about 80 hours in total, quantifying with the average Malaysian salary of a professional software programmer of RM15/hour [27], the development cost is calculated to be RM 1,200.00. |
| | Maintenance cost | 100.00 | 1 | 100.00 | | Average maintenance cost is estimated at [28] |
| | RaspPi power consumption | 3.60 | 1 | 3.60 | | [29] discovered average power usage of Raspberry Pi 4 (Idle 2.1W, Load 6.41W). Assuming smart door is used in private residential area, and since average household size in Malaysia in 2020 is 3.8 [30], can assume smart door is used 10 times per day. 1-time averages 30 seconds of Raspberry Pi usage. Calculation of kWh per month:<br>Non-idle: 30*10*6.41W*30s*1min/60s*1hr/60min*1k/1000 = 0.016025kWh in a month<br>Idle: 30*1435min*2.1W*1hr/60min * 1k/1000 = 1.50675 kWh in a month<br>Total in one month is 1.522775 kWh, which costs RM0.30/month in TNB standards, so RM3.60/year [31]. |
| | | | | | | |
| | TOTAL COSTS | | | | 3,127.50 | |
| | | | | | | |
| | **Savings** | | | | | |
| | Burglary prevention in | 5,000.00 | 1 | 5,000.00 | | Refers to the mode costs of crimes in Malaysia at [32] |

| | | | | | | |
|---|---|---|---|---|---|---|
| | damages and losses | | | | | |
| | Burglary prevention in medical cost | 200.00 | 1 | 200.00 | | Refers to the mode costs of crimes in Malaysia at [32] |
| | | | | | | |
| | TOTAL SAVINGS | | | | 5,200.00 | |
| | | | | | | |
| | **(Savings - Costs)** | | | | **2,072.50** | |

The only difference from the calculation of COA 3 is the cost addition of the smartphone with fingerprint sensor.

| Solution | Item | Unit amount (RM) | No. of years | Amount via years (RM) | Total amount (RM) | Comments/References |
|---|---|---|---|---|---|---|
| **COA 3** | **Costs** | | | | | |
| **System C** | Project Kit components (x3) - One time | 402.90 | 1 | 402.90 | | Costs provided by ECE4810 Toolbox Loan Form 2022, [23] |
| | RaspPi Kit (x3) - One time | 1,296.00 | 1 | 1,296.00 | | Costs provided by ECE4810 Toolbox Loan Form 2022, [23] |
| | Additional component - PiCamera (x1) - One time | 125.00 | 1 | 125.00 | | Cost found on Cytron Marketplace, [24] |
| | Additional component – Smartphone with fingerprint sensor (x1) - One time | 150.00 | 1 | 150.00 | | Assumed using the most affordable/price efficient smartphone that has an inbuilt fingerprint sensor. Cost found on Lazada [33]. |
| | Development cost - One time | 1,200.00 | 1 | 1,200.00 | | Project is equivalent to work of 1 professional software programmer based on the Constructive Cost Model (COCOMO) [25], [26]. Since project used about 80 hours in total, quantifying with the average Malaysian salary of a professional software programmer of RM15/hour [27], the development cost is calculated to be RM 1,200.00. |
| | Maintenance cost | 100.00 | 1 | 100.00 | | Average maintenance cost is estimated at [28] |
| | RaspPi power consumption | 3.60 | 1 | 3.60 | | [29] discovered average power usage of Raspberry Pi 4 (Idle 2.1W, Load 6.41W). Assuming smart door is used in private residential area, and since average household size in Malaysia in 2020 is 3.8 [30], can assume smart door is used 10 times per day. 1-time averages 30 seconds of Raspberry Pi usage. Calculation of kWh per month:<br>Non-idle: 30*10*6.41W*30s*1min/60s*1hr/60min*1k/1000 = 0.016025kWh in a month<br>Idle: 30*1435min*2.1W*1hr/60min * 1k/1000 = 1.50675 kWh in a month<br>Total in one month is 1.522775 kWh, which costs RM0.30/month in TNB standards, so RM3.60/year [31]. |
| | | | | | | |
| | TOTAL COSTS | | | | 3,277.50 | |
| | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **Savings** | | | | | |
| | Burglary prevention in damages and losses | 5,000.00 | 1 | 5,000.00 | | Refers to the mode costs of crimes in Malaysia at [32] |
| | Burglary prevention in medical cost | 200.00 | 1 | 200.00 | | Refers to the mode costs of crimes in Malaysia at [32] |
| | | | | | | |
| | TOTAL SAVINGS | | | | 5,200.00 | |
| | | | | | | |
| | **(Savings - Costs)** | | | | **1,922.50** | |

## 8.2 Appendix B: Detailed calculation of cost and benefit for each COA (5 years)

| Solution | Item | Unit amount (RM) | No. of years | Amount via years (RM) | Total amount (RM) | Comments/References |
|---|---|---|---|---|---|---|
| **COA 1 & 2** | **Costs** | | | | | |
| **System A & B** | Project Kit components (x3) - One time | 402.90 | 1 | 402.90 | | Discussed in Appendix B |
| | RaspPi Kit (x3) - One time | 1,296.00 | 1 | 1,296.00 | | Discussed in Appendix B |
| | Additional component - PiCamera (x1) - One time | 125.00 | 1 | 125.00 | | Discussed in Appendix B |
| | Development cost - One time | 1,200.00 | 1 | 1,200.00 | | Discussed in Appendix B |
| | Maintenance cost | 100.00 | 5 | 500.00 | | Discussed in Appendix B |
| | RaspPi power consumption | 3.60 | 5 | 18.00 | | Discussed in Appendix B |
| | | | | | | |
| | TOTAL COSTS | | | | 3,541.90 | |
| | | | | | | |
| | **Savings** | | | | | |
| | Burglary prevention in damages and losses | 5,000.00 | 5 | 25,000.00 | | Discussed in Appendix B |
| | Burglary prevention in medical cost | 200.00 | 5 | 1,000.00 | | Discussed in Appendix B |
| | | | | | | |
| | TOTAL SAVINGS | | | | 26,000.00 | |
| | | | | | | |
| | **(Savings - Costs)** | | | | **22,458.10** | |

| Solution | Item | Unit amount (RM) | No. of years | Amount via years (RM) | Total amount (RM) | Comments/References |
|---|---|---|---|---|---|---|
| **COA 3** | **Costs** | | | | | |
| **System C** | Project Kit components (x3) - One time | 402.90 | 1 | 402.90 | | Discussed in Appendix B |
| | RaspPi Kit (x3) - One time | 1,296.00 | 1 | 1,296.00 | | Discussed in Appendix B |
| | Additional component - PiCamera (x1) - One time | 125.00 | 1 | 125.00 | | Discussed in Appendix B |
| | Additional component – Smartphone with fingerprint sensor (x1) - One time | 150.00 | 1 | 150.00 | | |
| | Development cost - One time | 1,200.00 | 1 | 1,200.00 | | Discussed in Appendix B |
| | Maintenance cost | 100.00 | 5 | 500.00 | | Discussed in Appendix B |
| | RaspPi power consumption | 3.60 | 5 | 18.00 | | Discussed in Appendix B |
| | | | | | | |
| | TOTAL COSTS | | | | 3,691.90 | |
| | | | | | | |
| | **Savings** | | | | | |
| | Burglary prevention in damages and losses | 5,000.00 | 5 | 25,000.00 | | Discussed in Appendix B |
| | Burglary prevention in medical cost | 200.00 | 5 | 1,000.00 | | Discussed in Appendix B |
| | | | | | | |
| | TOTAL SAVINGS | | | | 26,000.00 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **(Savings - Costs)** | | | | **22,308.10** | |