ECE 4810 IOT Project [20 Marks]

Group: 6

Group Members (Name and ID):
1. Clifton Mak, 29439701

2. Chew Lik Siang, 29035058

3. Jolene Ong Su Lynn, 29592038

4. Lim Wei Jun, 29036348

Submission Date: 7/11/2020

1.0 Abstract

The purpose of this project is to combine aspects of machine learning and Internet of Things (IoT) principles to design a fully functional smart door system. Several subsystems have been implemented in our smart door system to provide a holistic user experience.

IoT describes the communication between devices that enables transfer and usage of data within a system. Doors are the main access point for any household; hence it is a crucial aspect to be considered in terms of home security. IoT is used because it enables the user to remotely monitor the current conditions of their household. The user is able to receive alerts when suspicious activity is detected and timely updates regarding the current condition of their household.

For this project, the Raspberry Pi is used as the main microprocessor. The AdaBoost Decision Tree supervised machine learning model is used to train the system to classify movement based on data collected from three ultrasonic sensors. Temperature and humidity sensor are also used to gather data about the surrounding environment.

Furthermore, the data collected by the ultrasonic sensors, data analyzed by the machine learning model and username and password of the users will also be encrypted before storing it into the system. This will then increase the security level of the system by preventing any suspicious people that try to manipulate the data. Besides, the data collected will also be further analyzed by the system and used as a feedback to the user through telegram.

This report details several aspects of our project, which includes the design methodology used in this project, project results and analysis, and feasibility evaluation on the design that was used with other design alternatives.

2.0 Introduction

The main problem statement introduced by this project is the vulnerability of households to several security breaches, such as cyber threats and burglar break-ins. The proposed solution to this is to design a robust system that can connect the user virtually to their home system regardless of their current location.

The objectives of this project are as follows:

1. To ensure that only authorized individuals are able to access the door and home security system by implementing additional preventive security measures.
2. To ensure that the data collected is protected against data breaches by providing encryption and decryption methods.
3. To ensure that the user is able to remotely monitor the conditions of their home by using an IoT system.
4. To ensure the versatility of the system by providing additional functionalities.

Ultrasonics sensors are stationed at the door to gather data regarding any movement located in front of the door. This data is then processed by an AdaBoost on top of decision tree supervised machine learning model to determine the nature of the movement. Based on this deduction, the system is able to determine the presence of any suspicious activity and inform the user accordingly. The collected data will be encrypted before storing it for further review.

At startup, the system will prompt for a user ID and password, along with a key. This user input will be encrypted before checking if the correct user credentials are entered. Since the user credentials are encrypted, even if the ID and password database is leaked, this information will be useless to the hacker without knowing the encryption key used.

The system sends timely updates to the user with info about the current humidity and temperature conditions, as well as if any suspicious activity is detected. If suspicious activity is sensed by the system, a video will automatically be captured by the camera in front of the door and sent to the user. As for the implementation on the data collected from the temperature and humidity sensor in the system is when the surrounding temperature is low and high humidity, which signifies that it was a rainy day, the system will allow people to stand still in front of the door without sending an alert video to the user. Then for the case where the surrounding temperature is high and low humidity and at the same time the system is getting a continuous motion passing from left and right in front of the door, it will send an alert video to the user to tell that somewhere around the house might be on fire. This will then provide a chance for the user to save their property. As an added feature, the user has the option to send a QR code to enable temporary access to a specialized pop box for depositing mailed packages.

To deactivate the security system, extra security measures are taken. The user first needs to key in the ID, password and the correct encryption key to deactivate the system. Then, a two-factor authentication message will be sent to the user, to ensure added security. The security system will only be deactivated if 2FA matches the random generated code from the system. Afterwards, the user is able to obtain the decrypted data file that contains info about the movements in front of the door and the data collected by the ultrasonic sensors.

3.0 Literature Review

3.1 Review on a simple smart door system

The state of art of smart door systems are designed to implement a home security system by the integration of smart phones and IoT. The introduction of a Smart door lock system is one of the most popular security measures nowadays. It provides added real-time security and convenience for the user.

For the IoT system reviewed, a Raspberry pi, servo motor, pi camera and LED are used to construct the Smart door lock system. The Blynk app is used to build the Graphical User Interface (GUI) to obtain user input. OpenCV library is used as the open source software library for computer vision.

The structure of the system works by taking pictures of the visitor at the front door with the Pi camera. After processing with the Raspberry Pi, facial detection is applied to determine the face of the visitor and it is sent to the user. The user will be able to decide whether or not to enable access to the current visitor. After which, the Raspberry Pi receives the user's decision and controls the servo motor to either lock or unlock the door accordingly. The LED lights up accordingly to notify the visitor of the owner's choice to either allow or deny access to the premises. [1]

3.2 Real Time smart door system

IoT and Machine Interpersonal Communication (M2M) technologies are also developed for the purpose of smart home systems. A real time smart door system allows communication between the house owner and visitors. Message notifications along with footage of the visitor will be sent to the house owner as well as the option to video chat with the visitor. Facial recognition, voice recognition and positioning detection are integrated to the smart door system in order to identify visitors to the home.

Intelligent motion sensors placed on the door enables the early warning system. It can be used to monitor high risk people, such as children or elderly with health concerns. The system will be able to track their motion and send alerts to the owner if they leave or attempt to leave the premises.

As a security measure, the communication between the smart phone and the IoT system will be end to end encrypted to ensure other people are unable to access important data. Text to speech features are also integrated in the smart home system. [2]

3.3 Smart Lock

Physical keys are the main method of restricting room access for most people in this day and age. Physical keys however carry with them a great number of security issues such as risk of physical loss, inventory tracking and lock-picking. Hence, the proposed system, Lockmate, offers a solution through the use of QR codes as a means of authentication. QR codes are cheap and easily produced and can be easily tracked digitally ensuring an up to data access log of people entering and exiting. Compromised QR codes can also be easily deleted or disabled. The system was designed using a Client-Server architecture and an Arduino board. [3]

4.0 Methodology

4.1 Design Prototype Overview

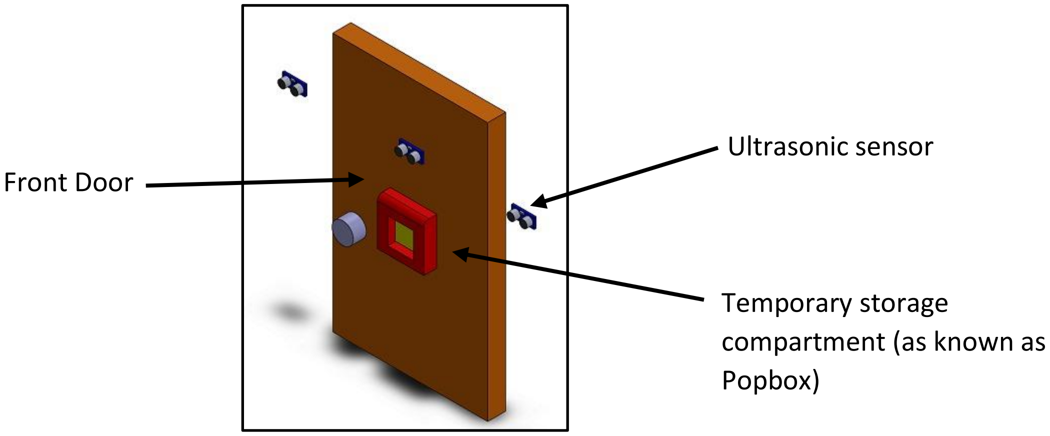
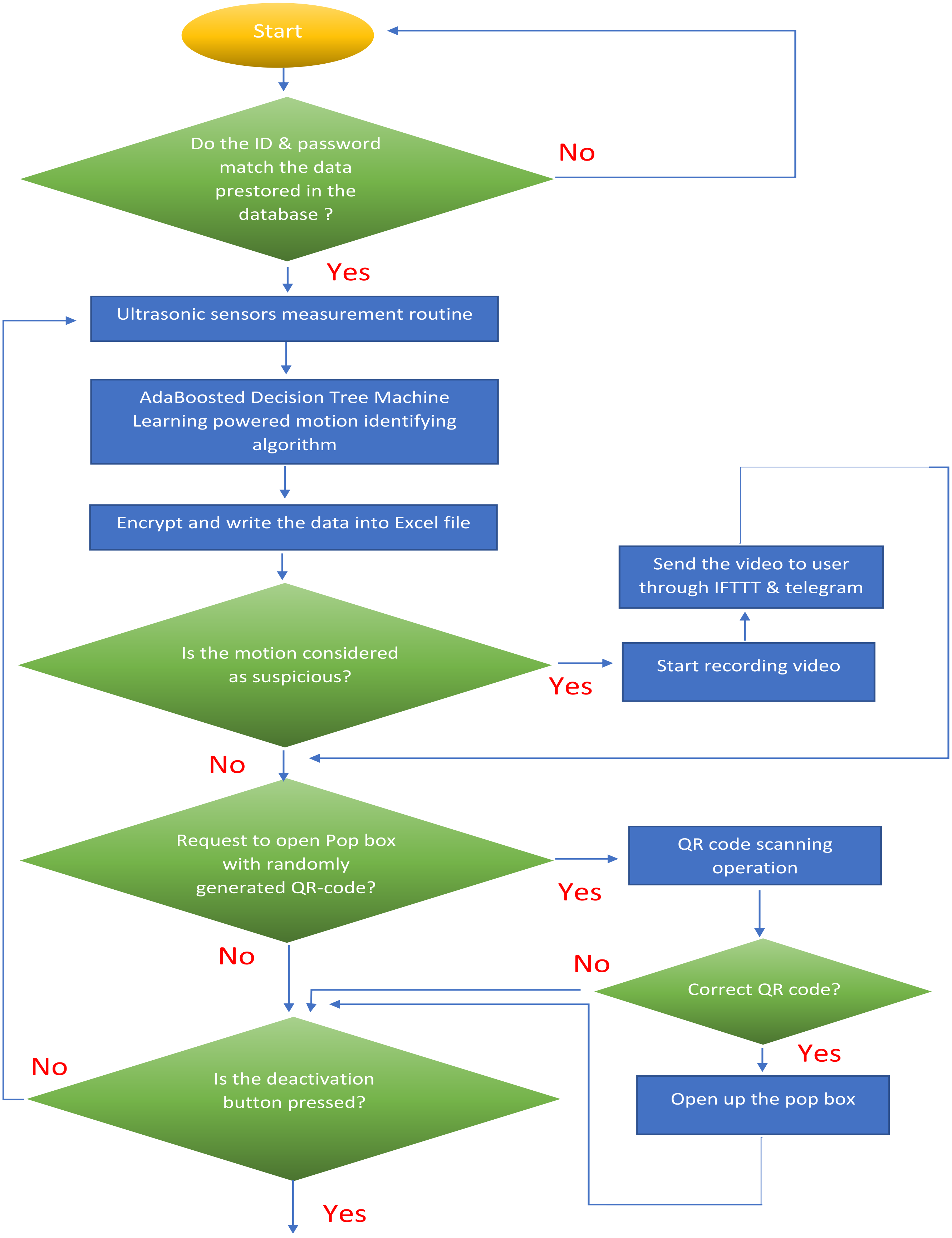


Figure 1: Prototype of the smart door design

Figure 1 shows the prototype design of the smart door system. It highlights the position of the 3 ultrasonic sensors and the popbox structure. The overall system algorithm is shown in the flow chart in Figure 2.


Start
Do the ID & password match the data prestored in the database ?
No
Yes
Ultrasonic sensors measurement routine
AdaBoosted Decision Tree Machine Learning powered motion identifying algorithm
Encrypt and write the data into Excel file
Send the video to user through IFTTT & telegram
Is the motion considered as suspicious?
Yes
Start recording video
No
Request to open Pop box with randomly generated QR-code?
Yes
QR code scanning operation
No
No
Correct QR code?
No
Is the deactivation button pressed?
Yes
Open up the pop box
Yes

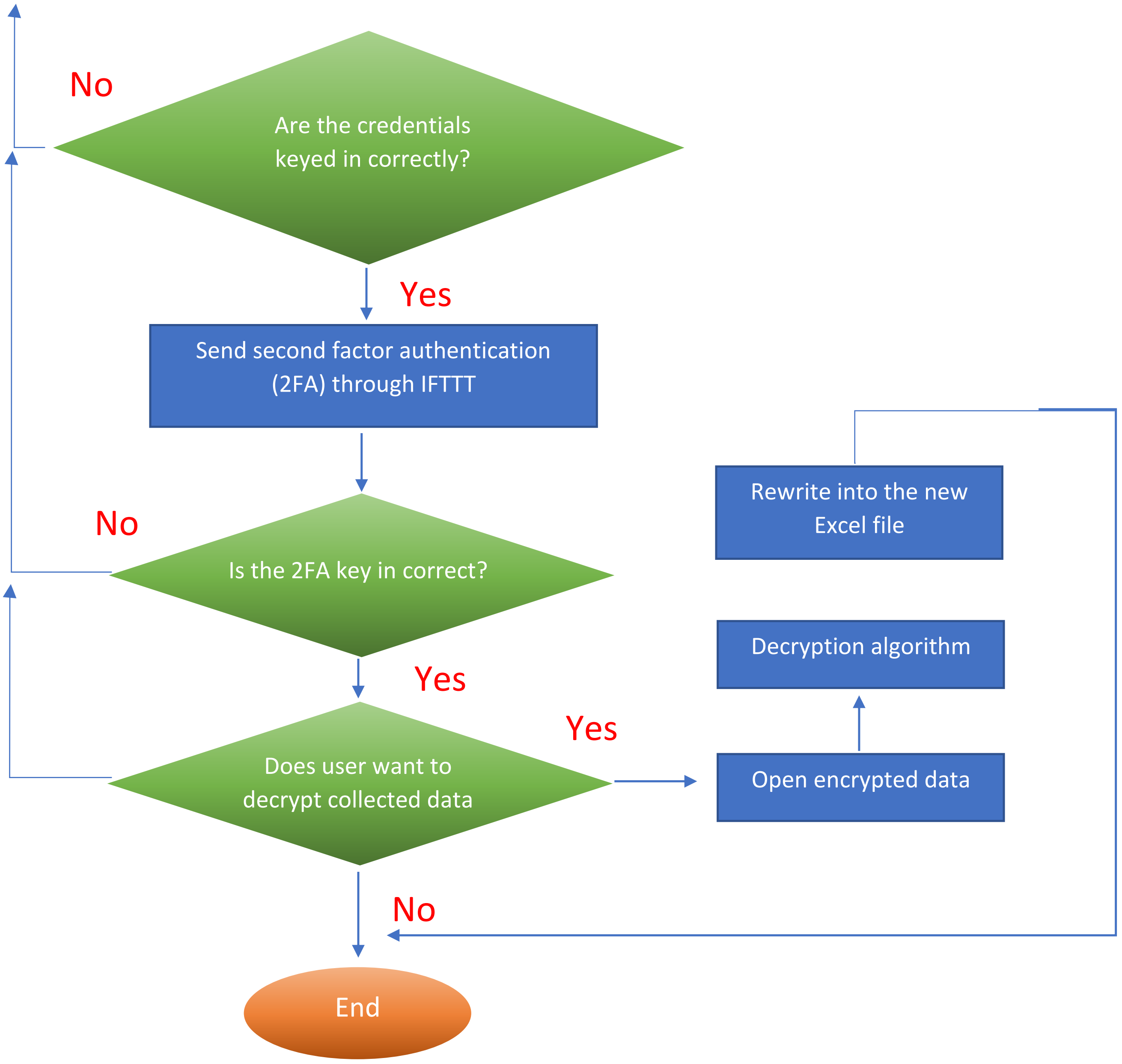

No
Are the credentials keyed in correctly?
Yes
Send second factor authentication (2FA) through IFTTT
No
Is the 2FA key in correct?
Yes
Rewrite into the new Excel file
Decryption algorithm
Yes
Does user want to decrypt collected data
Open encrypted data
No
End

Figure 2: Flow chart of the system overview

4.1 Motion Detection System (Activity 1)

Upon activating the security system, the three ultrasonic sensors placed outside the door will start to collect distance measurements. The readings from all the ultrasonic sensors will be compared and the direction with the smallest reading is recorded. This process is repeated for a total of 31 distance points before calculating the velocity of the object for the selected direction.

This collected data is passed into the AdaBoost Decision Tree Machine Learning powered motion identifying algorithm. Hence, it will determine the motion type based on the input and output the type of motion, ‘nobody’, ‘standstill’, ‘pass left’, or ‘pass right’. After collecting five iterations of motion type data, the system counts the number of times ‘nobody’ occurs. The readings from the humidity and temperature data are collected and passed into the system. Hence, combined with the current humidity and temperature conditions, the data is analysed to determine if suspicious is detected or not.

The flowchart in Figure 3 further explains the methodology adapted for this activity.

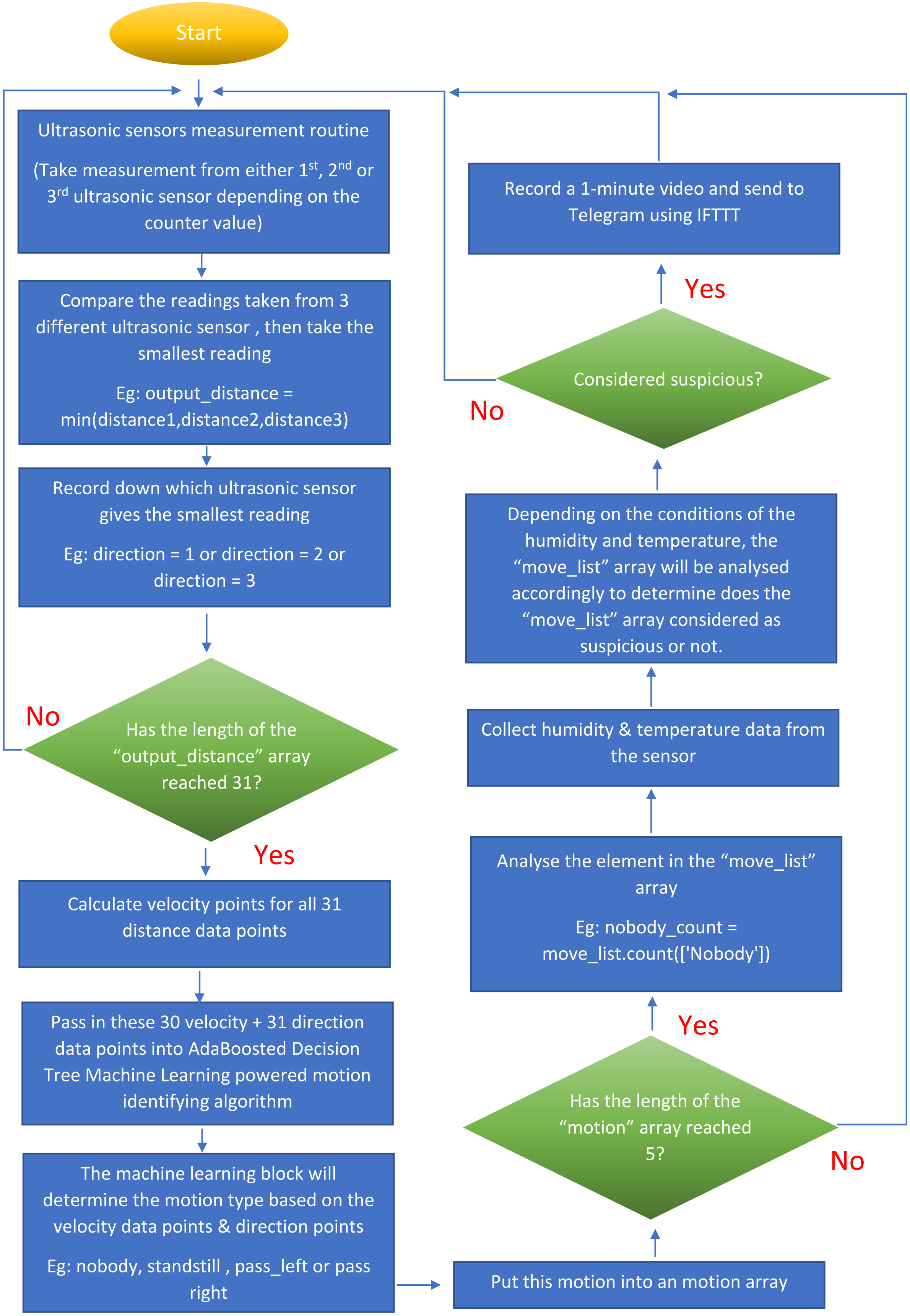
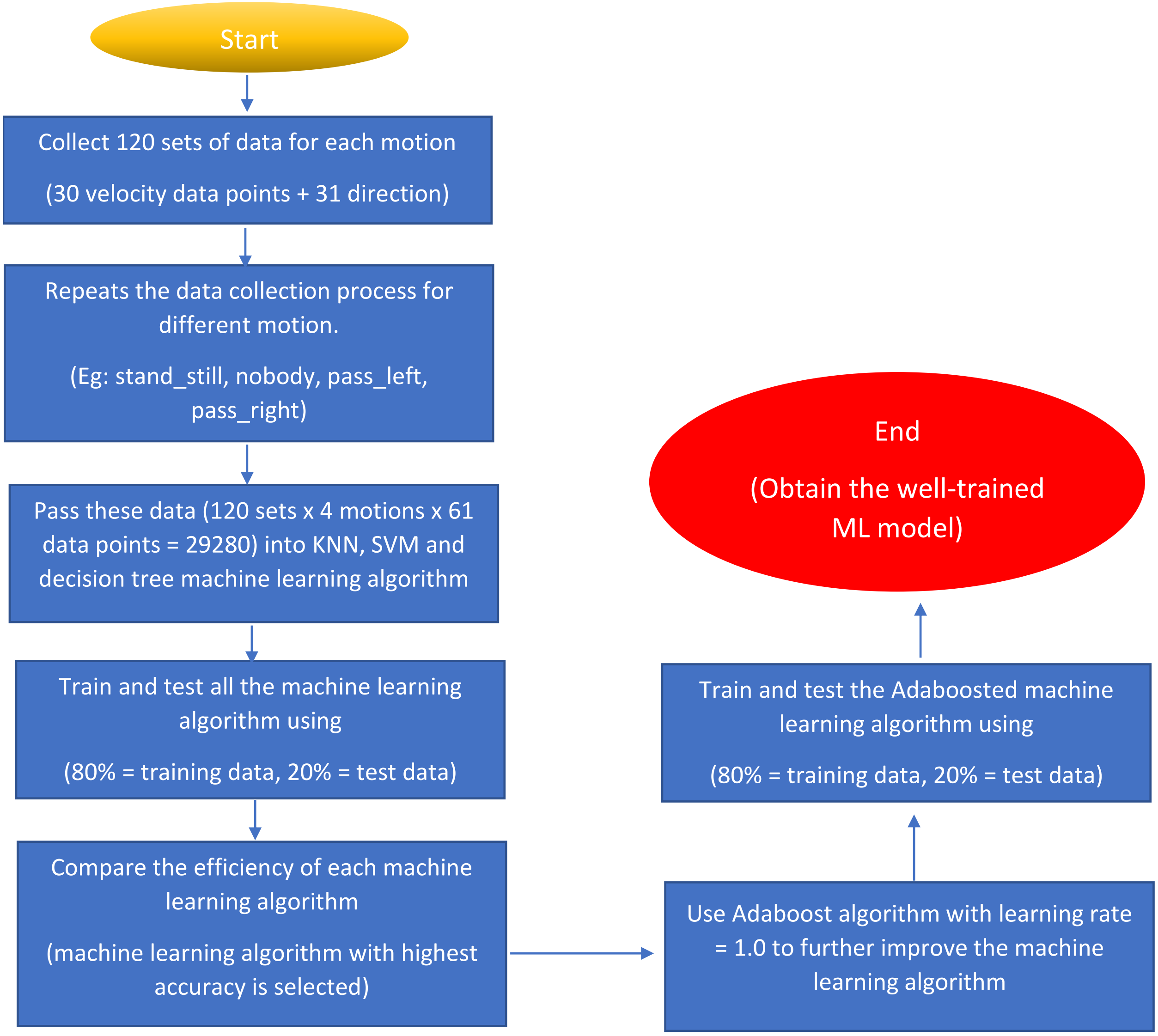

Start
Ultrasonic sensors measurement routine
(Take measurement from either 1st, 2nd or 3rd ultrasonic sensor depending on the counter value)
Compare the readings taken from 3 different ultrasonic sensor , then take the smallest reading
Eg: output_distance = min(distance1,distance2,distance3)
Record down which ultrasonic sensor gives the smallest reading
Eg: direction = 1 or direction = 2 or direction = 3
Has the length of the "output_distance" array reached 31?
No
Yes
Calculate velocity points for all 31 distance data points
Pass in these 30 velocity + 31 direction data points into AdaBoosted Decision Tree Machine Learning powered motion identifying algorithm
The machine learning block will determine the motion type based on the velocity data points & direction points
Eg: nobody, standstill , pass_left or pass right
Put this motion into an motion array
Has the length of the "motion" array reached 5?
No
Yes
Analyse the element in the "move_list" array
Eg: nobody_count = move_list.count(['Nobody'])
Collect humidity & temperature data from the sensor
Depending on the conditions of the humidity and temperature, the "move_list" array will be analysed accordingly to determine does the "move_list" array considered as suspicious or not.
Considered suspicious?
No
Yes
Record a 1-minute video and send to Telegram using IFTTT

Figure 3: Flow Chart of Activity 1

4.2 Machine Learning Algorithm (Activity 2)

In order to use the machine learning algorithm for our system, the machine was first trained with 120 sets of data for each class (stand still, past left, past right and nobody). The data is passed into different types of machine learning algorithms in order to pick the most efficient method. Hence, AdaBoosted Decision Tree model is chosen as the selected machine learning algorithm. The flowcharts in Figure 4 and Figure 5 will provide further details on the training phase of the machine learning model and way of implementing the machine learning model.

Training phase



Start
Collect 120 sets of data for each motion
(30 velocity data points + 31 direction)
Repeats the data collection process for different motion.
(Eg: stand_still, nobody, pass_left, pass_right)
Pass these data (120 sets x 4 motions x 61 data points = 29280) into KNN, SVM and decision tree machine learning algorithm
Train and test all the machine learning algorithm using
(80% = training data, 20% = test data)
Compare the efficiency of each machine learning algorithm
(machine learning algorithm with highest accuracy is selected)
Use Adaboost algorithm with learning rate = 1.0 to further improve the machine learning algorithm
Train and test the Adaboosted machine learning algorithm using
(80% = training data, 20% = test data)
End
(Obtain the well-trained ML model)

Figure 4: Flow chart of Training phase of Activity 2

Implementing the machine learning algorithm

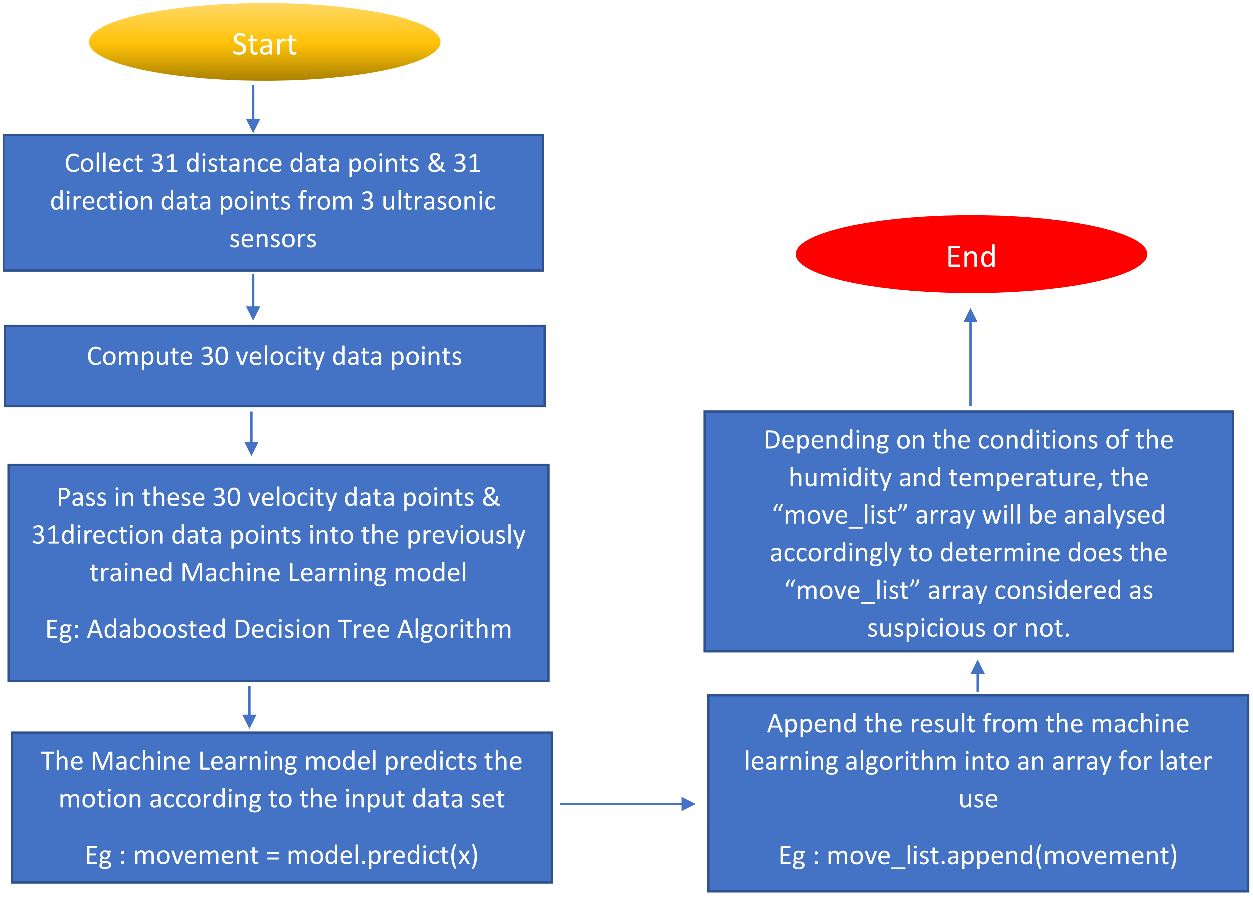

Start
Collect 31 distance data points & 31 direction data points from 3 ultrasonic sensors
Compute 30 velocity data points
Pass in these 30 velocity data points & 31direction data points into the previously trained Machine Learning model
Eg: Adaboosted Decision Tree Algorithm
The Machine Learning model predicts the motion according to the input data set
Eg : movement = model.predict(x)
Append the result from the machine learning algorithm into an array for later use
Eg : move_list.append(movement)
Depending on the conditions of the humidity and temperature, the “move_list” array will be analysed accordingly to determine does the “move_list” array considered as suspicious or not.
End

Figure 5: Flow chart of the implementation phase of Activity 2

4.3 Environment monitoring system (Activity 3)

When the system is activated, the temperature and humidity sensors will collect real time data of the surrounding environment. Based on this data combined with the data results on the motion of an object from the machine learning codes, the system will determine whether or not suspicious activity is detected.

The process and decision process for this is detailed further in the flow chart in Figure 6.

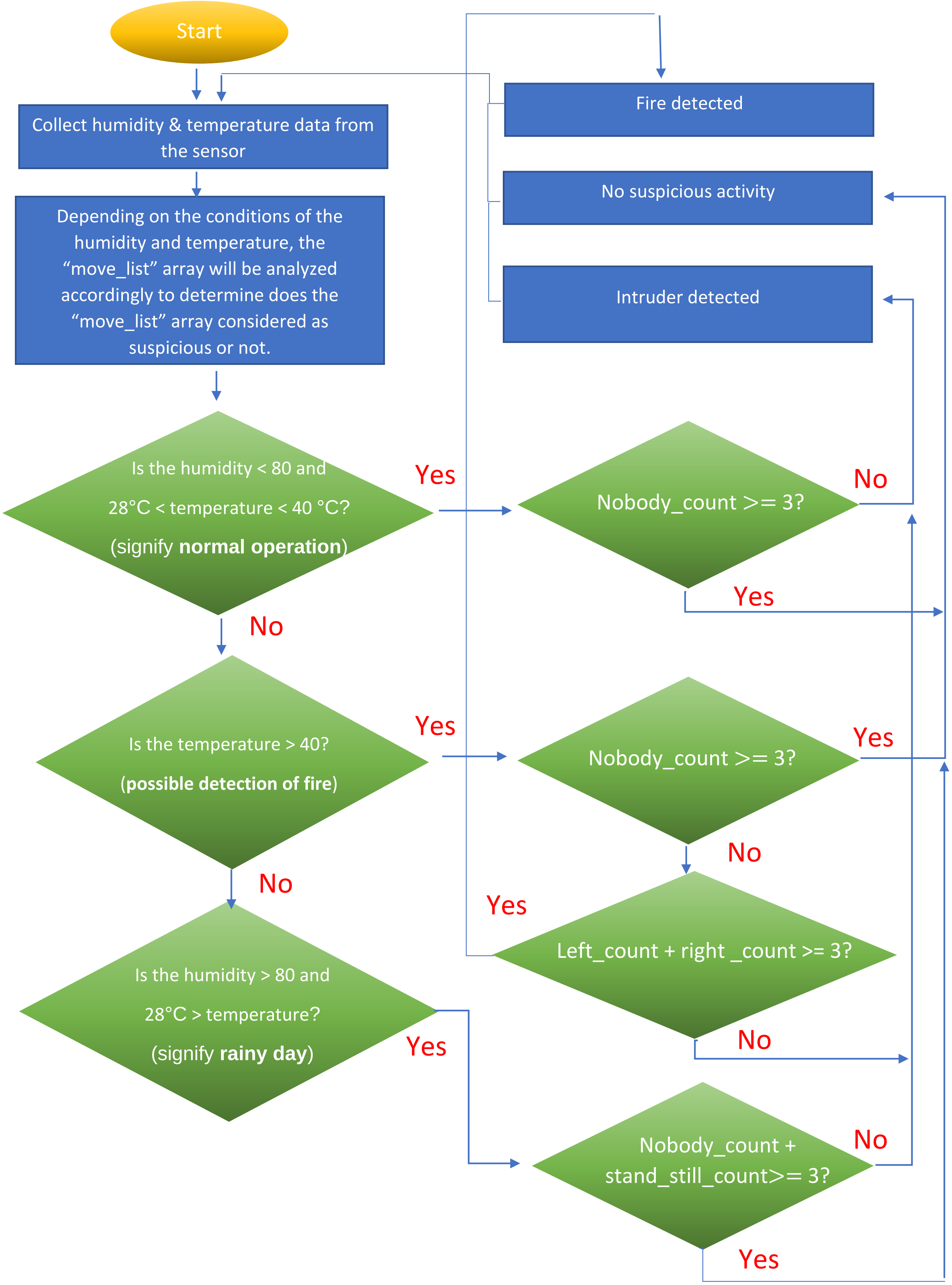

Start
Collect humidity & temperature data from the sensor
Depending on the conditions of the humidity and temperature, the "move_list" array will be analyzed accordingly to determine does the "move_list" array considered as suspicious or not.
Is the humidity < 80 and 28°C < temperature < 40 °C? (signify normal operation)
Yes
No
Is the temperature > 40? (possible detection of fire)
Yes
No
Is the humidity > 80 and 28°C > temperature? (signify rainy day)
Yes
Fire detected
No suspicious activity
Intruder detected
Nobody_count >= 3?
No
Yes
Nobody_count >= 3?
Yes
No
Yes
Left_count + right _count >= 3?
No
Nobody_count + stand_still_count>= 3?
No
Yes

Figure 6: Flow chart of Activity 3

4.4 Encryption and Decryption Algorithm

A self-developed encryption algorithm is implemented into the system, to ensure the data stored is safe.

When attempting to login, the user will be prompted for a username, password and unique key. These user inputs will be encrypted using an encryption algorithm that is determined by the unique key. Hence, this encrypted username and password will be crosschecked with pre-registered and encrypted credentials in the existing system database. If the encrypted credentials match the user input, the system will enable successful login.

The unique key is a 3-digit code that contains the sequence and type of encryption methods that would be used to encrypt the user input. Each digit corresponds to a type of encryption method. The user input would be passed into three different encryption methods based on the sequence of the key. The three main encryption methods used are transposition cipher, Caesar cipher, and the substitution cipher. Each of these encryption methods has different variations in regards of step size for Caesar cipher, dictionary used for substitution cipher, along with size and pattern used for transposition cipher.

To secure the data that is collected by the system, the data collected by the ultrasonic sensors will also be encrypted. The numerical data collected will be encrypted with a set key, which passes the data through two Caesar ciphers with different step sizes, followed by a substitution cipher. The type of motion which is determined by the machine learning code will be encrypted by a transposition cipher before storing in the system database.

If required, the user has the option to obtain the decrypted data file from the system after successful login. Then, the system will perform decryption accordingly before outputting the original data file for the user.

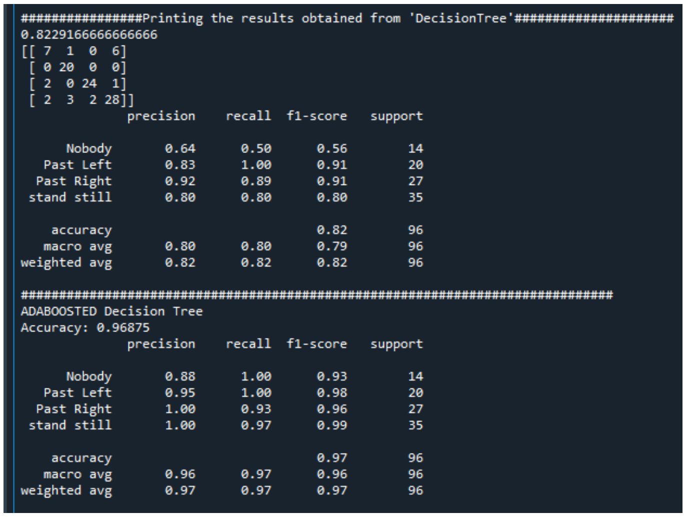
5.0 Results and Analysis

5.1 Communication of the system with the user

The scenario that the system will send an alert to the user on Telegram is when suspicious movements in front of the door are detected. It will then turn on the Pi Camera to record a 1 min video, and send it to the user saying an intruder is trying to break into the house. In addition to the video updates, the user will also be updated on the activity in front of the door every hour. Besides, the system also implements a two-factor authentication code containing 4 numbers will be sent to the user on Telegram after entering the correct username and password. The user will then need to input the same code in 1 minute to deactivate the system. Furthermore, there is also a fire alarm system where user will be alerted with a video when there is a continuous motion of passing left or right and the surrounding temperature of the door is high and low humidity.

The system is able to send any kind of messages and videos to the user through Telegram from the utilization of FileStack (a cloud storage) and Webhook (a HTTP push API that assists apps to send real time information).

5.2 Machine Learning results



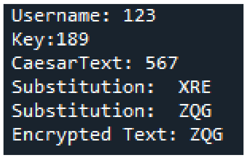
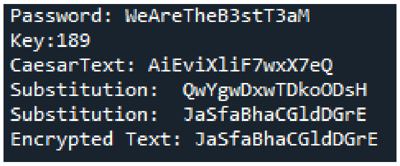
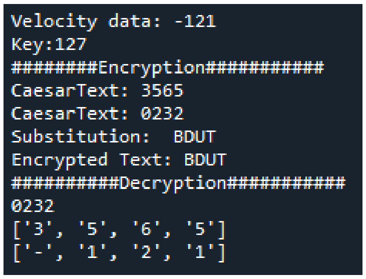
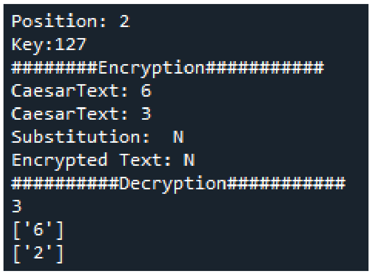
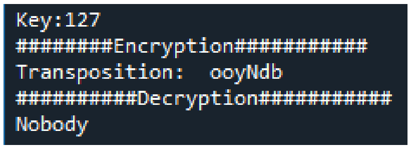
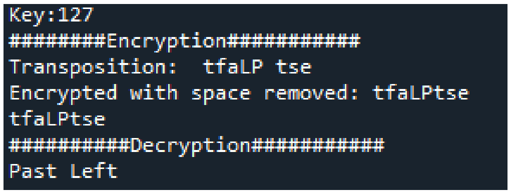
```
################Printing the results obtained from 'DecisionTree'#####################
0.8229166666666666
[[ 7  1  0  6]
 [ 0 20  0  0]
 [ 2  0 24  1]
 [ 2  3  2 28]]
              precision    recall  f1-score   support

      Nobody       0.64      0.50      0.56        14
   Past Left       0.83      1.00      0.91        20
  Past Right       0.92      0.89      0.91        27
 stand still       0.80      0.80      0.80        35

    accuracy                           0.82        96
   macro avg       0.80      0.80      0.79        96
weighted avg       0.82      0.82      0.82        96

##############################################################################
ADABOOSTED Decision Tree
Accuracy: 0.96875
              precision    recall  f1-score   support

      Nobody       0.88      1.00      0.93        14
   Past Left       0.95      1.00      0.98        20
  Past Right       1.00      0.93      0.96        27
 stand still       1.00      0.97      0.99        35

    accuracy                           0.97        96
   macro avg       0.96      0.97      0.96        96
weighted avg       0.97      0.97      0.97        96
```

Figure 7: Results on the accuracy of the machine learning algorithm

The supervised machine learning algorithm Decision Tree was used in the system because the distance data collected from the ultrasonic sensors may contain outliers and the outliers in the data are also needed to show that the object is passing from one ultrasonic sensor to another. Hence using SVM machine learning method it will not be able to create a clear boundary in the data with quite a number of outliers, hence this will cause the machine learning algorithm to have a low accuracy in predicting the data later on in the machine. From Figure 7 above, it is shown that the decision tree learning algorithm can have an accuracy of around 82.29% and in order to allow this algorithm to perform faster and more accurately in the system later on, AdaBoost algorithm is added on the Decision Tree algorithm, such that it will use an iterative approach to make the weak classifier a strong one. This will then improve the accuracy of the pervious machine learning algorithm to 96.88%.

5.3 Encryption and Decryption algorithm

Table 1: Examples of the encryption and decryption algorithm performed by the system

Examples	Explanations
 Username: 123 Key:189 CaesarText: 567 Substitution: XRE Substitution: ZQG Encrypted Text: ZQG  Password: WeAreTheB3stT3aM Key:189 CaesarText: AiEviXliF7wxX7eQ Substitution: QwYgwDxwTDkoODsH Substitution: JaSfaBhaCGldDGrE Encrypted Text: JaSfaBhaCGldDGrE	The database will store the encrypted version of the login details of the user. So, when the user input their username and password with the key allocated to them into the system, the plaintext will be encrypted based on the key used. Then it will be used to compare with the encrypted version in the database to grand access to the system when both of them tally.
 Velocity data: -121 Key:127 ########Encryption########### CaesarText: 3565 CaesarText: 0232 Substitution: BDUT Encrypted Text: BDUT ##########Decryption########### 0232 ['3', '5', '6', '5'] ['-', '1', '2', '1']  Position: 2 Key:127 ########Encryption########### CaesarText: 6 CaesarText: 3 Substitution: N Encrypted Text: N ##########Decryption########### 3 ['6'] ['2']	The velocity data collected will be encrypted according to the key, '127'. Key '127' corresponds to an encryption using our self-developed encryption method which is a combination of Caesar cipher (offset 1), Caesar cipher (offset 4) and substitution type 7 (random dictionary created by us). As explained in the methodology section, this sequence of encryption will be done on the message element by element. It can be seen from the results that 3 layers of encryption must be decrypted in order to get the original message.
 Key:127 ########Encryption########### Transposition: ooyNdb ##########Decryption########### Nobody  Key:127 ########Encryption########### Transposition: tfaLP tse Encrypted with space removed: tfaLPtse tfaLPtse ##########Decryption########### Past Left	The motion that was predicted by the machine learning algorithm will be encrypted by row transposition with a size 4 only. Spaces between words are removed after encryption to make it a bit more difficult to decipher. These spaces are added back after decrypting.

6.0 Feasibility Evaluation with Cost Benefit Analysis

The smart door system is implemented to ensure no intruders trespass any area through the smart door while also checking for any possible sources of fire in the area when owner is not in the premise. There are different solutions with different range, power consumption and price. The assumptions and constraints are that the area where the smart door is implemented is not a busy area. The cost benefit analysis was calculated based on the first-year usage.

6.1 Alternative Courses of Action

All 3 systems will start a camera to record when there are any suspicious activities and also uses a temperature and humidity sensor to detect the condition of the surrounding environment.

Course of Action 1: System A

System A as shown in Appendix A uses a single ultrasonic sensor to detect any movement towards or away from the door and standing still in front of the door. It has a small coverage of the area and consumes small amount of power the amount of data that is able to collect by one ultrasonic sensor is limited and might not be good enough to predict the motion of an object.

Course of Action 2: System B

System B as shown in Appendix A uses two ultrasonic sensors to get a two-dimensional data; one is used to detect motion along the hallway in front of the door and another is used to detect motion at the door. The ultrasonic sensor on the door will only be triggered when another ultrasonic sensor detects something moving along the hallway. It has a small coverage of area but it is able to predict motion of an object much precisely as compared to System A.

Course of Action 3: System C

System C is the current design used in the project as discussed above, uses 3 ultrasonic sensors with all 3 of them detecting motion in the same direction. This design configuration has the largest coverage of the area and will able to predict the continuous motion of an object in front of the door much more precisely and hence be able to differentiate between a suspicious motion from a normal motion of an object. The data collected is also a two-dimensional data; direction (left or right) and position (at which sensor). With a two-dimensional data, more ways of analyzing the motion can be implemented. However, the drawback of this is the power consumption will be the highest because an extra ultrasonic sensor will be used.

6.2 Lists of costs and benefits

Table 2: Tabulation of costs and benefits

Costs		
Items	Price (RM)	Comments
HC-SR04 ultrasonic sensors	2.90	per unit
Raspberry Pi-4 Model B	239.00	per unit [4]
2k ohms resistor	0.05	per unit
1k ohms resistor	0.05	per unit
Wiring and installation	75.00	100m wires cost RM25 [5] + service installation of RM50 (one time)
Electrical consumption for 1 ultrasonic sensor	38.88 per year	On average 1kWh cost around RM0.40 per month [6] and power consumption of an ultrasonic sensor is 0.27kWh per day
Benefits		
Security guard salary	1579	Salary for 1 guard per month [7]
Reduced power consumptions	30.00 per year	Power can be saved by reducing the frequency of activating the sensors or starting up the rasp pi camera. The value obtained is an assumption
Reduced chances of break-ins	-	-
High accuracy in motion detection	-	Can accurately detect suspicious movements

Table 3: Calculation of quantifiable costs and benefits for all courses of actions

Course of action, COA	Item	Amount (RM)	Comments
COA #1	HC-SR04 ultrasonic sensors	-2.90	1 unit
System A	Raspberry Pi-4 Model B	-239.00	1 unit
	2k ohms resistor	-0.05	1 unit
	1k ohms resistor	-0.05	1 unit
	Wiring and installation	-75.00	1 time
	Electrical consumption for ultrasonic sensor	-38.88/year	1 sensor
	No security guard	+18948/year	1 person
	Total cost	-355.88	First year
	Total benefit	+18948	First year
	Total benefit – cost	18592.12	First year
COA #2	HC-SR04 ultrasonic sensors	-5.80	2 units
System B	Raspberry Pi-4 Model B	-239.00	1 unit
	2k ohms resistor	-0.10	2 units
	1k ohms resistor	-0.10	2 units
	Wiring and installation	-75.00	1 time
	Electrical consumption price for ultrasonic sensor	-77.76/year	2 sensors

	Reduced power consumptions	+30/year	1 year
	No security guard	+18948/year	1 person
	Total cost	-397.76	First year
	Total benefit	+18978	First year
	Total benefit – cost	18580.24	First year
COA #3	HC-SR04 ultrasonic sensors	-8.70	3 units
System C	Raspberry Pi-4 Model B	-239.00	1 unit
	2k ohms resistor	-0.15	3 units
	1k ohms resistor	-0.15	3 units
	Wiring and installation	-75	1 time
	Electrical consumption price for ultrasonic sensor	-116.64	3 sensors
	Reduce power consumptions	+30/year	1 year
	No security guard	+18948/year	1 person
	Total cost	-439.64	First year
	Total benefit	18978	First year
	Total benefit – cost	18538.36	First year

The quantifiable are non-quantifiable benefits are summarized below,

Table 4: Quantifiable and Non-quantifiable Benefits

Course of Acton, COA	System A	System B	System C
Quantifiable 1st year	RM 18592.12	RM 18580.24	RM 18538.36
Non-Quantifiable	• Reduced chances of break-ins	• Reduced chances of break-ins	• Reduced chances of break-ins • High accuracy in motion detection

6.3 Comparing alternatives

The accuracy in motion detection was selected as the decision criteria. The criteria was selected as all the motion data collected would be used and trained on the machine learning algorithm. The more accurate the data, the better the machine model can correctly detect suspicious motions and reduce the chances of a false alarm. The new total net returns after applying the weightages are summarized in Table 5.

Table 5: Comparing alternatives using decision matrix

	Decision matrix			COA #1		COA #2		COA #3	
No	Criteria	Weight	Weight	System A	Score	System B	Score	System C	Score
1	Low accuracy in motion detection	20 %	0.20	18592.12	3718.42	18580.24	3716.05	0	0
2	High accuracy in motion detection	80 %	0.80	0	0	0	0	18538.36	14830.69
	Total net return				3718.42		3716.05		14830.69

6.4 Recommendation and Justification

Three Courses of Action (COAs) were developed to determine which security system is the most feasible. Based on Table 5 as using accuracy in motion detection as the decision criteria, COA #3: System C has the greatest total net return and should therefore be the system to be implemented. System C uses 3 ultrasonic sensors to detect movement in front of the door. It has the largest coverage area among all 3 systems. Although system C has the highest power consumption among all systems, it is the system that gives the most accurate motion detection. It is the only system that can determine whether the person is moving left or right at the door to determine if movement is suspicious. System B is able to perform the same function but because the sensing coverage of the ultrasonic in the perpendicular direction is small, it is unlikely that a person will move left and right in a straight line, and hence may go out of the ultrasonic sensing range. This would then give inaccurate motion readings. In addition to this, the two-dimensional data obtained from system C will enable not only the direction of motion to be determined but also the position at which the person is standing in front of the ultrasonic sensor.

7.0 Conclusion and References

In conclusion, in this project our team has successfully implemented a smart door system by combining a few subsystems into one whole fully functional system that is able to eliminate the vulnerability threat for households from any burglar break ins. The smart door system consists of 3 ultrasonic sensors, 1 temperature and humidity sensor, 1 Pi Camera and a monitor attached to the Raspberry Pi which is the main processor of the system. After performing cost benefit analysis on 3 different design alternatives that is considerable for this project, the current design configuration is able to provide the highest total net return in 1 year.

Machine learning and principles of Internet of Things (IOT) has also been successfully implemented into the design of the smart door, such that the smart door system is able to communicate with the users by providing feedback through Telegram. The system is designed to send a one-minute video showing the surrounding of the door to alert the user when a suspicious movement is detected. Otherwise, the user will also be updated with the movement of any object in front of the door in a timely manner.

The system uses the AdaBoost on top of decision tree supervised machine learning model to analyze the data collected from the 3 ultrasonic sensors to predict on the motion of any object in front of the door. Furthermore, there is an encryption algorithm included in the system to further secure the system. All the data from collected from the ultrasonic sensors and motion of the object determined by the machine learning algorithm will be encrypted and stored in the database of the system. The user is also able obtain the decrypted version of the data for further use if needed.

Then the user will need to login using their username and password along with a unique key. All the details input by the user will be checked with the encrypted version of the pre-register details saved into the database, and if they match, the system will be able to either activate or deactivate the system. However, for deactivating there is one extra security layer which is the two-authentication factor feature, it will send a code to the user's through Telegram. If and only if the person is able to input the correct code in one minute, then only the system can be deactivated.

Also, the temperature and humidity sensor, was mainly used to detect the environment around the door. Other extra feature that is also included in the system is the capability to scan QR code using the Pi Camera. Lastly, all the features discussed above is able to control by the user under one simple and user-friendly graphical user interface (GUI).

In the process of designing this project, our team has realized that there are still room for improvement to this current system. For example, the Pi Camera can be used as a face recognition module that is able to alert the user if any suspicious face was detected. Overall, our team is able to produce a smart door system that can fulfill all the project requirements.

References

[1] K. Sri Viraja, K Bharath Kumar, C. Keerthi, G. Sandeep, Ed., “IOT Based Smart Door System” in International Journal for Research in Applied Science, Apr 2018. [Online]. Available: https://www.ijraset.com/fileserve.php?FID=15444. [Accessed 4 November 2020]

[2] Burak S, Tolga K, Huesyin K, Ed., “Real Time Smart Door System for Home Security” in International Journal of Scientific Research in Information Systems and Engineering, Dec 2015. [Online]. Available: https://www.researchgate.net/publication/328530952_Real_Time_Smart_Door_System_for_Home_Security. [Accessed 2 November 2020]

[3] A.Raifiuddin, M.Ghazali, “Lockmate: Digital Door Lock System Using QR Code” , 2017. [Online]. Available: https://engineering.utm.my/computing/proceeding/wp-content/uploads/sites/114/2018/04/Lockmate-Digital-Door-Lock-System-Using-R-Code.pdf [Accessed 7 November 2020]

[4] Raspberry Pi-4 Model B, Cytron, 2020. [Online]. Available: https://my.cytron.io/p-raspberry-pi-4-model-b-4gb?r=1&gclid=Cj0KCQiAhZT9BRDmARIsAN2E-J2uFMl2ecMxGRlL--yPYfBYg9BUZuKnIT2hZfCEUUMR6hZareuzAQkaAtWxEALw_wcB [Accessed 6 November 2020]

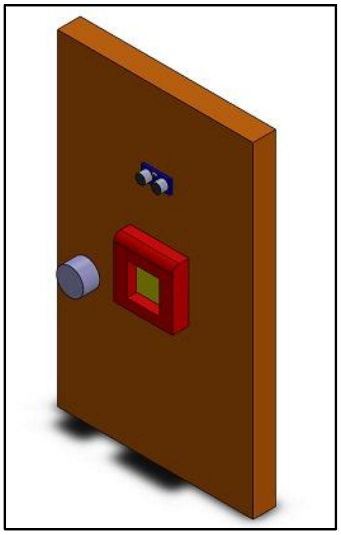
[5] Single Core Cable, Cytron, 2020. [Online]. Available: https://my.cytron.io/c-single-core-wire/p-single-core-cable-roll-blue?src=category

[6] “Pricing and Tariffs.” Tenaga National. https://www.tnb.com.my/residential/pricing-tariffs [Accessed 4 November 2020]

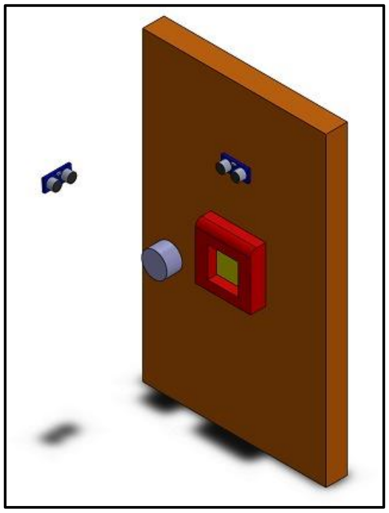
[7] “Security Guard Salaries in Malaysia.” Indeed.com. https://malaysia.indeed.com/salaries/security-guard-Salaries [Accessed 3 November 2020]

Appendix

Appendix A: System A and B configurations

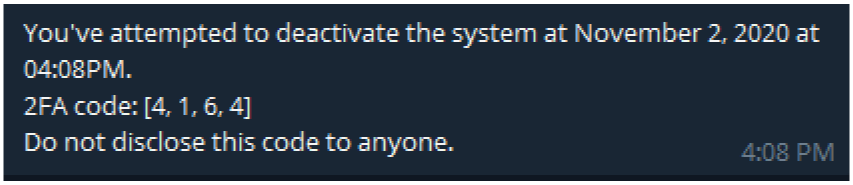


System A



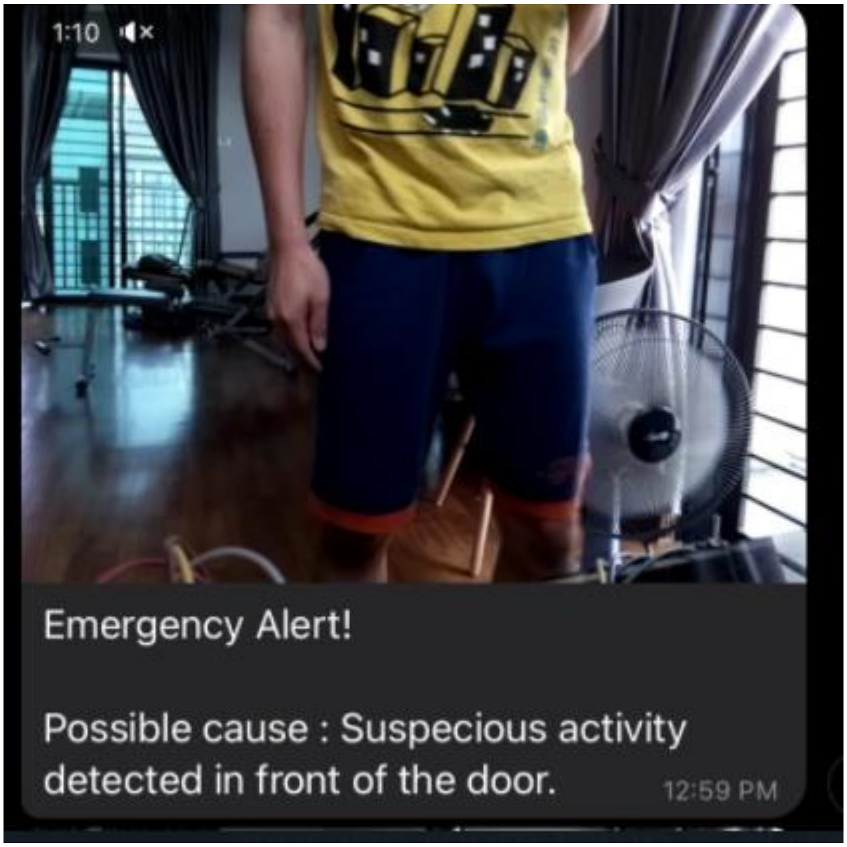
System B

Appendix B: Telegram notifications



You've attempted to deactivate the system at November 2, 2020 at 04:08PM.
2FA code: [4, 1, 6, 4]
Do not disclose this code to anyone.

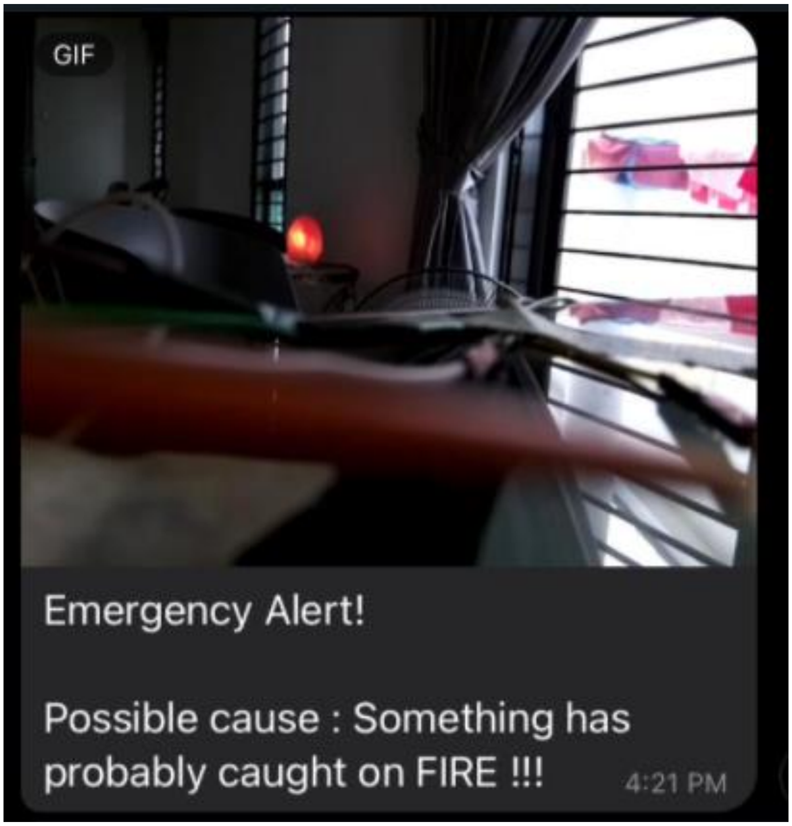
2FA notification



Emergency Alert!

Possible cause : Suspecious activity detected in front of the door.

Video alert for suspicious activities

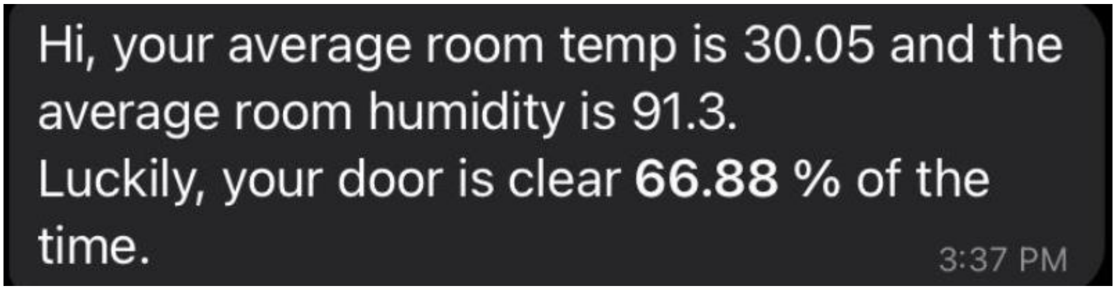


Emergency Alert!

Possible cause : Something has probably caught on FIRE !!!

4:21 PM

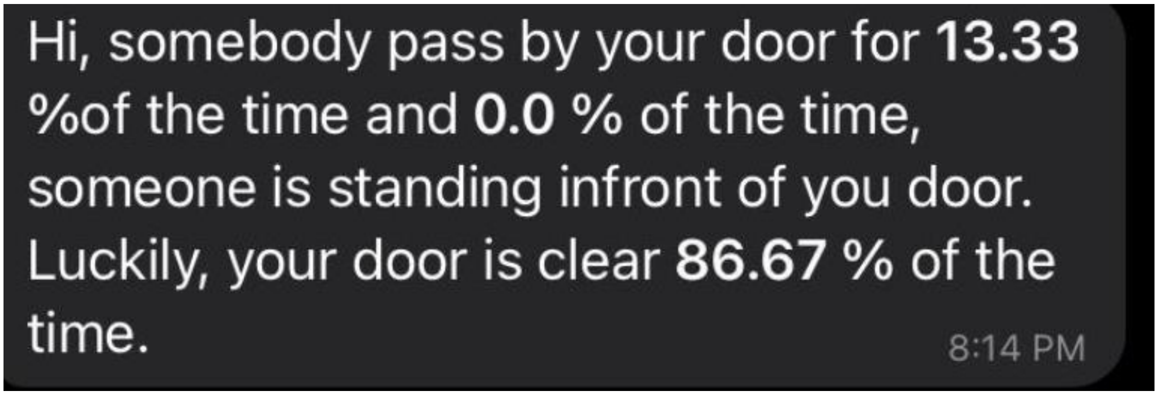
Video alert for possible fire detection



Hi, your average room temp is 30.05 and the average room humidity is 91.3.
Luckily, your door is clear **66.88** % of the time.

3:37 PM

Telegram message for room temp and humidity



Hi, somebody pass by your door for **13.33** %of the time and **0.0** % of the time, someone is standing infront of you door.
Luckily, your door is clear **86.67** % of the time.

8:14 PM

Telegram message for motion updates

Reflection Summary

Self-Reflection for Clifton Mak (29439701)

Throughout the working of this project, I was involved in a few activities. I was first involved in the conversion of H264 video format to MP4 format. The webhook service only accepted videos with the mp4 format and therefore requiring the subprocess library for conversion. I also assisted in the data collection and machine learning algorithm. Different motion data was collected before analyzing which machine learning model was the best. The machine model will predict suspicious movements before recording the video and sending it to telegram. Furthermore, I also helped in coming up with the algorithm and assisted with the coding of the encryption and decryption algorithm of the user's credentials and excel sheet data. I also involved myself in the debugging of codes and algorithm for activities 1,2,4 and 5. When it came to integration of all the subsystems, everybody's contribution was involved. For the report, I worked with Lim Wei Jun to complete the results and analysis section and the feasibility evaluation with cost benefit analysis.

In terms of communication and commitment, I attended every meeting/discussion on Zoom or WhatsApp. To communicate more effectively, I made sure to research my ideas first before entering any discussion with teammates. Any ideas proposed by my teammates was always considered and thoroughly analyzed together to determine the suitability of implementation. Deadlines were always reminded, and positive motivation was also provided to my teammates to ensure completion of work.

Self-Reflection for Chew Lik Siang (29035058)

At the beginning of the project, I first started to draft out an overview of the whole project structure by listing out some of the possible subsystem. This draft becomes sort of a masterplan to refer to throughout the whole project process. To make our design to stand out from the others, I have reviewed some products that are available in the market and proposed to include some interesting features such as the second factor authentication authorization as well as the QR code scanning function in our project. Moreover, I have mainly contributed to connecting our security system to the Internet by setting up Webhooks in IFTTT. This includes establishing FileStack connection as well as setting up the algorithm to produce a random generated code to be sent as the 2FA to the user through Telegram. On the other hand, I have also worked on drawing out the flowchart for the whole system to help explaining the overall structure of the system in the report.

In terms of communication and commitment, I have attended every single meeting. To establish a healthy discussion environment in the team, I am always open to any constructive suggestions even if they could be contradicting with my own. I believe that there is no absolute answer in a design question and every option is a possible solution as long as it is justifiable. Normally, I will help to summarize the result after a long discussion and give a clear conclusion on what should be done.

Self-Reflection for Jolene Ong (29592038)

At the beginning and planning phase of the project, my team and I had several discussions to brainstorm ideas to be implemented for the project. During these discussions, I would voice out my opinions and discuss further with my team in order to come up with the best approach to our problem statement. I have attended most of the online Zoom discussions with my team. In terms of contribution to the project, I was mainly tasked with the encryption and decryption algorithm for our security system. I managed to successfully implement an algorithm that enables our system to decrypt the data excel file that has been encrypted by a combination of Caesar Cipher, Substitution Cipher, and also Transposition Cipher. Alongside that, I helped out the team to debug and solve coding errors that have been faced along the entire process of the project. I also participated in the process of the integration of several subsystems along with the whole team at the final phases of completing this project. For the report, I have mainly worked on the abstract, introduction, literature review and some explanation parts in the methodology section.

Overall, I have gained a further appreciation for IoT systems and how it can be integrated with different subsystems to create a fully-functioning model. My team was very helpful in terms of providing positive support to each other throughout the entire process. We would remind each other of completion deadlines, and worked together to come out with solutions when any team member faced difficulty.

Self-Reflection for Lim Wei Jun (29036348)

At the start of the project, we all discuss and plan out the features that we are going to implemented into the smart door system. Then, I was involved in producing the codes for collecting data from the ultrasonic sensors for the use in training the machine learning algorithm later on as one of the main features in the smart door system. Then after interpreting the data collected by my teammates some fine tuning was made and we choose on using the decision tree classifier later on. When my teammates were collecting data for the machine learning algorithm, I was working on the codes to produce the Graphical User Interface (GUI) used by the smart door system. The design of it is meant to be simple and able the provide feedback on the current process that the smart door system is working on. Besides, I also participated in debugging the codes for the encryption and decryption algorithm for the excel file and finally merge the whole subsystem into the main codes. As for the report, I was involved in producing the results and analysis, cost benefit analysis and conclusion. In terms of the communications and commitment, I attended most of the meeting on Zoom. Our team uses platform such as Google Drive, Zoom and Whatsapp to smoothen our communication process. Our team will frequently remind each other on the task has to be done to make sure that we are able to complete the project before the deadline. Any suggestion and discussion will be considered by each on the teammates and try to google to find the possible solutions. If there is any doubt on the project our team will also try to consult with the lecturer, Dr Joanne.