Progress in Engineering Application and Technology Vol. 4 No. 1 (2023) 459-467

PEAT

Homepage: http://penerbit.uthm.edu.my/periodicals/index.php/peat
e-ISSN : 2773-5303

IoT Application for the Development of Home Security Systems

Mah Yuenn Wen[1], Mohd Hezri Mokhtar[1]*

[1]Department Electronic Engineering Technology, Faculty of Engineering Technology,
Universiti Tun Hussein Onn Malaysia, 84600 Pagoh, Johor, MALAYSIA

*Corresponding Author Designation

DOI: https://doi.org/10.30880/peat.2023.04.01.048
Received 10 January 2023; Accepted 8 February 2023; Available online 8 February 2023

Abstract: With the rise of house-break-in cases as it becomes common in our daily life, the home security system acts as an important tool for keeping our safety and security. This project aims to develop a home security system with a combination of several locking systems with a notifications system through an IoT application. In this project, the home security system has two layers of authorization: (1) an RFID system and (2) a Digital System. For the locking system, RC522 was chosen as an RFID reader and a 4x4 Matrix Keypad was chosen as the digital input for the locking system, then they will interface with Arduino Mega 2560. For the notification and alert systems, ESP32 Cam was chosen to capture the photo and upload it to Google Drive while the LDR sensor module was chosen as the data input for the activation ESP32 Cam. If the RFID tag or password is unsuccessful, the yellow LED will turn on for the LDR sensor to detect then ESP32 Cam will capture a photo. When the folder of Google Drive updates a photo, the IFTTT bot in Telegram will send an alert message with a photo to users. The alert message with photos can help decrease the crime rate and help police offices to identify unauthorized persons more efficiently.

Keywords: Iot, Home Security System, RFID, Locking System, IFTTT Bot

1. Introduction

According to the crime statistics publication 2021 of the Malaysian Government. There is 14.9 % of cases of house break-ins and thief happen in Malaysia[1]. Nowadays, the Internet of Things (IoT) has very commonly been used in our daily life. With the help of IoT, home security systems can be improved. Home Security System is one of the systems that included security hardware and it was invented by Marie Van Brittan Brown [2]. According to the research, about 60% of burglars indicated the presence of an alarm that might cause them to seek an alternative target altogether. But with these statistics, only 17% of households were equipped with home security systems. A study at UNC Charlotte concluded that burglars commonly do not break in if there is alarm system is installed [3].

Corresponding author: hezri@uthm.edu.my

Based on previous studies, most security systems are developed using RFID technology and digital systems [4][5]. Some security systems have developed a system that requires an OTP for entering [6][7]. While some of the projects are to develop a system that can send an alert message and control the locking system through an application on a mobile phone [8][9].

For this project, a home security system using an IoT application is developed that will help users to use a more secure home security system. In general, home security work in solenoid lock which is not so secure. A keyless door lock using RFID and a digital keypad lock is proposed in this work to solve the problem. Most of the burglaries targeted residential areas with only simple solenoid locks. The RFID lock system can only detect users with tags or cards in certain areas. If out of the range of the area, the lock will not be detected. Thus, the lock system also contains a digital lock system that works with Keypad and Arduino Mega 2560 microcontroller. If an unauthorized entry, ESP32 Cam will directly take the photo and send it to Google Drive, the user will be received the photo message from the IFTTT bot in the Telegram Application.

This project aims to help protect our safety and security. The other purpose of this project is to help decrease the rate of house break-in cases to produce safe and harmonious neighborhoods. With the help of IoT technology, it can help all users take note of the alert message from time to time.

This project's objectives are to design a home security system with a combination of several unlocking systems and to develop a system that includes the features of sending an alert message with a photo to a mobile phone. Due to the prototype being needed, the functionality of the prototype is needed to test.

2. Materials and Methods

The material and method of this project are based on the previous project studied which corresponds to the components that are needed. Based on the objective of this project is to design and develop a system with a combination of several unlocking systems that includes the features of sending an alert message using an IoT application to a mobile phone.

2.1 Materials

The main electronic components that are used in this project are Arduino Mega 2560 and ESP32 Cam. The rest are listed below in Table 1.

Table 1: The list of components

List of Components	
- RFID-RC522	- I2C LCD
- 4x4 Matrix Keypad	- LDR Sensor Module
- 12V Solenoid Lock	- LEDs
- Buzzer	- 5V Relay Single Channel
- 12 V adapter	- NodeMCU ESP8266
- 220-ohms Resistor	

2.2 Procedure

The creation of this project begins after a thorough examination of prior projects as well as the selection and acquisition of appropriate components. The technique used to evaluate this project is based on the System Development Life Cycle (SDLC). The system block diagram and system flowchart will be produced as guidance for the project execution throughout the project process.

2.2.1 System Block Diagram

The details of the system block diagram (refer to Figure 1(a) and Figure 1(b)). Arduino Mega 2560 is the microcontroller for the locking system (refer to Figure 1(a)). The power supply is connected to the microcontroller. For the first authorization part, the RFID reader is connected to read the RFID tag. For the second authorization part, a 4x4 Matrix Keypad is connected as the digital input for keying the password. Thus, the LEDs and LCD are connected as the output to display the status of the locking system. There are 3 LEDs connected: Red LED for showing the door is locked or unsuccessful authorized, Green LED for showing the door is open and Yellow LED for activating the alert system. Yellow LED is the output for unauthorized entry, it will be the data input for the LDR sensor to detect the light for activating ESP32 Cam. Next, 12 V of the solenoid lock is connected to the relay for controlling the lock system.

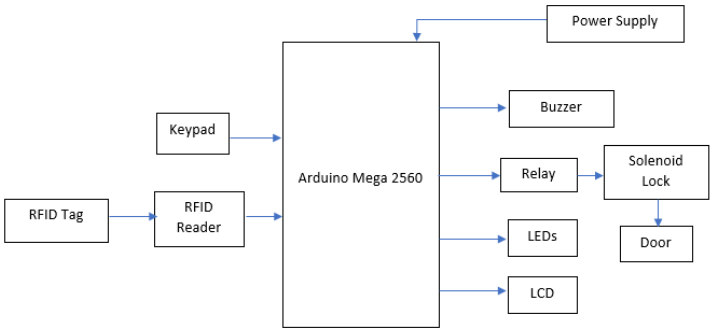


Figure 1(a): Locking System

For the alert and notification part (refer to Figure 1(b)), ESP32 Cam is the microcontroller for sending notifications through the Telegram Application. Due to ESP32 Cam does not have a USB port, NodeMCU ESP8266 was chosen as the USB port for uploading code. While the LDR sensor module is the data input for activating ESP32 Cam. Once the ESP32 Cam is connected to Wi-Fi then it is ready for capturing a photo.

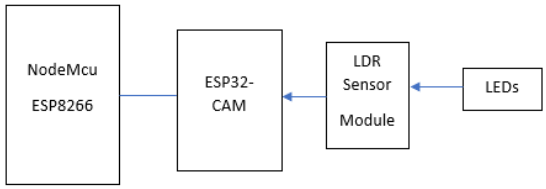
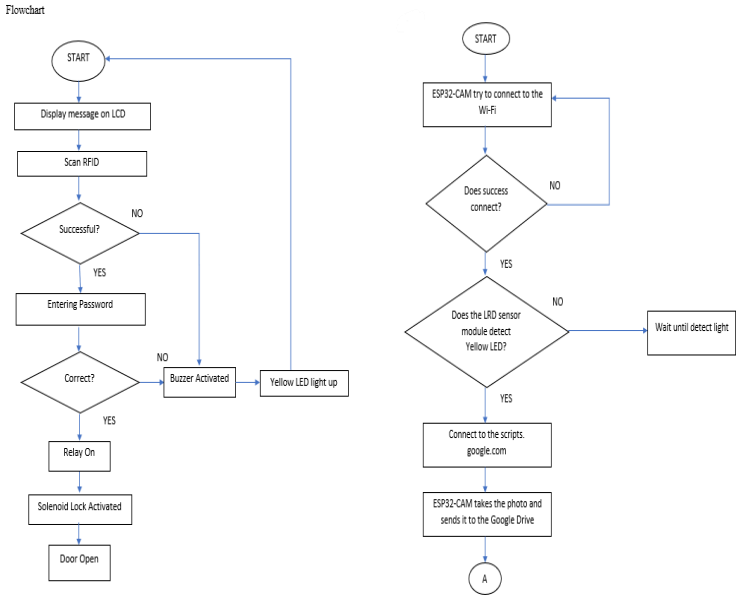


Figure 1(b): IoT and notification System

2.2.2 System Flowchart

The program will start with initializing all connected components (refer to Figure 2(a)). For the first layer of authorization, the interrogator read the RFID tag. If successfully read the RFID tag, Green LED will be turned on and LCD will display the welcome message then proceed to the next layer of authorization. The second layer of authorization is required to enter the password, if the correct password is entered the Green LED and relay will be turned on then LCD will display the welcome message. On the other hand, if the wrong password is entered or the wrong tag has been scanned, the buzzer, Red LED and Yellow LED will be turned on and the alert message with a photo will send out. This system will continuously be running if there is power supplied to the system.

ESP32 Cam will start to connect to Wi-Fi, then will standby waiting for the LDR sensor to detect the Yellow LED's light (refer to Figure 2(b)). If the light is detected, it will connect to the script waiting for the connection to be successful. If successfully connected, ESP32 Cam will capture the photo and send it to Google Drive. Then, it will continue to proceed to process A (refer to Figure 3).



(a) **(b)**

Figure 2: System Flowchart (a) Arduino Mega 2560 (b) ESP32 Cam

The process of sending an alert message with a photo using the IFTTT platform (refer to Figure 3). After the process of creating Applets for connection between Google Drive and the Telegram Application, the ESP32 Cam captured the photo and uploaded it to the folder of Google Drive. When the folder "ESP32-CAM" in Google Drive receives a new photo, the IFTTT bot will automatically send the photo to the user in the Telegram Application. The process of creating a web app to automatically upload photos to Google Drive's folder using Google Apps Scripts (refer to Figure 4).

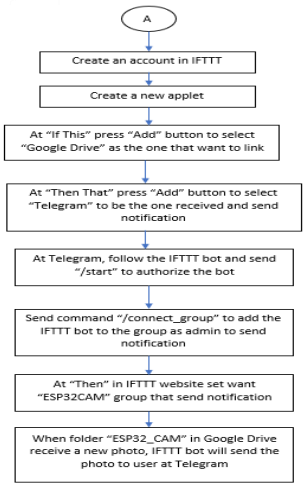


Figure 3: The process of sending an alert message with a photo

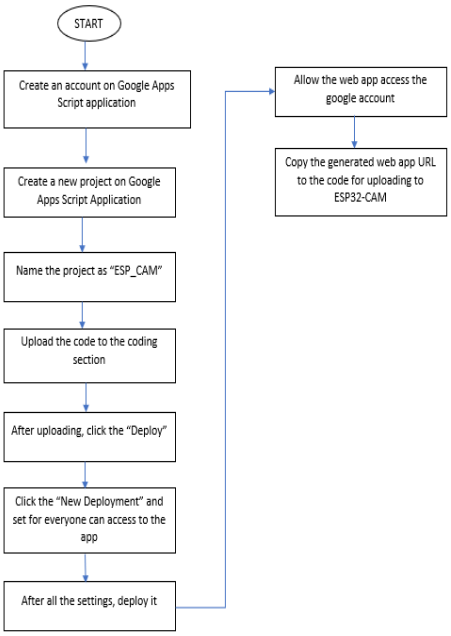


Figure 4: Process of Creating Webapp in Google Apps Script

3. Results and Discussion

This section discusses the results obtained from the tests that have been carried out. The prototype and hardware have been successfully built and developed; the analysis has been done to discuss these components' functionality. The experiments and troubleshooting for this system are discussed in an orderly. The result of the whole hardware prototype (refer to Figure 5). The details of the prototype will be discussed in the below subtopics.

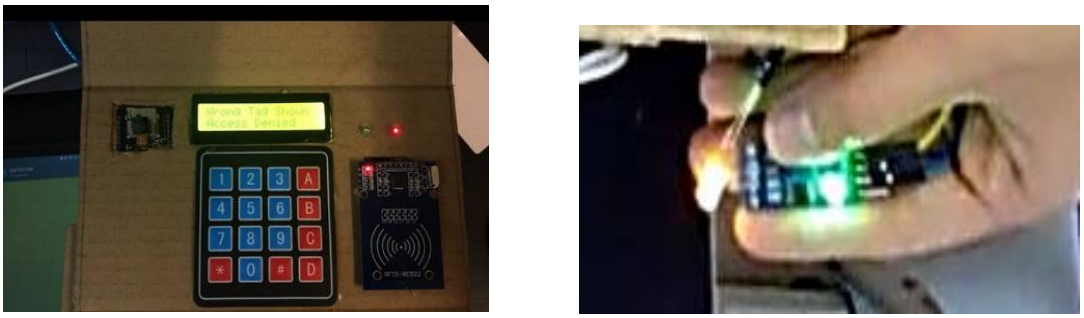
Figure 5: Hardware Prototype

3.1 Results

3.1.1 First Level of Authorization: RFID System

For this first level of authorization, the Arduino Mega will be in charge of the microcontroller for this system. RC522 was chosen as the RFID system and formed by RFID tags and a reader. When the reader reads the right tag, the user can proceed to the second authorization level (refer to Figure 6). On the other hand, when the reader reads the wrong tag, the alert system will be activated. The Red LED and buzzer will be turned on, Yellow LED will be turned on as the input of the LDR sensor to activate the ESP32 Cam for capturing photos (refer to Figure 7(a) and Figure 7(b)).

Figure 6: Pass accepted readily proceed to the second level authorization

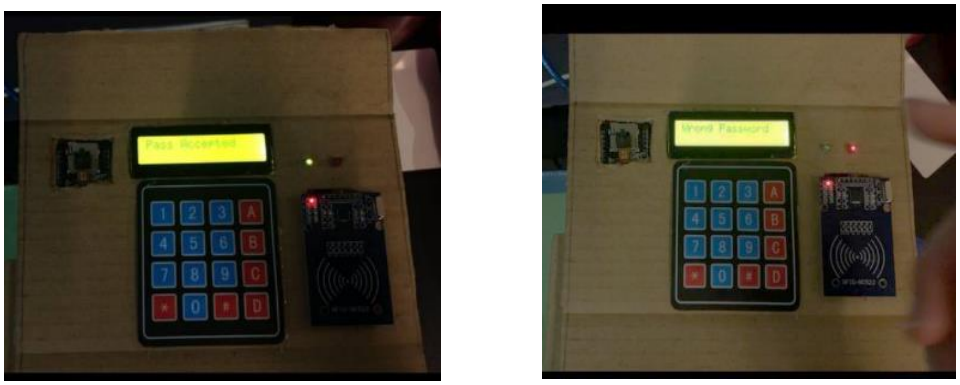


(a) **(b)**

Figure 7(a) Denied message display on LCD, Red LED and buzzer are turned on
(b) Yellow LED turned on as input for the LDR sensor module when unauthorized entry

3.1.2 Second Level of Authorization: Digital Lock System

The second level of authorization is formed by a 4x4 Matrix Keypad. When the user has passed through the first authorization level, they need to enter the password to unlock the door. The activation of the solenoid lock when entering the correct password (refer to Figure 8(a)). The result of entering the wrong password and activating the alert system (refer to Figure 8(b)).



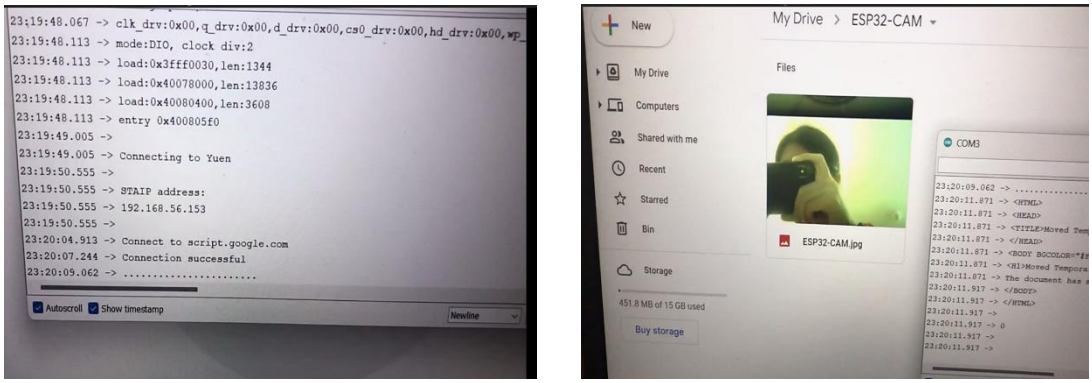
(a) **(b)**

Figure 8: (a) Pass Accepted (b) Wrong Password Entered

3.1.3 Alert System and IoT Application System

For this IoT Application and alert system part, ESP32 Cam was chosen as the microcontroller to receive the signal from the LDR sensor module. When there is an unauthorized entry, the LDR sensor will detect the Yellow LED (refer to Figure 7(b)). First, ESP32 Cam will be connected to Wi-Fi and be ready for activation. When the ESP32 Cam is activated, the photo will be captured and sent to the

Google Drive folder name “ESP32-CAM” (refer to Figure 9(a) and Figure 9(b)). While the IFTTT platform was chosen as Applets for the connection between the Google Drive folder and the Telegram Application. When there is a new photo that has been updated on the ESP32-CAM folder, the IFTTT bot will send a message with the photo to the user through the Telegram Application (refer to Figure 10).



(a) **(b)**

Figure 9: (a) ESP32 Cam is connected to Wi-Fi and is activated (b) The photo captured is updated to the ESP32-CAM folder in Google Drive

Figure 10: IFTTT bot sends the alert message with the photo that updated through Telegram

3.2 Tables of Functionality Tests

The functionality tests and troubleshooting for this project will be discussed in this section. There are 5 tests that have been done to make sure all the components can run smoothly. The functionality of every component involved in this project was listed below in Table 2 and Table 3.

Table 2: The Functionality of All Components that Connected with Arduino Mega 2560

Number of experiments	LCD	Red LED	Green LED	Yellow LED	Buzzer	Relay	Solenoid Lock	RC522	Keypad
1	Off	On	On	On	Off	Off	Off	Off	On
2	On	On	On	On	On	Off	Off	On	On
3	On	On	On	On	On	On	On	On	On
4	On	On	On	On	On	On	On	On	On
5	On	On	On	On	On	On	On	On	On

Table 2 shows the experiments that were carried out to test the functionality of the component that connected with Arduino Mega 2560 after hardware installation had been carried out. For the first experiment, the locking system failed to work. The LCD failed to display the message and RC522 failed to read the tag. Thus, the Relay failed to function when there is an authorized entry. Buzzer also fails to function when there is an unauthorized entry. For the second experiment, the LCD can display the message and the buzzer can function as expected. After the second times of experiment is being carried out, problem-solving has also been applied so far, the prototype can function as expected.

Table 3: The Functionality of All Components that Connected with ESP32 Cam

Number of experiments	ESP32 Cam	LDR Sensor Module	Google Drive	Telegram (IFTTT bot)
1	Off	On	Fail	Fail
2	On	On	Fail	Fail
3	On	On	Success	Fail
4	On	On	Success	Success
5	On	On	Success	Success

Table 3 shows the experiments that have been carried out to test the functionality of the components that connected with ESP32 Cam after hardware installation. In the first experiment, ESP32 Cam failed to connect to the Wi-Fi due to poor networking, so uploading photos to the Google Drive folder failed, and sending an alert message with a photo through Telegram also not functioning as expected. In the second experiment, ESP32 Cam successfully connected to the Wi-Fi and sent photos to Google Drive failed due to a mistake in coding. So, the Telegram bot will not function when there is no updated photo in the Google Drive folder. In the third experiment, the photos can upload to Google Drive, but the Telegram bot is not functioning due to the communication between Telegram Application and Google Drive. After solving all the problems, the fourth and fifth times of experiments are carried out to make sure the prototypes of sending an alert message can function as expected.

3.3 Discussion

The result of the functionality of this prototype is obtained through the experimental work to ensure the final prototype can be functional as expected and no malfunction happened at the end of the project. The problem encountered when making the first experiment for the installation of hardware was that the LCD could not display the message due to the wrong address of the LCD being written in the code. Therefore, the identifying address of the LCD is needed. The buzzer was not able to turn on due to the connection between the buzzer and Arduino Mega 2560. While the relay is also not able to turn on due to the soldering connection problem. The solenoid lock is connected to the relay. When the relay is not functioning then the solenoid lock also fails to function. So, checking for the connection should be done before starting to experiment with the functionality.

For the IoT application and alert system part, in experiment 1 the ESP32 Cam failed to connect to Wi-Fi so it is unable to send the photo to Google Drive. Before starting the second experiment, the problem of connecting Wi-Fi must be modified. The problem of failure to send photos when ESP32 Cam has captured the photo happens due to the coding that wrote in Google Apps Scripts. For the second experiment, the failure of sending an alert message with a photo through Telegram by IFTTT bot due to the communication between Google Drive and Telegram in the IFTTT Applets. The modifying of the coding that wrote in Google Apps Scripts must be carried out to let the functionality of sending photos to the Google Drive folder and the IFTTT bot can send the alert message with a photo to the user through the Telegram Application.

4. Conclusion

In conclusion, this project aims to develop a home security system that contains multiple lock systems and users can receive the alert message with photos from time to time through the Telegram Application which is more crucial for personal and variable safety. Based on the findings, the home security system with two layers of authorization, notification, and alert system using IoT Application are successfully developed. The alert message with photos can help users to know the status of the security system from time to time.

In the future, this project can be improved by adding the features of biometric recognition such as face recognition or sound recognition to unlock. Last, the function of monitoring and controlling the locking system using IoT system applications by a given command also can be added to this project for more user-friendliness and security.

Acknowledgment

The authors would like to thank the Faculty of Engineering Technology, Universiti Tun Hussein Onn Malaysia for its support.

References

[1] S. A. Indicators, "Prime Minister ' S Department Department of Statistics Malaysia Press Release," no. November, pp. 2019–2022, 2021.

[2] M. Van Brittan and B. October, "Marie Van Brittan Brown (1922-1999) •," p. 38707, 1999, [Online]. Available: https://www.blackpast.org/african-american-history/brown-marie-van-brittan-1922-1999/

[3] U. Decisions, T. O. Burglarize, and F. The, "The University of North Carolina at Charlotte Department of Criminal Justice & Criminology PERSPECTIVE," no. December, pp. 1–64, 2012.

[4] H. Myint and M. Z. Tun, "Secure Door Control System using RFID Card," *Int. J. Adv. Sci. Res. Eng.*, vol. 06, no. 04, pp. 69–73, 2020, doi: 10.31695/ijasre.2020.33787.

[5] S. Mohammed and A. H. Alkeelani, "Locker Security System Using Keypad and RFID," *Proc. 2019 Int. Conf. Comput. Sci. Renew. Energies, ICCSRE 2019*, no. July 2019, pp. 1–5, 2019, doi: 10.1109/ICCSRE.2019.8807588.

[6] A.Hemalatha;G.Gandhimathi, "Password Based Door Lock System using 8051 Microcontroller," *Electron. Hub*, vol. 7, no. 11, pp. 1–5, 2017, [Online]. Available: https://www.electronicshub.org/password-based-door-lock-system-using-8051-microcontroller/

[7] S. A. Prity, J. Afrose, and M. M. Hasan, "RFID Based Smart Door Lock Security System," *Am. J. Sci. Eng. Res.*, vol. 4, no. 3, pp. 162–168, 2021, [Online]. Available: www.iarjournals.com

[8] F. yusuf aji Cahyono, N. Suharto, and L. D. Mustafa, "Design and Build a Home Security System based on an ESP32 Cam Microcontroller with Telegram Notification," *J. Jartel J. Jar. Telekomun.*, vol. 12, no. 2, pp. 58–64, 2022, doi: 10.33795/jartel.v12i2.296.

[9] A. Singh *et al.*, "IOT BASED SMART LOCK," *Int. Res. J. Mod. Eng. Technol. Sci.*, pp. 2582–5208, Accessed: Dec. 25, 2022. [Online]. Available: www.irjmets.com