

Home Surveillance with Encrypted Video Data

Siti Nur Aisyah Abdul Hei¹, Mohd Azahari Mohd Yusof^{1*}

¹Fakulti Sains Komputer dan Teknologi Maklumat,
Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, 86400, MALAYSIA

DOI: <https://doi.org/10.30880/aitcs.2023.04.02.005>

Received 21 August 2023; Accepted 06 November 2023; Available online 30 November 2023

Abstract: Home surveillance with encrypted video data focuses on helping to solve the problems of people's insecurity about their home security when leaving it for a long time. The open-source mobile application and unprotected video data was also a problem that needed to be solved. In this paper a home surveillance with movement detection sensors is proposed. Subsequently, developing a secure application system that comes with notification features to control the problem is discussed in this report. The method used is on a house prototype by combining the sensors and connection with application which has several security elements. It had a good result and achieve the expected objectives for both the sensors and the application's security features in terms of its efficiency. Along with the Internet of Things (IoT), the home surveillance system functions worked as expected and the user can receive real-time situation notifications about their house.

Keywords: IoT, Security, Sensor, Home Surveillance

1. Introduction

Thieves are increasingly breaking into houses with no home surveillance. The owner has previously taken steps to safeguard their property, but thieves may determine if the owner is now travelling elsewhere for an extended time or not by studying the house's circumstances. Moreover, the owner is unable to learn about any occurrence that occurred in real time. Furthermore, the security of some applications or systems, particularly those associated with the automation controller that controls the home security system, is inadequate and not secure. On top of that, the installed Closed-circuit Television (CCTV) might be hacked by the attacker [1]. This will cause a huge problem for the user because, at that moment, the security system that was applied to their house was not reliable anymore.

Therefore, a project called Home Surveillance with Encrypted Video Data was proposed to cater for the problem stated by using Internet of Things (IoT) technology. The objectives of the project are to develop an Arduino prototype of secure home surveillance by using the movement sensor and camera module together with a secured mobile application called Link Home will be developed too that can connect with the system and receive a notification. This project is divided into five scopes; the study domain is related to the home surveillance system by using IoT and secure applications with security elements, the case study location will be based on a house prototype, the individuals involved are the

*Corresponding author: mdazahari@uthm.edu.my

homeowners and the tenant, the user list for this project are admin and regulars users and two main modules which are IoT and Application. This project focused on using the Arduino with movement sensors and a camera module that will be connected to a secure mobile application. The significance of this project is assisting homeowners in tracking their home security with the help of movement and video sensors and easing homeowners' concerns by allowing them to control the sensor from their phone via a secure app, particularly for encrypted [2] video data.

The rest of the paper is organized as follows: Section 2 discusses the literature review of the related work and existing applications. The methodology used to develop the application including the analysis and design is described in Section 3. Followed by section 4 which discusses the analysis results of the user acceptance test. Finally, the last section concludes the work and highlights the possible future improvement of the application.

2. Related Work

2.1 Home Surveillance

Home is a location where humans may be safe from danger, poor weather, and sleep. A security system protects a home or building from invaders by protecting its interior and entrance points, such as doors and windows and basement windows [3]. With the use of surveillance technology, homeowners may actively prevent home invasions. One sort of surveillance for homes is Wireless Security System is a cellular network that wireless security system components utilise to communicate with the control panel. A wireless security system is easier to install and adjust than a wired security system. However, network interference and outages can hinder the functioning of a wireless security system, and because it is powered by batteries, users may lose power if they do not change them on a regular basis [3].

2.2 Internet of Things

The Internet of Things (IoT) is a vast network of interconnected people and things that gather and exchange data about their interactions with one another and their surroundings [4]. It can range from a wristband that monitors people's heart rates and the number of steps they've taken that day to a device that monitors how far and how quickly they are thrown. Several IoT tools, including the Arduino UNO R3, Ultrasonic Sensor, PIR Sensor, ESP-32 Camera Module, and NodeMCU, are required to develop the prototype for the proposed system. These tools will be used to construct the prototype in accordance with the plan and to meet the project's goal.

2.3 Comparison of the Existing System with the proposed system

Table 1 shows the comparison of three existing systems together with the proposed system. Its purpose is to ensure that the previously mentioned features can be implemented or that the proposed system can be improved.

The comparison of the three current systems with the proposed system is shown in Table 1. All of the systems in the table are IoT-based, and the microcontrollers utilised are Arduino UNO in systems 1 and the proposed system, and Raspberry Pi in systems 2 and 3. For the following feature, both system 1 and the proposed system use a mobile application; however, system 2 uses a web application, while system 3 does not. Both system 2 and the proposed system employ MYSQL for their databases, whereas system 1 uses Google Firebase, system 2 with the inclusion of CV, and system 3 uses Dropbox cloud storage. Next, the suggested system contains the characteristics register, login, and data encryption, but none of the other systems does. System 1 includes password management, whereas the proposed system includes password hashing. However, neither System 2 nor System 3 has a password function. All four systems can take an image snapshot, and for notification, system 1 utilised SMS, while system 2 used both SMS and alarm calls. System 3 made use of both SMS and email, whereas the suggested system made use of application notifications.

Table 1: Comparison system

Function	A Real-Time Controlled Loop Home Android using Firebase [5]	IoT Based Surveillance using	Smart Automation Raspberry using IoT [6]	Home with Pi	Smart Indoor Surveillance Monitoring Using Raspberry [7]	Home System Pi	Home Surveillance with Encrypted Video Data (Proposed System)
IoT Based	Yes		Yes		Yes		Yes
Microcontroller	Arduino UNO		Raspberry Pi		Raspberry Pi		Arduino UNO
Application	Mobile		Web		No Application		Mobile
Database	Google Firebase		MYSQL		Dropbox Cloud		MYSQL
Register & Login	No		No		No		Yes
Data Encryption	No		No		No		Yes
Password	Password Management		No		No		Password hashing
Snapshot Picture	Yes		Yes		Yes		Yes
Notification	SMS		SMS & Call	Alarm	Email & SMS		Application

3. Methodology/Framework

The methodology used for this project is prototyping [8]. The prototype will be built, tested, and reworked when needed until an acceptable prototype is achieved by using this methodology. Figure 1 shows the framework of the prototype model and details of the process are explained in the next section.

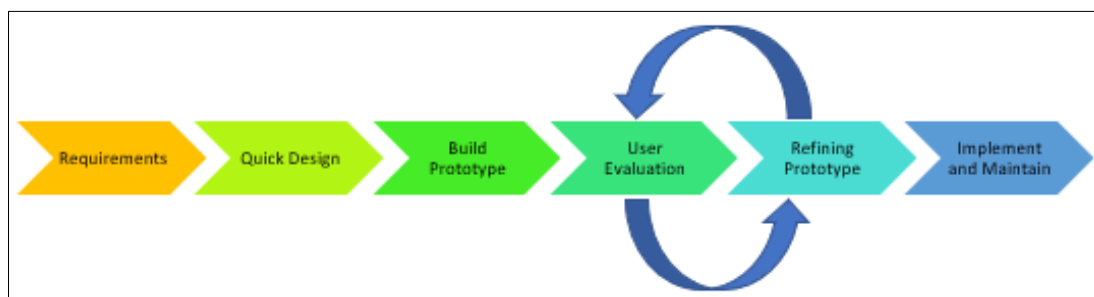


Figure 1: Project Methodology Framework Phases.

3.1 Requirement Gathering and Analysis

The first step in this phase is to build a project plan in Microsoft Excel using a Gantt Chart to assure the success of this project and that the total time necessary for all stages does not exceed the limit established for this final-year project. By utilising IoT and secure apps, the scope needs were identified as being further towards home monitoring systems. The homeowners and tenants were chosen as the targeted users in this phase. During this stage, a survey was issued to potential consumers to learn more about the specific difficulties. The Arduino UNO, ultrasonic sensor, PIR sensor, and camera module have been determined to be the needed components. The decided required software is the Arduino IDE for the sensors and Flutter for mobile application development.

3.2 Quick Design

This phase contributes to the development of the prototype. Throughout this phase, the drawings of the physical prototype model, technical layout or general system architecture, and mobile application user interface are planned out, and every aspect of the model is studied. This phase also includes database design to acquire a big picture of which data will be gathered later for this project. The Unified Modeling Language (UML) diagram will be used in all design documentation. Figure 2 depicts a drawing of the

physical prototype model which shows the idea of where the position of the ultrasonic sensor, PIR sensor, and camera will be placed at the house prototype later.

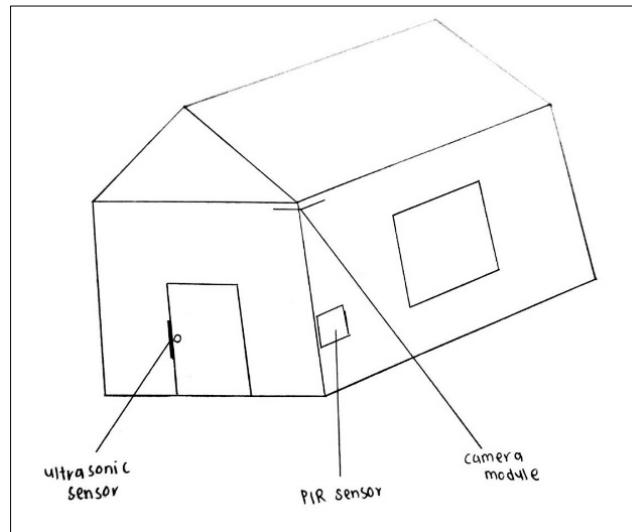


Figure 2: House prototype model sketch

Figure 3 depicts the overall system architecture schematic. The architecture shows the flow of how this project will be. A user will use a mobile application to start the process. The password entered by the user will be hashed and stored in the database. If the credential entered is matched with the data in the database, the user is considered an authorized user and can continue with the other activities in the mobile application. When the user powers on the prototype, the sensors in the Arduino will start to work. The camera module will be a surveillance video camera and the video will be encrypted. The movement modules will detect any movement and capture the video and images. The data will be encrypted and stored in the database. An alert and notifications will be sent to the user through the mobile application to alert the user.

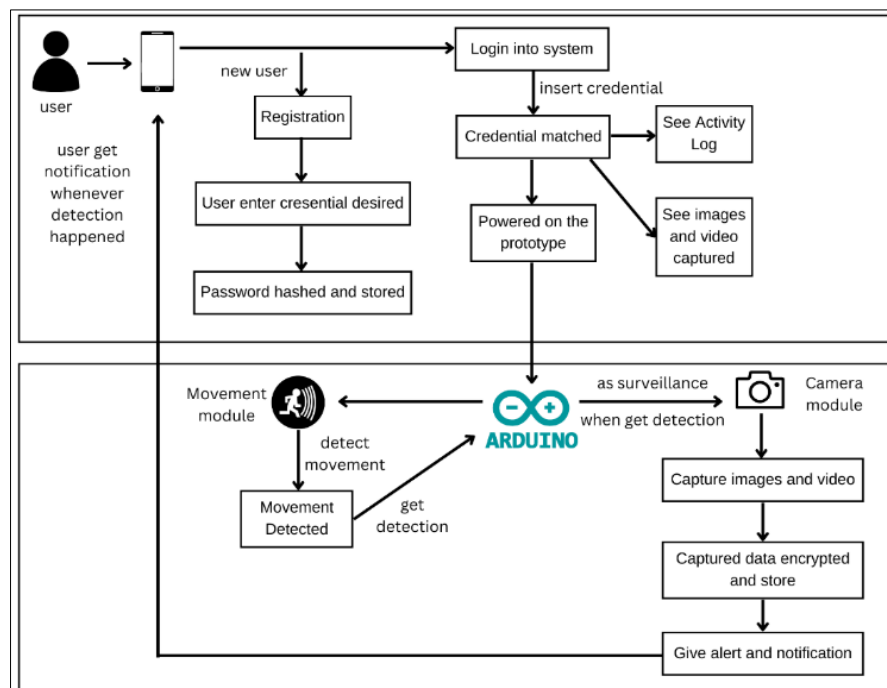


Figure 3: The sketch of the general system and application architecture for the project

Figure 4 shows the wireframe page for sensor control which has a button to start the sensor operation that was related to the IoT modules and the video stream page that is related to the ESP32-cam module video stream which consists of the video and a button to do a screenshot as a sample of the mobile user interface design. The rest of the designs are attached in Appendix A which is for the login and register page wireframe, Appendix B for the admin and user main page wireframe and Appendix C for the list of user and log data page wireframe.

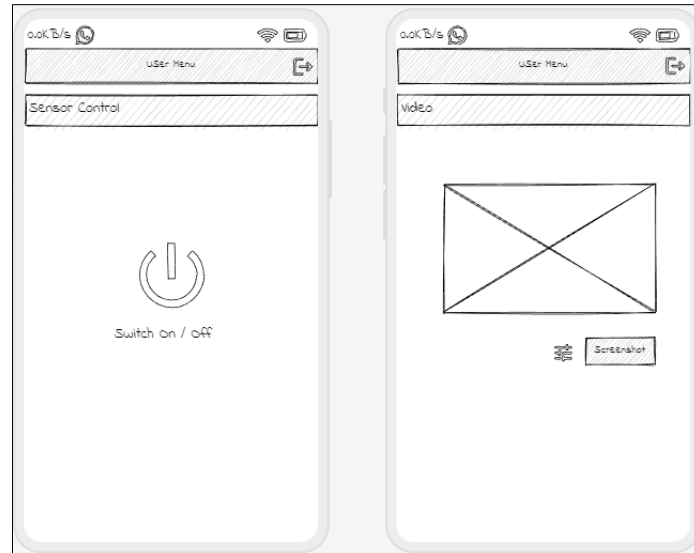


Figure 4: Operation and video page wireframe

Figure 5 shows the Entity Relationship Diagram (ERD) for the database design to give a means to fully understand how data is accepted into the table and the relationship between each table in the database. The database is made up of five tables: admin, user, operate, images, and log. Figure 6 shows the context diagram that shows the interaction between the user and admin as entities and the Link Home application. Data Flow Diagram (DFD) level 0 in this project shows how the information flows in the system between users, database and operations which are register users, login, operate sensor, save images and generate log activity. Appendix D contains the DFD level 0 for this project's mobile application. Appendix E and Appendix F contain the activity diagram flow for the regular user and for admin in Link Home mobile application.

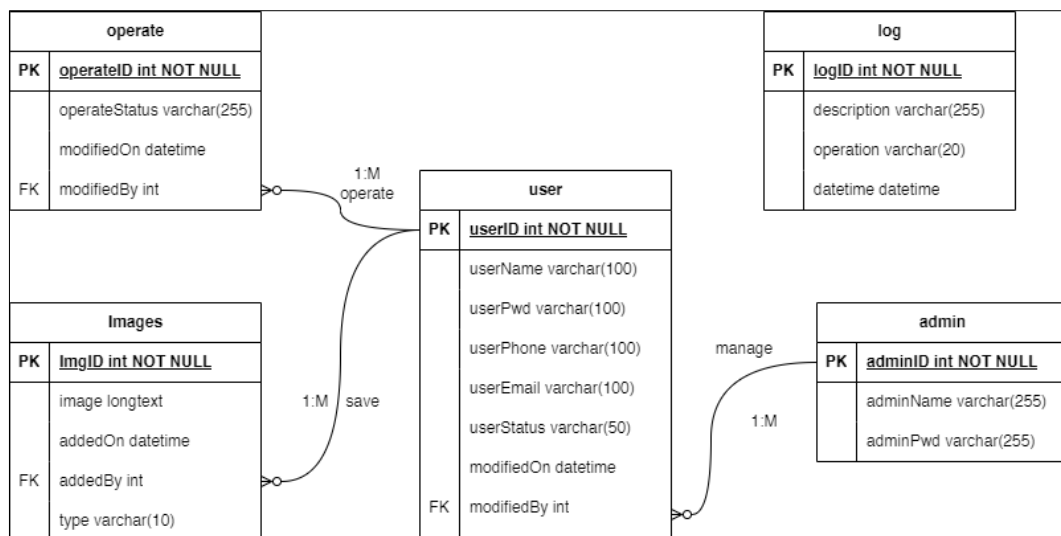


Figure 5: ERD for the proposed project

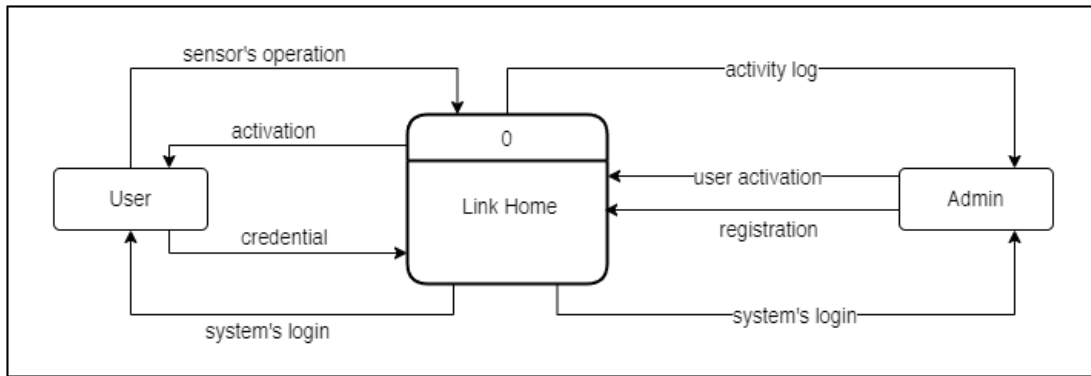


Figure 6: Context diagram of Link Home

3.3 Build Prototype

For this project, multiple parts of the prototype will need to be constructed and then connected one by one. Building a physical prototype, finishing the code for all sensors for the prototype, designing a mobile application, and integrating the security features are the components.

Physical prototype materials such as cardboard, glue, tape, paper, and anything else that might aid in the creation of the housing prototype are necessary. The sensors will then be wired together before being applied to the housing prototype. After completing the prototype model, the code for each component and the method for connecting it was researched online and updated in accordance with the project specifications. Then, using Flutter, a mobile application will be created. The mobile application design will be based on the user interface design, and all of the functionalities here will be tested and connected to the database. Finally, the most important thing to implement is the security element in the mobile application after all important modules are finished and developed.

3.4 User Evaluation

At this point, the completed project prototype model will begin to undergo testing to see how effectively it will perform before the initial evaluation. It is helpful to identify the prototype's advantages and disadvantages. This phase is used to determine whether or not all project components are functioning properly. A test plan is required to determine whether the proposed system's features functioned as planned. Table 2 demonstrates how the test plan will be put to the test based on the description and the expected results.

Table 2: Test Plan

Category	Description	Expected Results	Actual Results
Sensors	Ultrasonic sensor	Able to sense the distance of the door.	Pass/Fail
Sensors	PIR sensor	Able to detect movement.	Pass/Fail
Sensors	Camera module	Able to capture the video as CCTV.	Pass/Fail
Sensors	Connection	Able to connect between sensors and application	Pass/Fail
Application	Login	Able to enter and verify credentials.	Pass/Fail
Application	Register user	Able to enter details and added to the database.	Pass/Fail
Application	View activity log	Able to display the description and the timestamp.	Pass/Fail
Application	User Activation	Able to display and activate or inactivate the user.	Pass/Fail
Application	Start sensor operation	Able to connect with the sensors.	Pass/Fail
Application	Notification	Able to give notifications to users.	Pass/Fail
Application	Screenshot image from video	The video was shown and can screenshot the image.	Pass/Fail

After all of the modules have been tested, an evaluation will be produced based on how well the entire project's prototype is performing and whether or not the project's objectives have been met during the process. The project's prototype's strengths and weaknesses will then be highlighted in order to create a better prototype based on the test results. This phase will be performed once the prototype-refining process is completed to see if the prototype still requires improvement.

The test plan comprises not only the intended project functionality but also a security checklist test plan to determine whether the security elements introduced in the project functioned as expected. The security checklist consists of the checklist details shown in Table 3.

Table 3: Security checklist

No	Checklist	Actual Results
1.	Ensure the error message does not inform which part of the validation is incorrect.	Pass/Fail
2.	Ensure the password's strength.	Pass/Fail
3.	Password should be hashed in the database.	Pass/Fail
4.	Ensure private data such as user phone number and email address are encrypted in the database.	Pass/Fail
5.	Ensure all activity that happened through the system was listed in the log activity.	Pass/Fail
6.	Ensure video and images are encrypted and only the user can have the original data.	Pass/Fail

3.5 Refining Prototype

After the prototype had been built and reviewed, the next step was to eliminate the faults that had been detected during the previous stages. The prototype's strengths and shortcomings were found from the initial user assessment phase after testing and analysing user responses. Following the resolution of all concerns, the initial user review step will be carried out to identify any new issues or faults.

3.6 Implementation and Maintenance

During this phase, the project was significantly enhanced, and the system is frequently maintained and debugged to minimise downtime and prevent catastrophic failures. By testing the prototype, this phase will determine the project's usefulness and efficiency for both sensors and the application's security. This is to ensure that the final product is of the highest quality, that no modules fail, and that any problems can be handled effectively after the project is done.

4. Results and Discussion

The module implementation and the results of the testing that was done in two ways which are by using the test plan planned before and the user acceptance test (UAT) will be explained in the next section.

4.1 Module Implementation

There are twelve modules in this project which are the CCTV module, movement sensor module, locked door open sensor module, Wifi Transceiver module, password hashing module, data encryption module, login module, registration module, user activation module, log data module, notification module and video stream and screenshot module. The most important module among all of them is the Wifi transceiver module, data encryption module, notification module and video stream and screenshot module. Those modules will be explained in the next section.

4.1.1 Wifi Transceiver or Connection Module

The application needs a connection with the sensors from Arduino UNO to control it by switching on or switching it off. This module is about how the connection between the mobile application and the sensors by using the NodeMCU and Arduino UNO. The connection is by sending commands from the mobile application to NodeMCU and NodeMCU will send the message to Arduino UNO to start the sensors. Then, from Arduino UNO, it will send messages telling about any sense from the PIR sensor and Ultrasonic sensor to NodeMCU and then it will send to a mobile application to get the message about the sensor. Figure 7 shows the connection flow between the mobile application, NodeMCU and Arduino UNO.

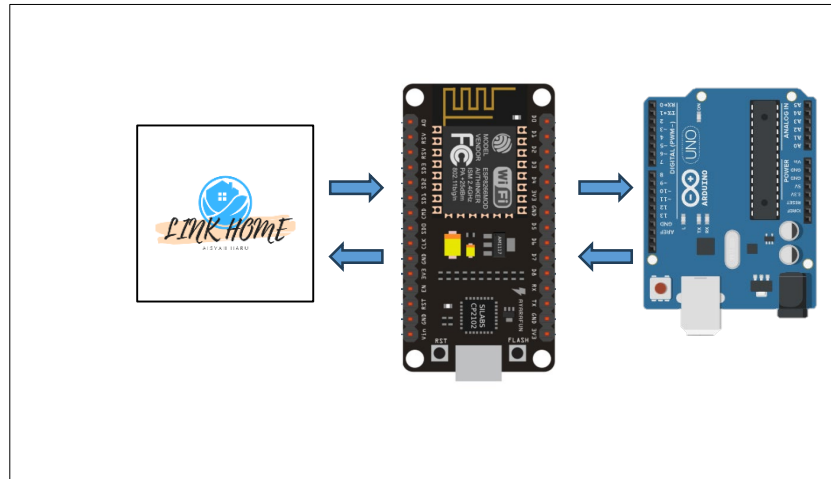


Figure 7: The connection flow between apps, NodeMCU and Arduino UNO

4.1.2 Data Encryption Module

Data encryption is added to this project to protect private data from being exposed in plain text form. The encryption method used for this project is AES using the openssl functions in PHP. Parameters such as encryption key, encryption vector, decryption key and decryption vector are needed to use the 'openssl_encrypt' and 'openssl_decrypt' functions. The purpose of this module is to encrypt the plain text in the database specifically for the data that can be considered private data such as mobile phone and email addresses. Figure 8 shows the code segment on how the encryption and decryption code was used in the PHP code.

```
$phoneEncrypt = openssl_encrypt($phone, $ciphering, $encryption_key, $options,
    $encryption_iv);
$phoneDecrypt = openssl_decrypt ($fetchData["userPhone"], $ciphering,
    $decryption_key, $options, $decryption_iv);
```

Figure 8: Encryption and decryption function in code

4.1.3 Notification module

This module is to alert the user about the current situation of the house. The notification started when the user click the button start on the operation page. The notification will state that the operation started at the mobile phone notification. Then, if a motion was detected from the PIR sensor, a notification stating 'Motion Detected' will be shown in the notification list on the mobile phone. When the door was opened unexpectedly sensed by an Ultrasonic sensor, the notification will state that the door was open, saying the current house condition is in danger. The same happened if the user clicks the button to switch off the sensors. The code for the notification is by using the local notification library in Flutter as shown in the code segment in Figure 9.

```
await notificationService.showLocalNotification(
  id: notiid++,
  title: 'Operation Started',
  body: 'The operation has started successfully.',
  payload: 'operation_started',
);
```

Figure 9: Notification code segment in Flutter

4.1.4 Video Stream and Screenshot Module

This module enables the user to watch the video stream and take a screenshot from a mobile application and save it into a database with encryption. It uses an 'in-app view' to get directly from the web view page by taking the IP address to get the video stream as shown in Figure 10. This module also connects the application to the PHP code for encryption and inserting for screenshot activities whenever the user clicks the screenshot button. The code for the connection to the PHP code is shown in Figure 11. The user interface for this module is shown in Figure 12.

```
child: InAppWebView(
  key: UniqueKey(), // Add this line
  initialUrlRequest: URLRequest( url:
Uri.parse('http://192.168.118.24:81/stream'),
  ),
  initialOptions: InAppWebViewGroupOptions(
    crossPlatform: InAppWebViewOptions(
      cacheEnabled: false,
      javaScriptEnabled: true,
    ),
  ),
  onWebViewCreated: (controller) {_webViewController = controller; },
  onLoadError: (controller, url, code, message) {
    setState() {
      _isError = true;
    });
    print('Error loading web page: $code, $message');
  },
),
```

Figure 10: Code segment to view video stream in the application

```
var id = test.id;
var url = "https://link-home00.000webhostapp.com/saveImage.php";
final response = await http.post(Uri.parse(url), body: {
  "id": id,
  "image": base64Encode(bytes),
});
```

Figure 11: Code segment to connect the PHP code

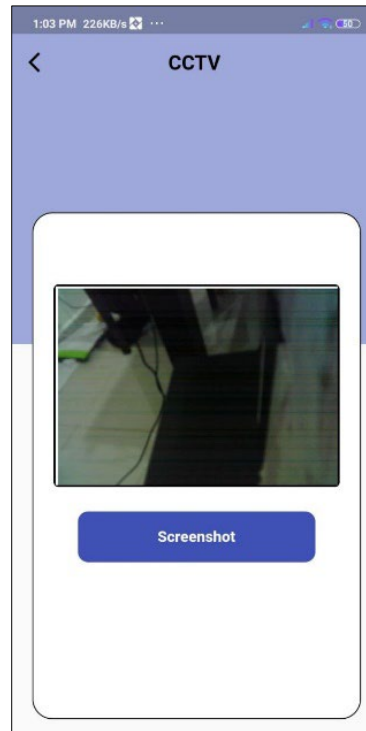


Figure 12: The user interface for the video stream module

4.2 Testing Result from Test Plan

The testing was carried out once the project development was completed, following the previously developed test plan. The test was performed on a physical module depending on the category, and the result is shown after the module was tested. Based on the result shown in Table 4, each of the test plans resulted in a pass result according to the expected results.

Table 4: Test plan result

Category	Description	Expected Results	Actual Results
Sensors	Ultrasonic sensor	Able to sense the distance of the door.	Pass
Sensors	PIR sensor	Able to detect movement.	Pass
Sensors	Camera module	Able to capture the video as CCTV.	Pass
Sensors	Connection	Able to connect between sensors and application	Pass
Application	Login	Able to enter and verify credentials.	Pass
Application	Register user	Able to enter details and added to the database.	Pass
Application	View activity log	Able to display the description and the timestamp.	Pass
Application	User Activation	Able to display and activate or inactivate the user.	Pass
Application	Start sensor operation	Able to connect with the sensors.	Pass
Application	Notification	Able to give notifications to users.	Pass
Application	Screenshot image from video	The video was shown and can screenshot the image.	Pass

The test plan also contains a security checklist test plan to ensure that the project's security elements operated as planned. Therefore, a test was performed based on the test plan, and based on the results shown in Table 5, each of the test plans on the security checklist resulted in a pass result according to the expected results.

Table 5: Security checklist result

No	Checklist	Actual Results
1.	Ensure the error message does not inform which part of the validation is incorrect.	Pass
2.	Ensure the password's strength.	Pass
3.	Password should be hashed in the database.	Pass
4.	Ensure private data such as user phone number and email address are encrypted in the database.	Pass
5.	Ensure all activity that happened through the system was listed in the log activity.	Pass
6.	Ensure video and images are encrypted and only the user can have the original data.	Pass

4.3 UAT Result

Five volunteers were accepted to be testers for this project's user testing. The tester was given an Android Package (APK) file to download into his or her mobile phone. The functioning of the sensors and the design of the mobile application are being tested. The findings will be based on the tester's rating of 1 (poor) to 5 (outstanding). The results of this project's user acceptability testing are shown in Table 6.

Table 6: UAT result

No	Aspect Tested	Scales					Total
		1	2	3	4	5	
1.	Login Functionality				1	4	5
2.	Registration functionality				2	3	5
3.	View log data functionality				2	3	5
4.	User activation functionality				1	4	5
5.	Operation functionality				4	1	5
6.	Video stream functionality				5		5
7.	Screenshot functionality				2	3	5
8.	Update user data functionality				3	2	5
9.	Prototype functionality				1	4	5
10.	Design				5		5

Most of the testers agreed that the prototype worked as planned. Here are some of the tester's recommendations for improving the prototype, particularly the mobile application. The ideas for operation functionality are provided, and the mobile application may display the current condition of the sensors so that the user is not confused. There are also issues with the video stream capability; the tester stated that the video is too small and that it does not always appear in the application. However, the majority of testers are pleased with the outcomes.

5. Conclusion

This project has achieved the three objectives stated in the earlier chapter of this report. It has implemented movement detections and video captures to detect any movement around the house and when the door is opened unexpectedly. It also implemented a secure application system that only allows an authorized user to take control of the security system, the encryption of video storage data, and other security elements, allowing homeowners to not have to worry constantly about their houses. However, several disadvantages can be concluded, including:

- The connection between Arduino Uno and NodeMCU still has to use a serial monitor in Arduino IDE to send commands to the mobile application.

- The video streaming can not capture images automatically when movement was detected from the sensors.
- Admin has to be added manually by the developer before the admin can use it as an admin to manage the mobile application system.
- The mobile application was only tested on Android phone users, therefore, this project still did not know its efficiency for IOS mobile phones.

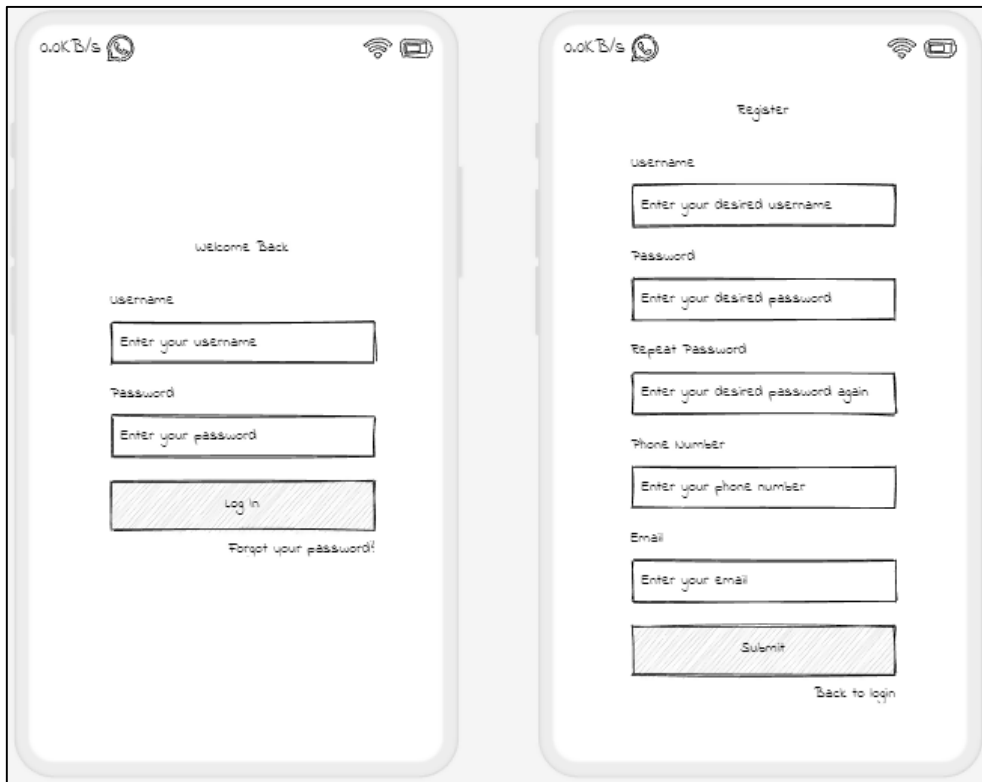
For encouragement for the continuation of the current project, several future implementations can be suggested to add to this project:

- Improve the way to connect the Arduino Uno and NodeMCU by using an additional WiFi module instead of using a serial monitor that still needs to connect to the computer.
- The video can automatically detect a person and snap a picture of them when movement was detected from the sensors.
- Add a new account for admin automatically each time the system was bought or accepted to use.
- Test on IOS mobile phone users to make sure that this project can be used by multiple mobile phone platforms.

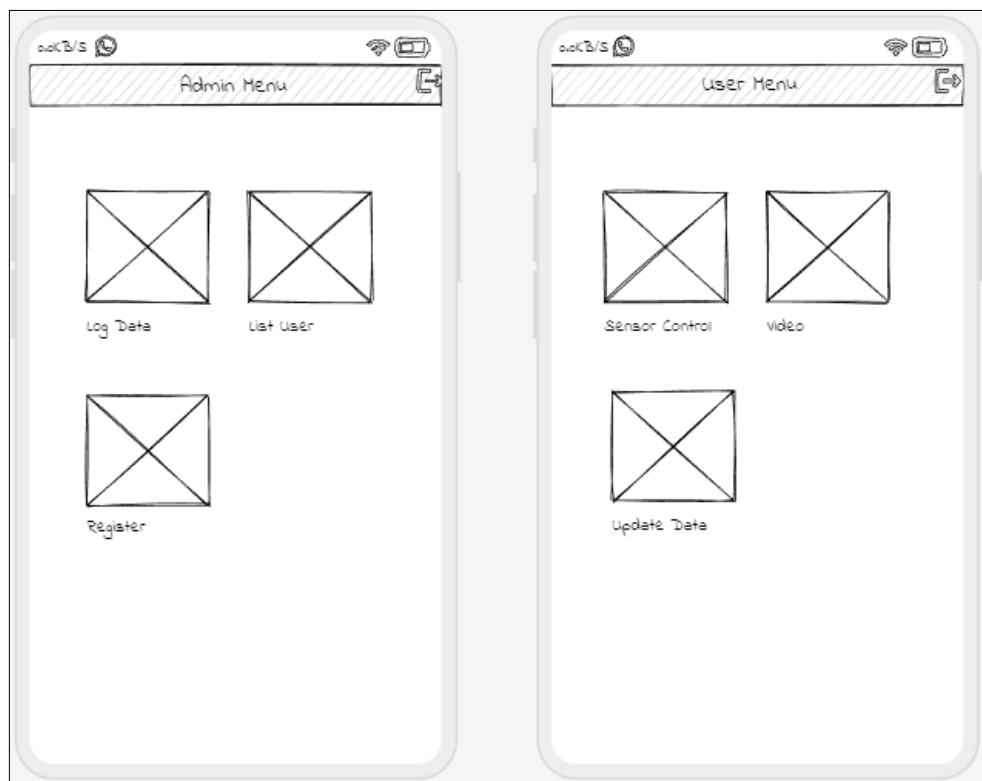
Acknowledgement

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

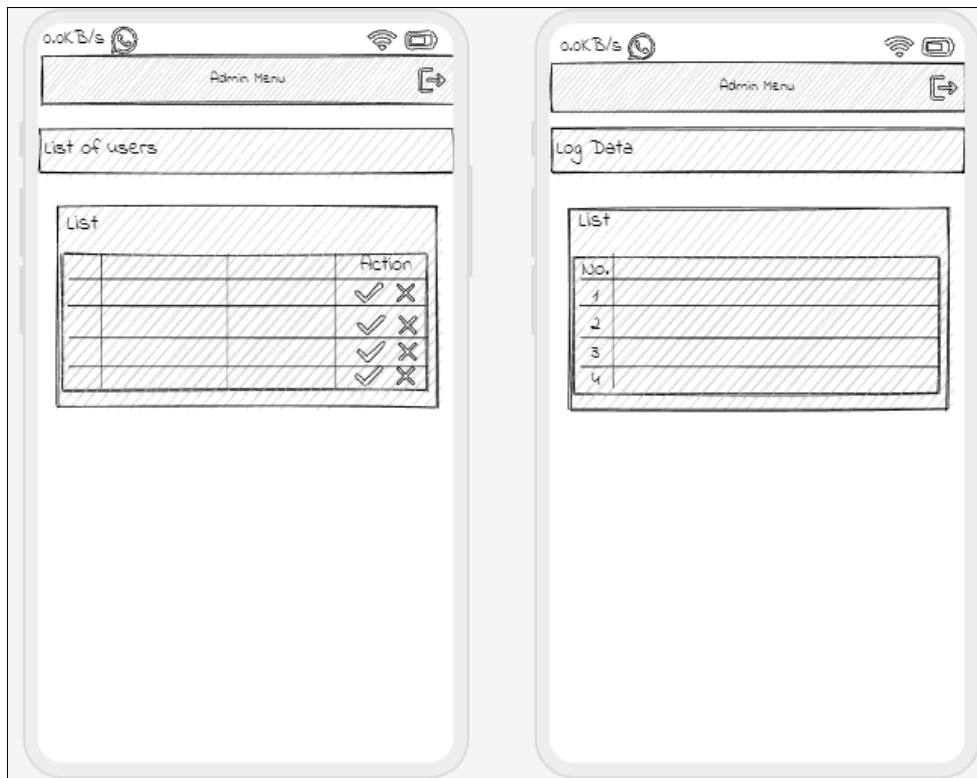
Appendix A



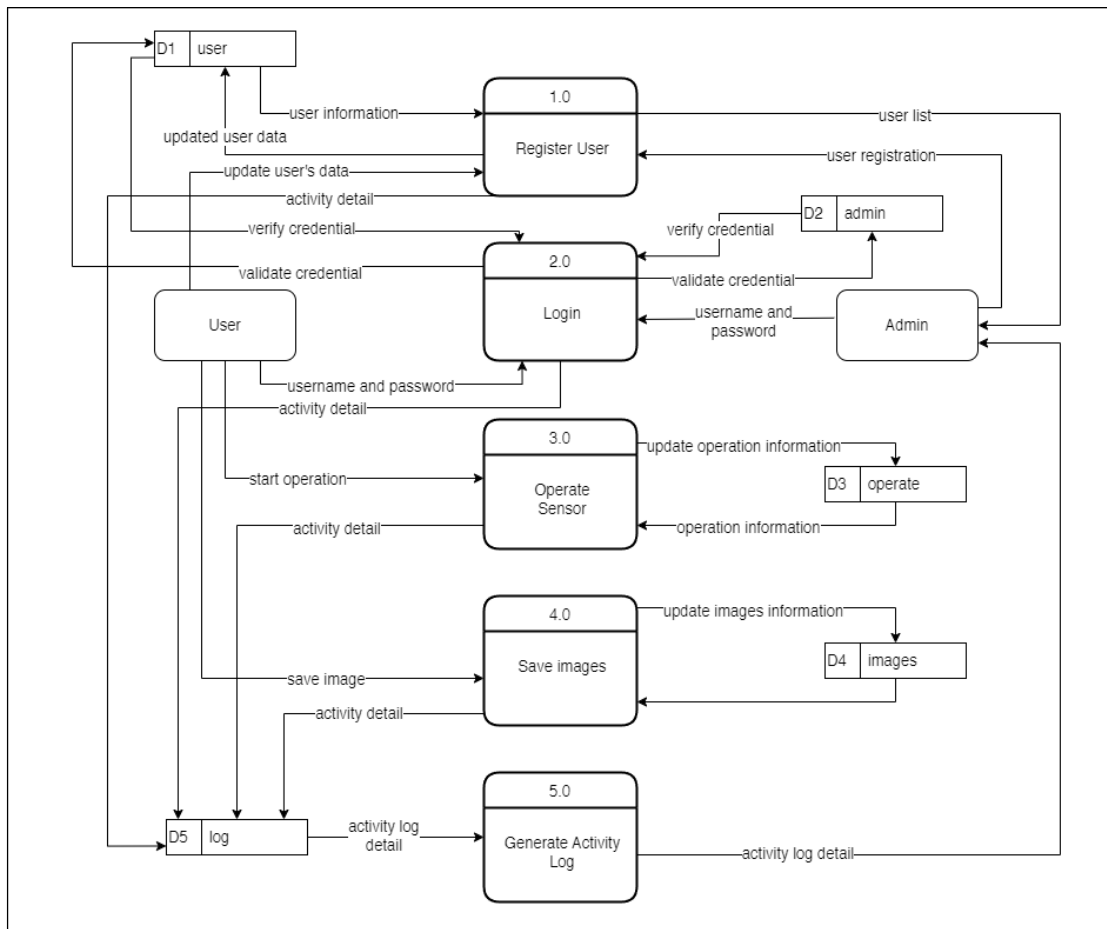
Appendix B



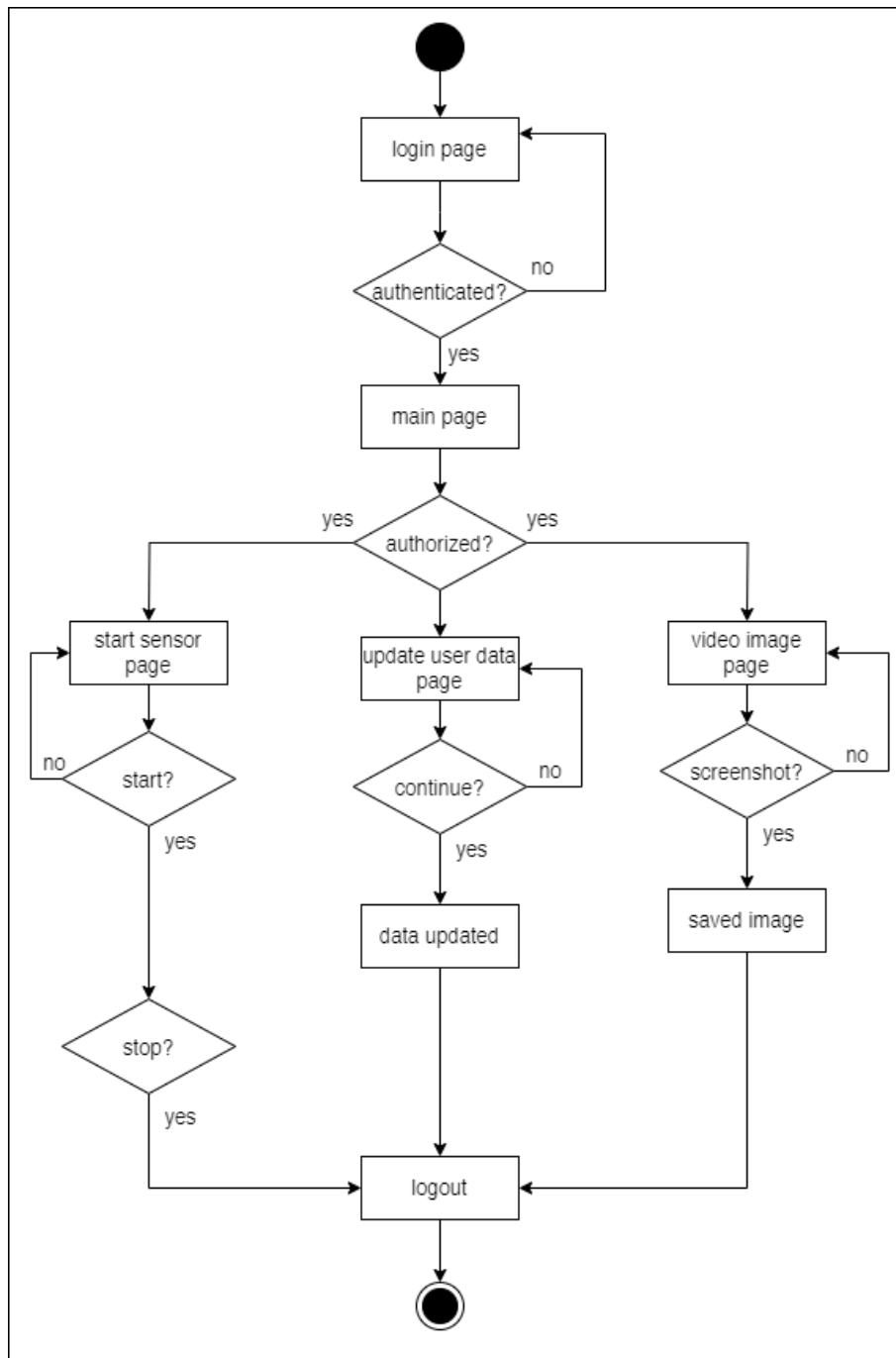
Appendix C



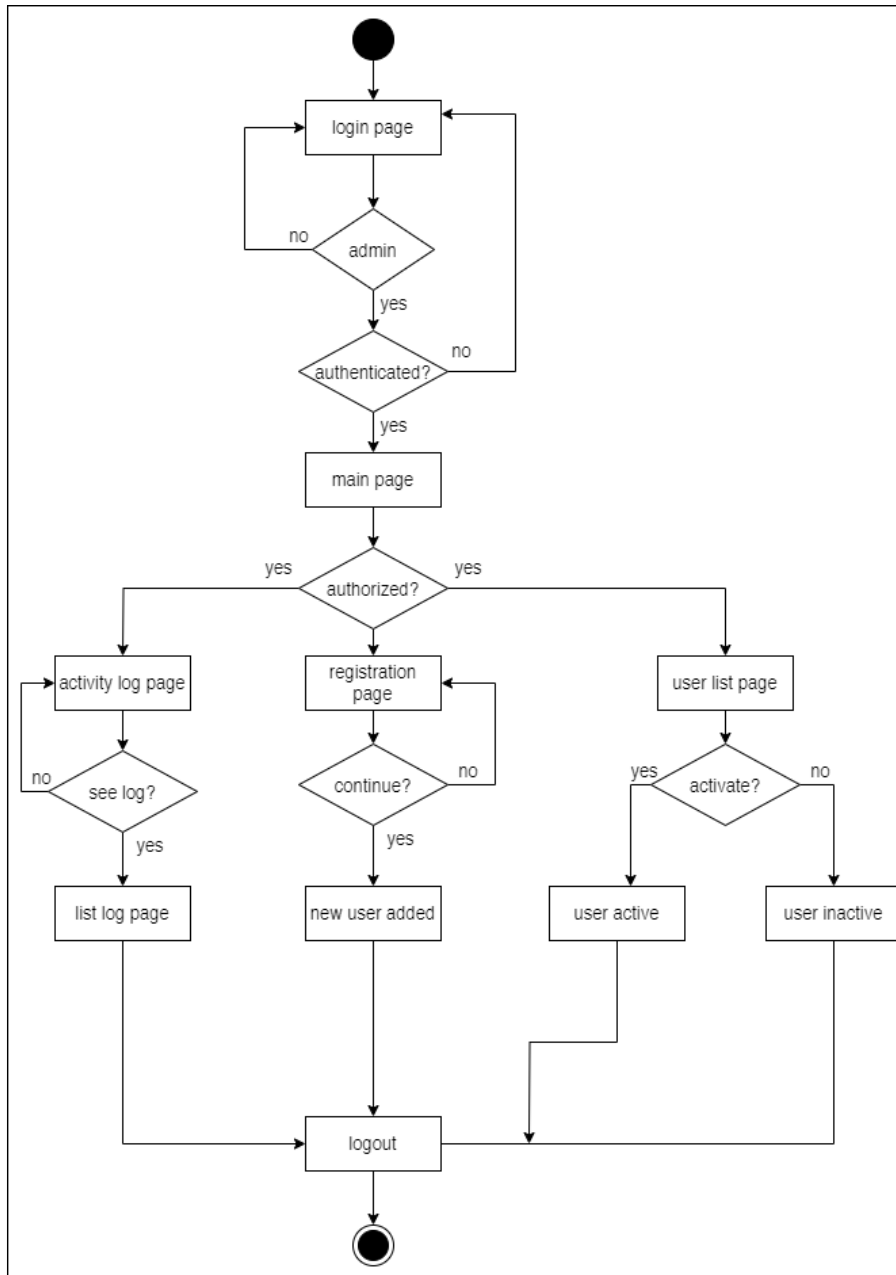
Appendix D



Appendix E



Appendix F



References

- [1] H. Labus, "Your CCTV devices can be hacked and weaponized," HelpNetSecurity, Oct. 27, 2022, [Online]. Available: <https://www.helpnetsecurity.com/2022/10/27/cctv-hacks/>. [Accessed May 01, 2023].
- [2] Q. Zhang, "An overview and analysis of hybrid encryption: The combination of symmetric encryption and asymmetric encryption," in Proceedings - 2021 2nd International Conference on Computing and Data Science, CDS 2021, Institute of Electrical and Electronics Engineers Inc., Jan. 2021, pp. 616–622. doi: 10.1109/CDS52072.2021.00111.
- [3] M. Lauren and A. Samantha, "What Is A Home Security System?," Forbes, Nov. 15, 2022, [Online]. Available: <https://www.forbes.com/home-improvement/home-security/what-is-a-home-security-system/>. [Accessed Dec. 05, 2022].
- [4] C. Jen, "What is the Internet of Things (IoT)?," IBM, Nov. 17, 2016, [Online]. Available: <https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/>. [Accessed Dec. 05, 2022].
- [5] T. Ahmed, A. T. Bin Nuruddin, A. Bin Latif, S. S. Arnob, and R. Rahman, "A Real-Time Controlled Closed Loop IoT Based Home Surveillance System for Android using Firebase," in 2020 6th International Conference on Control, Automation and Robotics, ICCAR 2020, Institute of Electrical and Electronics Engineers Inc., Apr. 2020, pp. 601–606. doi: 10.1109/ICCAR49639.2020.9108016.
- [6] V. Patchava, H. B. Kandala, and P. R. Babu, "A Smart Home Automation technique with Raspberry Pi using IoT," in 2015 International Conference on Smart Sensors and Systems, ICSSS 2015, Institute of Electrical and Electronics Engineers Inc., Mar. 2017. doi: 10.1109/SMARTSENS.2015.7873584.
- [7] L. H. Keat and C. C. Wen, "Smart Indoor Home Surveillance Monitoring System Using Raspberry Pi," Joiv: International Journal on Informatics Visualization (Sep 2018), vol. 2, no.4-2, pp. 299-308, 2018, doi: <http://dx.doi.org/10.30630/joiv.2.4-2.172>.
- [8] M. Matthew, "Prototype Model in Software Engineering," Guru99, Nov. 19, 2022, [Online]. Available: <https://www.guru99.com/software-engineering-prototyping-model.html>. [Accessed Dec. 20, 2022].