بسم الله الرحمن الرحيم

AN-NAJAH NATIONAL UNIVERSITY

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY

Computer Engineering Department

Hardware Graduation Project

Broadcasting House

Students
Fathi F. F. Ali
Ezz Addin Kukhun

Supervisor
Dr. Suleiman Abu Kharmeh

Presented in partial fulfillment of the requirements for Bachelor degree in Computer Engineering.
May, 2023

ACKNOWLEDGMENTS

First, allow us to express our sincere appreciation and gratitude to Professor Suleiman Abu Kharmeh for his immense contribution and support . His relentless efforts have made a lasting impact on the academic community and we are deeply grateful for his guidance, support, and encouragement throughout this project.

We would also like to extend our sincerest gratitude to our parents and families for their unwavering support throughout the entire project process. Your guidance, encouragement, understanding, and patience have been invaluable in helping us reach this milestone. We are sincerely grateful for your unconditional support throughout all of our endeavors. Thank You!

In addition, we would like to thank the Computer Engineering Department for their hard work and dedication. Your commitment to excellence has enabled us to develop innovative solutions that have helped us reach our goals. We thank you for your invaluable contributions, which have been instrumental in helping us succeed.

Finally, thank our friends who provided happy distractions to rest our minds outside of our project. Turns out it was much needed. Thank you for being part of this journey with us!

DISCLAIMER

The following paper presents an overview of Broadcasting House, our hardware graduation project. It was written by Fathi FathAllah and Ezz Kukhun to meet a handful of prerequisites for the Bachelor's degree in Computer Engineering at An-Najah National University.

The writers' views and opinions are entirely their own and do not necessarily represent the official stance or policy of any other agency, organization, university, or corporation. An-Najah National University disclaims any liability for the information included in this paper.

TABLE OF CONTENTS

Acknowledgments 1

List of Figures 5

Abstract 6

Chapter 1: INTRODUCTION 7

1.1 Statement of the problem 7

1.1.1 Inadequate Entry Points 7

1.1.2 Limited Surveillance Systems 7

1.2 Objectives 8

1.3 Scope of the work 8

1.3.1 Establish Effective Access Control 8

1.3.2 Implement Surveillance System 8

1.3.3 Enable Remote Monitoring 8

1.3.4 Integrate Alarm and Emergency Response System 9

1.4 Significance 9

Chapter 2: CONSTRAINTS AND EARLIER COURSE WORK 10

2.1 Constraints 10

2.1.1 Budget Constraints 10

2.1.2 Real-World Visualization 10

2.2 Earlier Coursework 10

Chapter 3: RELATED WORK 11

Chapter 4: METHODOLOGY 12

4.1 System Design 12

4.2 Used devices and modules 12

4.2.1 Arduino Mega 12

4.2.2 ESP32 14

4.2.3 ESP32-CAM 15

4.2.4 Servo Motor MG996R 16

4.2.5 Servo motor SG90 (Micro servo) 17

4.2.6 KeyPad 18

4.2.7 Fingerprint Sensor JM-101B 19

4.2.8 IR Sensor MH Series 20

4.3 The operational mechanism of the system 21

Chapter 5: RESULTS AND DISCUSSIONS 22

5.1 Results 22

5.1.1 System Design and Implementation 22

5.1.2 Surveillance and Monitoring 22

5.2 Discussion 22

Chapter 6: CONCLUSION 23

Chapter 7: FUTURE WORK 24

References 25

LIST OF FIGURES

4.1 Arduino Mega Board 13

4.2 ESP32-WROOM 14

4.3 ESP32-CAM 15

4.4 Servo Motor MG996R 16

4.5 Micro servo SG90 17

4.6 Keypad matrix 4*4 18

4.7 Fingerprint sensor JM-101B 19

4.8 IR sensor 20

ABSTRACT

Smart home security systems have become increasingly popular in recent years, offering homeowners enhanced convenience and comfort. Smart home security systems integrate various technologies and devices to create a comprehensive network that ensures the safety and security of the home. These systems typically consist of components such as motion sensors, door/window sensors, surveillance cameras, and smart locks. This paper investigates Broadcasting House as it being a graduation project and as a system that implements many features related to smart house security first principles. This project has been able to do so, by proposing our a cost-effective accurate house security architecture.

CHAPTER 1

INTRODUCTION

In an increasingly interconnected world, technology has become an essential part of our lives. Additionally, the conceptual idea of smart homes has gained a significant amount of popularity. With the ability to control various parts of our living environment through electronic devices, smart houses offer comfort, and enhanced efficiency. However, as we embrace the benefits of these advanced systems, it becomes crucial to address the potential security vulnerabilities, specifically those related to protecting our homes against thieves and intruders.

1.1 Statement of the problem

The inherent insecurity of regular residential houses, which lack sufficient security features and fail to provide effective protection against potential threats is a considered to be the problem at hand. This issue exposes homeowners and occupants to risks such as property theft, invasion of privacy, and physical harm. Bearing that in mind, our main concerns in this thesis are:

1.1.1 Inadequate Entry Points

The Security of Inadequate Entry Points, such as poorly reinforced doors and vulnerable locks with no relation to smart systems. Those can be easily exploited by intruders.

1.1.2 Limited Surveillance Systems

Many regular houses lack comprehensive surveillance systems, including security cameras, motion sensors, and alarms, leaving homeowners unaware of potential security breaches and reducing the chances of timely intervention.

1.2 Objectives

The objective of this thesis is to propose practical and efficient security solutions while raising awareness among homeowners and security guards. By granting them full access to their house systems and providing them with real-time updates on the latest events, this research aims to empower them with the knowledge and tools to enhance the security of their homes.

1.3 Scope of the work

1.3.1 Establish Effective Access Control

The focus of this work involves designing and digitalizing a secure home system that significantly enhances security measures. By utilizing innovative technologies and strategic design, the aim is to develop a robust and efficient system that effectively strengthens the security of homes. Biometric authentication, keyless entry systems or smart locks, are used to ensure that only authorized individuals can enter the home. This helps prevent unauthorized access and enhances the overall security of the property.

1.3.2 Implement Surveillance System

The objective is to integrate advanced surveillance systems, including high-quality security camera, motion sensors, and alarms, to monitor the internal part of the home. This will enable real-time monitoring, detection of suspicious activities, and timely intervention in case of security breaches.

1.3.3 Enable Remote Monitoring

The objective is to design a secure home system that allows homeowners and security guards to remotely monitor various security features, such as surveillance cameras, alarms, and access control systems, through mobile applications or web interfaces.

1.3.4 Integrate Alarm and Emergency Response System

The objective is to integrate an alarm system that immediately notifies homeowners, security services, or emergency responders in the event of a security breach or emergency situation, such as a fire or medical emergency. This ensures swift response and appropriate action to mitigate potential threats.

1.4 Significance

Our project offers a cost-effective solution in comparison to advanced and sophisticated house security systems, while still providing the essential benefits of protecting lives, safeguarding property, enhancing personal safety, increasing resilience, and empowering individuals to take control of and monitor their residential security.

CHAPTER 2

CONSTRAINTS AND EARLIER COURSE WORK

2.1 Constraints

2.1.1 Budget Constraints

Optimal operation and implementation of a security system require the utilization of high-quality sensors and advanced security cameras. However, due to budget constraints in our Graduation project, we faced limitations in the resources available for designing a secure house system. Despite this, we have successfully overcame these constraints by leveraging cost-effective yet effective electronic devices. Our design concept remains accurate and reliable, showcasing the effectiveness of our approach within the given constraints.

2.1.2 Real-World Visualization

We made a concerted effort to create a project visualization that closely aligns with real-world conceptual ideas. Constraints related to physical installation, scalability, and compatibility with any other house existing infrastructure may need to be taken into account.

2.2 Earlier Coursework

- Microprocessors and Microcontrollers courses: Helped us grasp how to use any sort of electrical device as well as how to interface such devices with Microcontrollers/Microprocessors.
- Microcontrollers Lab: We became more acquainted with the practical aspects of connecting and developing systematized programs with actual Arduino/PIC boards.

CHAPTER 3

RELATED WORK

In order to assist home security , this literature review will examine current research related to Smart Home Security System. Research studies that have discussed this approach and how successfully these digitalized services will be the focus.

The first paper examined was "A Review on Security in Smart Home Development", Robles et al., 2010. The study indulges into the realm of smart homes and their security aspects. Additionally, it explores specific tools designed for smart home security. The research focuses on the establishment of such systems using wireless communication, similar to what we have implemented in our project. However, the study employs ZigBee and other related protocols for device-to-device communication. Furthermore, it highlights the numerous benefits of smart secure homes, which enhance convenience and ease in daily life. Home networking not only offers peace of mind but also keeps homeowners informed about ongoing events, whether they are at work or on vacation. In case of emergencies, security systems integrated into smart homes can provide invaluable assistance.

The second and last paper, "Design and Implementation of an IoT-Based Smart Home Security System", Hoque and Davidson, 2019. As part of our graduation project proposal, we aim to develop a cost-effective design. This paper presents the framework for a budget-friendly intelligent home system, specifically focusing on the implementation of door sensors. These sensors will promptly alert users through an Android application whenever a door is opened within the house. Similar to our project, the architecture in the paper utilizes an Arduino-compatible Mega 2560 microcontroller board. Additionally, it communicates with a web server that employs a RESTful API via the Raspberry Pi board. Because our method is localized within the home, neither a webserver nor an RPI board are required in our instance.

CHAPTER 4

METHODOLOGY

4.1 System Design

The system represents by wood box which has these dimensions 55cm*35cm*14cm, it is divided into four rooms, each room supplied by sensors to detect thieves. There is also a camera stand which is put on the motor at the top of the house.

4.2 Used devices and modules

4.2.1 Arduino Mega

The Mega 2560 Arduino, [1] is a microcontroller based on ATMega2560 with 16MHz. Why we used it in our project? The Arduino mega considered an enhanced version of the Arduino standard boards, it has many features that facilitate our work in this project. It has more I/O pins, memory. In this part we will justify our usage of the Arduino mega in our project through some important points:

- Digital I/O pins: Arduino Mega contains of 54 digital I/O pins, while Arduino UNO contains just 14 digital I/O pins. In our project, we used several components, we used four IR sensors, finger print sensor, two motion sensors, 4X4 Keypad, and ESP 32 camera. And we have to mention that the Arduino mega contains 6 pins for interrupts and we used all of them for sensors, and UNO contains just two interrupts. We can say that the Arduino mega coverage our need and facilitated the work with this enough number of Digital I/O pins.

- Serial Communication: Arduino Mega contains four hardware UART serial ports, and as we studied previously, we use these serial ports for communication with other devices. In our project, we used three components which they need a communication with the Arduino mega, ESP32, ESP32Cam, and finger print sensor.

Arduino UNO has just one hardware UART serial port, and this is not compatible with our needs in communication with several devices.

- Memory: Arduino mega these specifications related to the memory:
  - Flash Memory: It used mainly to store the code which is uploaded. And it has large size in Arduino Mega which is equal 256KB, and it equal 32KB in Arduino UNO. So, with Arduino mega, we can write complex and extensive programs.
  - SRAM (Static Random-Access Memory): It used to store variables, data, and stack space during program execution. It a size 8KB, which is larger than the memory size in Arduino UNO 2KB.
  - EEPROM (Electrically Erasable Programmable Read-Only Memory): It is a non-volatile memory which it used to store data that needs to be retained when power is disconnect. The Mega has an EEPROM with 4KB size, and UNO with 1KB.

So, with these differences between memory specification in Mega and UNO, it is recommended to use mega if writing more complicated code is needed, and even store larger data. And Arduino UNO it is recommended for simple to mid-level programs.

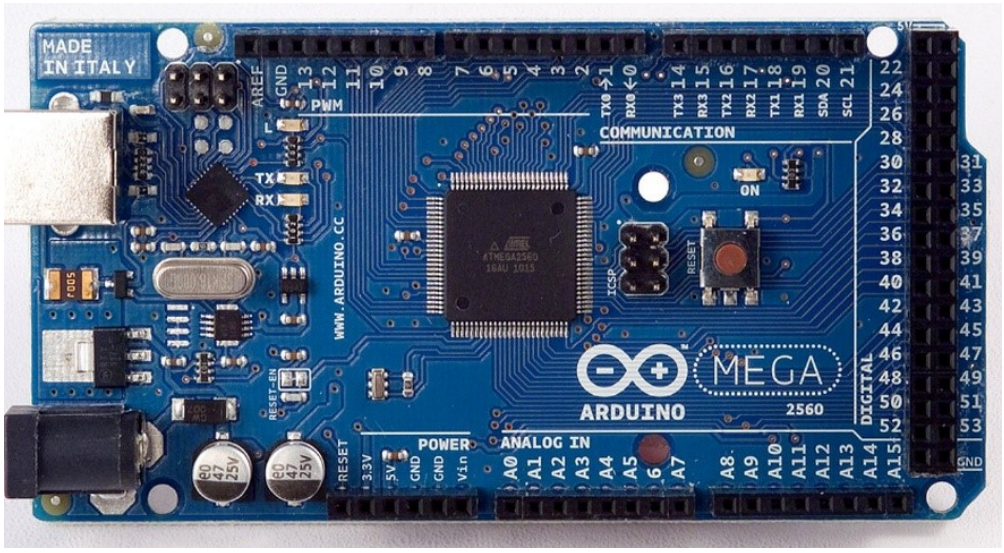

Figure 4.1: Arduino Mega Board

4.2.2 ESP32

ESP32, [2] It is a microcontroller which is based on the Xtensa LX6 dual-core processor, running at 160 or 240 MHz. The ESP32 has two built in modules, Wi-Fi and Bluetooth, It supports Wi-Fi protocols as 802.11b/g/n, and Bluetooth 4.0 and 5.0. So, with ESP32, we can build systems which they will be able to connect to the devices through Wi-Fi. The ESP32 contains GPIO pins - input/output pins which we can use them for interfacing with external devices, and sensors. The number of them ranges between 25-36 depending on the development board.

But why we used it in our system? As we mentioned above, the ESP32 has two modules one of them for Bluetooth, and the other for Wi-Fi, and in our system, if thief is detected, the system has to send a notification to mobile application of the house owner that there is a thief detected, and this application need a connection to the Wi-Fi.

You may ask us why we didn't use ESP8266 for Wi-Fi connection? The ESP32 has more features and capabilities rather than ESP8266.It offer high data rates, and better range. It also provides additional features like Wi-Fi scanning, soft access point mode, and mesh networking.

Figure 4.2: ESP32-WROOM

4.2.3 ESP32-CAM

ESP32-CAM, [3] is a development board that designed specifically for projects that they require Wi-Fi connectivity and image or video capturing.

The ESP32-CAM development board provides GPIO pins, flash memory, and other peripherals to support the ESP32 microcontroller's functionality. It also includes an OV2640 camera module, which is capable of capturing still images and streaming video.

In our system, we used it for live streaming. So, when a thief is detected, the camera will start live streaming to show the house owner where the thief is move inside his house.

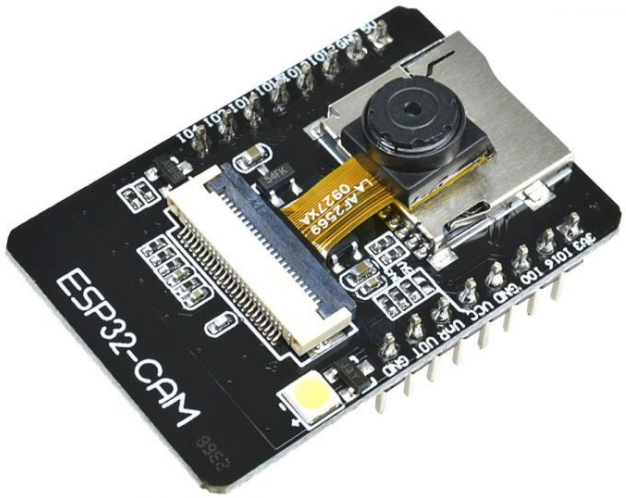

Figure 4.3: ESP32-CAM

4.2.4 Servo Motor MG996R

MG996R ServoMotor, [4] is a popular servo motor, and it is known for its high torque and fast speed. It operates typically on voltage range between 4.8V to 7.2V. It can rotate from 0 to 180 degree. It has dimensions 40mm*20mm*40mm.

We put the servo at the top of the house, and we used it in our system to put the camera on its horn, so when a thief is detected at some room in house, it will move its horn toward this room, and the camera will show the house owner the movement of the thief inside this room through live streaming.

When we start our work in the project, we used stepper motor, and we wrote an algorithm for this process, and now you will ask yourself why we change to use servo motor? The stepper motor is slow, and we have to be careful for its angle movement, so if we try to make it move clockwise, we will assign a positive number for its angle, and if we try to make it move anticlockwise, we will assign a negative value for its angle. And we have to know that the stepper motor hasn't a reference point. After facing these difficulties, we decided using servo, so the servo has reference point at angle 0, and it is fast as we mentioned above, and servo angle just represents by positive number.

Figure 4.4: Servo Motor MG996R

4.2.5 Servo motor SG90 (Micro servo)

Is a popular servo motor, it provide limited torque compared to larger servo motors but it is suitable for lightweight mechanisms and projects. It operates typically on voltage range between 3.3V to 6V. It can rotate from 0 to 180 degree. It has dimensions 22.8mm*11.8mm*31mm.

We used it in our system to control the lock of the door. We linked the horn of this servo with a wire, and this wire linked with lock of the door. So, when the person enter correctly (scan his fingerprint successfully), the horn of the servo will pull the lock through this wire, and the door will open.

Why we didn't use it with camera? Because the MG996R servo motor generally offers a faster rotational speed than the SG90 servo motor, and it is better than micro servo to hang the stand of the camera.

Figure 4.5: Micro servo SG90

4.2.6 KeyPad

A keypad with size 4*4 used in our system as a first level for security, so when the user types the password correctly, he/she will enter to the house, and then he will move to the second level to authenticate himself through fingerprint which we will talk about it in the next topic. Also, we used keypad to enable the security system when the house owner go outdoor with his family, or we can say when the house is empty. So, if we assumed that there is a thieves enter to the house, it will catch him directly, because he doesn't know the inner password, and he doesn't have a stored fingerprint in the house.

Figure 4.6: Keypad matrix 4*4

4.2.7 Fingerprint Sensor JM-101B

As we know it is considered as one of biometric security types, JM-101B Fingerprint, [5] operates on 3.3V, and its dimensions 48mm*21mm*24mm. We have to ask ourselves that how the Arduino communicate with fingerprint sensor? They communicate serially, the fingerprint sensor has two connections for TX, and RX, and they connect with Arduino through one of the UART ports on the Arduino. What is the added value of fingerprint sensor to our system? When anyone enter to the house newly, a timer of 25 seconds will start counting until the person authenticate himself that he or she is one of the house members. So, if the timer ended without authenticate himself, the system will consider this person that he/she is a thief, because it is impossible that there is a thief can store his fingerprint inside any house doesn't belong to it.

Figure 4.7: Fingerprint sensor JM-101B

4.2.8 IR Sensor MH Series

A device that detects and responds to infrared radiation. It is commonly used in various applications for proximity sensing, object detection, and remote-control systems. We have to know that operates on 3.3V to 5V.

IR sensors can have different detection ranges depending on the specific model and application. Some IR sensors have short-range detection up to a few centimeters, while others have longer-range detection of several meters. The detection range is influenced by factors such as the power of the IR emitter, the sensitivity of the receiver, and the environmental conditions.

In our system, we used it to detect if there is a thief enter to the house. We had put IR sensors in the rooms of the house. Assume that the house owner goes out with his family, or the house become empty, the system has to be enabled. So, if the thief enters to the house from the sides, not from main door, and the IR sensor of one of rooms detect him, a notification will send to the house owner that there is a thief detected, and the camera will show the user where the thief is existing through live streaming.

You may ask yourself why we didn't use motion sensor (PIR) to detect the thief? We used the PIR firstly for motion detection, and when we tested it, we tested it in non-restricted area, and it gave us good responses. But when we put the PIR sensor inside some room in the project, it gave us false responses. When we read more about PIR, we discovered that it is too sensitive, and it needs large area to work well (not restricted).

Figure 4.8: IR sensor

4.3 The operational mechanism of the system

The house is surrounded by different sensors to prevent the thief from entering the house, and there are sensors inside rooms of the house to catch the thief if he enters successfully to the house. There are different scenarios that the thief follows them to enter the house, and we worked on cover these scenarios:

- Assume that the thief knows the house password: The system has two levels of the security, the first one is typing the house password through keypad in order to open the lock of the door, so if the entered password was correct, then a timer of 25 seconds will start counting. Through this duration the user has to authenticate himself through scanning his fingerprint on the fingerprint sensor which is considered the second level of security, so if the user failed to authenticate himself through this duration, the system will consider him that he is a thief, because logically, it is impossible that there is thief define his fingerprint in some home, so when the thief is detected, a notification will send to the mobile application to the house owner, and live streaming will start to show the house owner where the thief is move. By this process, the house owner will know and verify that there is a thief try to enter and steal his house.

- Assume that the thief tries to enter from windows of the house, not from main door: The house surrounds by different sensors that they will detect the thief, so if these sensors detect a thief, a notification will send to the house owner, and the alarm system will be activated.

- Assume that no one inside the house, and thief exploited this chance, and he entered from one of house windows: If the house owner will go out with his family, which we mean that the house will become empty, the house owner will activate the security system before he goes out by enter an inner password. So, if the thief then enters the house from one of the its windows, the sensors will detect that there is someone at home, also the timer will start counting until the thief authenticate himself through fingerprint sensor.

CHAPTER 5

RESULTS AND DISCUSSIONS

5.1 Results

The project aimed to design and build a comprehensive smart house security system that utilizes advanced technologies such as Internet of Things (IoT) to enhance home security.

5.1.1 System Design and Implementation

A secure accurate cost-effective systematized smart house security system was successfully designed and implemented, utilizing various components such as surveillance cameras and motion sensors.

5.1.2 Surveillance and Monitoring

The surveillance cameras installed in above the house and provided continuous monitoring of the premises and inside the house. Live video feeds could be accessed through the system's mobile application, enabling real-time monitoring of the property.

5.2 Discussion

Although our project yielded promising results, it is important to acknowledge certain limitations. The sensors utilized in our project were primarily intended to showcase the fundamental principles of detecting potential thieves. However, it is important to note that these sensors operated on a single dimension. In practical applications, careful consideration must be given to the process of selecting appropriate sensors to ensure optimal performance and accuracy in detecting security threats. Furthermore, continuous improvements can be made to enhance the accuracy of threat detection and expand the system's compatibility with a wider range of IoT devices.

CHAPTER 6

CONCLUSION

The completion of this project has been an enriching journey that has significantly contributed to our professional and personal growth in the field of computer engineering. It provided us with valuable opportunities to explore various aspects of embedded system design and programming, ranging from fundamental functionalities to more advanced concepts. Through this project, we also had the privilege of working with diverse technologies and electronic devices, expanding our knowledge and skills in areas that were previously unfamiliar to us. Moreover, the collaborative nature of the project fostered an environment that promoted teamwork and enhanced our hardware skills. Working collectively on tasks enabled us to leverage each other's strengths and overcome challenges together. This experience further honed our abilities to collaborate effectively and reinforced the importance of teamwork in achieving successful outcomes.

In conclusion, the graduation project, Broadcasting House, was developed as a hardware solution aimed at assisting and enhancing home security. It serves as a valuable and effective resource for homeowners seeking to improve the safety of their residences. Moreover, Broadcasting House not only provides assistance in ensuring security but also offers a cost effective approach to home protection.

CHAPTER 7

FUTURE WORK

Future work could involve exploring ways to further improve the security system, such as:

- Expansion of IoT Device: Further expand the system's compatibility with a wider range of IoT devices and sensors. This could include integration with active infrared sensors and other related devices.

- Integration of Advanced Detection Technologies: Explore ways to integrate the image processing-based thief detection system with our existing smart security systems. This could involve incorporating the image processing algorithms into a broader smart home security system, enabling a more comprehensive and integrated approach to home security.

- Mobile Application Enhancements: Improve the mobile application interface and enhance its functionality to provide users with greater access control over their home, ultimately resulting in an enhanced user experience. This may involve incorporating additional features that empower users to have more control over various aspects of their house, elevating their overall satisfaction with the application.

REFERENCES

Arduino. ([1]). *Mega2560* [https://docs.arduino.cc/hardware/mega-2560].

ESP32. ([2]). *Wroom* [https://www.espressif.com/sites/default/files/documentation/esp32-wroom-32_datasheet_en.pdf].

ESP32-CAM. ([3]). *Camera* [https://docs.ai-thinker.com/en/esp32-cam].

Fingerprint. ([5]). *Sensor jm-101b* [https://www.seli.tn/Doctech/CAP038.pdf].

Hoque, M. A., & Davidson, C. (2019). Design and implementation of an iot-based smart home security system. [doi:10.2991/ijndc.k.190326.004]. *Int. J. Networked Distributed Comput.*, *7*(2), 85–92.

Robles, R. J., Kim, T.-h., Cook, D., & Das, S. (2010). A review on security in smart home development. *International Journal of Advanced Science and Technology*, *15*.

ServoMotor. ([4]). *Mg996r* [https://www.arduino.cc/reference/en/libraries/servo/].