Smart Door Unlock System with Android App

[1]Jeenat Sultana*, [1]Shusmoy Chowdhury, [1]Moynul Hasan Tushar & [1]Md.Hemayet Uddin
[1]Department of Computer Science and Information Technology, Southern University Bangladesh, Bangladesh
jeenatcse@gmail.com; 1305108.sc@ugrad.cse.buet.ac.bd; tmoynulhasan@gmail.com; uhemayet9@gmail.com

Abstract

A room is secured when it is locked and especially when the lock is ensured not to unlock by an unauthorized person. There are many methods to lock and unlock a door such as face detection, voice recognition, speech recognition, use of password and pin code, biometric technology etc. where each method serves the purpose of digital keys. As the availability of android devices are increasing day by day, the digital keys are working by means of android apps. We implemented our system to accomplish two purposes. One is to assure authorization i.e. no unauthorized user can get access to the secured room. The other one is to transfer the authorization to an unauthorized person who needs the permission to access in case of emergency. To meet the first goal, we used face detection and speech recognition and used random one-time password for the second one. Both the ways are implemented in android apps and connected to the Arduino Nano via Bluetooth module. Additional devices were used to strengthen the security of the system by detecting forceful attack by the intruders. Our objective was to design the system with enhanced security and affordable cost.

Keywords**:** *Android App, Arduino Nano, Face Detection, IoT, Speech Recognition.*

1. Introduction

Locking system plays an important role in the security system of our houses. As we cannot remain all the times in our home, we need to ensure proper security when we are not there. Once different kinds of locks with the keys were used to serve the purpose. With the blessing of science and technology humans are designing and implementing new kinds of locks to protect their houses from unwanted troubles. On the other hand mobile phone is one of the common phenomenon in our daily life. So if we can connect our security system with our mobile phone it will be more effective and helpful to us.

Now-a-days our home is getting automated from the very entrance with unlocking a door to the handling of home appliances. The use of android devices as automated controllers meets not only the need of digital keys but also the high resolution mobile camera replaces the need of external closed circuit camera. Moreover, tagging the recognized faces in an image is now an in-built application of the mobile camera. Bearing in mind all these facilities we, in our project, focused on the secure entrance to a private room.

The project is implemented as a part of home automation system [1] and is an effective example of internet of things (IoT) [2]. We have used multiple layered security in the system to provide two different types of user access. The first type of user is the one who has the authorization to enter the room. With his smart phone containing the designed app, he goes through the procedure of face detection and security question checking. The

*Corresponding Author
ISSN: 2005-4238 IJAST

second type of user is the one who is not a regular accredited user but has the consent to access the room for a certain time period. He can request and gets a one-time password (OTP) through the app. Face detection and recognition is measured by Principal component analysis (PCA) algorithm [3] [4] which is a very common one for the purpose. Again, using smart phones as keys lessen the possibility of forgetting to carry the physical keys.

The rest of the paper is organized as follows. In Section 2 we have discussed the related works done by different researchers regarding this topic. The section 3 is the methodology of our project which is divided into two subsections. In the first subsection we have discussed the system design of our project and in the next subsection we have discussed about the hardware components used in our project. Section 4 deals with the system implementation. Section 5 analyzes the results from testing to cost calculation. Finally section 6 concludes with final remarks.

The motive of this project is to make smart unlock system connected with an android app which can ensure the proper security of our houses.

2. Related Works

Anjali Patel et al. [5] introduced an idea of secure door locking system using Raspberry pi (RPi) server system to control the video camera for capturing images on a relay and unlock the door comparing the image of the user with the images in database. Using Raspberry pi server system possess a secure system with high expense, not easily affordable by an individual.

Vamsi, T. K., et al. [6] proposed a real-time face recognition system for door unlocking using LBPH algorithm. The algorithm was used to convert the color image to a pixel matrix format before storing to the database. The pixel values in the matrix are compared to the pixel values of the user's image for detecting his or her face.

Retha Dinar Hayu Arifin et al. [7] designed a system where the door is unlocked using speech command or pincode and the speech command or pincode is given via smart phone.

Agbo David O.et al. [8] implemented a system of door unlocking using password via Android App.

Abdul Azeemet al. [9] implemented face recognition for door unlocking using the viola jones method for face detection and the Local Binary Patterns Histograms for face recognition.

Patel, P.et al. [10] proposed and implemented the door locking and unlocking system with smart phones using wi-fi connectivity. Every of the above mentioned researches ensures high security but encompasses components that are lavish and needs experts to design.

In our paper we proposed and implemented a cost-effective door unlock system using face detection and speech recognition via Android app. Along with the system we added the facility of requesting for a password, an alarm system in case of intruder attack and a LCD display to interpret the progress of work. We designed our system economically and kept it simple so that not only an official but also an ordinary being can bear the expenses and use the system for securing his own room.

3. Methodology

3.1. System Design

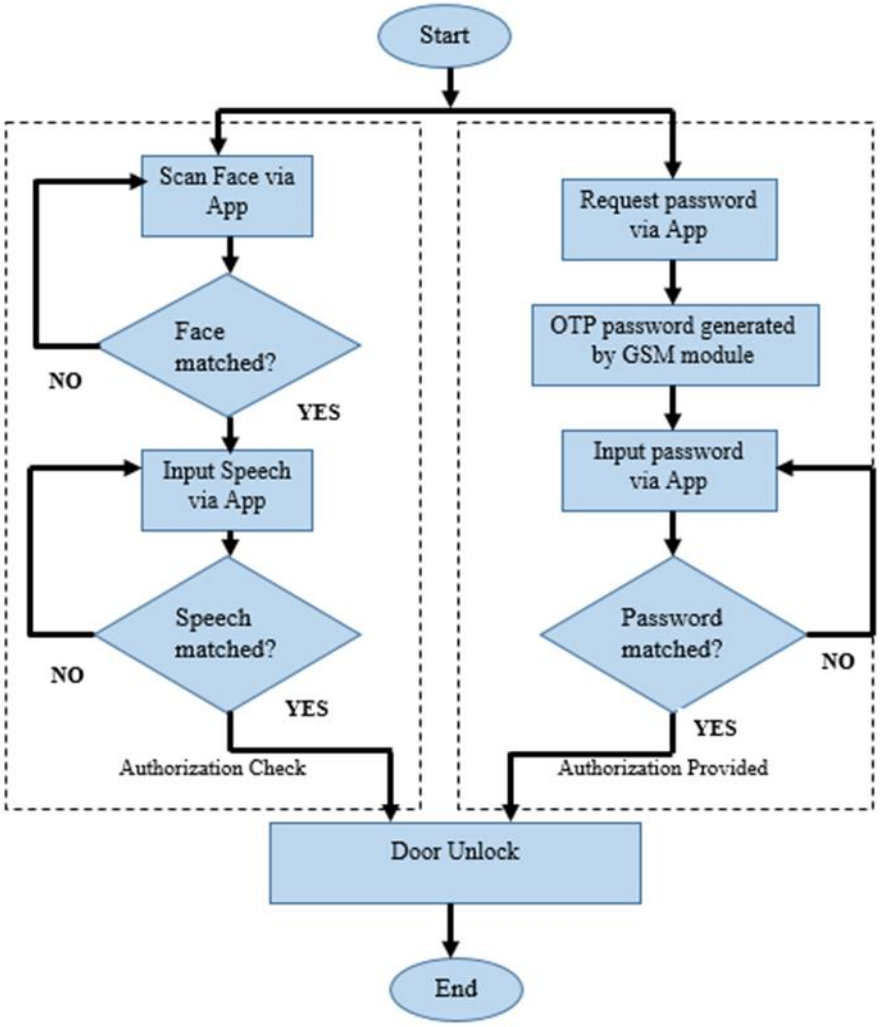

Figure 1. Flow Chart of the System

In order to ensure the authorized access, we have implemented two-layer security with face detection and speech recognition. This layered security is implemented in Android App and the app is connected to the microcontroller "Arduino Nano" via Bluetooth module.

The person or a number of persons who are authorized to unlock the door, are previously face scanned and stored in the database. As depicted in figure 1, when the authorized person is willing to unlock the door, he first scans his face through the App and after being matched with the stored image, he enters the second layer of security which is speech recognition. The speech recognition is done by implementing a number of security questions. We have used three security questions to ensure the matching of speech. To pass the speech recognition phase magnificently, all the three questions are needed to be answered acceptably. The security questions can be altered at a regular time interval. Either of the security layer (face detection and speech recognition) is maintained,

the door is kept locked. If a person, in case, is able to pretend to be authorized and breaks the face detection layer, the speech recognition layer is there to keep the system secure. This system is implemented specifically to secure a room or bank vault or a server room which is accessible by a limited number of authorized persons. The persons who are authorized are provided the app to use as a key.

Another way is collaborated with the system to work in case of giving authority to an unauthorized user. Passwords are the hidden keys to access a chamber. The benefit of password over keys is its portability over the network. An unauthorized user whose image is not in the database but needs the authority can request for a password to unlock the door using the app. The request is processed by sending a message containing a random password from the GSM module to the authorized person. He can then convey the password to the person wanting authority. The person then can input the password through the app and if matched with the generated one, the door is unlocked.

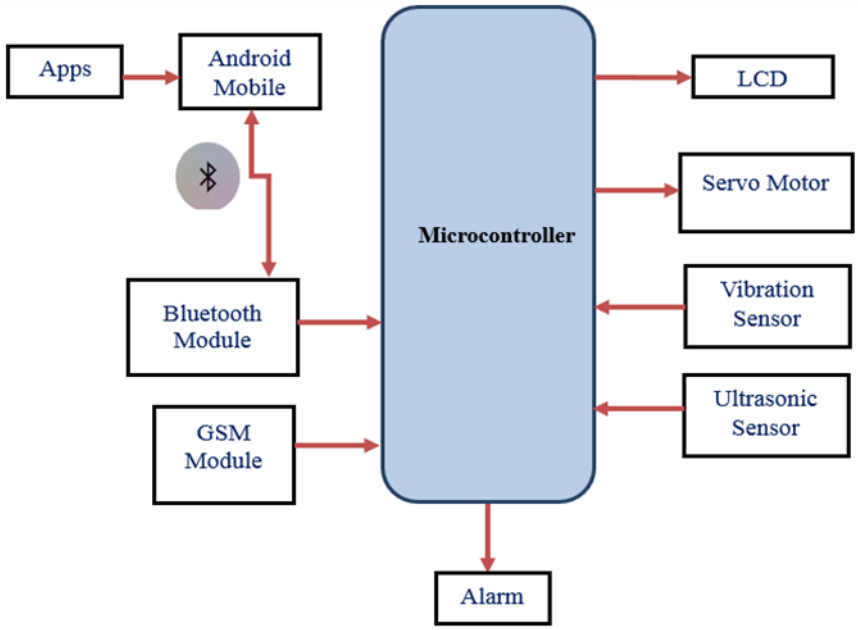

Figure 2. Block Diagram of the System

A number of devices and sensors are connected to the Arduino nano as shown in figure 2. A vibration sensor and an ultrasonic sensor are connected to detect the attack by the intruder if he wants to open the door forcefully. An alarm is set when the vibration sensor senses the attack and an alert message is sent to the authorized user automatically from the GSM module.

A LCD display module is connected show the system progress i.e. what is going on behind the scene. A glimpse of the circuit diagram that was implemented using the block diagram is depicted in figure 3.

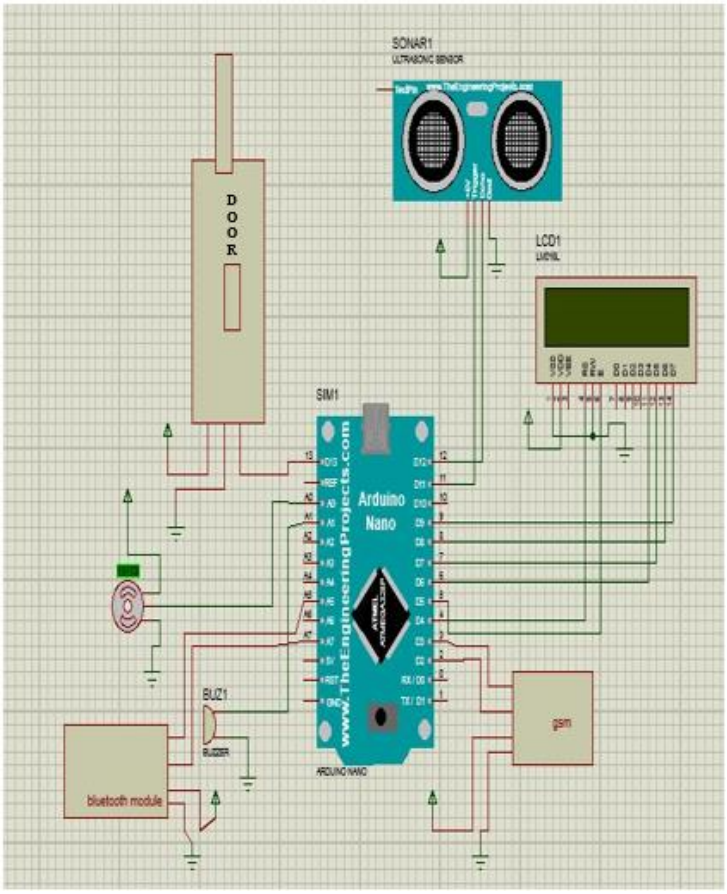

Figure 3. Circuit Diagram

Our system will operate in three different phases. The first phase is to capture and creating a database, the second one is to scan the image of the authorized user or the intruder and compare it with the images in the database and third phase is to provide the intruders report to authorized user and allow him to take actions over the network.

3.2. Hardware Components

The list of hardware components employed in the circuit [11] are i) Arduino Nano ii) Power Supply Circuit (SMPS) iii) Vibration sensor iv) Ultrasonic Sensor v) Bluetooth Module (Hc05) vi) GSM Module (SIM 800L) vii) Transistor viii) LCD ix) Buzzer x) Servo Motor xi) Diode xii) Vero Board.

3.2.1. Arduino Nano

Arduino Nano is the main controlling unit to which other modules and sensors are connected [9]. It is a microcontroller board designed by Arduino.cc. The microcontroller used in the Arduino Nano is Atmega328, the same one as used in Arduino UNO. It is a microcontroller board well-known for its small size and flexibility and possess a wide range of application areas. Initially, we captured the images of the authenticated users to create a database for Arduino Nano module storage system and this database is compared to the live image captured and provided by the camera module of android device. After comparing two images using PCA algorithm [3][4], output is considered to be positive/negative as this controller is digital; and based on the output response, it gives commands to GSM module.

3.2.2. Vibration Sensor

Vibration sensors, also known as piezoelectric sensors, are versatile tools for the measurement of various processes. These sensors use the piezoelectric effect, which measure changes in pressure, acceleration, temperature, strain or force by converting them to an electrical charge. The vibration sensor is used in the system to detect any kind of unethical access when an intruder wants to break the door.

3.2.3. Ultrasonic Sensor

The HC-SR04 ultrasonic sensor uses sonar to determine distance to an object like the way bats do. It offers excellent non-contact range detection with high accuracy and stable readings in an easy-to-use package. It comes in complete with ultrasonic transmitter and receiver module. It provides 2cm - 400cm non-contact measurement function. In our system, this sensor works simultaneously with the vibration sensor to detect attack.

3.2.4. Bluetooth Module

The version of Bluetooth module we used in our system is the HC-05 module. It has a default Baud rate of 38400. The android app gets the connectivity with the Arduino Nano via this module.

3.2.5. GSM Module

GSM is an open and digital cellular technology used for transmitting mobile voice and data services. A GSM digitizes and reduces the data, then sends it down through a channel with two different streams of client data, each in its own particular time slot. *SIM800L* GSM/GPRS module is a cheap miniature *GSM modem* that is used for IoT projects. In our system, GSM module is used for sending a message to the authorities after comparing the captured image with the stored images and based on whether the output is positive or negative. If the output comes out positive it means the person is identified and the door is unlocked.

3.2.6. Servo Motor

The servo motor is commonly used for automation technology in the industrial application areas. It is a self-contained electrical device that can rotate parts of a machine with high efficiency and great perfection. The output shaft of this motor can be moved to a particular angle. We used the servo motor to unlock the door.

4. System Implementation

We implemented the system in two different categories. First we designed the hardware module using the block diagram and circuit diagram in figures 2 and 3. Then we designed the android app using the flowchart in figure 1. The implemented circuit is shown in figure 4. The designed app depicted in figure 5 is connected to the circuit via Bluetooth module.

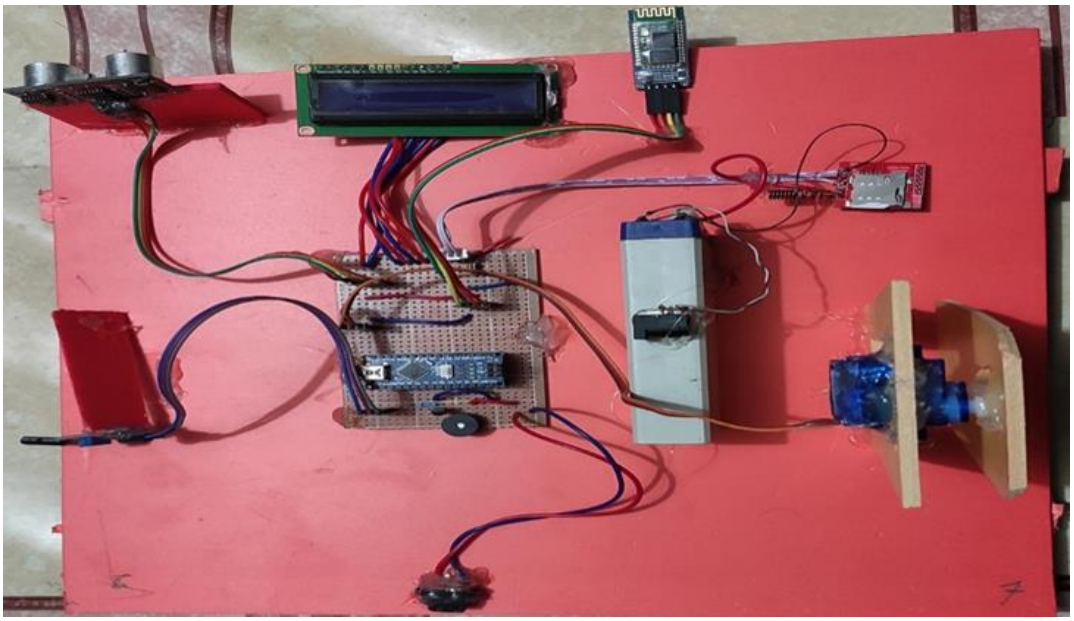

Figure 4. Project Circuit View

The android app is responsible for the detection and recognition of face and speech. The app is designed using android studio. PCA algorithm is used for detecting and recognizing the face in the image.

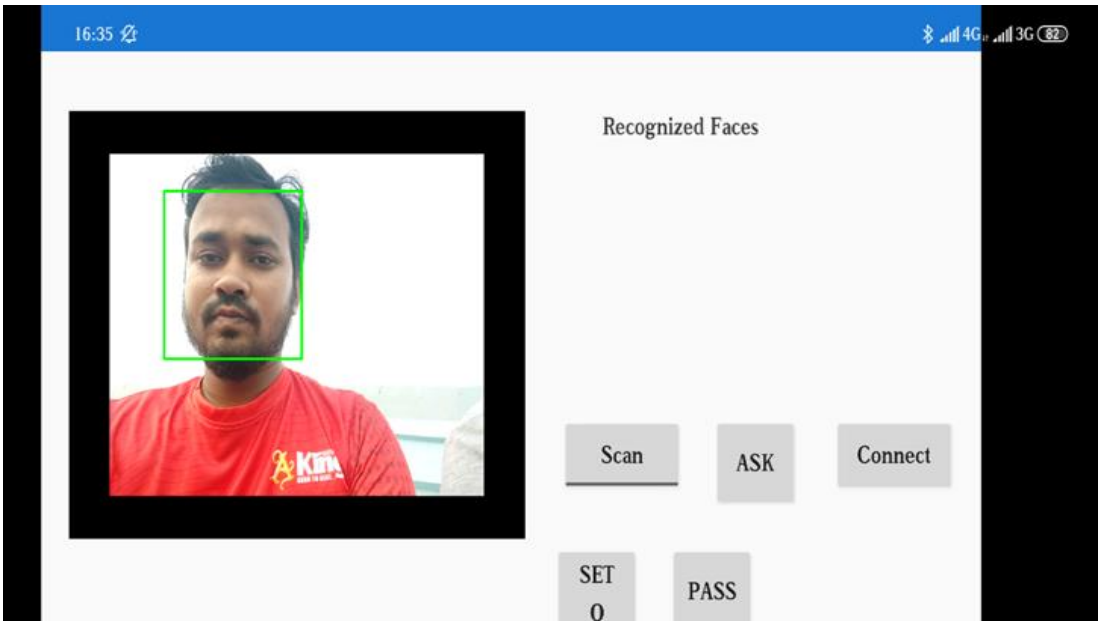

Figure 5. Android App View

5. Result and Discussion

The system is tested with number of authorized and unauthorized faces for both of the phases of security. The first phase of checking authorization was done with about 20

faces. After the detection of faces, the user is asked three security questions. Each of the data falls in either of the categories represented in table 1.

Table 1. Result Testing For Authorization Check

Serial Number	Face check	Question check	Door condition	System
1	OK	OK	Open	OK
2	Wrong	OK	Close	OK
3	OK	Wrong	Close	OK
4	Wrong	Wrong	Close	OK

If both the 'Face check' and 'Question check' are ok then door is automatically opened and system is assured as 'OK'. If any of checking is evidenced wrong then the door is kept closed and system is also ok. We got 98% accuracy in testing the result.

Table 2. Result Testing For Providing Authorization

Serial Number	Request for OTP	Input OTP	Door condition	System
1	OK	OK	Open	OK
2	OK	Wrong	Close	OK

We tested the second phase of security of providing authorization with 10 different users though this phase is unaffected by the variation of users. Every time a new OTP is generated and as referred in table 2 if only the user inputs the valid OTP through the app, the door is opened and closed otherwise. In both the cases the system is ok. We got 100% accuracy in the testing of this phase.

Table 3. Cost Calculation

Serial Number	Components name	Cost (in BDT)
1	Vibration sensor	80
2	Bluetooth sensor (Hc05)	260
3	Ultrasonic sensor	80
4	LCD	110
5	Vero board	20
6	Buzzer	10
7	Arduino Nano	60
8	Power Supply (SMPS)	80
9	GSM Module (SIM 800L)	450
10	Servo Motor	150
11	Battery	95
12	Others	200

	Total Cost	1695 tk.

As one of the prime objectives of our research was to design the system economically, we calculated the cost in BDT as depicted in table 3. The hardware cost of the system is 1695 tk. only which is quite reasonable and serves our objective successfully.

6. Conclusion

We designed the System to ensure security with less human effort in an affordable cost. The system is very simple, economic, and reliable and the needed hardware components are easily available. It is also portable and easily upgradable. Our target was to secure a single room with less authorized access so that the device internal storage is enough for the database in order to keep the cost to minimum. We used an effective alarm and notification system in case of intrusion detection so that the valid users can take necessary actions in shorter span of time. As we focused on securing a specific room in a reasonable manner, our database was kept small. If we need to implement the system for the entire home or office where a larger group of people need access, firebase can be used as an extended database. Moreover, a close circuit camera with Raspberry pi can be considered as future scope for better computing.

References

[1] Panwar, G., Maurya, R., Rawat, R., Kanswal, R., & Ranjan, P. (2017). Home automation using IOT application. International Journal of Smart Home, 11(9), 1-8.

[2] Sharma, V., & Tiwari, R. (2016). A review paper on "IOT" & It's Smart Applications. International Journal of Science, Engineering and Technology Research (IJSETR), 5(2), 472-476.

[3] Vinat A., Akshay Kumar C., Gaurav Shenoy, K.N. Balasubramanayam Murthy, S. Natarajan. (2015). ORB-PCA based features extraction technique for face recognition. International symposium on computer vision and internet.

[4] Makwana, H., & Singh, T. (2014). Comparison of different algorithm for face recognition. Global Journal of Computer Science and Technology, 13(9).

[5] Patel, A., & Verma, A. (2017). IOT based Facial Recognition Door Access Control Home Security System. International Journal of Computer Applications, 172(7), 11-17.

[6] Vamsi, T. K., Sai, K. C., & Vijayalakshmi, M. (2019). Face Recognition based door unlocking system using Raspberry Pi. International Journal of Advanced Research, Ideas and Innovations in Technology,(IJARIIT), ISSN.

[7] Arifin, R. D. H., & Sarno, R. (2018, March). Door automation system based on speech command and PIN using Android smartphone. In 2018 International Conference on Information and Communications Technology (ICOIACT) (pp. 667-672). IEEE.

[8] David, A., Chinaza, M., & Jotham, O. (2017). Design And Implementation Of A Door Locking System Using Android App. Int. J. Sci. Technol. Res, 6(08), 198-203.

[9] Abdul Azeem, Sathuluri Mallikharjuna Rao, Kandula Rama Rao, Shaik Akbar Basha, Harsha Pedarla, Modela Gopi, "Door Unlock using Face Recognition", International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 6, Issue 4, April 2017.

[10] Patel, P., & Ajani, S. (2016). "The Digital Locking and Unlocking System Based on Android for Smart Phone", International Journal of Advanced Research in Computer Science and Software Engineering, 6(2).

[11] Louis, L. (2016). "Working Principle Of Arduino And Using It", International Journal of Control, Automation, Communication and Systems (IJCACS), 1(2), 21-29.