International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 10 Ver III || Oct 2018 || PP 59-64

Iot Based Smart Secure Abode

Raksha K R[1] , Nagashree H S[2]
[1](Computer Science, PESIT-BSC, India)
[2](Information Science, BNMIT, India)
Corresponding Author; Raksha K R

Abstract : *Increased home security threats like theft, trespassing events and energy crises causing power cuts in developing and under-developed nations are alarming issues. The paper discusses a project that successfully combats these problems by implementing a dual layer lock for the main door of the residence using an arduino system so as to increase the security level. A dual layer lock works well to provide additional security when compared to an conventional uni-layer lock. It also allows remote access control of the appliances using an android application to direct power consumption. The android application also comes up with a door control system via a internet source to check guests arrival in absence of owner. The system suggested here thus subsides the security and energy related issues at a home level.*

Keywords : *IoT, Arduino Mega 2560; Biometric Identification, Spoof Attacks*

Date of Submission: 08-10-2018 Date of acceptance: 23-10-2018

I. INTRODUCTION

The growth of Internet Of Things Domain is significantly revolutionizing our homes, cites and world at large. The Internet Of Things here is used for a smart home network, with a Arduino Mega 2560 embedded system in order to control the home devices and to allow these appliances to exchange data using the internet connectivity.

The research woes its roots to the project Smart Secure Abode which has been built from a systematic study of various Smart Home models. The paper aims at solving the issue of home security threats and energy crisis at large. For the first time a dual layer lock for a house has been developed which proves to be more secure than a uni-modal lock. The project also extends to handle guests arriving home by means of remote access control of the main door. A dual layer lock consists of a fingerprint identification as the first layer and a password authentication system as the second layer. This type of combination lock system exhibits higher levels of security by overcoming the disadvantages of a uni-modal locks and can effectively be a part of the smart home model in the future.

The second part of the proposed smart home system is the smart android connect. The android application helps the user interact with the arduino mega system by providing remote access control via an internet connection. Today the internet world statistics says approximately 99% of the people are able to access the internet [1]. The availability of 4G/3G internet bands and Wi-Fi connections allows the proposed system to be accessed from any part of the world.

In this paper we propose development of a dual layer lock and the use of a smart phone with an android application for improved security purposes. Our major contributions are as follows:

- developed and implemented a Dual layer door lock IoT system for house member authentication.
- implemented an android application for directing power flow for the appliances using the internet.
- developed a mechanism to handle guests in absence of the owner by providing remote access to the main door using an android application.

1.1. PROBLEMS WITH KEY BASED LOCKS

The ancient physical locks can be easily broken, keys can be duplicated or lost. When the number of house members increase managing a physical key or making multiple their duplicates is a tedious task [2]. Thus a regular lock system comes up with multiple disadvantages which can be solved using a keyless system.

The rest of the paper is organized as follows: the next section deals with related work. In this section, we discuss the difference between our project and other existing systems. Then we discuss the details of the proposed system. This section is then followed by evaluation and extension of our system . Finally we conclude with some future advancements to our system.

II. Related Work

Smart locks have been in the market from almost a decade [3]. Currently all the locks available are uni-layer locks. The uni layer usually stands for a password lock, RFID card lock or an biometric lock.

Even Kiwikset a door lock which is predominantly sold in today's market mainly in The United States is also a uni layer lock with a smart key and android connect [4]. The Kiwikset locks come up with a password control layer and are capable of generating up to 30 unique keys for members and guests. Our system definitely provides better security due to the existence of another layer and also eliminates the generation of multiple unique keys.

A paper by Imran Quadri and P.Satish talk about a home security system with a web interface and password control lock [5]. Another reference paper by Jayashree and group discuss a finger print based lock system and shared access [6]. The paper by Wu ping and group, describes an intelligent remote monitoring system and biometric authentication [7]. All the above type of lock systems are a uni modal system. The uni modal biometric finger print systems are faced with a variety of problems like noise in the sensed data, cuts, and spoof attacks [8].

Ming Wang and group's paper talks about a Wi-Fi module and Smart Controller system for controlling the appliances [9]. Freddy K Santoso and Nicholas C H paper describes a Wi-Fi based IoT smart home system that allows communication between IoT devices and also uses an android app to control and monitor devices [10]. Kumar Mandula and group's paper talks about a micro-controller based arduino board based system [11].

We overcome the problems of finger print as a biometric by enrolling more than one finger print for the same person and the additional combination with password system allows us to nullify a spoof attack on the biometric system. Even in case a hacker hacks the password system using a brute force method still crossing the first layer of finger print security is challenging. The priority order of the dual layer lock makes hacking a difficult task.

The android application communicates with the arduino system via the internet which allows remote access. The remote access to the door in additions helps the system to handle the arrival of guests.

III. Architecture Of The System

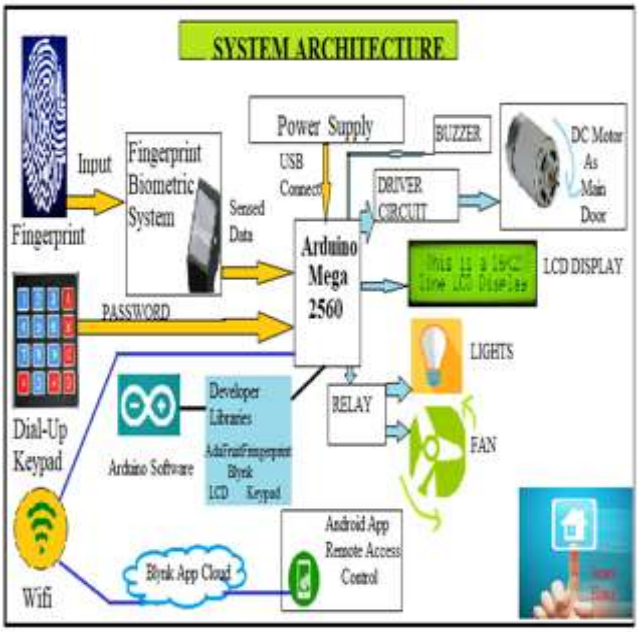

Figure 1: The System Architecture Along With Android App

The power of the proposed architecture lies in the dual layer door lock system. The android application is also an added advantage to direct power supply to the appliances, and to access the door lock remotely.

The Figure 1. shows a door lock consists of two layers. The first layer is built by the finger print authentication layer which checks for the finger print against the prints enrolled in the database. Once the finger print is identified the system readily posses the second wall of security the password lock. The password lock being the second layer has a direct dependence on the finger print biometric lock. Only when a member of the house is able to provide sufficient data inputs for both the layers only then the arduino mega system causes the motor to rotate, which in turn causes the door to open.

At times when the member of the house or a trespasser fails to pass the biometric lock layer; a buzzer is made to ring and a notification is sent to the android application. Even under similar cases when the user has

successfully passed the finger print lock layer and has discrepancies related to the password. Again a notification and a buzzer is raised to alarm about an unauthorized access.

The android application poses an ability to connect to any available source of internet access. It comes up with three buttons and a notification center. The three buttons controls an appliance like lights, fan, door lock respectively. An additional set of buttons or switches can be created to handle many more appliances. This direct power control is a real need of a smart home.

The project effectively handles circumstances when a guest or a familiar person arrives surprisingly and the owner is away from the house. Accordingly the house owner can provide entry to the guest by simply accessing a button on his android application. Further down the paper explains the various parts of the system.

3.1. HARDWARE

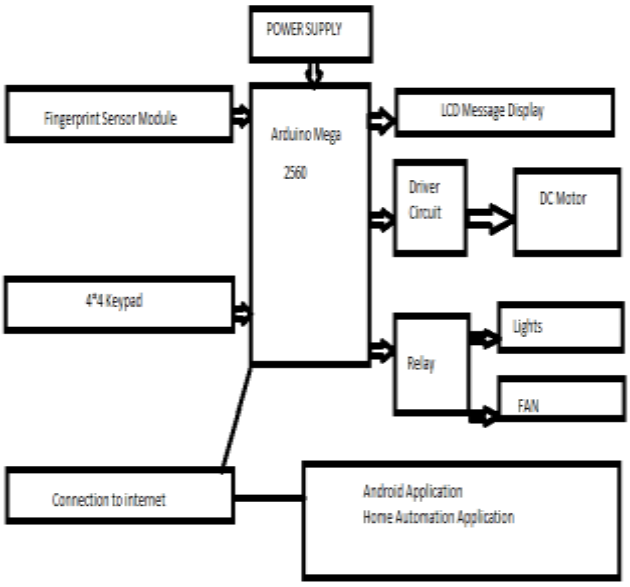

Figure 2: The System Hardware Circuit Block Diagram

The Figure 2. explains the base hardware circuit. The circuit consists to various hardware components attached to the arduino mega 2560. The fingerprint sensor module and keypad are used to take inputs from the user.

The Arduino Mega 2560 is used to handle a large number of I/O lines [12]. It also comes up with a large memory capacity and multiple digital and analog pins.

The finger print sensor module can store up to 162 finger prints. This large storage capacity allows us to store more than one finger print per person. So that in case of any cuts, or bruises on one finger, the second enrolled finger can always be used.

The 4*4 dial up keypad is used for the creating the second layer lock. The DC motor connected via the driver circuit is the actual main door lock indicator. The buzzer acts effectively to raise an alarm. The relay board helps the arduino to link to the appliances.

The LCD display provides communication with the user by displaying all the major messages. The message set includes enrollment, authorization and access.

In addition the circuit consists of a DC motor that acts as the main door dock. It is controlled directly by the arduino mega 2560 and by the android application indirectly. It has been connected to the arduino via a driver circuit so as to balance the voltage with regard to the DC motor. The relay board helps in managing the load of the appliances connected. Currently the circuit consists of a light and fan only as an appliance. In the future there can be a n addition of higher order appliances ranging from heating to lighting systems with an inclusion of voltage stabilizers and a change from arduino mega 2560 to raspberry pie board can also be considered.

The buzzer works well and notifies all illegal access cases, this is directly connected to arduino mega. It also alarms simultaneously with the android notification.

Figure 3: The Hardware Components

3.2. SOFTWARE

The programming language used to build the system is arduino via the Arduino IDE.

The enrollment code: approximately two finger prints per person is enrolled using a unique numeral from 1-162 numbers. The finger print is stored in the flash memory of the biometric module. Then finger prints consisting of ridges and valleys is observed for a minutiae pattern then the distance and angles are computed and finally it is converted to a unique numeric codes.

The Authentication and appliance control code: it deals with the two layer door lock authorization and the remote access control code of the appliances. The code also works on the notification system and message display.

3.3. ANDROID APPLICATION

Blynk android application from the Google Play Store is used as a base application for the Smart Secure Abode android application [13]. Using the inbuilt application interfaces Blynk libraries in the arduino coding the application suitable to our project is developed.

Android application allows access of appliances as well as the main door by directing the instructions to the arduino mega via the internet.

The execution process involves an implementation of the Blynk server file available with the Blynk library file set. The server file helps create a link to the Blynk cloud. Thus the data for directing the power flow travels via the server and provides control by the internet.

The Figure 4. shows three buttons for light, fan and door respectively. Additional buttons can be added for further extension of appliances. The figure also comes up with a image of the notification that the owner will receive when an unauthorized person will try to barge in to the house.

The application is currently available only for android devices but in the near future iphone applications can also be incorporated. This will allow a wide range of users to use the smart abode system. And will also increase the market for the system.

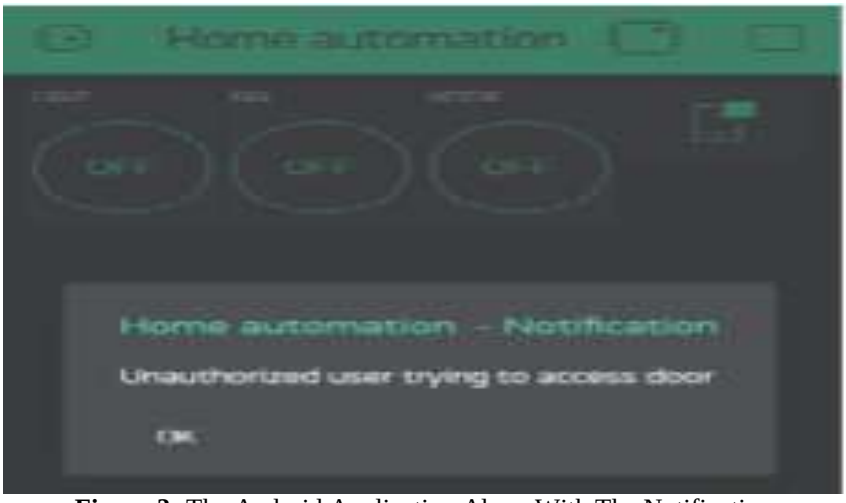

Figure 3: The Android Application Along With The Notification

IV. EVALUATION OF THE SYSTEM

The system is tested to satisfy the various requirements both at unit level as well as at the system level. The system is also evaluated for its timing and also its handling of special cases. The pros and cons of the system throw more light on the system application.

4.1. TESTING

Unit Testing: Under this each module is tested individually. We mainly checked for the proper functioning of the different devices.

Integration testing: are done to check whether all the systems interact correctly. And to check how the two layers of the lock work as whole.

Considering special cases when an unauthorized user tries to break in, a real time notification is sent. In cases where the house member forgets the password. A password reset option from the android application can be provided in the future.

4.2. BENEFITS

The advantages are plenty in number like:

- Increased security due to handling of spoof attacks and brute force attacks.
- Real time alerts and better responsive service due to the availability of the android application.
- Enables new operating model with better resource management.
- A successful system handling both security and energy systems.

4.3. COSTS

- The use of biometric sensors makes the lock system a bit more expensive than the normal lock and key system. Nevertheless it multifold the potential security levels.
- The absence of a camera for visual monitoring of the users would definitely simplify the guest case working and also guarantee higher security levels.
- The system still has to be developed for considering specially able people.

V. SMART CONNECT

5.1. SMART CONNECT TYPES

The availability of smart speakers like Google Home and Amazon Echo have helped establish a control to the smart home [14,15]. These speakers accept voice instructions as an input and with the help of an artificial intelligent agent like - Google Assistant for Google Home and Alexa for Amazon Echo; they execute the commands.

Currently these speakers monitor and control home automation system with the help of an application linked to the agents.

5.2. LINKING

We predict that in the near future the android application developed in our project could be attached to such speakers in order to direct power supply to the appliances .

Such a system will revolutionize the home automation and will provide a more convenient platform to operate the devices.

5.3. APPLICATION

The existing systems require a ready connection to a set of Smart Devices [15,16]. i.e. devices with Wi-Fi connect and many more. With the addition of the smart home application to these speakers in the near future. A need for such Smart Devices can be minimized thus reducing the cost on the whole. Since the project Smart Secure Abode uses regular devices controlled by the arduino and the android application, the need for Smart Devices is vanquished.

VI. CONCLUSION

In conclusion the paper lucidly describes the need for a dual layer security lock system rather than a mere uni modal lock. The paper enhances the usage of a keyless system and also efficiently portrays as to how to develop such a system. The project described here is an upright and simple solution to the energy and security crisis. The guest case handling by the system is definitely the one option the world is looking for. In addition the project comes with a flexible architecture for future enhancements.

FUTURE ADVANCEMENTS

The System can adapt to use a magnetic door lock in replacement of a dc motor to lock and unlock the door. Since it is more effective while considering a practical door lock system.

The future adoptions may consider placing a camera for continuous monitoring of activity in front of the door. Also the use of biometric device can be replaced by a camera for facial recognition along with a IR sensor and lights for authentication layer one. Such an advancement is beneficial but the accuracy of the algorithms used will have to be studied.

A voice control system with real time voice recognition software can be incorporated. For this a microphone will have to be installed. An level of testing with regard to spoof attacks. The system can also be connected to app hosting Smart Connect system which will develop an advanced smart home system.

A multi modal system with combination of two biometrics will actually not be advantageous as it may again fail to handle specially able people.

ACKNOWLEDGEMENTS

We are highly indebted to all the authors whom we have referenced in this paper.

REFERENCES

[1]. Thewebsite on internet statistics"Internet World Stats- Usage and Population Statistics" https://www.internetworldstats.com/stats.html
[2]. The website "Pros and Cons of Having Normal Locks and Keys" http://www.allamericanlocksmiths.net/news/pros-cons-locks-house-keyed-alike/
[3]. Jamie O'Toole, "The 23 types of locks you must know" published on November 10,2016 http://www.rekey.com/locksmith/types-of-locks/
[4]. The website on latest locks "Kiwikset door locks" https://www.kwikset.com/
[5]. Syed Ali Imran Quadri, P. Sathish "IoT based home automation and surveillance system" published in the IEEE journal 2017, http://ieeexplore.ieee.org/document/8250586/
[6]. Jayasree Baidya, Trina Saha, Ryad Moyashir, Rajesh Palit, "Design and implementation of a fingerprint based lock system for shared access" published in the IEEE journal 2017, http://ieeexplore.ieee.org/document/7868448/
[7]. Wu Ping, Wu Guichu, Xie Wenbin, Lu Jianguo, Li Peng, "Remote Monitoring Intelligent System Based on Fingerprint Door Lock" published in the IEEE journal 2010, http://ieeexplore.ieee.org/document/5522970/
[8]. The IEEE paper "Biometrics Systems under spoofing attack: An evaluation methodology and lessons learned" published in IEEE Signal Processing Magazine, Volume 32, Issue:5, Sept 2015; ISSN: 1053-5888
[9]. Ming Wang, Guiqing Zhang, Chenghui Zhang, Jianbin Zhang, Chengdong Li, " An IoT-based Appliance Control System for Smart Homes" 2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP) June 9 – 11, 2013, Beijing, China.
[10]. Freddy K Santoso, and Nicholas C H, " Securing IoT for Smart Home System" 2015 IEEE International Symposium on Consumer Electronics (ISCE)
[11]. Kumar Mandula, Ramu Parupalli, CH.A.S.Murty, E.Mages "Mobile based Horne Automation using Internet of Things (IoT)" published in 2015 International Conference on Control, lnstrumentation, Communication and Computational Technologies (lCCICCT)
[12]. The website on arduino "Arduino- Arduino Mega 2560" https://www.arduino.cc/en/Main/ArduinoBoardMega2560
[13]. The website on blynk application "Getting Started with Blynk" https://www.blynk.cc
[14]. The article "Amazon Echo" http://en.m.wikipedia.org
[15]. The website for google home "Google Home-Smart Speaker and Home Assistant- Google Store" http://store.google.com
[16]. The article "Smart Devices" http://en.m.wikipedia.org

Raksha K R "Iot Based Smart Secure Abode ""International Journal of Engineering Science Invention (IJESI), vol. 07, no. 10, 2018, pp 59-64