

A Mobile Fingerprint based Smart Home Automation System

Veldanda Vijaya Kruthi¹, Sama Vishnu Vardhan Reddy², Badavath Srikanth³, Yennaboina Vishnu Vardhan⁴, Pasladi Satish Chandra⁵

^{1,2,3,4} Student, Department of Electronics and Communication Engineering, Teegala Krishna Reddy Engineering College

⁵ Assistant Professor, Department of Electronics and Communication Engineering, Teegala Krishna Reddy Engineering College

Abstract—This includes a smart and affordable door lock enhanced with a fingerprint interface. For implementing, we will be using the Atmega328, a mobile with fingerprint sensor, Bluetooth module, motor and some other hardware devices. The fingerprint sensor will be integrated in the mobile phone and the digital Lock is facing inner side of the door, so that people can't have access to the controlling system from outside. The latches will be fixed inside the door panel, so that the thickness of the door can help the latch's strength. We'll use a few latches within the panel to divide the force among them if tried to force in. The fingerprint sensor in the mobile will take the fingerprint of the user and forward it to the microcontroller to match with its records. If the print matches with one of the fingerprints of the microcontroller's memory, the microcontroller will lock or unlock the latch, based on its current state. If the fingerprint is foreign to the microcontroller, the buzzer will buzz and the user will have to try again. Here we create a Android App in a MIT App inverter or kodular and this App is very secure because it is not present in the play Store. Mobile phone is connected to the entire hardware with Bluetooth connectivity. The same android app is having different operating switches to control lights and fan of a house.

Index Terms— Bluetooth, Fingerprint, Microcontroller MIT App inverter

I. INTRODUCTION

These days office/corporate environment security is a major threat faced by every individual when away from home or at the home. When it comes to security systems, it is one of the primary concerns in this busy competitive world, where human cannot find ways to provide security to his/her confidential belongings manually. Instead, he/she finds an alternative solution which provides better, reliable

and atomized security. This is an era where everything is connected through network, where anyone can get hold of information from anywhere around the world. Thus chances of one's info being hacked are a serious issue. Due to these risks it's very important to have some kind of personal identification system to access one's own information. Now a days, personal identification is becoming an important issue all around. Among mainstream personal identification methods, we mostly see password and identification cards techniques. But it is easy to hack password now and identification cards may get lost, thus making these methods is quite unreliable.

II. EXPERIMENTAL METHODOLOGY

A. Methodology

This project includes a smart, affordable door lock enhanced with a fingerprint interface. For implementing this project, we will be using the Atmega328, a mobile with fingerprint sensor, Bluetooth module, motor and other hardware devices. The fingerprint sensor in the mobile will take the fingerprint of the user and forward it to the microcontroller to match with its records. If the print matches with one of the fingerprints of the microcontroller's memory, the microcontroller will unlock the latch, based on its current state. If the fingerprint is foreign to the microcontroller, buzzer will buzz and the user will have to try again. Here we create an Android App in MIT App Inventor or Kodular. This App is secure since it is not present in play store. The mobile phone is connected to entire hardware via Bluetooth connectivity as same the

android app is having different operating switches to control lights and fans.

B. Analysis

In this model, we are using ATmega328 microcontroller which is connected to the power supply. A relay module is connected to it. Relay is an electromechanical device that uses an electric current to open or close the contacts of a switch. Whenever the user gives fingerprint via bluetooth if it matches with the records of the microcontroller then the L293d Motor Driver will unlock or open the lock, turns on green LED light and displays on LCD that the door is unlocked. Whenever the given fingerprint does not match with the fingerprint records of the microcontroller it turns on red LED light, turns on the buzzer and displays that it is an unauthorized access. Motor driver will keep the lock in the same lock position. In the same way we can turn on Light and Fan using the MIT app just by clicking the buttons. We have used PIR sensor, a passive infrared sensor is an electronic sensor that measures infrared (IR) light radiating from objects in its field of view. They are most often used in PIR-based motion detectors. PIR sensors are commonly used in security alarms and automatic lighting applications.

III. MODELLING ANALYSIS

In this model, we are using ATmega328 microcontroller which is connected to the power supply. A relay module is connected to it. Relay is an electromechanical device that uses an electric current to open or close the contacts of a switch. Whenever the user gives fingerprint via bluetooth if it matches with the records of the microcontroller then the L293d Motor Driver will unlock or open the lock, turns on green LED light and displays on LCD that the door is unlocked. Whenever the given fingerprint does not match with the fingerprint records of the microcontroller it turns on red LED light, turns on the buzzer and displays that it is an unauthorized access. Motor driver will keep the lock in the same lock position. In the same way we can turn on Light and Fan using the MIT app just by clicking the buttons. We have used PIR sensor, a passive infrared sensor is an electronic sensor that measures infrared (IR) light radiating from objects in its field of view. They are most often used in PIR-based motion detectors. PIR

sensors are commonly used in security alarms and automatic lighting applications.

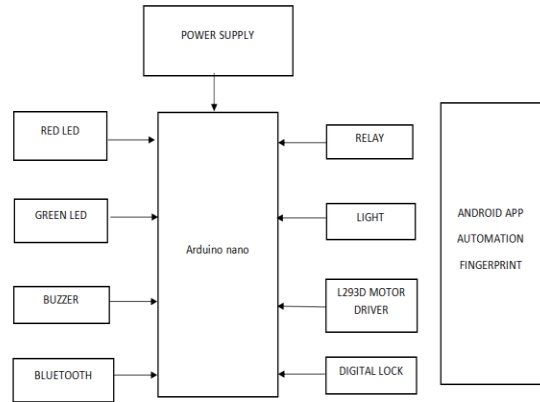


Figure 1: Block Diagram

IV. RESULTS AND DISCUSSION

Here is the practical implementation of “A mobile fingerprint based smart home automation system”. This prototype can be effectively utilized to control the home applications using mobile bluetooth. Whenever there is valid access green LED turns on and whenever there is an invalid access red LED and buzzer turns on.

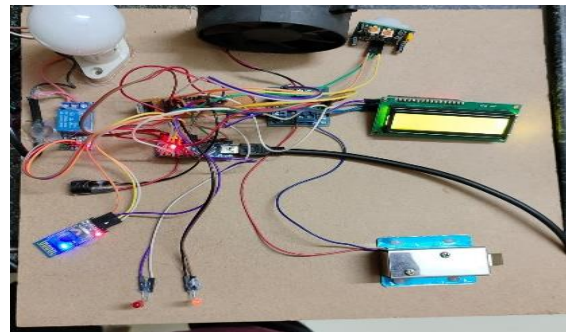


Figure 2: Green LED turns on when there is a valid access

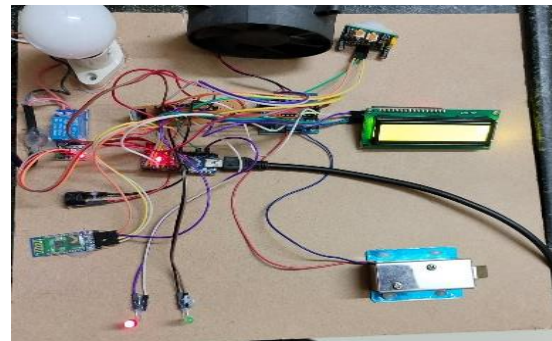


Figure 3: Red LED and buzzer turns on when there is an invalid access

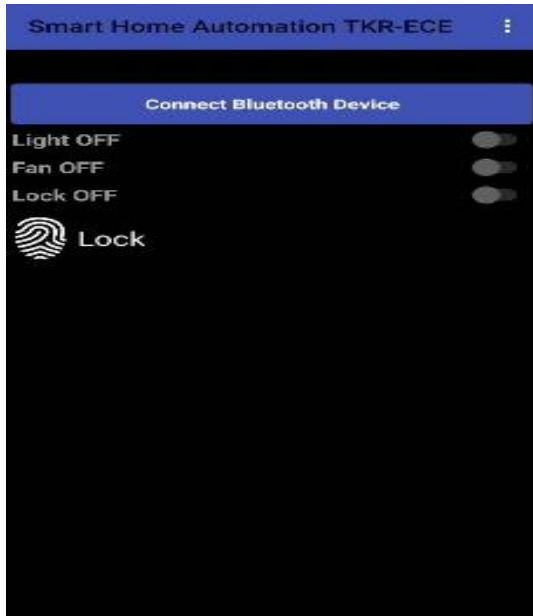


Fig 4: When the devices are OFF

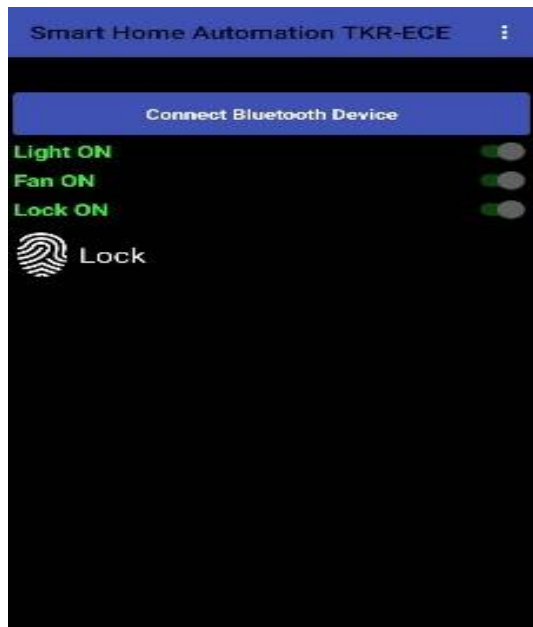


Figure 5: When the devices are ON

VII. CONCLUSION

The design and implementation of finger print based door lock system is customizable and flexible. This door locking mechanism is comparatively cost-effective than the available lock systems in the traditional market. Our finger print based lock system has high accuracy rate and is also quick to recognize fingerprints which enable seamless integration with the users and provides tighter security. In our country, private and government organizations are very much

concerned about security. Many companies are interested in using this type of locking mechanism but the system which is available have very high installation cost. Due to this excessive cost, many small firms cannot afford such systems. Keeping the installation cost in mind we planned to develop a system that should be affordable to both large and small firms.

REFERENCE

- [1] Anil K. Jain, Arun Ross and Salil Prabhakar. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and Video Based Biometrics, Vol. 14(1), January, 2004.
- [2] R. P. Wildes. Iris recognition: an emerging biometric technology. Proceedings of the IEEE, vol. 85, no. 9, pp. 1348-1363, September, 1997.
- [3] Anil K. Jain, Jianjiang Feng and Karthik Nandakumar. Matching Fingerprints. IEEE Computer, 43(2), pp. 36-44, February, 2010.
- [4] Mary Lourde R and Dushyant Khosla. Fingerprint Identification in Biometric Security Systems. International Journal of Computer and Electrical Engineering, 2(5), October, 2010.
- [5] Fernando L. Podio. Personal authentication through biometric technologies. Proceedings 2002 IEEE 4th International Workshop on Networked Appliances (Cat. No.02EX525), Gaithersburg, MD, 2002, pp. 57-66.