International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

DESIGN AND IMPLEMENTATION OF A FINGERPRINT BASED LOCK SYSTEM FOR SHARED ACCESS

K.MANISHA[1] D.DIVYA[2] B.PREMALATHA[3] A.NANDHINI[4] DR.A.KRISHNAMURTHY[5]

[1,2,3,4] B TECH Students, Department of ECE, Princeton Institute of Engineering & Technology For Women, Hyderabad, Telangana, India.

[5] Assistant Professor, Department of ECE, Princeton Institute of Engineering & Technology For Women, Hyderabad, Telangana, India.

ABSTRACT:

This paper presents an enhanced methodology in implementing and designing a security system for door locking purpose based on fingerprint, GSM technology, monitoring camera, alarm system and password system. This security system will provide enough security by limiting unauthorized people access and taking a record of those who pass through it. Sometimes unauthorized people or burglars try to break the door for evil intentions at a time when no one is available at a targeted place, so this paper introduces some security solutions for that problem and they are the main contribution of our paper. We introduce an alarm system to alert the people at the surroundings, GSM module that's used to send an SMS message to the registered user's (responsible person) and a web camera that's used to take a video for a person who tries to break the lock, password keypad that's used after fingerprint sensing to provide extra security. Definitely the registered users are the only persons who can access the lock, and the door closes after five seconds from the opening time. The method used to implement this experiment involves the use of a fingerprint scanner R305 that's interfaced with Arduino microcontroller-ATMEGA328P to control the locking and unlocking process of a door. During all the opening and closing processes, the16x2 Liquid Crystal Display (LCD) displays some commands which can be used to instruct the users like, place your finger on the sensor, the door is opened, the door is closed, the message is sent, please enter the password etc. If an unregistered user tries to access the door using their fingerprints, automatically his/her access is denied. The proposed door lock security system is can be used at homes, offices, banks, hospitals, and in other governmental and private sectors. Our proposed system was tested in real-time and has shown competitive results compared to other projects using RFI and password.

Keywords: IOT, Gas, Air pollution, with cloud resistance.

1. INTRODUCTION

Biometrics refers to the automatic identification of a living person based on physiological or behavioural characteristics for authentication purpose. Among the existing biometric technologies are the face recognition, fingerprint recognition, finger-geometry, hand geometry, iris recognition, vein recognition, voice recognition and signature recognition, Biometric method requires the physical presence of the person to be identified. This emphasizes its preference over the traditional method of identifying what you have such as, the use of password, a smartcard etc. Also, it potentially prevents unauthorized admittance to access control systems or fraudulent use of ATMs, Time Attendance Systems, cellular phones, smart cards, desktop PCs, Workstations, vehicles and computer networks. Biometric recognition systems offer greater security and convenience than traditional methods of personal recognition. Fingerprint recognition represents the oldest method of biometric identification which is dated back to 2200 BC. The use of fingerprints as a personal code has a long tradition and was already used. This system focuses on the use of fingerprints for door opening and closing. The fingerprint recognition software enables fingerprints of valid users of the vehicle to be enrolled in a database. Before any user can use the vehicle, his/her fingerprint image is matched against the fingerprints in the database while users with no match in the database are prevented from using the vehicle. A microcontroller stores the data equivalent of fingerprint of the master user. Comparison between this enrolled fingerprint and the fingerprint of the person who is about to use the vehicle is done by the micro- controller. If both the fingerprints are identical control circuitry of the microcontroller sends appropriate signals to the motor relays operating the door of the vehicle. If the fingerprints are not identical microcontroller sends signals to alarm circuitry to warn about an unauthorised use.

2. LITERATURE SURVEY

One more disadvantage of traditional lock is that when homeowners lose the key and have no alternative key, in this case, they should wait for long hours for a technician to come, otherwise they should break the door. Another challenge or disadvantage is that when the key is locked away or maybe misplaced inside the house, in this case even authorized persons won’t have access to his/her property or belongings. This will issue can be solved with the help of technician again and may cost the authorized [4]. In addition to providing access to the target building, personal belongings and important documents at homes or offices can be accessed depending on the lock system; personal belongings can be very valuable things such as expensive pieces of jewelry, confidential documents, and money in cash, etc. To overcome all those challenges and drawbacks in the traditional locks, smart security systems are developed which provide more security to the individuals, however, these systems are easy to use, to access, and can be reliable. Such of these security systems, the use of smartcards, voice technology, passcode, and biometrics [5-8]. In this work, we develop a biometric security system based fingerprint. Biometrics involves the science which can statistically analyze the biological characteristics. A biometric system is defined as a technology that can recognize and verify the identity of a person using a measurable physical or behavioural characteristic of the person. There are some conditions to choose characteristics such as performance, universality, collectability, uniqueness, acceptability, circumvention and permanence. Some other characteristics can be used by biometrics such as fingerprint, eye features, facial features, etc. [9]. Our work developed a biometric-based fingerprint which involves other technologies like GSM, cam web, and password keypad system. At present, there are six major biometric technologies available in today's market. They are Fingerprint recognition, Hand geometry recognition, Iris and Retina recognition, Voice recognition, Signature recognition, and Facial recognition. Of these recognition technologies, facial recognition, fingerprint recognition, and iris recognition are the most dominantly used for numerous applications. In this work, fingerprint recognition technology is considered. Fingerprint recognition technology is a technique that's used to detect and recognize different human fingerprints based on different patterns of fingers, which is found to be unique among each person. It is very common and maybe the best way of obtaining details of any person and identifying a person can be done most easily and conveniently [5]-[6]. Study of fingerprints for recognition and identification the individuals is scientifically called Dactylography. The main advantage of the fingerprint recognition method is that each person has a unique fingerprint pattern that remains the same and never changes throughout life, making the fingerprint recognition method an unfailing method of human identification.

3. RELATED STUDY

Door access control is accomplished by locks indoors [2]. Recent advancements in every phase of modern living and the world around us progressively digitized, it becomes very difficult for protecting one's confidential information. Old-fashioned passwords and keys are originally considered to be sufficient to provide secure data transactions or for any other purpose. However, in the current scenario, they became weak because of sophisticated hacker attacks and unauthorized users across the internet. With more and more electronic gadgets such as tablets, multiple sensors, smart phones, and cloud-based services, etc interconnected to the internet, and with simultaneous sending and receiving of data, there arises a need to keep the data unavailable to hackers and unauthorized individuals. To prevent this, passwords can be used. However, the problem is that the user may use the same password for multiple devices. Besides, these passwords are sometimes shareable and persons with strong technical knowledge can use a variety of methods to crack these passwords. During the time of civilization changes in different falling and rising manner, equipment, and tools used for security intentions developed by locksmiths [3]. In the period of medieval, there are many traditional methods were used to implement security tools. As days pass and time move on, that equipment and tools turned to be disused, as people could breach the perimeters of security set by the security equipment and supplement. . As a result, continually, people seek for more dependable and reliable measures of security. The blow winds of civilizations and industrialization movement all over the world have strengthened the deep intentions of individuals in manufacturing more advanced and sophisticated security systems which could be able to battle the obstacles and challenges of securing worthy possessions. Sometimes during the day, most of the homeowners leave their homes for different purposes, some of them go to their work offices, some of them go to schools, sport fields, farms, etc. thus, their homes will be easy to attack by burglars, because of homes' traditional locks which can be opened by the burglars in case if they have the same key or duplicate key to open the door, making their belongings such as jewelry, bank cards, money and other valuable things easy to steal, this is one of this disadvantages of using the traditional locks which has no security and no one can rely on.

4. PROPOSED SYSTEM

The block diagram of the implemented system involving all hardware components that are used to accomplish the security task. Arduino Uno microcontroller board acts as a master and it is the body of our project, while other hardware components act as slaves. The system behaves according to the written program and performs all mentioned security actions without human intervention, and all other automatic operations are carried out. All hardware components are of vital importance for the system to provide enough security, and all these tools work together under one controller.

Tx-out and Rx-in of the sensor are connected to the pin 2 and pin 3 of the Arduino Uno respectively. The electronic lock is connected with one of the output ports of the Uno. Making a network with the relay allows switching between the 5V and the 12V electrical components. Now we have attached the Arduino Uno to the laptop for registering fingerprints. We require the connection with the computer for assigning the ID to the prints. This can be done through Smartphone with Arduino application as well. We save the ID into the sensor and upload the code to the Uno. We disconnect the Uno with the computer and turn on the power adaptor. Once it gains power, the system boots up the fingerprint IDs saved inside and waits for a print to be matched. If no match is found, the keypad and the switch remain active. Once a match is found, the buzzer will buzz once and the lock will open. If no match is found, the system will not take any action at all. The scanner can perform over 100 scans per second, so when someone places a finger, it will respond instantly if the prints match. This system can store up to 126 fingerprint IDs. So, it can control the access of 126 different people. Review of the whole system

- 126 different fingerprints can be enrolled into the system to open door/doors.

- On placing a registered finger, the lock unlocks for 5 seconds with no noise or buzz.
- A 4-digit password can be entered through the keypad.
- Each key pressed results in a beeping sound. A successful code opens the door with a single buzz.
- An incorrect input will not open the door; the system will buzz shortly twice.
- 3 failed attempts on the keypad will make the system buzz continuously for 3 seconds notifying an intrusion attempt.
- On pressing the switch from inside, the lock unlocks for 5 seconds with a single buzz.

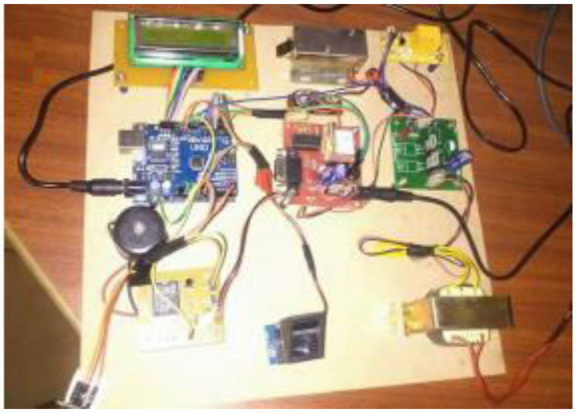

Fig.4.1. Hardware kit image.

The solenoid lock can be fixed on the door from inside and if it is at the closing state and then powered by an authorized person, the state will change to opening state and vice versa. The status of the solenoid lock is always displayed in the LCD screen, for example, if the door is opened then the status will be displayed in LCD. Different kinds of status are displayed by the LCD screen and each status denotes the current situation of the security system. The opening and closing situations of the solenoid lock are illustrated in the following figures; please focus on the lock to find out its situation. Our experiment is carried out with the help of several hardware components such as transformer, rectifier, LCD (16X2 lines), GSM Technology, keypad, piezo buzzer-12VAC, MEMS Sensor, optical fingerprint scanner-R305, solenoid door lock (NC-0837L). All these components are interfaced and connected to the Arduino Uno R3 microcontroller according to their functionality. It can be concluded that this security system can be improved by adding face recognition along with fingerprints in the more sensitive places which require higher security.

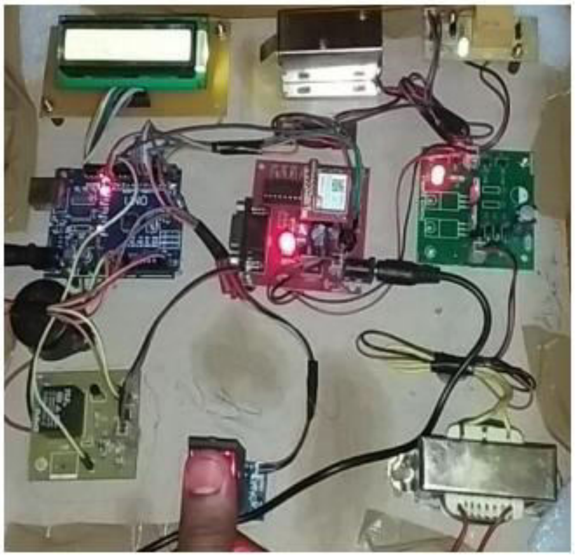

Fig.4.2. Door is closed

5. CONCLUSION

The design and implementation of fingerprint based lock system is customizable and flexible. This door locking mechanism is comparatively cost-effective than the available lock systems in the traditional market. Our fingerprint 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. This design can be improved by more intensive development and additional features such as more locks can be added to the system. Thus we do not need to spend so much for just one lock if this can be used to control several doorways. A system to save prints without the use of a computer could have been made, but it will require more parts than the ones we used.

REFERENCES

1. Winda WO, Mohammed S (2007) Intelligent Voice-Based Door Access Control System Using Adaptive-Network-Based Fuzzy Inference Systems for Building Security. J Comp Sci 3: 274-80.

2. Omijeh BO, Ajabuego GO (2013) Design Analysis of a Security Lock System Using Pass-Code and Smart-Card. IOSR J Elect Comm Eng 4: 64-72.

3. W.Dongdong, "Introduction of capacitive fingerprint sensor packaging technology," 2017 18th International Conference on Electronic Packaging Technology (ICEPT), Harbin, 2017, pp. 130-134.

4. R. Lazarick and P. Wolfhope, "Evaluation of 'non-traditional' fingerprint sensor performance," 2016 IEEE Symposium on Technologies for Homeland Security (HST), Waltham, MA, 2016, pp. 1-7.

5. S. Palka and H. Wechsler, "Fingerprint Readers: Vulnerabilities to Front- and Back-end Attacks," 2007 First IEEE International Conference on Biometrics: Theory, Applications, and Systems, Crystal City, VA, 2007, pp. 1-5.

6. T. Ogane and I. Echizen, "Biometric Jammer: Preventing surreptitious fingerprint photography without inconveniencing users," 2017 IEEE International Joint Conference on Biometrics (IJCB), Denver, CO, 2017, pp. 253-260.

7. K. L. Krishna, J. Madhuri and K. Anuradha, "A ZigBee based energy efficient environmental monitoring alerting and controlling system," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2016, pp. 1-7.

8. C. Lin and A. Kumar, "Matching Contactless and Contact-Based Conventional Fingerprint Images for Biometrics Identification," in IEEE Transactions on Image Processing, vol. 27, no. 4, April 2018, pp. 2008-2021.