Enhanced Security Methods of Door Locking Based Fingerprint

Hashem Alnabhi, Yahya Al-naamani, Mohammed Al-madhehagi, Mohammed Alhamzi

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: Security, System, Fingerprint, Sensor, Lock, Door, Access, Message.

I. INTRODUCTION

Security is considered as one of the most common issues that bring worries for a human being. We are all seeking practical solutions and suggestions which may keep our properties and privacies away from burglar's hands. Human being's home security and possessions can be one of the most essential challenges faced by individuals, corporate organizations or any other nation. This critical problem of lack of security of properties and intrusion into premises dates back to the early existence of humanity. Currently, building security can be easily achieved by the use of door security controls. It provides security limitations for unauthorized people and also takes information and records of all those who pass through it [1]. 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, smartphones, 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.

Revised Manuscript Received on January 05, 2020.

Hashem Alnabhi, Department of Electronics and Communications Engineering, Jawaharlal Nehru Technological University, Anantapur (Andhra Pradesh) India. E-mail; hashemalnabhi1994@gmail.com

Yahya Al-naamani, Department of Electronics and Communications Engineering, Jawaharlal Nehru Technological University, Anantapur (Andhra Pradesh) India. E-mail; yahyaan23@gmail.com

Mohammed Al-madhehagi, Department of Electronics and Communications Engineering, Jawaharlal Nehru Technological University, Anantapur (Andhra Pradesh) India. E-mail; mohammed736577@gmail.com

Mohammed Alhamzi, Department of Electronics and Communications Engineering, Jawaharlal Nehru Technological University, Anantapur (Andhra Pradesh) India. E-mail; maaymalhamzi@gmail.com

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 behavioral 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.

The sections of this paper are organized as follows. Section II discusses the design and implementation of the proposed biometric-based door locking system using Arduino UNO R3. Section III explains the preprocessing operations. Section IV. Flowchart of the entire working process. The hardware results and discussion are presented in Section V.

II. DESIGN AND IMPLEMENTATION USING ARDUINO UNO ATMEGA328P

Fig. 1. Shows 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.

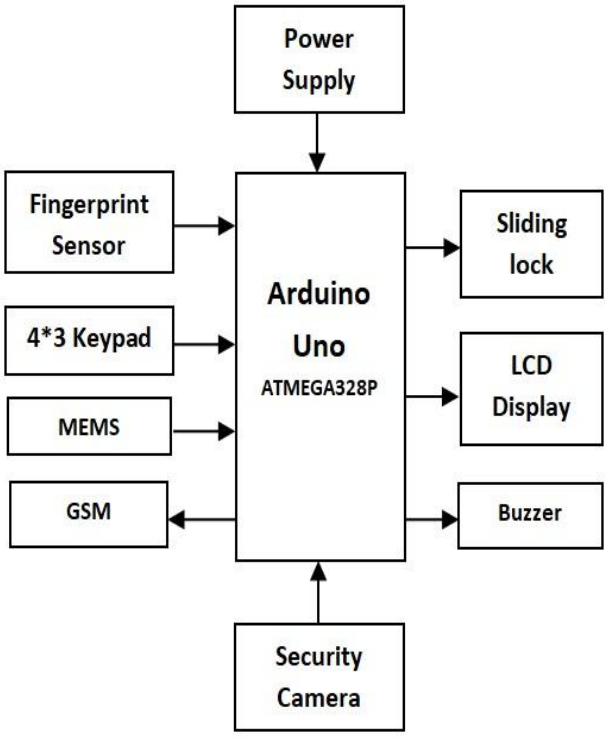

Fig.1. Block diagram design of biometric-based fingerprint door locking system

III. PREPROCESSING

the operation of fingerprint-based door locking system starts with adding fingerprints features of the authorized persons to the database of our system, by placing the finger on the fingerprint optical scanner, some features are extracted from the finger surface and stored to the database with specific ID and the name of the person can be added, the steps of this process are shown in fig.2. The features extracted from the finger surface are different from one person to another, this is because the finger's surface pattern has different characteristics related to core, ridges, island, and delta, pore, etc. these different characteristics of the fingerprint are illustrated in fig.3. if we want to check whether the fingerprint is already registered or not, it can be easily done by placing the finger on the optical scanner and then some features will be extracted from the finger and compared with stored features, if there is a similarity,

the door will open and if there is no any similarity, the door won't open.

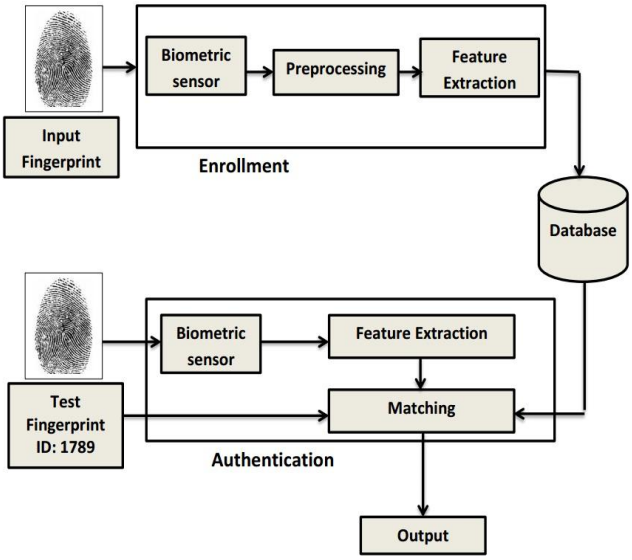

Fig.2 .The process of Extracting features from the finger surface and storing them in a database.

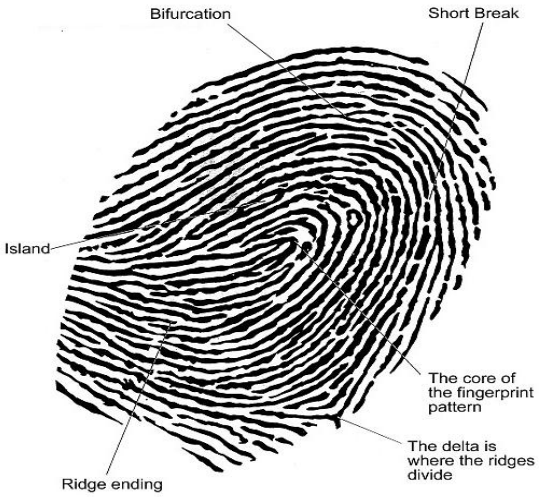

Fig.3. Typical View of finger surface pattern

IV. FLOWCHART

Fig.4 shows the hardware components of the system and the connectivity among them which is called the prototype of the entire system. Fig.5 shows the functional steps of our project, and all conditions are explained in this section. When the system is powered on, a sim card should be inserted into the GSM to be processed for a few seconds, after successful processing, LCD shows a command that says Network found as shown in fig. 6, and that means the system is ready to operate. At this stage, the welcome message will appear in the LCD screen as shown in Fig. 7. As we mentioned in section (III), our security system allows us to store the fingerprints and IDs of all persons who are considered to be registered, and all the corresponding data is stored in the database. The system provides double-check security by fingerprint and password. This security is tested and compared to other related projects and it is found to be more robust and secured. Nobody can open the door except the persons whose fingerprints are available in the database. If any stranger or bulger tried to open the door by placing his or her finger on the scanner, LCD shows that the fingerprint is not identified. if he/she tries to open the door more than three times the buzzer will be activated, thus will alert the people who are at the surroundings. In case he/she tries to break the door, by shaking, kicking the door or using any other tool, there is a sensor called Micro Electro Mechanical System which is very sensitive to small shakes as a result of shakes, it activates the GSM system to take an action and alert the responsible person by sending him/her a message as shown in fig. 8. In addition to that, the camera will record this crime, and with the help of all those mentioned technologies, it is possible to secure our homes, banks, and companies from such evil crimes by using this security system. But if any authorized person tries to open the door, he/she has to pass through two steps. The first step is placing the fingerprint for sensing and if it is successfully recognized, the system passes him/her to the next step that is entering the password; finally, the door will open and after 5 seconds will automatically close. The whole operation is controlled by the case program without our intervention, our job is to write the case program, fire it to the microcontroller board and make the connections between different hardware components.

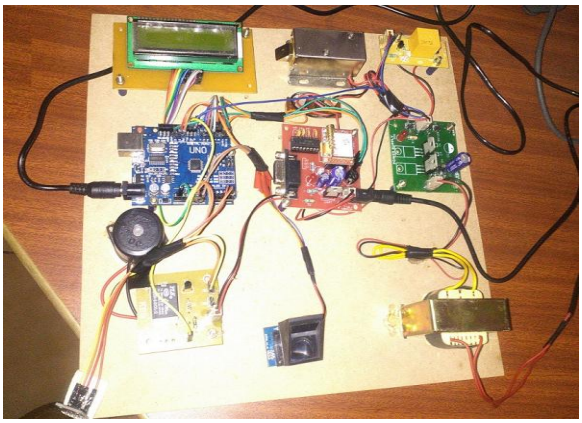

Fig.4. Prototype of the entire system

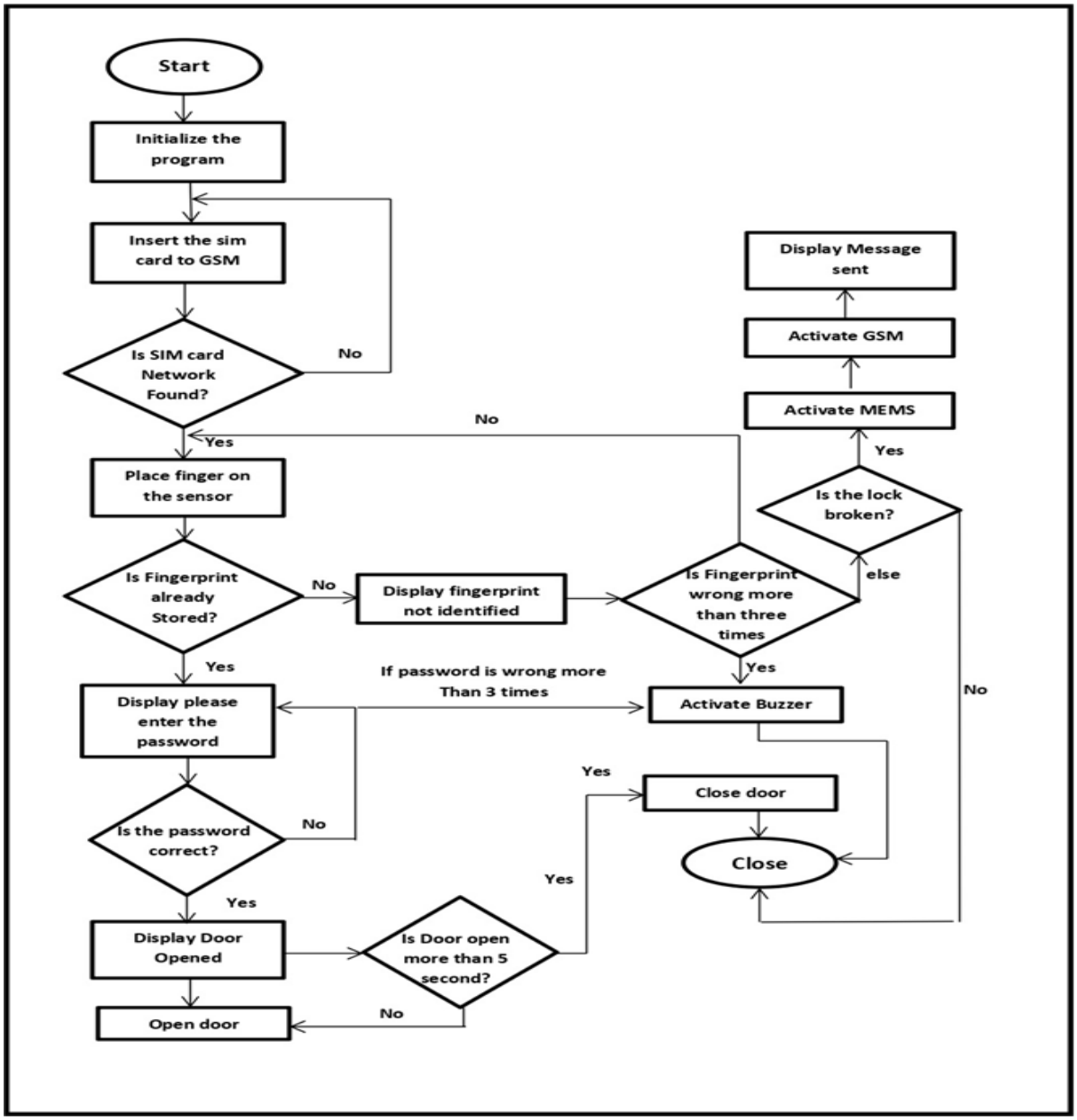

Fig. 5. Flowchart of system functionality

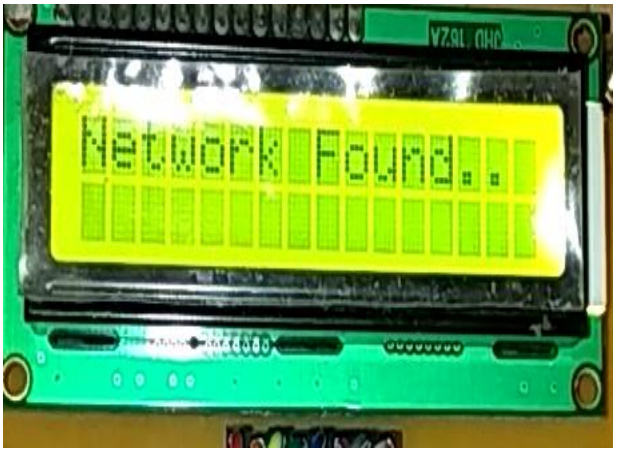

Fig.6. The LCD status after inserting the sim card

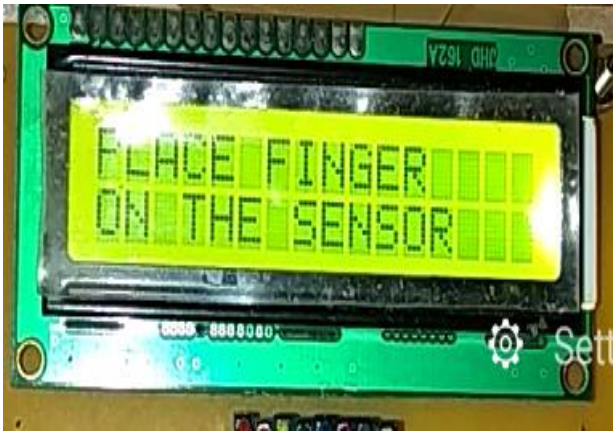

Fig.7. The LCD status when the system is powered on and ready to operate

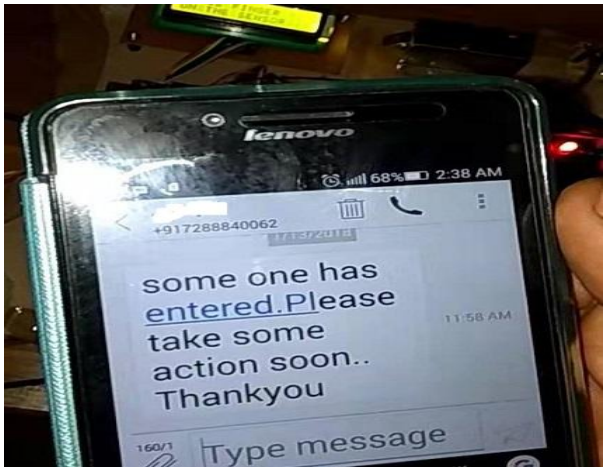

Fig. 8. The alerting message sent by GSM

V. RESULTS AND DISCUSSION

Implementation of our work is done in the real-time world, and our security system has shown competitive results compared to other door locking security systems. Arduino Uno R3 is the main microcontroller of the project and other hardware components are connected and interfaced with it. The functional relationship between the microcontroller and other hardware tools is complementary. We have used an optical fingerprint sensor (Fingerprint Reader R305) in our experiment. This sensor is very good as it is scratch-resistant and its image resolution is 500 pixels per inch. We have used Door lock solenoid (NC-0837L) for opening and closing purposes in our experiment and it is electromagnet which is made of copper wire winding with a plunger/cylinder in the middle. When authorized persons place their fingerprints and entering the correct password, the coil will be activated and energized, the plunger will be pulled into the center of the coil. Thus the solenoid will be able to pull from one end. So the solenoid lock operates once the power is drawn in its coil. 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 in fig.9 and fig. 10**.** 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.

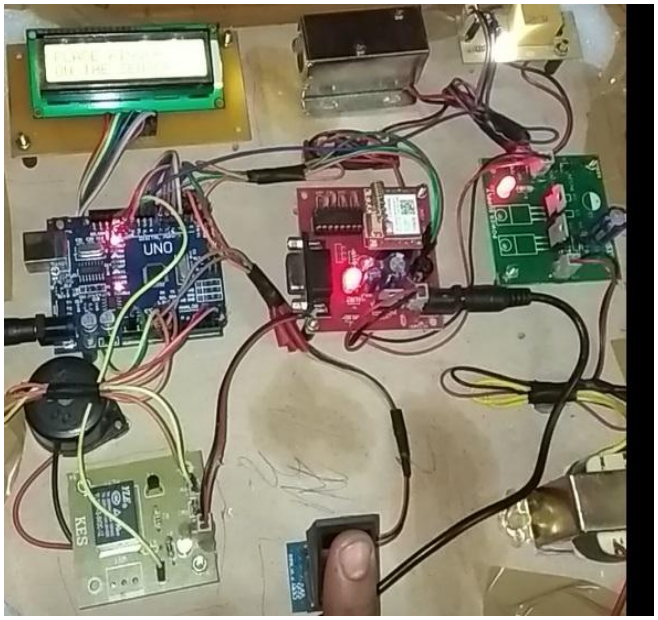

Fig.9. Door is opened

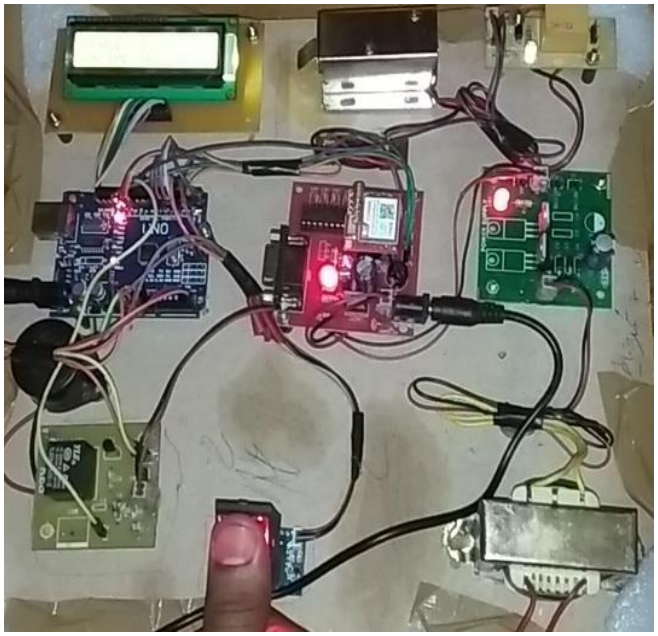

Fig.10. Door is closed

The details of the experiment results are illustrated in the following table:

N	LCD's Commands	Notes
1	Please enter sim card	When you power on the system, the system will ask to insert the sim card.
2	Network Found	After successfully processing the sim card inside GSM system.
3	Add a fingerprint	When you add a fingerprint of users to the database of the system.
4	Remove a fingerprint	When you remove any user's fingerprint from the database.
5	Place a finger on the sensor	When you want to test the system or to open the door.

6	Please type the password	When your fingerprint is successfully processed, the system will ask you to type the password.
7	Door is opened	When you successfully recognized as an authenticated user.
8	Door is closed	Door will be closed by sensing again the finger or after 5 seconds from opening time.
9	Alarm is active	When unauthorized person tries more than three times sensing his/her fingerprint.
10	Message sent	In case of anyone fails to open the door using fingerprint or tries to break the door, the message will be sent to the in charge person to take an action

VI. CONCLUSION

The proposed security system was tested in a real-time world, and its performance was recognized to be satisfactory. The security features that are added to the system such as GSM technology, password system, and web cam make it unique and competitive. The future scope of this work is very wide, and there are many other security tools can be added to the system to provide more security such as iris scanner for a person visual identification, fire sensors connected to the alerting alarms, and the system can be enhanced using artificial intelligence techniques to speed up and facilitate the process of identification of a person by using face recognition technique with a database of popular burglars.

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.

AUTHORS PROFILE

Hashem Alnabhi is currently studying a master degree in Information and Communication Engineering at Northwestern Polytechnical University- china. Received a bachelor's degree in Electronics and Communications Engineering from Jawaharlal Nehru Technological University, Anantapur, India in 2018. Received an advanced diploma in English Language from The Academic Canadian Institute, Yemen in 2013. Participated in many workshops related to Robotics, Electronics, Digital Image Processing and Artificial Intelligence. Participated in some online courses related to Machine Learning (Deep Learning) , and awarded a certificate of achievement in (IoT) from Curtin University, and a certificate of achievement in AI from Microsoft.

Yahya Al-Naamani is currently studying master degree in Digital Communication Engineering at Mewar University, new Delhi, India. Received a bachelor's degree in Electronics and Communications Engineering from Jawaharlal Nehru Technological University, Anantapur in 2018 .His area of research interest is digital communication and VLSI design.

Mohammed Al-MADHEHGAI is currently studying master degree in Electronics and Telecommunication at VIT affiliated to Savitribai Phule Pune University, Pune, India. Received a bachelor's degree in Electronics and communications Engineering from Jawaharlal Nehur Technological University, Anantapur, India in 2018. Attended a training course in IoT at Pralhad P. Chhabria Research Center (PPCRC). Attended IoT training program at VIT, Vellore, India.

Mohammed Alhamzi received a bachelor's degree in Electronics and Communication Engineering from Jawaharlal Nehru Technological University, Anantapur, India in 2019. Attended a training course at PPC Research Center, India 2017. Participated in many workshops related to IOT, Embedded Systems, Cyber Security and Malware Analysis. Presented a paper in National Conference on Implementation of Double Tail Dynamic Latch Comparator, India in 2019, and a paper on Renewable Energy Resources. Received a diploma in English Language from YALI, Yemen in 2014. Received an International Computer Driving license from Newhorizons Learning Center, Sana'a, Yemen in 2014.