Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 4, 2025

REVOLUTIONIZING HOME SECURITY: A BIOMETRIC AND GSM-ENABLED SMART DOOR LOCK SYSTEM

Muhammad Shahzaib[*1], Bilal Ahmed[2], Amna Sharif[3]

[*1,2,3]*Institute of Mechatronics Engineering, University of Engineering and Technology, Peshawar*

[*1]14pwmct0362@uetpeshawar.edu.pk

DOI: https://doi.org/10.5281/zenodo.15221602

Keywords
Authentication, Smart Lock, Security Concerns, Minimal Prerequisites, Electro-Mechanical Lock.

Article History
Received on 05 March 2025
Accepted on 05 April 2025
Published on 15 April 2025

Corresponding Author: *
Muhammad Shahzaib [*1]

Abstract

With the rising concerns over security due to increasing crime rates, ensuring the safety of homes, offices and institutions has become a top priority. Traditional security systems often require carrying keys, which pose challenges such as the risk of loss and the added cost of re-fabricating keys. While several studies have explored security solutions, there remains a significant need for further research to develop an effective security system. This paper introduces a smart lock prototype that offers a modern alternative to conventional locking mechanisms by integrating an electro-mechanical system for unlocking doors using passcodes and fingerprints, with real-time status displayed on an LCD. The system is built using an Arduino microcontroller and incorporates a fingerprint scanner, keypad, LCD display, and GSM module to provide user authentication, visual feedback, and instant alert notifications. The prototype supports up to 100 authorized users and is developed at a total cost of under $50, demonstrating both scalability and affordability. The key advantage of this smart lock is its combination of enhanced security, cost-effectiveness and ease of installation, making it a practical and efficient solution for modern security needs.

INTRODUCTION

According to an FBI statistics report, around 1.6 million burglaries happened annually in the USA. On an average, the loss is around 2300 dollars, which is more than the cost of the security systems cost [1]. In 2017, burglary cases reported in Lahore, Pakistan, were approximately 4,014, excluding the rest of the city [2]. Further, the Electronic Security Association states that about 90 percent of the burglars avoid those residential which have security systems installed [3]. The evolution of security measures dates back over 6,000 years, beginning with the early development of locks in ancient Egypt and Greece. The first locks, such as the pin tumbler locks, were crafted by skilled locksmiths using wood as their primary material. These early locks featured a wooden frame assembled with the door, into which a horizontal bolt with multiple openings was inserted. While rudimentary, this design provided an effective means of securing structures [4]. Building upon these early innovations, the Romans advanced lock design by replacing wood with metal, creating locks that were far more durable and capable of withstanding the forces of burglars. As time progressed, the complexity of locks increased, particularly during the late 18th century. This period saw the introduction of new designs aimed at enhancing security, including the level tumbler lock and the Chubb detector lock.

This historical progression of lock design highlights the continuous need for more advanced security solutions. Today, modern smart locks have emerged, addressing contemporary threats and incorporating

advanced technologies to safeguard homes and businesses. The evolution of locks—from simple wooden mechanisms to complex, technology-driven solutions—demonstrates the ongoing efforts to stay ahead of burglary risks and ensure the safety of individuals and their property. Despite the evolution of lock mechanisms and the integration of modern security systems, several existing solutions still exhibit critical limitations. Many commercial smart locks are either prohibitively expensive, lack reliable biometric authentication, or do not provide remote alert features such as GSM-based notifications. The aim of this study was to design and develop a prototype of an IoT-based smart door lock that enhances home and office security through the integration of fingerprint authentication, password entry, real-time status display, and GSM-based alert notifications, all implemented using a low-cost, microcontroller-based system.

I. LITERATURE REVIEW

Ranic Digital Lock [5] is the world's famous mobile communication security system. Ranic Digital Lock is frequently integrated for home and office use. The essential features are multi-level security, auto SMS responder, manual switch on/off button, signal indicator, liquid crystal display, and built-in keypad. Ranic Digital Lock introduces the implementation of SMS based commands for unlocking. For power failures, SMS is used. Spoken commands have been introduced through text messages. Through spoken commands, we can visualize and control with the help of the Android App. Mahesh et al.[6], introduced a system in which the android app is interfaced with the Bluetooth module. The Bluetooth module enabled to monitor the status and provided authentication at the door. The developed system can ramp up security. Pandurang et al.[7], created a model that enabled to provide authentication within a selected range. A linear actuator is used in their developed system, which obeys the micro-controller's command and then allows authentication at the door. This system also detects the user's motion from which the user can be seen. Das et al.[8], proposed a model to unleash the door via the RC4 cipher stream. RC4 cipher stream is a robust algorithm. The proposed method describes an Android app's design with a remote controller that has a Bluetooth module interfaced with it. The link between the server and the host will be developed by establishing a connection between the electronic module and the controller module. Thereby it enables us to unlock the door via commands incorporated between host and client. The developed model ensured authentication in real-time using the RC4 cipher stream algorithm. The proposed system allows to unlock and lock the door with a keypad, fingerprint sensor scanner, and face recognition. Although, the smart lock systems are the necessity of time but some drawbacks arise when we use the GSM module. GSM modules are not efficient in terms of security and cannot be relied upon and cannot be driven by every controller [9]. Also, the use of Bluetooth modules in security systems is risky due to the wider range and easy accessibility of more than one smartphone at a time frame [10]. RFID (Radio Frequency Identification) is sensitive when exposed to high frequency and can be defected [11]. Magnetic- field induced with high strength and frequency certainly defaced the surface of the RFID tag [12]. Hung et al.[13], formulated a model in which disparate receivers, transmitters are used and implemented popularly. Some of them are NFC based systems. Ibrahim and Kassem et al.[14], [15] proposed a GSM-based and WiFi-based system for door locks. This system has three components central control, actuator controller, and android application. The residents must be connected to a LAN network to open the door. The home network is associated with the system established via OTP cable. Commands are sent to central control to lock and unlock the door via WiFi. Nowadays, sensor alarm systems are used frequently for residential security purposes. John Mallory et al. [16], developed a security system that contains multiple sensors for fire, motion, and smoke for residential security. A monitoring system is created for effective communication between transmitters and receivers at the sensors and central monitoring system. The home security system was also described by Murakami et al.[17], in which different sensors and cameras were integrated at numerous spots. Furthermore, the combination of sensors and cameras are controlled via a central control system. Pratiksha et al.[18], described the amalgamation of SMS with GSM technology to access the lock under

the aegis of the end-user. Zhao et al.[19], described a wireless-based smart lock in which GSM technology is interfaced with multiple sensors like fire intrusion and infra-red sensors. This system was designed for nocturnal security. On further research of smart security systems, people showed more interest and were inclined towards a system that can be accessed by a smartphone. According to the smart home security report 2016 by IFSEC global and ASSA ABLOY, a survey was conducted worldwide, the Middle East, and Africa [20].

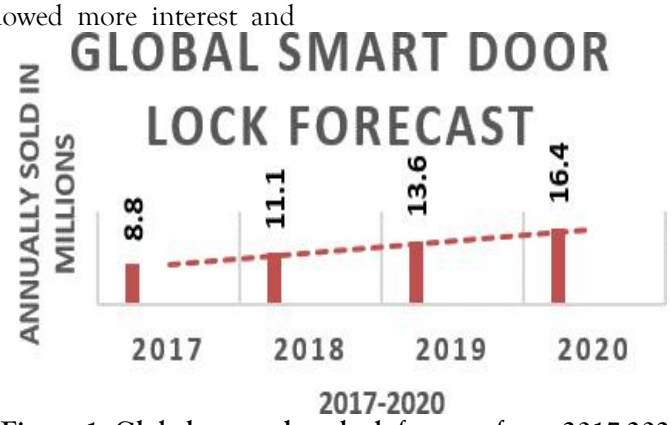

Figure 1. Global smart door lock forecast from 2017-2020

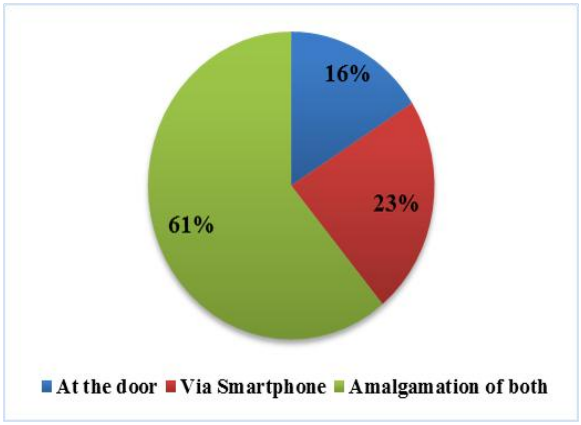

Figure 2. Assa Abloy survey about home security around the world

The above figure depicts the annually sold smart lock systems since, 2017 to 2020. The statistics indicate that an 86 percent increase has occurred in the sold smart lock systems since, 2017. Assa Abloy, the substantial lock-based company in Sweden, founded in 1994 surveyed home security in Europe, the Middle East and Africa with the inception of 2016. In that survey, more than half of the people were found using the lock operated via smartphones. Several questions were raised like the purpose of digital door locks, digital door locks versus mechanical locks, and how we would ideally like to access our door locks. Unlike traditional mechanical locks, these smart locks are more secure and reliable. Furthermore, most of the people in that survey were more inclined to use a locking system to have the right to access via smartphone and at the door. These certitudes invigorate the development of smart lock systems for security reasons. We aim to shrink burglaries using smart lock systems, which is the necessity of time in the current scenario. We added a camera in our smart lock system, enabling us to monitor the door's confined boundaries continuously.

II. SYSTEM ARCHITECTURE

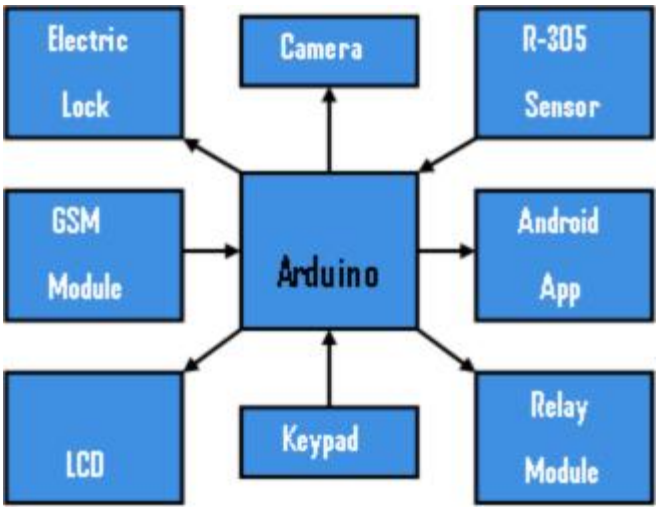

Figure 3. System Architecture using block schematic

The above block schematic represents a Smart Door Lock System controlled by an Arduino microcontroller.

The core of the system is built around an Arduino microcontroller, which functions as the primary control unit responsible for processing and managing system operations interfacing with various input and output devices to ensure secure access control. The system offers multiple authentication methods including a fingerprint sensor (R-305), a keypad for password entry, and an Android app for remote access via smartphone. A camera is integrated for surveillance, capturing images or video of users at the door. Once the Arduino validates the credentials, it sends a signal to the relay module to activate the electric lock, allowing or denying access. An LCD is used to display system status, such as access granted or denied. Additionally, a GSM module is included to send alerts or notifications via SMS, enhancing the security and communication features of the system. This multi-layered access control mechanism ensures that the door can be unlocked only through authorized means, providing both convenience and security in smart home or office environments.

III. COMPONENTS DESCRIPTION

A. Electric Lock

Figure 4. Electric Lock and adapter

An electric pulse is needed to operate an electric lock. The problem that arises in electromechanical locks is their lag time. That can be eliminated by using a good quality lock. The operational temperature range of this lock is 20 to 60 degrees centigrade. This lock is operated on 12V operating voltage. Electric lock and armature are mounted on a door. When an electric pulse is provided, the magnet gets powered; hence, the door gets unlocked.

The above figure depicts an electric lock, adapter and keys. This lock is energized by using power adapter and it can be unlocked via keys.

B. Arduino UNO

Arduino is an open-source software used to program electronic devices. Arduino UNO consists of 20 pins and operates in an 8- bit mode. Each pin, Analog/Digital, provides a 10-bit resolution. According to UNO's architecture, the program branch includes an instruction to complete in two cycles, whereas the instruction cycle includes one instruction per cycle. It uses a 16 MHz frequency clock. The flash memory of Arduino UNO is 32KB, out of which 0.5 is for boot loading. The Arduino we used operates at 5 volts and features 6 PWM (Pulse Width Modulation) pins along with 14 digital I/O pins.

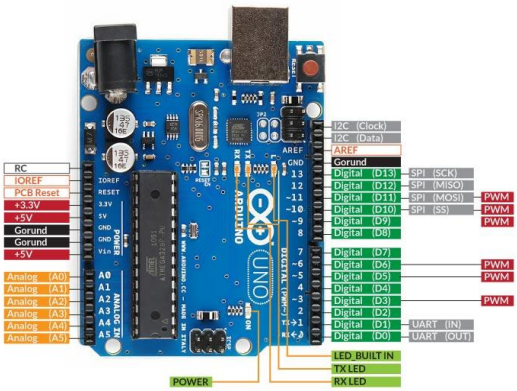

Figure 5: Arduino UNO and its pins description

C. Mobile Communication Module/GSM

GSM is a conventional module that expands and follows second-generation technology conventions, advanced cellular systems utilized by distinctive phones.

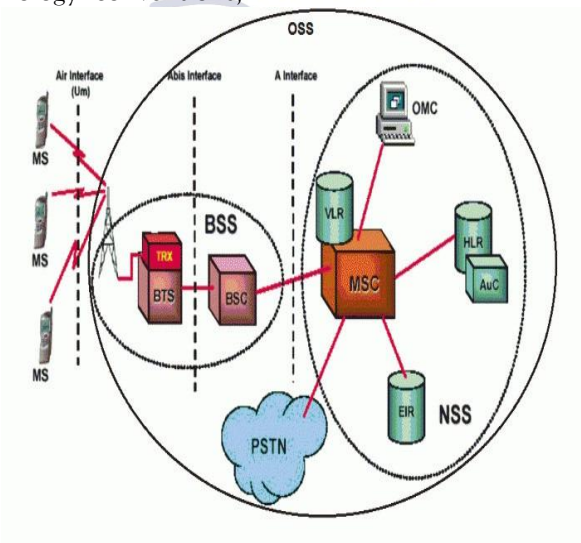

Figure 6: GSM architecture

The above figure depicts the System architecture of GSM and is divided into three categories front head, middle logic, and back end. The front-end comprises a mobile station (MS) that communicates with the base transceiver station (BTS) through a wireless air interface. Through mobile station, we use to call at other stations. The front head is connected to middle logic via a base station subsystem that provides signals. Additionally, the Base Station Subsystem (BSS) is divided into two main components: the Base Transceiver Station (BTS), responsible for signal transmission and reception,

and the Base Station Controller (BSC), which manages system control by directing traffic to other network stations. BSC is connected to the mobile switching center (MSC) via the "A" interface. MSC is used for switching calls. MSC and some registers are amalgamated in the network sub switching system (NSS). SIM900A is a 68-terminal device, and the module is interfaced with Arduino UNO. GSM module will deliver us SMS when a burglar will try to intrude on the lock.

The operating voltage of SIM900 is 3.5-4.5V DC. At the point, when the GSM shield gets any data from the portable system or any other GSM client, it will send the data to the controller by UART serial communication. GSM module is used in various cellular applications, robotics, computer peripherals, USB dongles, and automobiles. The GSM SIM900A is a dual-band drive. The GSM shield introduces a keypad, real-time clock, display, and UART interface. The operating temperature of the GSM shield is between -30°C to +80°C. For establishing the connection, the TXD pin of SIM900A is connected with RDX of Arduino Uno and vice versa. SC6600D chip is internally integrated with this module, which allows lower power consumption. The GSM shield has a memory of 32Mb and a flash memory of 4Mb. After every 577microseconds transmission burst happens, that carries a large number of electrical charges in a short interval. In these circumstances, the peaks of the ripple must be contained as far as possible.

D. Panoramic Camera

Panoramic Fish-eye camera is a surveillance-based camera through Panoramic Fish-eye camera is a surveillance-based camera through we can monitor a 360-degree comprehensive view. Apart from Surveillance, they are very economical, especially when we compare it with other cameras. It provides a 360-degree complete view without a blind spot. Most importantly, it captures every minute detail drawing image distortion, salt, and pepper noise. The 360-degree panoramic camera is designed for nocturnal security. Multi-channel mode and bundle stream modes are two modes of monitoring. Bundle stream mode incorporates the channels and forwards it to compatible VMS. While multi-channel mode forwards all channel to NVR, so they can be separated and modified accordingly. It offers 5/12 MP high-quality resolution that provides high performance and monitors everything. Most importantly, it has a two-way voice intercom, microphone, and built-in speakers for smooth and convenient communication. Fish- eye 360 cameras have high-frequency decoding capacity. The fish- eye camera can decode 25 and 30 fps for each channel under 4R and glass fish eye lens F2.014mm with a realistic view. Panoramic provides us a resolution of 1280×960 pixels, which is nearly equal to 1.3 Mega-pixel. The maximum video frame rate for this camera is 25 frames per second (FPS). The incredible feature of this camera is that it provides night vision. LEDs are installed for night vision feature, and their maximum range is 10 meters. It also offers 64GB storage. The power it needs for its operation is 5V and 1.6 A. The maximum power dissipation is 5 watts.

Figure *7.* Panoramic Camera

E. Liquid Crystal Display

This LCD contains two modes of operation and operates in 4 or 8-bit mode depending on the desired requirement and consists of 16 pins. The first two pins of this 16 x 2 LCD are the VCC (supply voltage) and the Ground Pin. The operating voltage of his

module is 5V, followed by the contrast adjustment pin.

Table 1: Timing Characteristics of LCD

Timing Characteristics of LCD			
Variables	**Symbols**	**Duration**	**Unit**
Setup Time	Ts	100	Nanoseconds
Rise Time	Tr	200	Microseconds
Delay Time	Td	60	Nanoseconds
Fall Time	Tf	300	Microseconds

The above table depicts the timing Characteristics of LCD. Setup time is the time needed for the LCD to start. In contrast, rise and fall time is the response time, which depicts when black pixels are converted into white pixels and vice versa. At the same time, the time required to print the status of output is the delay time.

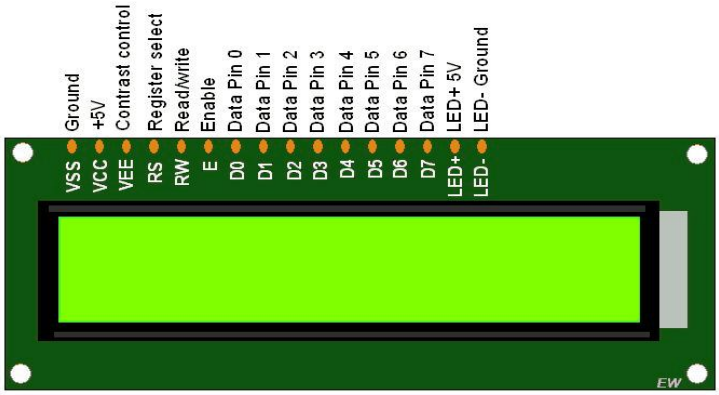

Figure 8: Liquid Crystal Display

The pin 3 or contrast adjustment pin is used to adjust the brightness. A 16x2 LCD module is equipped with two primary internal registers: one dedicated to command instructions and the other for data handling, both interfaced through the control pin (typically pin 4). The mode of registers is given as: At pin 4, selecting a high bit will initialize the data register, and selecting a low bit will initialize the command register. Pin 5 shows read/write modes. At pin 5 by selecting a high bit will initialize write mode, and setting a low bit will initialize read mode. Data pins start from pin 7 and end at pin 14.

F. Fingerprint Sensor

The R305 fingerprint sensor is a biometric device capable of capturing, processing, and storing fingerprint templates. It operates using a combination of optical image capture and internal DSP (digital signal processing) to convert scanned fingerprints into digital templates. This optical Fingerprint Sensor Scanner (R305) is interfaced with TTL UART. R305 can enroll and store 250 fingerprints. The optical scanner R305 can be interfaced with devices such as a micro-controller, Arduino, laptops.

The operating voltage of R305 while connecting with any micro-controller is 3-4V. But, Max232 is required for interfacing with personal computers or laptops serial ports. The operating voltage for R305 is 4-6V DC. The operational temperature range is from -20 to 40 degrees centigrade. R305 principle is based on comparing algorithm, that's why the searching time for identification is around 1 sec. It can read an image up to 500 dpi resolution. The R305 fingerprint sensor module is desegregated with an Arduino Uno using serial communication (UART). The sensor's TX and RX pins are connected to Arduino's digital pins via a software serial interface to allow simultaneous communication with other peripherals. The Adafruit Fingerprint Sensor Library

has been used to enroll and verify fingerprints. During the enrollment phase, fingerprints were captured, converted into templates, and stored in the sensor's internal memory. During verification, the sensor compared the input fingerprint with the stored templates and returned a match result to the Arduino. Based on the output, the Arduino triggered the appropriate action, such as unlocking an electric lock.

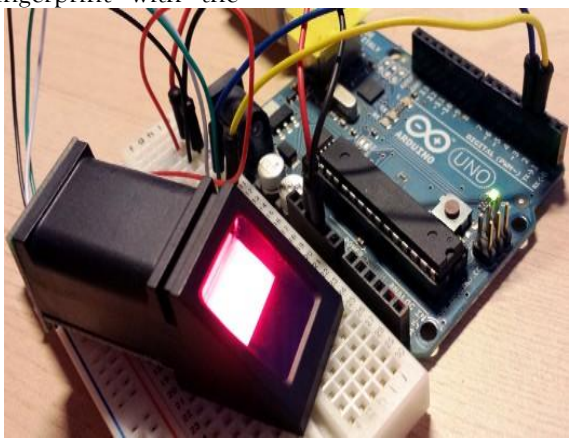

Figure 9. Finger print sensor in its On-State

IV. METHODOLOGY

The smart lock system prototype is designed for home security with ease. The proposed system has three phases. In the first phase, we integrated the keypad, fingerprint senor scanner (R305), and 16 x 2 Liquid Crystal Display (LCD). The purpose of integrating these modules is to provide authentication with ease to residential. It has its built-in app and can easily be accessed via mobile. While creating a smart lock system we knew that the user of this system can vary from common to highly educated person. That's why we integrated a fingerprint sensor scanner as well so, that a layperson can use this as well. The end-user of this Smart lock system has to enter the passcode via default keypad that will unlock the entrance for him. Similarly, the user can unlock via a fingerprint sensor scanner (R305) as well. The proposed smart lock system employs a biometric authentication process using the R305 fingerprint sensor to enhance security and convenience. To enhance the security framework, a second phase of development integrates a panoramic fisheye camera for visual surveillance and GSM technology for instant alerts.

In the third development phase, an Android application was added to support the physical security features. Available for download on the Play Store, this app allows users to remotely view the area around the entrance in real time.

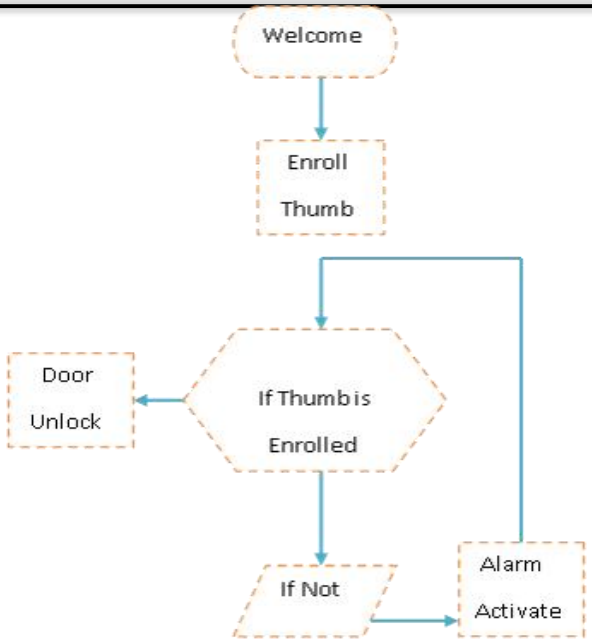

Figure 10. Flowchart of authentication process

The process begins with the user registering their fingerprint, which is then encoded and stored in the device's internal memory. During subsequent scans, the system compares the newly captured fingerprint with the stored template, and if a match is identified, the door is automatically unlocked. In case of an unrecognized fingerprint, an integrated alarm system is triggered to alert nearby individuals of a potential unauthorized access attempt. To accommodate multiple users, the R305 sensor is utilized for its capability to enroll and store up to 120 unique fingerprints, thereby allowing multiple authorized members to access the system without compromising security. Additionally, a password-based alternative using a keypad is provided, further increasing flexibility in authentication. To strengthen the security infrastructure, a second development phase incorporates a panoramic fisheye camera for visual monitoring and GSM technology for real-time notifications. Once access is granted—whether via fingerprint or keypad—the user receives an SMS alert stating "Door is Unlocked," thus offering immediate confirmation of entry. This multi-layered approach ensures that the smart door lock system not only prevents unauthorized access but also actively notifies the user, making it a robust solution against intrusion attempts. Furthermore, if the user is away from home, the system remains vigilant by sending an SMS notification even when an unauthorized attempt is made to unlock the door, thereby providing the user an opportunity to take preventive action against potential intrusions. The integration of a panoramic fisheye camera further enhances the system's surveillance capabilities by recording individuals who approach or attempt to access the door within its visual range.

In the third phase of development, an Android application was introduced to complement the physical security measures. This app, available for download on the Play Store, enables the user to remotely monitor the vicinity of the entrance in real time. Through the application, users can access live video streaming from the panoramic camera, thereby extending the reach of surveillance and allowing continuous monitoring regardless of the user's physical location. This comprehensive integration of biometric verification, GSM communication, video surveillance, and mobile accessibility reflects a holistic approach to smart home security, offering both proactive deterrence and reactive measures to ensure the safety of the premises.

Figure 11: Testing the components

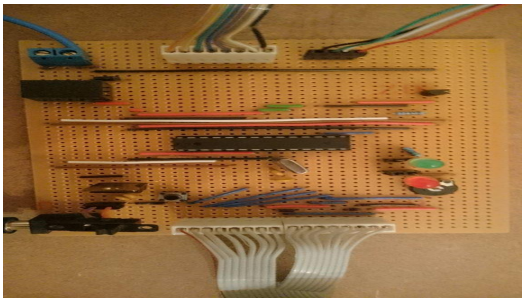

Figure 12: Assembling components on Veroboard

The above figure depicts the integration of Electric lock, GSM, Camera, Keypad, LCD, Fingerprint sensor with Arduino. Here Arduino acts as the central controller. The purpose of integration is to analyze and test whether each module is working according to the requirement.

The above figure represents the assembly phase of the smart lock system involved integrating electronic sensors, microcontrollers, and a power source onto a Veroboard, which was selected for its cost-effectiveness and ability to reduce excessive wiring during prototyping. Prior to final integration, all system components—including the Arduino microcontroller, fingerprint sensor, LCD, keypad, GSM module, and relay—were initially tested on a breadboard to ensure full functionality and compatibility. After successful validation, the components were transferred to the Veroboard for permanent installation. The Veroboard, characterized by its grid of uniformly spaced copper-lined holes (2.54 mm apart with 0.1-inch diameter), serves as a practical platform for mounting and soldering electronic components.

The system's embedded code, developed using the Arduino IDE, was compiled and uploaded to the ATmega328p microcontroller using its bootloader. A 12V relay was employed for switching purposes, functioning as an electronic switch to control the electric lock mechanism. When the Arduino detects an unlock or lock command—typically triggered via keypad or fingerprint input—it generates a pulse that energizes the relay's normally open (NO) pin, effectively activating the electric lock. All electrical connections were established using copper wires soldered onto the Veroboard to ensure reliable current flow. Proper safety precautions were observed during the integration process, particularly avoiding direct contact with the copper traces on the Veroboard, which could potentially lead to electrical shorts or component damage due to unintended conduction. This phase ensured a robust and compact hardware implementation, providing a solid foundation for the smart lock system's deployment.

VI. RESULT AND ANALYSIS

Figure 13: Final Prototype of Smart Lock System

The specimen of the smart Lock System was advanced for the home security system and is successfully extended. The following figure shows the prototype that has been developed.

The aforementioned figure depicts the final look of the smart lock system prototype in which liquid crystal display (LCD), keypad, fingerprint sensor scanner, electric lock, buzzer/alarm, and the panoramic camera is interfaced. This prototype's cost, including all the components, is around US 48.5 dollars, which is negligible compared to the loss of burglaries. More- over, the need for shielding against thefts and burglaries enhanced the keen interest towards ingenious lock systems. That keen interest in smart lock systems can be seen from the smart lock system market shares from 2014 onwards. According to a smart lock market share in 2019, around 1.2 billion was estimated. The market is projected to grow at an annual rate of 18.5% through 2027. In 2019, approximately 7 million smart lock systems were sold.

VII. VII. CONCLUSION AND FUTURE WORK

To overcome the global issue related security, we formulated a smart lock system that will provide smart security and easy authentication that is the need of time also. Smart door locks are the emerging locks that are coming with different specifications every year.

In reality, they are replacing lots of conventional locks. Most importantly they can be purchased with affordable prices with a variety of specifications like SMS notification, live streaming, built- in keypad, maximum storage capacity, etc. Even a normal person can operate these locks as well; this shows how these locks are elementary. And with security features, these locks make our homes more secured. The smart lock system provides easy authentication and intelligent security, fulfilling the demands of modern needs. Although the smart lock system is a guard against burglars, there are some recommendations that researchers should work in the future. Introducing face recognition and gesture sensors to the smart lock system will enhance flexibility. A power backup must be considered to operate the system. The android app will grant access to unlock or lock the door from remote areas through WiFi access.

ACKNOWLEDGMENTS

Praise and glories be to ALLAH Almighty, our creator, our source of inspiration, wisdom, knowledge and understanding. The achievement of any interdisciplinary project is contingent upon the collective collaboration, coordination, and input from various fields of knowledge. I am deeply appreciative of my professor's consistent willingness to offer profound guidance and direction, which greatly contributed to the success of this work. He has been a great advisor, mentor, and a tutor and providing me all the facilities, taking personal interest in the project and sparing his precious time. I am profoundly grateful to my family for their unwavering support and encouragement, for dedicating their time and resources to my well-being, and for creating a nurturing and conducive environment that fostered my progress and comfort throughout this journey. My Parents special prayers which never left me alone and especially during the project work in the moments of doom and disappointments these prayers took me out of darkness and were real source of encouragement.

FIRST A. AUTHOR received the B.S. and M.S. degrees in Mechatronics engineering from the University of Engineering & Technology, Peshawar in 2018 and 2021. After the completion of Bachelor's degree from 2018 to onwards, the undersigned worked as trainee engineer and design engineer at the Latif Ghee Industries Pvt. Ltd and National Radio Telecommunication Corporation.

REFERENCES

[1] U. C. Report, "Crime in the United States, 2015," pp. 2015–2016, 2016.
[2] O. Security and A. Council, "Pakistan 2019 Crime & Safety Report : Lahore," pp. 1–7, 2020.
[3] Safewise Team, "Home Safety and Security Stats and Facts | SafeWise." https://www.safewise.com/resources/security-stats-facts/ (accessed May 30, 2020).
[4] History of Keys, "History of Locks - Who Invented Locks?" http://www.historyofkeys.com/locks-history/history-of-locks/ (accessed May 30, 2020).
[5] "GSM." https://en.wikipedia.org/wiki/GSM.
[6] M. N. Jivani, "GSM Based Home Automation System Using App-Inventor for Android Mobile Phone," *Int. J. Adv. Res. Electr. Electron. Instrum. Eng.*, vol. 03, no. 09, pp. 12121–12128, 2014, doi: 10.15662/ijareeie.2014.0309042.
[7] B. Pandurang, J. Dhanesh, G. Akshay, and G. Rahul, "Smart Lock : a Locking System Using Bluetooth Technology & Camera," vol. 4, no. 1, pp. 136–139, 2016.
[8] Ravindra Das, *Biometric Technology – Authentication, Biocryptography, And Cloud-based Architecture*, no. May. CRC Press, 2009.
[9] M. Toorani and A. A. Beheshti, "Solutions to the GSM Security Weaknesses," Feb. 2010, doi: 10.1109/NGMAST.2008.88.
[10] K. S. G. B. Lia and W. S. M. S. G. B. Sanjaya, "Door-automation system using bluetooth-based android for mobile phone DOOR-AUTOMATION SYSTEM USING BLUETOOTH-BASED ANDROID FOR MOBILE PHONE," no. January 2014, 2016.
[11] A. H. Işilak, "Smart Home Applications For Disabled People By Using Wireless By Smart Home Applications For Disabled People By Using Wireless Sensor Network," *Eng. Proj. Rep.*, 2010.
[12] G. K. Verma and P. Tripathi, "A Digital Security System with Door Lock System Using RFID Technology," 2010.
[13] C. Hung, Y. Bai, and J. Ren, "Design and Implementation of a Door Lock Control Based on a Near Field Communication of a Smartphone," pp. 45–46, 2015.
[14] A. Ibrahim, A. Paravath, P. K. Aswin, S. M. Iqbal, and S. U. Abdulla, "GSM based digital door lock security system," *Proc. 2015 IEEE Int. Conf. Power, Instrumentation, Control Comput. PICC 2015*, 2016, doi: 10.1109/PICC.2015.7455796.
[15] A. Kassem, S. El Murr, G. Jamous, E. Saad, and M. Geagea, "A smart lock system using Wi-Fi security," *2016 3rd Int. Conf. Adv. Comput. Tools Eng. Appl. ACTEA 2016*, pp. 222–225, 2016, doi: 10.1109/ACTEA.2016.7560143.
[16] 581,606 J Mallory - US Patent 4 and undefined 1986, "Central monitor for home security system," 1986. Accessed: May 29, 2020. [Online]. Available: https://patents.google.com/patent/US4581606A/en.
[17] "US6759957B2 - Home security system - Google Patents." https://patents.google.com/patent/US6759957B2/en (accessed May 29, 2020).
[18] P. Misal, M. Karule, D. Birdawade, A. Deshmukh, and M. Pathak, "Door Locking / Unlocking System using SMS Technology with GSM / GPRS Services," vol. 5, no. 4, pp. 192–194, 2014.
[19] Y. Zhao and Z. Ye, "A Low Cost GSM / GPRS Based Wireless Home Security System," no. 6, pp. 567–572, 2008.

[20] S. Security, "Smart-Home Security Report 2016 : The Growing Market for Smart Door Locks Smart-Home Security Report 2016 : The Growing Market for Smart Door Locks," 2016.