Adaptive Biometric Smart Door Lock System with Time-Bound Access Using GSM Module

Geda Tejesh Chowdary
Department of Computer Science and Engineering
Amrita School of Computing, Bengaluru
Amrita Vishwa Vidyapeetham, India
bl.en.u4cse22114@bl.students.amrita.edu

Yelipe Gowtham
Department of Computer Science and Engineering
Amrita School of Computing, Bengaluru
Amrita Vishwa Vidyapeetham, India
bl.en.u4cse22163@bl.students.amrita.edu

Paramkusam Sriharsha
Department of Computer Science and Engineering
Amrita School of Computing, Bengaluru
Amrita Vishwa Vidyapeetham, India
bl.en.u4cse22141@bl.students.amrita.edu

Unnam Aditya
Department of Computer Science and Engineering
Amrita School of Computing, Bengaluru
Amrita Vishwa Vidyapeetham, India
bl.en.u4cse22160@bl.students.amrita.edu

Meena Belwal
Department of Computer Science and Engineering
Amrita School of Computing, Bengaluru
Amrita Vishwa Vidyapeetham, India
b_meena@blr.amrita.edu

***Abstract*- As more households employ domestic help, they need security systems, especially those which are efficient but user friendly. Previous biometric systems which use fingerprint scan offer high level of security but most of them cannot adapt to the different time schedules of employees like maids, without compromising the security. This paper introduces a new Smart Door Lock System that combines fingerprint authentication with remote homeowner controls. Homeowners can schedule the time when the maids can enter, hence providing added security. At these times, maids are given free access, and the homeowner is notified. If it is attempted outside these times, the system requires a onetime password (OTP) sent by the system. Additionally, the system uses an infrared (IR) sensor that activates the fingerprint scanner only when someone is at the door, which significantly improves power efficiency by reducing idle energy consumption. System effectively manages access based on predetermined schedules while enhancing both security and energy efficiency in residential settings.**

Keywords— maids, infrared sensor, biometric systems, one time password, fingerprint.

I INTRODUCTION

The increasing demand for high-security systems in homes, offices, and other areas has highlighted the deficiencies of the standard door locking systems, especially in areas where differentiation of the degree of access is necessary and must be made instantly. Standard approaches, including using keys or passwords, cannot address the dynamism of the rental structure involving owners, guests, and service providers. To tackle such issues, biometric authentication technologies for instance fingerprint recognition have in the recent past gained popularity due to keyless access. None the less, while biometric systems increase security in organizations, they lack adequate options for managing access in real-time, especially when the owner is not around.

To overcome the above challenges, this work has a masker key that operates the whole system i.e., the Arduino Uno [1] and employs the use of a GSM module to allow for remote and on-demand control using mobile communication in conjunction with a biometric fingerprint recognition system. The communication element in the form of the GSM module also enables owners to create time-sensitive PINs that would be useful for granting various degrees of access to Properties when required say for Maid or a Guest. This system makes sure that nobody can enter the restricted area without permission, for example during stipulated time or night. Furthermore, due to the incorporation of an automatic lock down of the permitted access period, even if the PIN is obtained by an unauthorized individual, the system protects itself from further access. These features make the solution more adaptive and responsive compared to the static approaches to access.

Although biometric systems such as fingerprint scans to unlock the technology enhance security, it does not possess the ways to control remote access and temporal limits on work access in the owner's absence. Besides, current systems are unsuitable for implementing temporary access rights which are useful for service providers or visitors. This project fills these gaps by integrating an identification mechanism using the fingerprint scan with GSM technology for OTP generation, remote access, and time-sensitive control. It reduces the risk of intrusion and gives automated restricted access depending on time or type of user.

The key contributions of this work are:

- Overall enhances the traditional lock systems.
- Integration of GSM module with biometric sensor improves security with on demand time limited access.
- Provides flexible access control for the different types of users.

The subsequent sections of our paper are as follows: Section II provides the related work. Section III discusses the methodology. Section 4 details out the implementation and explains the functionality of the system. Section V provides the results. Section VI concludes the paper with future work.

II LITERATURE REVIEW

Saroha et al. [1] have discussed a biometric smart door lock system, using face recognition in coordination with IoT for access and alertness. One of the measures of security in the system is the use of face recognition, and if this is not feasible then a passcode. It uses other mobile applications to send notifications. The paper reveals the efficiency of the given system with a backup, a failsafe, and effective power control. Khan et al. [2] present a prototype model of the IoT-SDLS based on double-access biometric authentication. The focus of the study is on its capacity for real time alerts and online cloud platform for tracking the status of door locks while being more reliable and safer than RFID and password- protected ones.

Balaji et al. [3] discuss a biometric based smart door locking system, with OTP to further improve the security aspects. The used biometric feature is used to authenticate the users while those who use the mobile applications are also required to enter a one-time password sent to their mobile phones. The system in safe access management in residential and commercial areas pointing out that the inclusion of a biometric check with OTP reduces the risk of entry by unlawful persons. Kolluru et al. [4] have proposed the face recognition based smart door lock system which uses the remote servo control to improve the security of the system's functioning. Their study is beneficial in demonstrating how the system lowers insecurity of unauthorized access through incorporation of facial recognition with IoT, as a solution that is implementable for domestic security purposes.

Simatupang and Tambunan [5] examine a multi-sensor security door lock that uses RFID, fingerprint and keypad to improve home security. An Arduino Uno microcontroller controls the solenoid door lock, allowing entry only after proper authentication through all the sensors. This system is characterized by its high level of stability and lower susceptibility to breaches when compared with mechanical locking systems. Belano et al. [6] have designed a microcontroller smart door lock system using the PIC16F877A microcontroller. For home automation and security, the system incorporates peripherals like keypad, IR sensor and so on. They outline how the system offers an effective method of home security with accountably passcodes and constant monitoring.

Siswanto et al. [7] the implementation of fingerprint biometric access control system with PIN based smart home. It incorporates an Arduino Mega 2560 microcontroller for controlling the subsystems and takes care of both the fingerprint identification and the PIN input. The study focuses on the simplicity of the system and its capability to fit into an embedded environment, and it also provides protection that is efficient against intruders. Elavarasi and Mohana [8] proposed a smart fingerprint authentication system IoT for improving the security level. The access control is done through a fingerprint scanner interfaced to an Arduino UNO while real-time notifications are provided through IoT. The study outlines the aspects of using the system in enhancing security since it deals with issues of keys and passwords, which can easily be lost or got by the wrong people.

Revanth et al. [9] presented an Arduino based fall detection system in a wheelchair with GSM for an alarm. A SIM 900A GSM module to send SMS alerts to caregivers or emergency contacts in the event of a failure. The GSM module is important for giving broad coverage, to make certain that alerts can be issued even when there are no internet connections the surveillance system is an excellent solution for distant monitoring. Mnyanda et al. [10] design a smart irrigation system that consists of a GSM module where the PIC16F690 microcontroller is implemented to manage the water properly. The GSM module is useful in sending text messages at times when the status of the irrigation system is and allows the farmers to control the usage of water from a distance. The main idea of this system is to provide least intervention by people so that irrigation remains on only when it needs to be, improving soil production that is necessary for agriculture.

Kumar et al. [11] discusses an efficient garbage monitoring system that integrates a GSM module for its real time fill level measurement and for sending alerts. The system sends signals to the authorities by means of the GSM network. Peculiarities of this system are also its affordable expenses, good scalability, and possibilities to improve the efficiency of waste management as well as to contribute to the matters of environmental safety and population health. Raj et al. [12] their research outlines the model of using UVISE and CoAP in a large-scale IoT system for tracking physical attribute on low-cost microcontroller. The system also shows effective data transmission and distant supervision in conditions characterized by limited space. It focuses on the ability of protocols to interconnect and expand for Industrial IoT.

Princy et al. [13] in their paper, deep learning models such as CNN, ResNet as well as VGG16 are discussed and used for plant disease detection with corresponding accuracy of between 72% and 92%. They focused uniquely on AI as the initiative that will help in decreasing the use of pesticides and promoting the upgrading of the methods of cultivation. Convolutional neural networks are used for optimal disease identification from plant image. Venkatesh et al. [14] their paper also designs face recognition security through Raspberry Pi, Pi camera, and a solenoid lock for door control. Face detection and logging of unauthorized access are from OpenCV with Haar Cascade Classifiers. The system affords a cheap, that is, real-time security solution based on the costs above.

Ravindran et al. [15] the access control proposed in their research combines face recognition and NFC and applies CNN models for identification purposes. It records the entry/exit data in a MongoDB database to increase security and user experience on its platform. The system therefore offers a new paradigm for cost effective and robust biometric solutions. Venkatasamy et al. [16] has put forward a Smart Door Unlock System which contains face recognition, fingerprint, RFID card, password and IoT technology for security viewpoints. A camera reads faces and an image matching algorithm grants access; a fingerprint scanner solves key problems. Primarily targeted to elderly people, the system disposes of complicated settings for door access.

A smart digital door lock system is developed by Park et al. [17] using methodology such as secret code, smart card, fingerprint. Its design is aided by a ZigBee module that will enable the door lock to act as the hub for home automation. It has an RFID reader, a touch LCD and motor modules for door operation which can be controlled through the internet. This design reduces the degree of installation that requires complex infrastructure. Other recent developments include Tilala et al. [18] propose a smart locking system in homes by developing an Android application which communicates with WeMos D1 module via Wi-Fi. The account credentials are protected by a static password and a dynamic OTP delivered through the app. The solution that is being proposed is functional in its simplicity as it does not need a lot of accessories, at the same time it is efficient in dealing with issues related to home security.

Smart home problems arising from the use of current wireless locking systems motivate Yadav et al. [19] to develop a smart lock system based on LoRa technology. LoRa comes with low power requirement coupled with very high range and bidirectional transmission opportunity. The system controls the lock status and sends notifications to the admin when intrusion happens and uses GSM if internet connection is a problem. Baidya et al. [20] incorporate a door lock security framework based on utilizing biometric fingerprint scanning as a more secure technique at home and workplaces. It solves some of the problems associated with the use of RFIDs and password-controlled doors, card access through fingerprints. When built on an Arduino UNO platform, it balances modularity in managing the user access. So, in this literature there is a lot of work on biometric smart door lock system. To incorporate new technology into this system we introduced a time bound system for maid access which adds an additional layer of security to the system.

III METHODOLOGY

A. SYSTEM ARCHITECTURE

The system in this project is developed with some hardware contacts say the Arduino Uno, fingerprint, GSM, IR, RTC and 16 x 1 LCD as shown in the below figure. These parts are compounded to form

an effective, secure access control solution with the incorporation of biometric authentication as well as real time remote access.

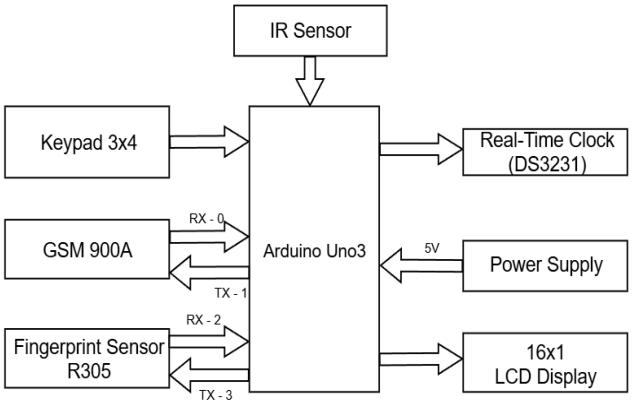

Fig 1. System architecture diagram

The architecture diagram presented in Fig 1 illustrates Arduino Uno biometric based door lock system equipped with fingerprint sensor, GSM module, IR sensor, relay module and E-lock. All devices are managed by the Arduino Uno; It operates with 5V voltage. When the fingerprint is identified the Arduino interface gives a signal which is directly displayed in the LCD screen. The GSM module within the range of 900 MHz-1800 MHz and a voltage of 3.4V-4.4V allows the owner OTP based access through phone. There is an IR sensor to monitor the entries and there is an RTC module to log the time. An LCD shows the operating status briefly and a keypad allows the user to enter information. This overall makes the system stronger and more secure by adding dynamic access methods such as OTP through GSM; granting flexible and monitored access to guests or others; and guaranteed timely access.

B. HARDWARE COMPONENTS

The hardware requirements that are used for this project are shown in Table 1.

Table 1 – Hardware Components

	Component	Utility
1	Arduino Microcontroller	Master key to operate whole door locking system.
2	Fingerprint Sensor	Stores fingerprints to enable unlocking and provides biometric scanning to approve the same.
3	GSM Module	Violations of access triggers an SMS alert, and OTPs are sent to the owner.
4	LCD Display	Shows the information like the status at the door, OTP, and all other related messages to the user.
5	IR Sensor	This helps in sensing a person and activates the fingerprint sensor.
6	Keypad	Permits entry by using the OTP in case of no fingerprints scan to be made.
7	Real-Time Clock Module	Effectively records time for purposes of time-limited access.
8	Power Supply (5V + 9V)	Supplies voltage and current as needed to operate all the components.

C. SOFTWARE MODULES

The software modules that are used for this project are shown in Table 2.

Table 2 – Software Modules

S. No	Module	Utility
1	Arduino IDE	Environment to set, develop, and upload instructions or program into the Arduino microcontroller.
2	GSM Library	Permits the Arduino and GSM module to exchange data to send out SMS alerts.
3	Fingerprint Library	Allows touching the fingerprint sensor for capturing and confirming fingerprints.
4	RTC Library	It is responsible for time functions required in analyzing and implementing time-based access control.
5	LCD Library	Allows the Arduino to handle display and management of messages, status and prompts to be conveyed on the LCD, effectively and clearly.

IV IMPLEMENTATION

The fingerprint-based door lock system aims to offer both high-security and efficiency at the same time and easy to manage home access. There is an IR sensor incorporated in the system to check for motion and only when this is detected does the fingerprint scanner get powered to scan a fingerprint. It categorizes users into three cases: owners (physical access), guests (one time password-based access), and maids (time based or OTP based access based on the time of entry).

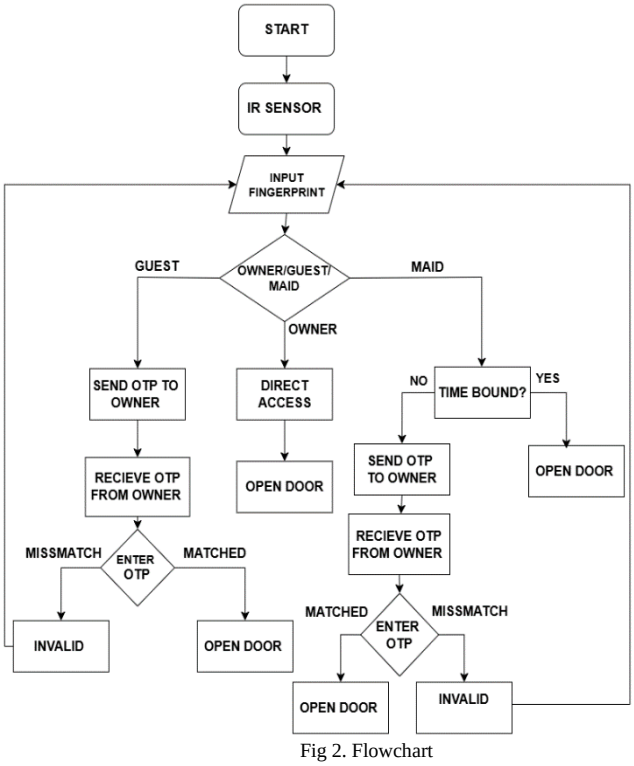

Fig 2. Flowchart

Fig 2 depicts the flowchart. The system ensures seamless and efficient fingerprint door lock management by categorizing user into four:

- **Owner Access:** owner is allowed based on their validation of their fingerprint scan with no need for an authentication step, which ensures convenience and quick access for owners
- **Guest Access:** Guests have OTP-based Authentication process. Once a guest fingerprint is matched by the system an OTP is created and sent to the homeowner for confirmation. Once the guest has provided the correct OTPs, the door opens and thereby can allow the right levels of controlled guest access.
- **Maid Access:** maids come with a specific time frame for easy access to the house without any disturbances in the day (around Morning 9-10 am). The door opens without the need for an OTP if the maid tries to enter within this timeframe. For entries during other parts of the day, the system requires an OTP which is needed for entry; enhances the security.
- **Invalid Attempts:** A deviation in the fingerprint or OTP also leads to an instant refusal of access; thereby addressing the susceptibility of the current security measures to malicious intrusions.

These structured ways provide better security and reduce the chances of unauthorized access while providing good user convenience to the homeowners, guests, and servants by intelligent access control. The circuit diagram of the prototype is shown in Fig 3.

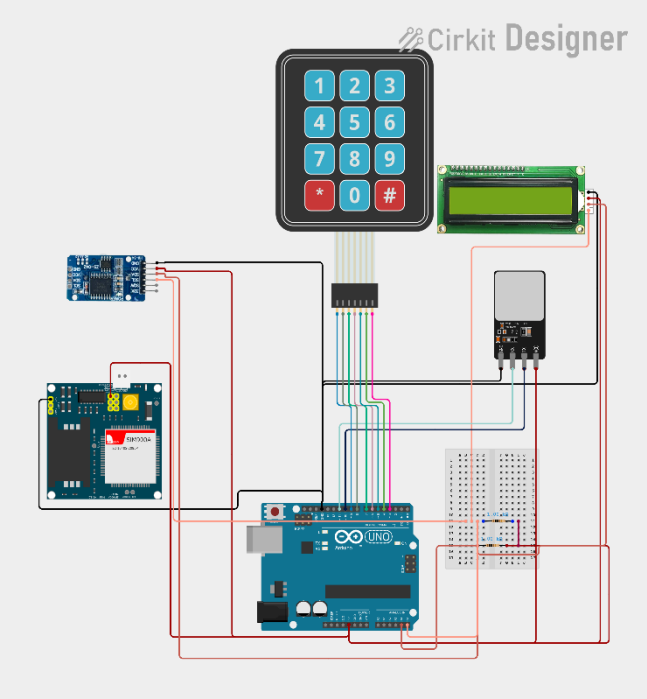

Fig 3. Circuit Diagram

V RESULTS

In this research, a biometric smart door lock system has been successfully designed. The system has been developed using the hardware that is mentioned in the methodology section. The code section was developed in the Arduino IDE. The IR sensor is used in our project, to activate (power up) the fingerprint sensor when an object is detected, otherwise the fingerprint sensor will not work. The whole prototype is shown in Fig 4 of the proposed system. In the results there are a total of three sections as there are three different scenarios in this work.

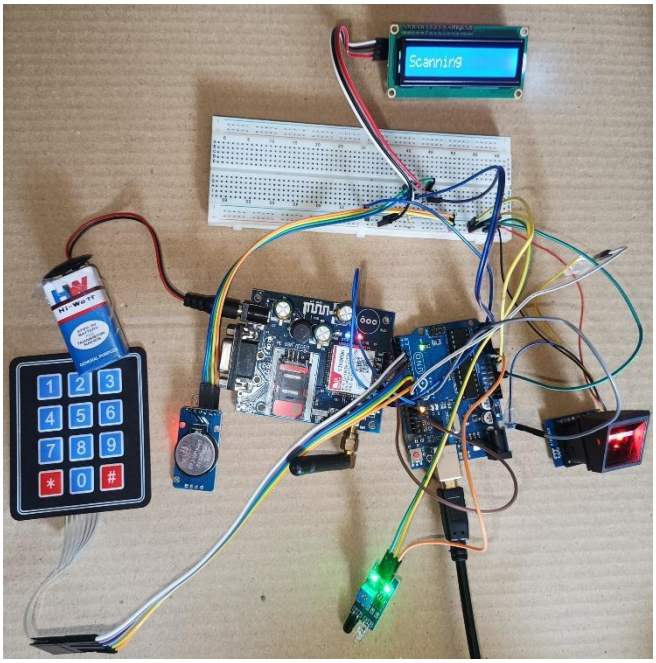

Fig 4. Prototype of the Proposed System

A. *OWNER ACCESS*

In this scenario, we have direct access to the owner. When the owner keeps his fingerprint, if the fingerprint is registered and the fingerprint is said to be the owner's fingerprint id, they will have direct access to the lock as they have the privilege to enter their home or their place. So, the implemented part of the owner's section is shown in Fig 5 where we get output on the LCD display as "Owner Entered".

Fig 5. Display of output when owner places his fingerprint

B. *MAID ACCESS*

This scenario, there are two different test cases. This case of maid is linked to the time bound part. The two cases are as follows:

i. *ACCESS WITHIN TIME-BOUND*

In this section, when the maid keeps the fingerprint, the Arduino microcontroller checks whether the fingerprint is already registered or not, if it is registered only then it checks whether the maid has entered within the time or not. If she has entered within allocated time, then the door will get opened and she will have limited time to finish her work. This time-bound scenario is the novelty part of the project as it is very much required in the real-life scenario. So, if she does not finish her work in the allocated time. She should wait until the owner enters. The owner will get the message that the maid entered his mobile phone. The message is shown in Fig 6.

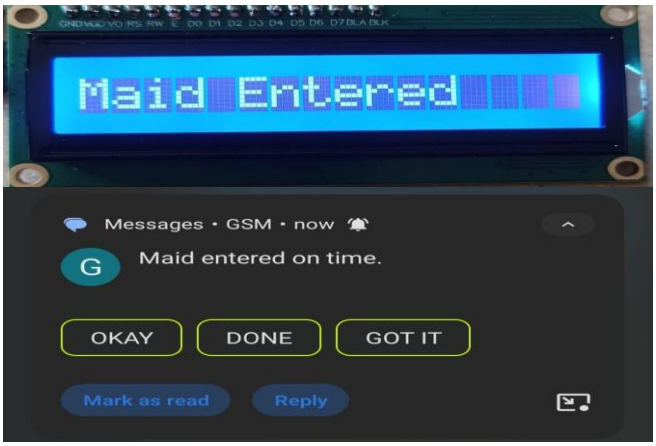

Fig 6. Message showing that the Maid entered on time

ii. ACCESS OUTSIDE TIME-BOUND

This part is when maid keeps the fingerprint, the Arduino microcontroller does this same routine check of the fingerprint detection. After that, this is a case where the maid wants to enter the home outside the time that is allocated to her. This is a case where the maid comes too late or early to work. In this case an OTP will be generated for this purpose, then the maid should get access from the owner and enter the OTP to attain access. This happens when the maid does not come to her regular hours of work. Fig 7 shows the "Maid Detected" message and OTP that has been generated through an alert message and Fig 8 shows the LCD display where there is a message to "Enter OTP" and the OTP will be represented in *'s when we enter it as it's a password.

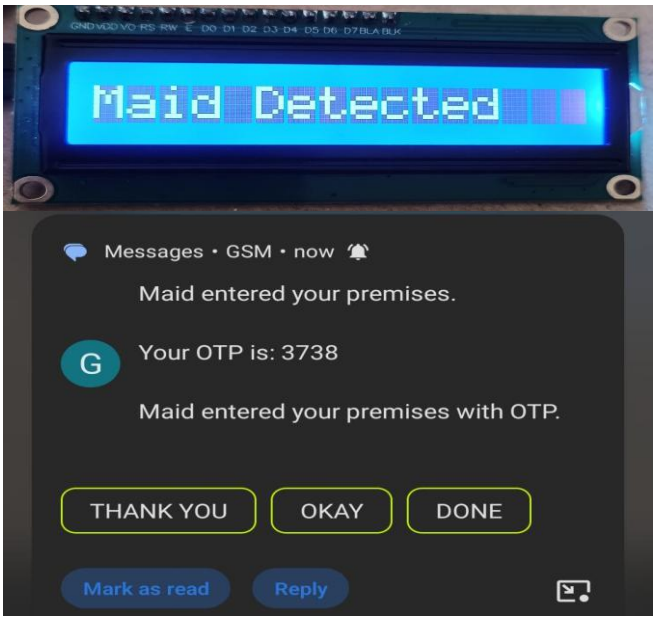

Fig 7. OTP generated message shown and the OTP is also shown

Fig 8. LCD Display shows "Enter OTP:" message

C. GUEST ACCESS

In this scenario, when an unknown person or guest keeps the fingerprint, the microcontroller does the same routine check of the whether the fingerprint is registered or not. As it's unregistered, an OTP will be sent to the owner. If the owner wishes to allow them into their home, then he will share the OTP with the guest. The guest enters the OTP and enters the home. The guest is a privileged person so, there is no time bound scenario for this case. The message shown when a guest or unknown person fingerprint is kept is shown in Fig 9.

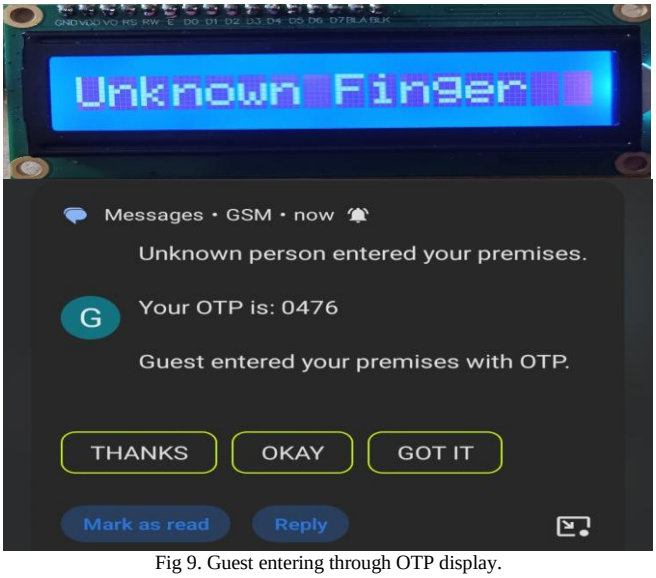

Fig 9. Guest entering through OTP display.

VI CONCLUSION AND FUTURE WORKS

This project proposes a secure Adaptive Biometric Smart Door Lock System with GSM module to allow temporary access on request for time-bound visitors. This system is the best solution of using both the biometric identification and the remote control of the system while improving the overall level of security. It effectively partitions the users into owners, maids and guests ensuring that there is restricted access to the house by time-based and One Time Password based authentication. Apart from security enhancement through the real-time clock modules and IR sensors, the system also enhances ways through which energy is utilized effectively, hence increasing operational efficiency. We can say that the results confirm the applicability of this system in terms of safety and the problems related to access in contemporary households. Future improvements could include the addition of machine learning to recognize the unusual performing access patterns, using face recognition for two-factor authentication, and developing an application interface for easier supervision. Further, the further extension of the system to commercial and industrial use with features that are integral and can be scaled up may add more value to its usefulness.

REFERENCES

[1] A. Saroha, A. Gupta, A. Bhargava, A. K. Mandpura and H. Singh, "Biometric Authentication Based Automated, Secure, and Smart IOT Door Lock System," 2022 IEEE India Council International Subsections Conference (INDISCON), Bhubaneswar, India, 2022, pp. 1-5, doi: 10.1109/INDISCON54605.2022.9862840.

[2] M. A. Khan et al., "Prototype Model of an IoT-based Digital and Smart Door Locking System with Enhanced Security," 2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2022, pp. 1-7, doi: 10.1109/MACS56771.2022.10023385.

[3] M. Balaji, P. N, N. Swathi, S. Atheek, M. Manasa and K. C. Kumar, "Biometric-based Smart Door Locking System using Biometric and OTP," 2023 7th International Conference on I-SMAC (IoT in Social,

Mobile, Analytics and Cloud) (I-SMAC), Kirtipur, Nepal, 2023, pp. 898-903, doi: 10.1109/I-SMAC58438.2023.10290425.

[4] C. Kolluru, A. G V, S. P. S, K. R. D and A. S. Kumar, "Development of Face Recognition-Based Smart Door Lock System with Remote Servo Control Authentication," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-6, doi: 10.1109/ICCCNT56998.2023.10307437.

[5] J. W. Simatupang and R. W. Tambunan, "Security Door Lock Using Multi-Sensor System Based on RFID, Fingerprint, and Keypad," 2022 International Conference on Green Energy, Computing and Sustainable Technology (GECOST), Miri Sarawak, Malaysia, 2022, pp. 453-457, doi: 10.1109/GECOST55694.2022.10010367.

[6] P. A. Belano, K. F. M. Campit, J. C. S. Mendoza, K. A. S. Rasing, J. R. B. del Rosario and A. A. Bandala, "Development of a Microcontroller-Based Smart Front DoorLock System," 2023 IEEE 15th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM), Coron, Palawan, Philippines, 2023, pp. 1-6, doi: 10.1109/HNICEM60674.2023.10589066.

[7] A. Siswanto, A. Efendi and E. A. Kadir, "Fingerprint Authentication In Smart Home Environment Based On Embedded System," 2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Maldives, Maldives, 2022, pp. 1-6, doi: 10.1109/ICECCME55909.2022.9988711.

[8] K. Elavarasi and V. Mohana, "Smart Fingerprint Authentication and Alert System Using IoT," 2023 2nd International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN), Villupuram, India, 2023, pp. 1-6, doi: 10.1109/ICSTSN57873.2023.10151621.

[9] C. V. S. Revanth, B. Alekhya and M. H. Abbas, "Arduino based Wheelchair Fall Detection System using GPS and GSM Module," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 1022-1026, doi: 10.1109/ICSCSS57650.2023.10169322.

[10] A. Mnyanda, H. T. Matsila and B. Monchusi, "Smart Irrigation System with GSM Module using PIC16F690," 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa, 2023, pp. 1-4, doi: 10.1109/ICECET58911.2023.10389440.

[11] P. S. Kumar, V. B. Sree, N. Ramanjaneyulu, S. Nagurvali, V. Rohith and R. S. Teja, "Effective Garbage Monitoring System Using GSM Module," 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), Krishnankoil, Virudhunagar district, Tamil Nadu, India, 2024, pp. 1-5, doi: 10.1109/INCOS59338.2024.10527614.

[12] Rathina Raj, Vishnu Kanthan, and Meena Belwal. "Design of CoAP Based Model for Monitoring and Controlling Physical Parameters." In Ubiquitous Communications and Network Computing: 4th EAI International Conference, UBICNET 2021, Virtual Event, March 2021, Proceedings, pp. 105-115. Springer International Publishing, 2021.

[13] Princy, K. T. M., and Meena Belwal. "Plant Disease Detection: A Comparative Study of Deep Learning Approaches." In 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA), pp. 1795-1801. IEEE, 2023.

[14] P. Venkatesh and P. Sreedharan, "Face Recognition Based Security System," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-6, doi: 10.1109/ICCCNT61001.2024.10726275.

[15] R. Ravindran, S. Udayakumar, Y. Revanth and K. Namitha, "Enhancing Access Control: A Biometric Approach with Facial Recognition and Near-Field Communication Integration," 2024 Second International Conference on Inventive Computing and Informatics (ICICI), Bangalore, India, 2024, pp. 263-268, doi: 10.1109/ICICI62254.2024.00051.

[16] N. R. S, R. Venkatasamy, J. A. Dhanraj, S. Aravinth, K. Balachandar and D. N, "Design and Development of IOT based Smart Door Lock System," 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT), Kannur, India, 2022, pp. 1525-1528, doi: 10.1109/ICICICT54557.2022.9917767.

[17] Y. T. Park, P. Sthapit and J. -Y. Pyun, "Smart digital door lock for the home automation," TENCON 2009 - 2009 IEEE Region 10 Conference, Singapore, 2009, pp. 1-6, doi: 10.1109/TENCON.2009.5396038.

[18] P. Tilala, A. K. Roy and M. L. Das, "Home access control through a smart digital locking-unlocking system," TENCON 2017 - 2017 IEEE Region 10 Conference, Penang, Malaysia, 2017, pp. 1409-1414, doi: 10.1109/TENCON.2017.8228079.

[19] A. Yadav, F. K. Rana, G. Raj, A. Yadav, A. Sachan and P. Bhardwaj, "Smart Door Locking System Using LoRa Technology," 2022 10th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing (ICETET-SIP-22), Nagpur, India, 2022, pp. 1-5, doi: 10.1109/ICETET-SIP-2254415.2022.9791632.

[20] J. Baidya, T. Saha, R. Moyashir and R. Palit, "Design and implementation of a fingerprint based lock system for shared access," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2017, pp. 1-6, doi: 10.1109/CCWC.2017.7868448.