Grenze International Journal of Engineering and Technology, Jan Issue

Smart Locking System using Internet of Things

Vinay Sapkal[1], Mokshad Nemade[2], Shriraj Nelekar[3], Aditya Narsale[4] Indrakumar Naragude[5], Om Narkhede[6] and Adithyakrishna Nattuvetty[7]
[1-7]Department of Engineering Sciences and Humanities, Vishwakarma Institute of Technology Pune, India
Email: sagar.janokar@vit.edu, {mokshad.nemade221, shriraj.nelekar22, aditya.narsale222, indrakumar.naragude22,om.narkhede22,adithyakrishna.nattuvetty22}@vit.edu

***Abstract*— Smart locking systems have arisen as a potential option for contemporary access control as a result of the Internet of Things' (IoT) quick development and the rising desire for increased security measures. In order to provide secure, practical, and adaptable access management, this research study examines the design, implementation, and assessment of a smart locking system that makes use of IoT technologies. To enable smooth integration with current door lock systems, the proposed smart locking system makes use of a combination of hardware and software components. The system's brain, a central control unit, manages access rights and coordinates communication between numerous components. Users are able to remotely manage and keep an eye on access to their properties thanks to user authentication carried out using a mobile application. This study adds to the expanding body of information on smart locking systems and offers helpful tips for researchers, professionals, and manufacturers that are interested in creating and using safe and clever access control systems. The results show how IoT technology can revolutionize conventional lock systems and support the growth of smart homes and smart cities**

***Index Terms*— Smart City, Smart Security, Internet of Things, Arduino Uno**

I. INTRODUCTION

In recent years, there has been a remarkable surge in the demand for access control systems that seamlessly replace traditional lock and key mechanisms while prioritizing security and convenience. Smart locking systems have emerged as a promising solution, harnessing advanced technologies, including biometrics and One-Time Passwords (OTPs), to address this growing need. Notably, biometric authentication, particularly fingerprint recognition, has garnered widespread acclaim due to its inherent and unique characteristics. The rise of smart locking systems stems from the inherent limitations of traditional lock and key methods. Physical keys are prone to loss or theft, and their duplication poses security concerns. In response to these challenges, smart locking systems have redefined the paradigm of secure and convenient access control. Smart locking systems offer several advantages. They eliminate the need for physical keys entirely, reducing the risk of unauthorized duplication. These systems employ a range of authentication methods, including biometrics, which stands out due to its uniqueness and near-impossibility of replication. Fingerprint recognition, in particular, offers an unparalleled level of security. Biometric authentication leverages an individual's distinct physiological characteristics, such as their fingerprints, to grant or deny access. Fingerprint recognition technology has matured significantly, offering speed, accuracy, and affordability. Its adoption spans various applications, from smartphones to access control systems.

Grenze ID: 01.GIJET.10.1.187

The key advantage lies in the difficulty of forging fingerprints, ensuring that only authorized personnel can gain access. Convenience is a hallmark of smart locking systems. Access control is streamlined, negating the need to carry keys or remember PINs. Users place their finger on a sensor, which rapidly and accurately identifies them, allowing swift access. This not only saves time but also minimizes the risk of lockouts due to misplaced keys or forgotten codes. Furthermore, smart locking systems often incorporate One-Time Passwords (OTPs), which enhance security. These dynamic codes are generated uniquely for each access attempt, adding layer of protection. OTPs can be delivered through mobile apps, SMS, or email, ensuring that even if an unauthorized individual obtains a registered fingerprint, access remains restricted without the valid OTP. The research paper aims to present a comprehensive study of a smart locking system's design, implementation, and evaluation, incorporating both fingerprint recognition and OTP verification. The paper will delve into the system architecture, the fusion of biometric and OTP technologies, and the development of a mobile application for remote access management. Additionally, the research paper will assess the system's performance, security robustness, and user acceptance through practical experiments and surveys

II. Literature Survey

A new three-level security system for smart lock systems has been introduced to improve security in homes, offices, shops, and banks. Users must pass at least two security levels out of fingerprint authentication, image password, and OTP message to gain access. The system also has a guest option with two-level security that changes the password randomly for security purposes. The system provides a high level of security for both authorized and guest users, and admin can enroll new users and register mobile numbers using the system. [1]

The Smart Bag is a lightweight luggage bag equipped with advanced electronic technology for advanced security and convenience. It features auto-trailing technology that reduces human efforts and follows passengers using ultrasonic and IR sensors. It also has proximity detection, GPS and GSM tracking, and a fingerprint locking system for added security. Additionally, it has a recharging port that can be used to charge mobile phones and laptops using an in-built power bank. [2]

The objective of the proposed security system is to provide a more efficient and user-friendly alternative to the traditional chain-lock and key protection for luggage during public transport. The system is password-protected and generates a warning alarm if someone tries to lift the luggage without entering the correct password. This feature makes the system helpful during travel in the bus or train, even at night, as it produces both audio and visual indications. The system is designed to be durable, portable, and cost-effective. [3]

This project aims to develop a smart locking system using the Internet of Things (IoT) to address security concerns in households and workplaces. Biometric locks are preferred over traditional keyed locks due to the risk of lost or stolen keys. A modern biometric lock requires no key and instead uses a biometric sensor. This project utilizes an Arduino nano-based device that provides physical security using the biometric sensor available in a smartphone. [4]

The project aims to implement a door lock system using a fingerprint sensor for high security. This modern lock allows only authorized individuals to unlock the door, eliminating the need for carrying keys. The system also offers additional security features such as OTP verification through a smartphone app. [5]

The project aims to develop a smart door that monitors the door state, sends an SMS to the owner when someone opens the door without unlocking it, and can be locked and unlocked by sending an SMS from a mobile phone. The system uses an Arduino UNO, GSM technology, and other electronic components, and also includes a lamp that turns on and off depending on the door's lock state. The system has been successfully developed, implemented, and tested in the laboratory, and is designed to be very economical and suitable for all kinds of houses. [6]

III. Methodology

The first step to make any system is to have a system architecture design. In this we determine what are the components that will be required for making the system. The system consists of a number of hardware components. The entire system is made using the Arduino UNO board which consists of the ATMega328 8-bit Microcontroller Unit(MCU). Other components that are used are:

- GT511C3 Fingerprint Sensor
- GSM 800 Module
- Sim Card(2G support)
- L298D Motor Driver
- DC Motor

• 2 12V/2A Power adapters
• Jumper Cable (Both Male-Male and Male-female)
• Serial Terminal

The next step is to design the circuit for the working of the model. The circuit design involves thinking of how all the connections are going to be which pin is connecting to what sensor.

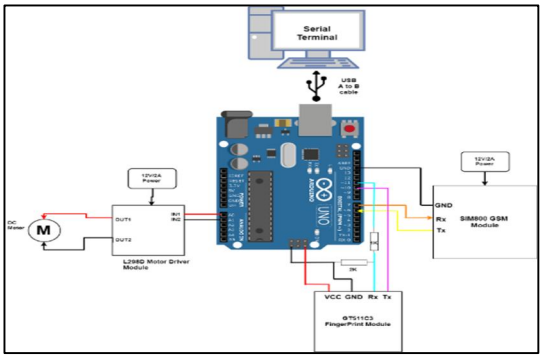

Figure 1. Circuit diagram

The flow of the working of the locking system is as follows, first there is the Arduino Uno board which is connected to the PC. Then the fingerprint sensor is connected to the Arduino Uno Board using jumper cables and resistors. Now the user keeps their finger on the fingerprint sensor and if the fingerprint matches to the one that is stored in the fingerprint sensor's memory then the control shifts to the second factor authenticator which is the OTP verification module.

But what if the fingerprint of the user isn't verified? Then the system gives the user three tries where he/she can verify it and if it still doesn't verify then the system completely locks itself. The method of reopening or again gaining access of the system is written in this paper's Future Scope.

Once the fingerprint of the user is verified then the GSM module connected to the Arduino Uno Board sends an OTP to the number which is registered by the name of the user.

On receiving the OTP, the user has to enter the OTP in the terminal and then if the OTP matches to the one sent to the user then the system is unlocked. Again if the OTP entered by the user is incorrect the user gets another chance where the system sends another OTP to the user, which they can enter into the system. But if that fails then the system locks itself completely. As mentioned above to regain access of the system, the method is in the Future Scope of this Paper.

Arduino programming is a popular open-source platform for developing and coding embedded systems. It simplifies the process of writing code for microcontrollers, making it accessible to both beginners and experienced programmers. Now, moving on the most important part of the system after the assembly of the circuit is the coding by which the system will work. Thus, The Third Step is for the Arduino Programming. In this we set up the Arduino Integrated Development Environment (IDE) and ensure the correct board and port are selected.

The required libraries for the fingerprint sensors, servo motor, and GSM module are imported so that their functions can beused to control the tasks for the system. In this project, the libraries imported are <AdaFruit_Fingerprint.h>, <SoftwareSerial.h>, <Wire.h>, <stdio.h> etc. Then initialize the pins and variables which will be used in the program. There are various number of functions used in the code for making the system. The first main function that is being used is the getFingerprintID() function where the user tells which ID the fingerprint is to be stored. Then the fingerprint scanner scans for the fingerprint and then stores the fingerprint in the specified ID.

Now, as the system that is proposed has a two-factor authentication aim, thus the second verification attempt will be done using the OTP password which will be entered by the user. Thus, there's another function which is used to check the maximum number of verifications attempts in the fingerprint sensor. After this a VerifyOTP () function is created where this is used to check of the OTP entered by the user is actually the OTP that was sent so that the lock can be opened safely.

There are many control statements that have also been used in the code such as for the verification of the fingerprint to the original, for the maximum verification attempts, for the verification of the OTP and many other places. The switch case has been used in the fingerprint sensor code to see give different outputs for the different types of inputs that are received by the sensor.

```
// returns -1 if failed, otherwise returns ID #
bool verifyFingerprint()
{
      uint8_t p = finger.getImage();
      if (p != FINGERPRINT_OK)
      {
        return false;
        }
        p = finger.image2Tz();
      if (p != FINGERPRINT_OK)
      {
        return false;
        }
        p = finger.fingerFastSearch();
      if (p != FINGERPRINT_OK)
      {
        return false;
        }

      return true;
}
```

Figure 2 Fingerprint verify code snippet

Testing and Debugging

The first step to test any code written in the Arduino IDE is to verify the code and then Upload the Arduino program to the Arduino Uno board. But if the program isn't verified then it displays the errors that are present in the code which then have to be debugged. So after the program is debugged and then completely transferred into the Arduino Uno board, then a thorough testing of all the components is done which includes the testing of the fingerprint sensor and its verification as well as its fingerprint ID storage memory, testing of the system on failure of three times, testing of the transition of right fingerprint to the GSM module.

Tests were also conducted to check if the OTP is received on the entered phone and then the entered OTP matches to the one sent to the user.

Simulation of all the types of cases was tried and conducted on the system so that there are no ways of breaking into it in any other way.

One of the main issues that was faced was that there was a connection issue with the components data transfer. Another option that was tried for the data transfer issue was using an I2C connection between two different Arduino Uno boards where the fingerprint sensor was connected to one of the Arduino Uno board and the GSM Module was connected to another. Then an I2C connection was established between the two and the run was checked. But that also didn't give an efficient transfer and verification of the data so the current system was again tested and after removing a couple of bugs and shifting connections the final result was achieved.

Performance Evaluation

After the testing of the system an evaluation phase was conducted where the accuracy and performance of the system was checked.

The system was tried upon by placing the fingerprint in an upside down manner, smudged fingers and it was found that the system is accurate in upside down placing but not accurate with the smudged fingerprints.

Another evaluation that was done was to change the Sim Card to check which Provider was giving a faster service. It was noticed earlier while testing that sometimes the Airtel Sim wasn't sending the OTP to the user and sometimes it was. So another Sim, Jio was tried upon which it was noticed that everytime the OTP was sent from the system it was received by the user. This was another evaluation discovery.

TABLE I. COMPARISON TABLE OF GSM MODULES

GSM Band	Accuracy Percentage	Cost in INR
GSM 800A	99%	1000
GSM 900	98%	1200
GSM 1800	97%	1400
GSM 1900	96%	1600

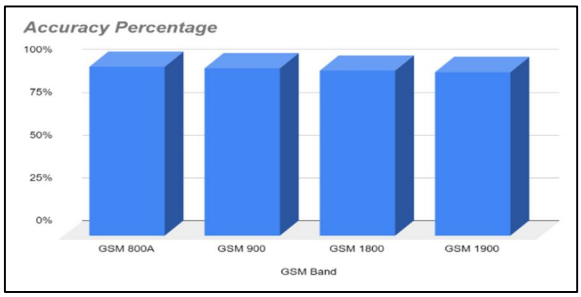

Figure 3. Accuracy vs gsm module graph

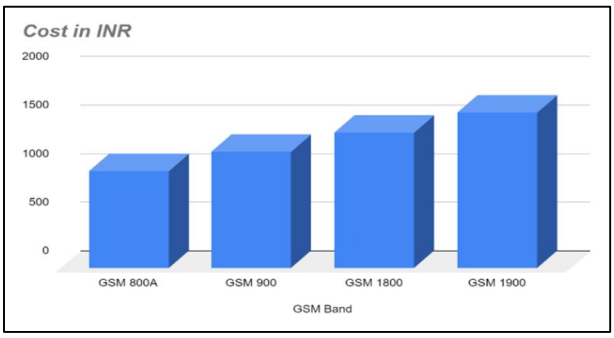

Figure 4. Cost vs gsm module graph

Advantages of this system

• *Convenience*: Users do not need to remember and input complex passwords or carry physical keys. They can access the smart lock using their fingerprint, which is both convenient and secure.
• *No Risk of Lost Keys or Forgotten Passwords*: With a smart locking system, there's no risk of losing keys or forgetting passwords. Users always have their fingerprint with them, making access hassle-free.
• *Integration with Smart Home Systems*: These smart locking systems can often integrate with other smart home devices and systems, such as security cameras and home automation systems, to provide a comprehensive and cohesive security solution.
• *Quick Response to Security Threats*: In case of a security breach, OTP-based systems can quickly change the authentication code, rendering stolen or compromised codes useless.

IV. RESULTS

The entire aim of the system that was created was to make a efficient locking system which didn't cause any sort of hassle to the user. The system which was proposed is clearly depicted in the figure 5 shown below.

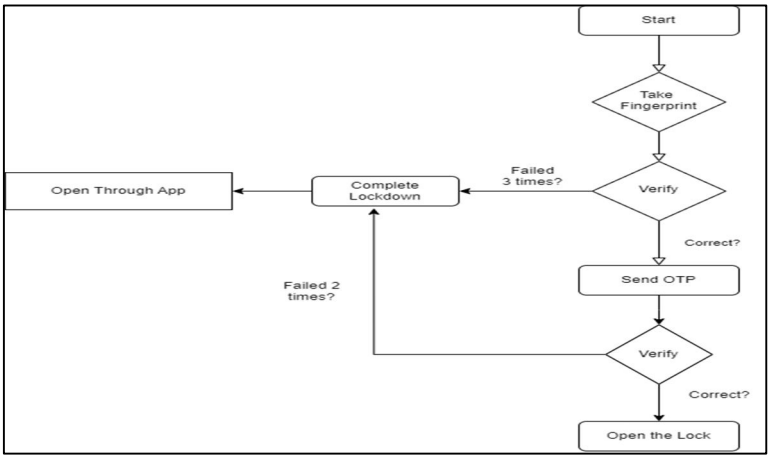

Figure 5. Flowchart of the system

As mentioned earlier in the methodology section, the experimental setup can be seen in the figure 1. There is a main laptop to which the Arduino Uno board is connected and then to the Arduino Uno board there are the Fingerprint Sensor as well as the GSM Module is connected. To the Arduino Uno board the motor driver is also connected which controls the movement of the DC motor attached so that the user can know that the system is unlocked. Using this setup the entire system is made functional. All the connections are done using Jumper Cables and then to maintain the voltage of specific components resistors are used so that appropriate amount of current is passed through so that the components don't get spoilt.
Then the entire code is run and all the test cases have been tried on the system upon which many results have been derived such as the different orientation of the fingers gives different results on the fingerprint sensor and also that the different sim cards upon being used give a different behaviour of the style of sending the OTP's.
The entire system was also tried upon in real life and user feedback was tried to be incorporated. The user feedback was mainly for not receiving the OTP's for which we tried changing the module's sim and it got sorted out. Other feedbacks have been written in the future scope for future implementation. There were also other feedbacks which were the limitations of the system which are mentioned below –
• *False Rejections and False Acceptances*: Fingerprint sensors can occasionally generate false rejections (legitimate users are denied access) or false acceptances (unauthorized users gain access). The accuracy of the fingerprint sensor can be affected by factors like dirt, moisture, or changes in the user's fingerprint due to injury or age.
• *Biometric Data Privacy*: The storage and protection of biometric data are critical. If the fingerprint data is not adequately secured, it can be vulnerable to theft or misuse.
• *Cost*: High-quality fingerprint sensors and OTP authentication systems can be expensive, making the initial investment relatively high.
• *Battery Life*: Many smart locks require batteries to operate. If the batteries run out without warning, it can lead to an unexpected lockout. Some locks have low-battery indicators, but this is still a potential issue.
• *Loss of Physical Key Backup*: Some smart locks eliminate the need for physical keys altogether. If the system fails or the user is locked out without a backup key, it can be challenging to regain access.

V. FUTURE SCOPE

The aim of this is to aid to the existing systems to improve the security and also make the process much more efficient and easier. Although this is an efficient model, it has a lot of scope for improvement. Our future scope includes making the system available for everyone so that the problem will be easily solvable. Some topics to research further on can be:

• *Making an App for the system*

In the proposed system on entering the wrong fingerprint or even the OTP a couple of number of times the system locks itself completely. So, an app can be made so that the system on completely locking itself can be unlocked or the access can be regained after verifying the personnel on the app. The app can also be used to know which user has entered the system as every registered user's data will be saved in the App and every time someone enters the system the app can notify the admin who has entered. There is another use case of the App, which is if the system completely fails itself and nothing is working then this app can be used to completely factory reset the system and gain complete control and erase all the data that is present in the system.

• *Multi-Modal Biometrics*

Combining multiple biometric modalities, such as fingerprint, facial recognition, and voice recognition, to create even more secure authentication systems could be a future research direction.

• *User experience and interface*

Research on improving the user experience, including user-friendly interfaces for configuring and managing the smart locking system, is vital. Simplifying the setup process and enhancing the user interface can make these systems more accessible to a wider audience.

• *Implementing Artificial Intelligence and Machine Learning*

Implementing AI and machine learning algorithms for continuous monitoring and anomaly detection in smart locking systems to identify and respond to security threats.

• *Integration with IoT and Smart Home Ecosystems*

Expanding the integration of smart locks with broader Internet of Things (IoT) and smart home ecosystems can lead to more seamless and interconnected security solutions. Research may explore how to enhance interoperability with other devices and services.

VI. Conclusion

In conclusion, the rising demand for access control systems underscores the need for innovative security solutions, with the Smart Locking System incorporating biometrics and One-Time Passwords (OTPs) standing out as a promising response. This research paper aims to provide a comprehensive understanding of the system's design, implementation, and evaluation, highlighting its advantages such as keyless entry through fingerprint recognition and streamlined access control.

The paper delves into the fusion of biometrics and OTP technologies, the development of a remote access management mobile application, and empirical assessments of performance, security, and user acceptance. As a transformative solution applicable in residential, commercial, and industrial settings, the Smart Locking System emerges as an innovative and effective approach to secure and convenient access control, reinforced by practical insights and user feedback.

References

[1] W Meenakshi N, Monish M, Dikshit K J, Bharath S “Arduino Based Smart Fingerprint Authentication System” in IEEE(2019).

[2] Piyush Mestry, Prathamesh SawantdesaiSuhasini S. Goilkar, Ankush Sutar, Tukaram Kocharekar “Smart Bag with theft prevention and real time tracking” in IJTSRD(2018).

[3] Sanchari Das, Sajal Prasad Karan, Gopal Chandra Jana, S Jagjit Singh, Swati Banerjee, Santana Das, Sanghamitra Layek “Programmable Luggage Security System” in IJARSE(2015).

[4] Karthik A Patil, Niteen Vittalkar, Pavan Hiremat, Manoj A Murthy “Smart Door Locking System using IoT” in IRJET(2020).

[5] Anirudh R, Chandru V, Harish V “ Multilevel Security Biometric Authentication Locking System using Arduino Uno” in IOS Press(2021).

[6] Sialee Leekongxue, Li Li, Tomas Page “Smart Door Monitoring and Locking System using SIM900 GSM Shield and Arduino UNO” in IJERT(2020).

[7] M. Shanthini, G. Vidya and R. Arun, "IoT Enhanced Smart Door Locking System," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2020, pp. 92-96, doi: 10.1109/ICSSIT48917.2020.9214288.

[8] M. Pavelić, Z. Lončarić, M. Vuković and M. Kušek, "Internet of Things Cyber Security: Smart Door Lock System," 2018 International Conference on Smart Systems and Technologies (SST), Osijek, Croatia, 2018, pp. 227-232, doi: 10.1109/SST.2018.8564647.

[9] Sujita B. Dabekar, Sandhyarani A. Lahade, Manasi S. Lunge, Prof. Deepali Yewale, “IOT Based Smart Door Locked System Using Node MCU”, Volume 10, Issue VII, July 2022 in International Journal for Research in Applied Science & Engineering Technology.

[10] M. M. H. Ali, V. H. Mahale, P. Yannawar and A. T. Gaikwad, "Overview of fingerprint recognition system," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 2016, pp. 1334-1338, doi: 10.1109/ICEEOT.2016.7754900.

[11] M. Yuchun, H. Yinghong, Z. Kun and L. Zhuang, "General Application Research on GSM Module," 2011 International Conference on Internet Computing and Information Services, Hong Kong, China, 2011, pp. 525-528, doi: 10.1109/ICICIS.2011.137.

[12] M. H. Eldefrawy, K. Alghathbar and M. K. Khan, "OTP-Based Two-Factor Authentication Using Mobile Phones," 2011 Eighth International Conference on Information Technology: New Generations, Las Vegas, NV, USA, 2011, pp. 327-331, doi: 10.1109/ITNG.2011.64.