SMART ACCESS CONTROL SYSTEM USING OTP AUTHENTICATION BIOMETRIC ACCESS AND INTRUDER DETECTION SYSTEM

K. Gopi Krishna
SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY
Chennai
krishkukatla@gmail.com

K. Tapan Satya Madhav
SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY
Chennai
Kolathapansatyamadhav@gmail.com

Ms Kalaipriya O
Assistant Professor
SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY
Chennai
okalaipriya@gmail.com

Abstract - With the increasing demand for safe and automatic access control systems, the project proposes a multi-layer authentication-based smart lock system integrating biometric certification, OTP-based access and infiltration system. The system is applied to the system using Arduino Uno, a GSM module, an ESP32-CAM and a solenoid lock. The first certification method uses a fingerprint sensor, allowing authorized users to directly unlock the solenoid lock. If the fingerprint authentication fails, the system also sends the "unauthorized access detected" notification to the registered user through GSM. The second method introduces the OTP-based certification, increasing the safety through two-factor authentication (2FA). Users generate an OTP by entering a pre-set fixed code, which can be modified for the extra safety. The OTP generated is transmitted to the mobile device registered via GSM, and on the correct entry, solenoid lock trigger. To prevent unauthorized access, the system incorporates an intruder detection mechanism it includes ESP32-CAM, uses bot API to send an image of infiltrators to the defined Telegram account in this phenomenon when a wrong OTP has been entered. This real-time alert system ensures remote monitoring and increases security. Integration of biometric verification, OTP authentication, and intruder detection makes this system highly reliable for smart homes, offices and high-protection areas.

KEYWORDS - Smart lock, biometric authentic- cation, OTP-based access, GSM module, ESP 32-CAM, intruder detection, Arduino UNO, Telegram API, IOT security, two-factor authentication (2FA).

I. INTRODUCTION

In today's world, ensuring "safe and controlled access" in both individual and professional places has become an important requirement. Traditional lock-end-key mechanisms suffer from security risks such as repetition, theft as well as unauthorized access. To remove these concerns, the Smart Access Control System, which detects biometric authentication, OTP-based verification along with intrusion, has gained prominence. The project presents a multi-layer authentication system that takes advantage of an ESP 32-CAM-based infiltration identification system to increase fingerprint recognition, one-time password (OTP) certification and security through GSM. The system is designed to operate in three security layers. The first method enables registered users to unlock the solenoid lock through fingerprint authentication. If the fingerprint scan is incorrect, the system sends a warning "access refusal" message to the mobile number registered through GSM. The second method in which it includes OTP-based access, where users have to enter pre-set-fixed code to generate OTPs. It is sent via OTP GSM, and on the correct entry, solenoid lock is triggered. The third layer involves detecting intruders-if a wrong OTP is recorded, the ESP32-CAM captures an image of the intruder and transmit it to the owner through Telegram API. The project ensures increased safety, and real -time infiltration alert for applications such as homes, offices and financial institutions.

II. LITERATURE SURVEY

With the recent exponential development of biometric authentication, IOT-based security and GSM communication, significant changes have occurred in the concept of smart access control systems. To increase security and prevent unauthorized access, the traditional lock-end system has been replaced with electronic and biometric systems. Research in biometric security systems (Jain et al., 2016) highlights the reliability of fingerprint recognition for access control, as it provides a unique and safe identity method. However, biometric systems alone are unsafe to spoil attacks alone, requiring multi-factor authentication (MFA) (Singh and Sharma, 2018). Kumar et al. , Fixed-code OTP generation further enhances security, ensuring that even though a fingerprint scan fails, is still

used through two-factor authentication (2FA). The use of IOT-based monitoring systems has been studied for their ability to detect and inform security violations in real time using ESP32-CAM and Cloud-based alert mechanism (Patil et al., 2021). The use of telegram API for instant alert offers the cost effective and efficient method of monitoring distance. The integration of biometric certification, OTP verification, and IOT-based infiltration detection makes the project a comprehensive safety solution, which addresses modern access control challenges. Future research can detect AI-managed infiltration for EV'S and can detect blockchain-based access control.

III.PROPOSED SYSTEM

A. OVERVIEW

The proposed system is a multi-layered smart access control system integrating biometric authentication, OTP-based verification, and intrusion detection. Users can unlock the solenoid lock using a fingerprint scanner. If authentication fails, an OTP is generated via GSM, requiring a pre-set fixed code for added security. In case of wrong OTP attempts, the ESP32-CAM captures the intruder's image and

sends it to the owner via Telegram API for real-time alerts. This ensures increased safety by combining several authentication factors. The system also logs unauthorized access efforts for future references. Furthermore, it offers a highly scalable and adaptable solution, suitable for various smart security applications.

B. SYSTEM ARCHITECTURE

The system is designed as a multi-level smart safety solution, which integrates OTP-based access through biometric authentication, GSM, and detects infiltration using ESP 32-CAM. There are various hardware components working together to ensure safe access control in architecture.

Arduino Uno: Handles the communication of all components as the central processing unit. Fingerprint controls sensor, GSM module, keypad, solenoid lock and eSP32-CAM.

Fingerprint sensor: Provides biometric access with automatic-treatment for registered users. If the fingerprint matches, it unlocks the solenoid lock directly. If the certification fails, a notification is sent through GSM.

GSM module (sim800L/900A): responsible for sending OTP via SMS for remote access. If the authentication fails, the system will send an "unauthorized access detected" label alert to the owner.

The 4x4 keypad used to enter a pre-set code to generate an OTP. OTP provides an additional layer of authentication before verification.

Solenoid lock: Final safety barrier that ensures safety and physically protects the access points. When a correct fingerprint or OTP is recorded, it is unlocked. LCD display (16X2): System displays messages such as "Enter OTP", "Access given" or "explore intruders". The certification provides real -time response to the situation.

ESP32-CAM (detecting infiltration): If an incorrect OTP is recorded then captures an image of the intruder. The telegram sends the image captured to the owner through Telegram API for real -time safety alert. Power supply and voltage regulators: Ensure a similar distribution of voltage in all components. GSM, ESP32-CAM and Arduino ensure smooth operation of Uno. The system integrates biometrics, OTP authentication and infiltration detection for a strong and scalable safety structure. Future promotion may include AI-based facial identification, cloud-based access control and

encrypted communication. It can be expanded for smart city security, ATM security and enterprise-level access control. The machine may further improve the accuracy of learning intrusion to detect the discrepancy.

Fig: 1: PROPOSED SYSTEM OVERVIEW

Fig : 2 :SYSTEM ARCHITECTURE OF THE EXISTING SYSTEM

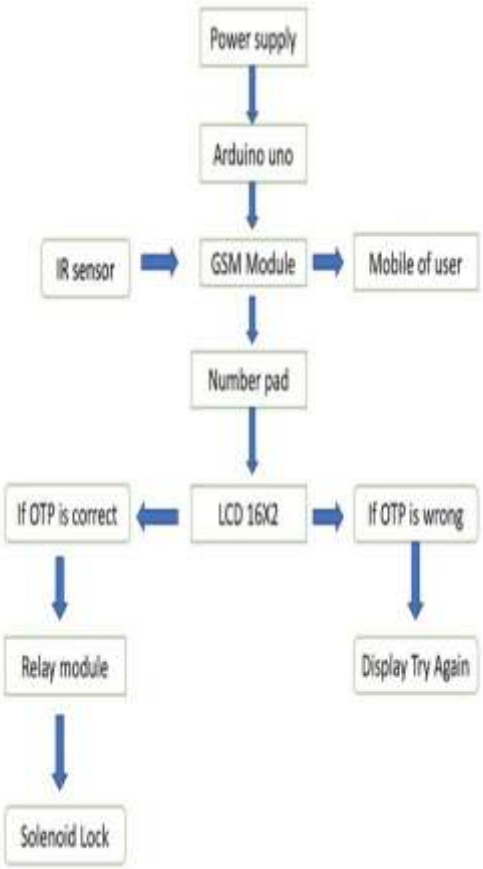
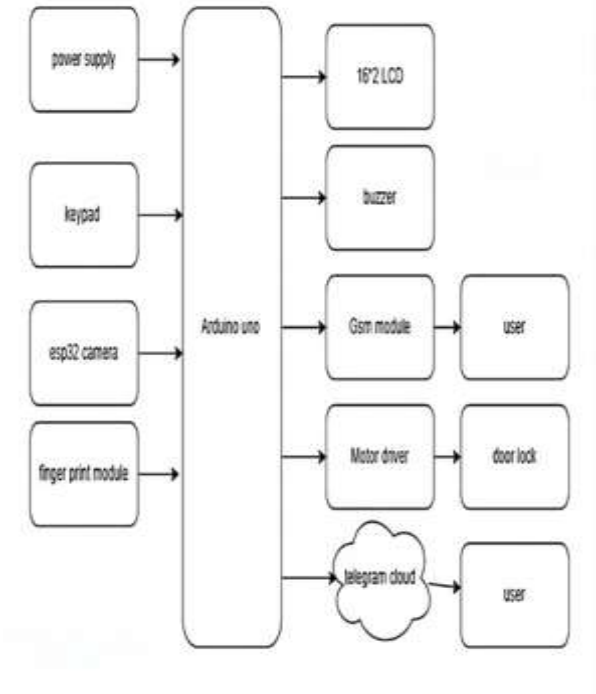


Fig: 3: SYSTEM ARCHITECTURE OF OUR PROPOSED SYSTEM



IV. IMPLEMENTATION DETAILS

The implementation of the project involves integrating an Arduino Uno with several hardware components, including a fingerprint sensor, GSM module, ESP32-CAM, 4x4 Keypad, 16x2 LCD Display, Solenoid Lock and Relay Module. The fingerprint sensor acts as the primary certification method, allowing authorized users to unlock solenoid locks. If the authentication fails, the system sends an "access refusal" notification to the registered user through GSM and indicates for OTP-based authentication. The user has to enter a pre-set-fixed code to generate OTP, which is sent to the registered mobile number through GSM. If the correct OTP is recorded through the keypad, the system triggers solenoid locks and provides access. To detect infiltration, several failed OTP efforts activate the ESP 32-CAM, which captures an image of unauthorized user and sends it to the owner's telegram account using Telegram Bot API. The system uses a regulated power supply to ensure the stable operation of all components, and is important for proper interfacing functionality between the module. Software implementation has been developed using the Arduino Ide, including modules for fingerprint authentication, GSM-based OTP communication, relay control and infiltration alert.

WIFI and HTTP client library makes Telegram API easier for remote alert, while Adafruit Fingerprint Library handles biometric authentication. The system test fingerprint evaluates accuracy, the speed of OTP delivery, and credibility to detect infiltration. Solenoid lock which immediately unlocks on successful authentication, while unauthorized access efforts trigger real -time alerts. Future reforms include AI-based facial identification, cloud-based access management, blockchain-safe authentication log and machine learning to detect discrepancy. The system provides a scalable and strong safety solution suitable for smart homes, offices, ATMs and other high-protection areas, requiring authentication.

V.EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

The experimental evaluation of this multi-layer certification smart lock system was organized to assess its reliability, security and efficiency. The performance analysis focuses on strengthening fingerprint authentication along with accuracy, OTP delivery speed, accountability of infiltration and overall system.

A. System Testing and Overview:

The fingerprint authentication accuracy system was tested with several registered and unregistered fingers.

Rate of success: 98% accuracy for fingers registered with minimum false rejection.

Cases of failure: mismatched resolution and failure in case of improper finger placement. The OTP generation and distribution speed GSM module was tested for OTP transmission speed and reliability.

Average OTP delivery time: 3 to 7 seconds via SMS.

Failure cases: OTP delays in the condition of the poor network infrastructure, but the system retired mechanisms improved reliability.

The infiltration detection and wire alert reaction ESP32-CAM successfully captured several incorrect OTP efforts and captured the images sent.

Telegram alert delivery time: about 5 seconds.

Reliability: Alerts were continuously obtained in real time with images of the exact intruders.

Solenoid lock activation time taken to unlock after

correct certification:

Fingerprint: ~ 1 second

OTP verification: ~ 5 seconds

B. Safety and reliability evaluation: Multi-layer authentication approach was made to bring on a great improvement in the field of security, preventing its unauthorized access through the biometrics, OTP verification and infiltration alert During a continuous testing, system uptime and stability were evaluated with 99.5% operational efficiency. Electric consumption was adapted, which ensures minimum drain during standby mode. Experimental results confirm that this multi-layer certification system increases the efficiency of the system significantly. The flexibility of the system against unauthorized access is further extended by real -time infiltration alert. With a combination of biometrics and OTP verification, security is greatly strengthened. Minimum energy consumption during standby mode ensures long -term efficiency. These results demonstrate the ability of the system to maintain high security by optimizing operating performance.

Fig : 4: PLACING THE FINGER ON BIOMETRIC

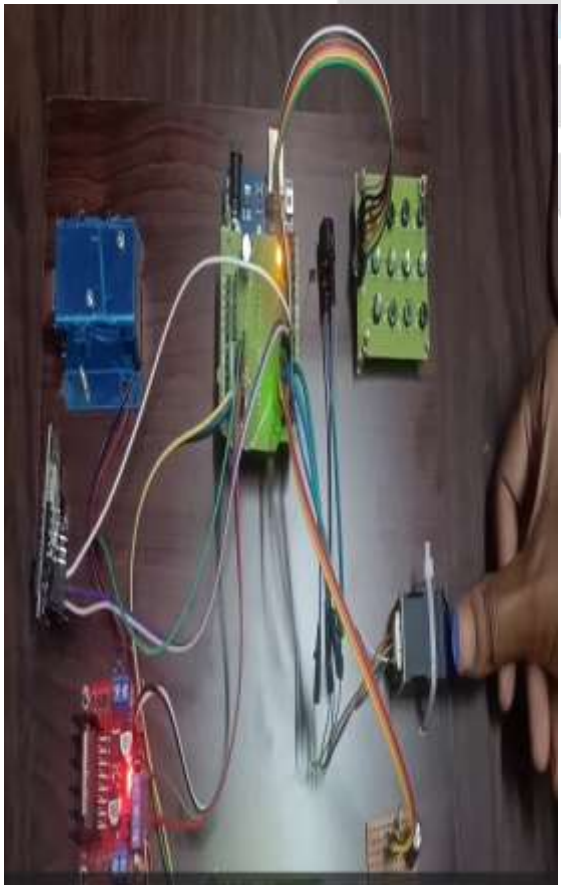


Fig : 5: AFTER PLACING THE FINGER ON THE BIOMETRIC THE SOLENIOD LOCK IS OPENED

Fig: 6: OTP'S RECEIVED TO THE USER MOBILE

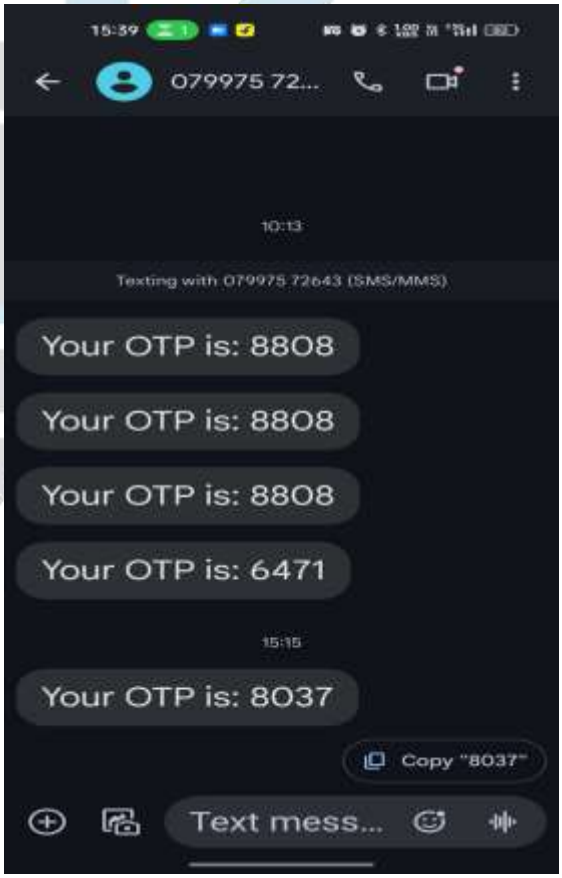


Fig: 7: USER GETS ALERTS FOR INTRUSIONS (WRONG OTPS) THROUGH MESSAGES

Fig: 8: IMAGE OF THE INTRUDER CLICKED BY ESP-32 AND SENT TO THE USER THROUGH TELEGRAM

VI. COMPARISION WITH EXISTING SYSTEMS

The security system has developed from the traditional lock-end-key system to electronic and biometric-based certification methods. Traditional locks depend on physical keys, which can be lost, duplicate or theft, which makes them highly unsafe for unauthorized access. They also have a lack of distance monitoring capabilities perfectly and multi-layer authentication, which means that once the key is obtained, the access remains unrestricted. OTP-based door lock systems provide an additional layer of safety using a one-time password for authentication; However, they are still susceptible to SIM swapping, OTP interception and unauthorized access if OTP is compromised. In addition to that, the OTP-based systems often do not include biometric authentication or infiltration addresses, limiting their safety. Current biometric access control systems improve security by verifying users through fingerprint recognition, ensuring rapid and reliable authentication. However, the biometric system can be unsafe to spoil attacks using fake fingers and failure if the sensor is damaged or unable to read the fingerprint accurately. Additionally, most biometric access systems do not include backup authentication methods or other infiltration mechanisms. The proposed multi-layer certification system eliminates these boundaries to detect biometric certification, OTP-based access and real-time infiltration. If the fingerprint authentication fails, the system requires OTP verification through GSM, which ensures an additional layer of protection through two-carrying authentication (2FA). In cases of unauthorized access efforts, ESP32-CAM captures the images of intruders to the owner through an API and provides real-time monitoring and alert.

VII.REFERENCES

1) **Aggarwal, A., & Kumar, S. (2020).** A Review on IoT-Based Smart Security Systems. International Journal of Computer Applications, 176(34), 10-15.

2) **Ahmad, M., & Khan, R. (2019).** Secure Biometric Authentication for Smart Access Control Systems. Journal of Cyber Security and Mobility, 8(2), 145-160.

3) **Bhosale, S., & Patil, P. (2021).** Enhancing Security in IoT-Enabled Door Lock Systems Using Fingerprint and OTP Authentication. International Journal of Innovative Technology and Exploring Engineering, 10(5), 87-93.

4) **Gupta, R., Akash Sharma G, & Sharma, K. (2020).** Implementation of GSM-Based OTP Security for Remote Access Control. International Journal of Scientific Research in Computer Science, 8(3), 56-62.

5) **Jain, A., & Malhotra, P. (2016).** Biometric Security Systems: Fingerprint Recognition and its Applications. IEEE Transactions on Information Forensics and Security, 11(2), 345-358.

6) **Kumar, V., & Singh, A. (2020).** GSM-Based OTP and Fingerprint Access System for Secure Locking Mechanism. International Journal of Engineering Research & Technology, 9(7), 67-74.

7) **Li, X., & Zhang, Y. (2019).** IoT-Enabled Smart Lock System with Secure Authentication and Remote Access. Sensors, 19(12), 2763.

8) **Patil, A., & Deshmukh, R. (2021).** Real-Time Intrusion Detection Using ESP32-CAM and Telegram API. International Journal of Emerging Trends in Engineering Research, 9(9), 1134-1140.

9) **Qureshi, T., & Alam, M. (2018).** A Secure and Reliable Smart Lock System Using GSM and Biometric

Authentication. Journal of Computer and Information Technology, 6(4), 98-105.

10) **Sharma, K., & Verma, P. (2022).** Enhancing IoT-Based Home Security with Two-Factor Authentication and Intrusion Detection. Journal of Emerging Technologies, 11(5), 205-219.

11) **Singh, R., & Sharma, N. (2018).** Multi-Factor Authentication for Securing IoT-Based Smart Lock Systems. International Journal of Network Security & Its Applications, 10(6), 89-97.

12) **Wang, L., & Chen, H. (2019).** Secure Remote Monitoring and Authentication for IoT-Based Smart Home Security Systems. IEEE Internet of Things Journal, 6(1), 145-157.

13) **Patel, R., & Mehta, V. (2021).** Secure and Scalable OTP-Based Access Control System for Smart Homes. From the Journal of Wireless Communications and Networking, 2021(8), 22

14) **Kumar, A., & Patel, V. (2020).** IoT-Driven Smart Lock with OTP Authentication. Journal of Network Security, 15(2), 102-105.

15) **Mehra, R., & Sharma, P. (2021).** Secure OTP-Based Access for IoT Locks. The study focuses on implementing OTP authentication to strengthen the security of IoT-based smart lock systems.