Robust Security Framework with Biometric Authentication

R.Yogeshwari[1], V. Nithya Poorani[2], G. Gopperumdevi[3], S. Ruckmani[4],
[1,2,3,4]*Assistant Professor, Department of Electronics and Communication, Sri Bharathi Engineering College for Women, Pudukkottai*

***Abstract*— A complete security solution that combines voice recognition, facial detection, and GSM-based OTP has been proposed to tackle the rise in fraud. Voice identification ensures authorised access by verifying users through the analysis of speech patterns. By using facial traits to confirm identity, face detection improves security. By greatly reducing the possibility of unwanted access, this biometric authentication technique gives the verification process a further level of reliability. Additionally, the system uses a GSM-based OTP, which sends a one-time, time-sensitive password to the user's mobile handset. Users enter the OTP for additional verification after voice and facial recognition are successful. The possibility of unwanted access to lockers is greatly decreased by this multi-factor authentication solution. By combining these technologies, security is strengthened and fraud exposure is reduced.**

***Keywords*— GSM, biometric authentication, Security system, OTP configuration, voice and facial recognition**

I. INTRODUCTION

Traditional authentication techniques like passwords and PINs are no longer adequate in the face of growing cyberthreats. Numerous attacks, including malware, social engineering, and violent attacks, can target these systems. Biometrics—particularly voice and facial recognition technologies—have become more dependable and safe substitutes. By limiting access to sensitive information or locations to authorised individuals, these technologies, which are based on distinct physiological and behavioural characteristics, provide a better level of security. By combining voice recognition, facial detection, and one-time password (OTP) authentication, security flaws are fixed and unwanted access becomes more challenging.

Biometric authentication is used by healthcare facilities to safeguard patient information and adhere to privacy laws. Biometric technology are also used by government organisations for national security and border control. The use of machine learning (ML) algorithms into these systems further improves their dependability as they develop, enabling ongoing enhancements to security procedures and anomaly detection.

Machine learning (ML) enhances security systems' capacity for long-term adaptation and improvement. ML algorithms find patterns in large datasets that enable real-time detection of questionable activity. An intelligent, automated security infrastructure is produced by combining this with the Internet of Things (IoT) for smooth communication and artificial intelligence (AI) for decision-making. Furthermore, a type of AI called deep learning has shown promise in jobs like fraud detection and picture recognition, guaranteeing that security systems continue to withstand changing threats. A new era of extremely safe and effective systems for safeguarding sensitive locations and expensive assets is being ushered in by the combination of face and voice recognition, OTP authentication, and AI-powered machine learning.

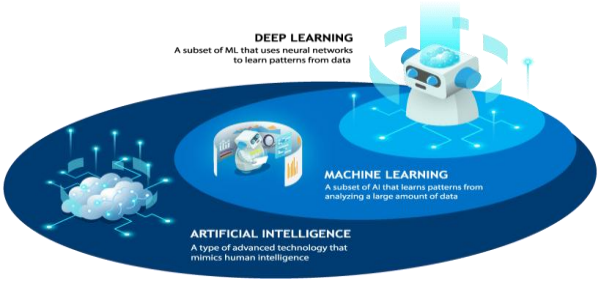


Fig 1.1 Artificial intelligence

II. LITERATURE SURVEY

1. **“**An Integrated Security System for Bank Lockers Using Gated D-Latch” by SilpaKesav Velagaleti (2023): The design of a 45nm CMOS Bank Locker Security (BLS) system is presented in this study along with an analysis of power usage at different process corners and supply voltages (600mV to 1.2V).

2. "Enhancing Bank Locker Security: Machine Learning-Based Facial Recognition with Two-Factor Authentication" by Rishabh Bhardwaj (2023): Innovative bank locker security solution that combines a two-factor authentication framework with CNN and ML-based facial recognition.
3. "Internet of Things (IoT) for Bank Locker Security System" by Ajay Kumar; Priyan Sood (2023): Using facial recognition, the technology enables the manager to grant or refuse user access.
4. "Advance Computing in IoT based High-Security Smart Bank Locker" by Bhawna Khokher; Mamta B Savadatti (2023): This allows solutions for permitting or preventing access, indicates users of unwanted access, and has fire alarms for further defence.
5. "Smart Bank Locker Using Fingerprint Scanning and Image Processing" by Arvasu Chikara; Pallavi Choudekar (2020): The Arduino microcontroller opens the lock after authentication and sends alerts when access limits are exceeded.

III. EXISTING SYSTEM

Because mechanical locks were easily tampered with in the past, electronic locks such as RFID and password-based systems became more popular. By using RFID tags to authenticate users, RFID systems eliminate password-related problems and offer faster, more secure access. When compared to conventional locks, these technologies provide greater protection.
Since they rely on technology, they are susceptible to failures or power outages. They may be vulnerable to hacking, in which case professionals could get around security. They usually entail greater expenses for upgrades, maintenance, and installation. When combining electronic locks with pre-existing systems, compatibility problems could occur.

IV.PROPOSED SYSTEM

For efficient access control, the suggested security system integrates GSM, voice recognition, and face detection technologies. Face detection examines facial features, whereas voice recognition uses a PC MIC input to confirm the individual. The authentication procedure is controlled by an Arduino microcontroller. When identification is successful, the door lock is opened by a DC motor. Unauthorised access sets off an alarm, alerting security and law enforcement. Additionally, a bell is activated to notify anyone in the vicinity of the breach. Only authorised access is guaranteed by this multi-layered security.

4.1 SYSTEM ARCHITECHTURE

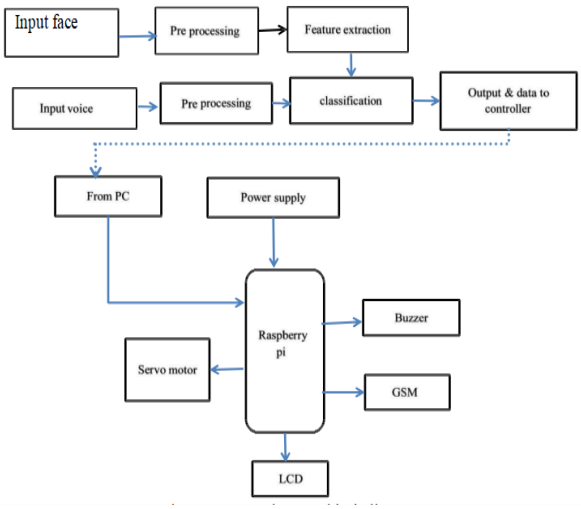


Fig 4 .1 Block Diagram

4.2 HARDWARE SETUP:

RASPBERRY PI:
The Raspberry Pi Foundation created the Raspberry Pi, a low-cost, multipurpose single-board computer. It is perfect for do-it-yourself computing and electronics applications since it packs a CPU, GPU, RAM, and I/O ports into a small package. It supports a wide range of applications, including programming, multimedia, and Internet of Things devices, despite its low specifications. Numerous innovative initiatives are made possible by its open-source nature and robust community support.

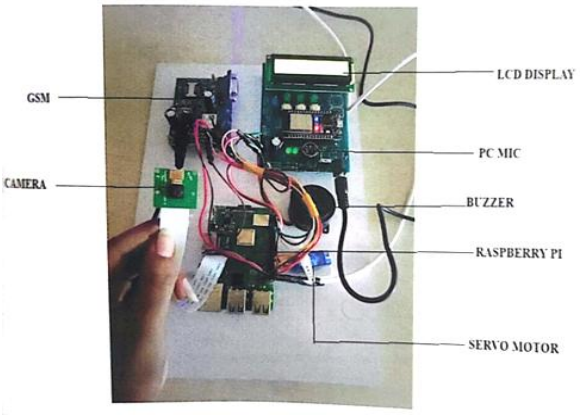
BUZZER:
By converting audio signals into sound, a buzzer can alert or prompt with a variety of sounds, such as melodies and sirens. Alarm systems, timers, sirens, and household appliances all use it. While excited buzzers need a square wave signal to function, self-excited buzzers operate on DC voltage.

GSM:
The most popular digital mobile network in the world is called GSM (Global System for Mobile Communication). Prior to sending data over particular frequency ranges, such as 900 MHz or 1,800 MHz, it digitises and compresses the data. The development of GSM has improved mobile telecommunications through the use of

technologies like EDGE, UMTS, GPRS, and HSCSD.

POWER SUPPLY:
For the purpose of power equipment such as servers or laptops, a power supply transforms electrical current into the appropriate voltage, current, and frequency. Both DC to DC and AC to DC modes of operation are possible. Power supply can be external (standalone) or internal (integrated into devices).

LCD (LIQUID CRYSTAL DISPLAY)
LCD (Liquid Crystal Display) screen is an electronic display module and find a wide range of applications. A 16x2 LCD display is very basic module and is very commonly used in various devices and circuits.



4.2 Kit Image

SERVO MOTOR:
A servo motor is a rotary actuator that uses an encoder or potentiometer as a feedback mechanism to precisely control angular position. Accurate position control is ensured by its closed-loop operation. Because of its compact size, variable speed, and torque, servo motors are perfect for robotics and automation applications.

4.3 SOFTWARE SETUP:
PYTHON 3.7.4
Guido van Rossum is the creator of Python, a high-level, interpreted, object-oriented programming language. Its basic syntax and English keywords make it easy to read. Both procedural and object-oriented programming are supported by Python, which is widely utilised by tech behemoths like Google, Amazon, and Facebook. For software engineers, it's an essential language to learn, particularly for web development.

Fig 4.3 Python

MYSQL
Based on SQL, MySQL is an open-source relational database management system that Oracle supports. With the help of several SQL queries, such as insert, update, delete, and select, users may manage and modify data. Both novices and experts can benefit from the tutorial. For better comprehension, it also includes MySQL interview questions.

WAMPSERVER
WampServer is a Windows web development environment. It allows you to create web applications with Apache2, PHP and a MySQL database. Alongside, PhpMyAdmin allows you to manage easily your database. WAMPServer is a reliable web development software program that lets you create web apps with MYSQL database and PHP Apache2.

V.RESULT AND DISCUSSION

For increased security in high-security zones, the technology combines voice identification and facial recognition with dual authentication. This guarantees strong defence against unwanted access.
The technology minimises false positives by identifying authorised users with high accuracy thanks to sophisticated algorithms. Administrators can react quickly to security issues since real-time monitoring notifies them of questionable activity.
To suit certain requirements, high security administrators might alter authentication levels and protocols. The system is nevertheless easy to use even with its sophisticated security features, guaranteeing a flawless experience for both employees and clients. The following are important system benchmarks:
Accuracy: Making sure that authorised users can be reliably identified using speech and facial patterns.
Speed: Quick data processing to provide uninterrupted real-time access.

Security: Bringing in place safeguards against spoofing and impersonation, such as encryption.
Reliability: Ensuring consistent performance under various conditions.
Scalability: The ability to handle a growing user base without sacrificing performance or security.
In high-security applications this multi-layered strategy improves security and user experience.

APPLICATIONS

- High security
- Security Locker
- Smart Home Security
- Industrial Authentication
- Device Authentication

Fig 5.1 Image Training Process

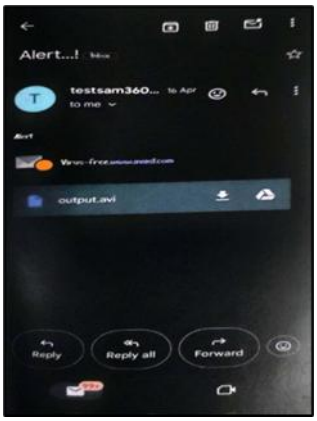


Fig 5.2 OTP send via Gmail

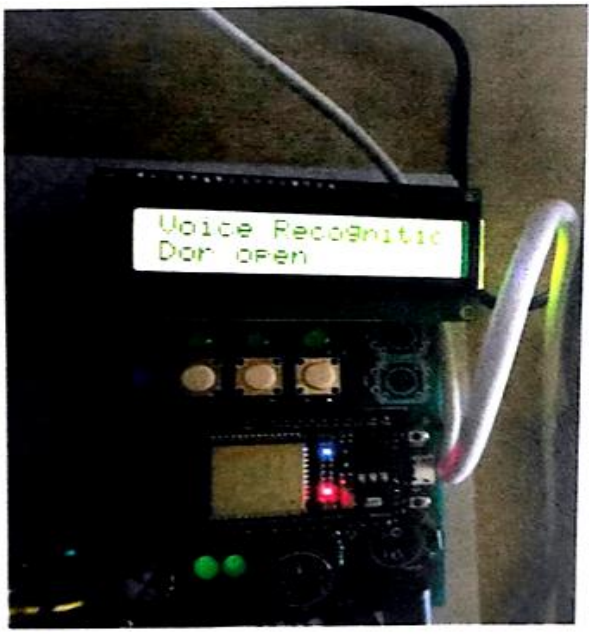


Fig 5.3 Final Output Image

VI.CONCLUSION

Through the integration of voice identity, facial detection, GSM technology, and an Arduino microcontroller, the suggested security device provides a reliable solution for high-security locations. It prevents unwanted entrance by limiting access to registered users solely through the use of voice and facial recognition modules. The actual door lock is operated by a servomotor, and communication is enhanced by a modem. In order to quickly identify and address any unauthorised access attempts, the system also has a security alarm system and real-time monitoring. Its intuitive interface makes operating simple, and its adjustable security settings offer versatility. Strong security and a flawless user experience are guaranteed by this multi-layered strategy. The technology improves user safety and confidence and is a major security development for high-risk regions, especially in financial institutions.

REFFERENCE

[1] Sagar S. Palsodkar*, Prof S.B. Patil, “Review: Biometric and GSM Security for Lockers” Int. Journal of Engineering Research and Applications, Vol. 4, Issue 12(Part 6), December 2014.
[2] R.Ramani , S. Selvaraju , S.Valarmathy, P.Niranjan , “High security Security System based on RFID and GSM Technology’’, International Journal of Computer Applications (0975 – 8887) Volume 57– No.18, November 2012
[3] P. Sugapriya#1, K. Amsavalli#2, “Smart Banking Security System Using Pattern Analyzer”, International Journal of Innovative Research in Computer and Communication Engineering, Vol.3, Special Issue 8, October 2015
[4] M.Gayathri, P.Selvakumari, R.Brindha “Fingerprint and GSM based Security System” International Journal of Engineering Sciences & Research Technology, ISSN: 2277-9655, Gayathri et al.3(4): April, 2014
[5] Mary Lourde R and DushyantKhosla “Fingerprint Identification in Biometric Security Systems” International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010
[6] Pramila D Kamble and Dr. Bharti W. Gawali “Fingerprint Verification of ATM Security System by Using Biometric and Hybridization” International Journal of Scientific and Research Publications, Volume 2, Issue 11, November 2012

[7] Ashish M. Jaiswal andMahipBartere "Enhancing ATM Security Using Fingerprint And GSM Technology", International Journal of Computing Science and Mobile Computing Vol. 3, Issue. 4, April 2014

[8] Abhilasha A Sayar1 , Dr. Sunil N Pawar2 , "Review of High security System Using Embedded System" , International Journal of Advanced Research in Computer and Communication Engineering .,Vol. 5, Issue 2, February 2016

[9] SanalMalhotra, "Banking Locker System With Odor Identification & Security Question Using RFID GSM Technology". International Journal of Advances in Electronics Engineering – IJAEE Volume 4 : Issue 3

[10] Vaijanath R. Shintre, Mukesh D. Patil, "Banking Security System Using PSoC". International Journal of Advanced Research in Computer and Communication EngineeringVol. 4, Issue 7, July 2015.

[11] E. Rohadi et al., "Internet of Things: CCTV Monitoring by Using Raspberry Pi," 2018 International Conference on Applied Science and Technology (iCAST), Manado, Indonesia, 2018, pp. 454-457.

[12] A. Rakshit and A. Chatterjee, "A Microcontroller-Based IR Range Finder System With Dynamic Range Enhancement," in IEEE Sensors Journal, vol. 10, no. 10, pp. 1635-1636, Oct. 2010.

[13] C. Jensen and W. Scacchi, "Collaboration, Leadership, Control, and Conflict Negotiation and the Netbeans.org Open Source Software Development Community ," Proceedings of the 38th Annual Hawaii International Conference on System Sciences, Big Island, HI, USA, 2005, pp. 196b-196b.

[14] R. Johar, S. M. Qaisar, A. Subasi and R. F. Kurdi, "A Raspberry Pi Based Event Driven Quasi Real Time Attendance Tracker," 2018 IEEE 3rd International Conference on Signal and Image Processing (ICSIP), Shenzhen, 2018, pp. 418-422.

[15] R. V. Golhar, P. A. Vyawahare, P. H. Borghare and A. Manusmare, "Design and implementation of android base mobile app for an institute," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016, pp. 3660- 3663.