

AI Based Smart Locker Security System Using Multi Authentication System

Nilofurnisha.J^{1*},Durga.S²,Vishnupriya.P³,Kaviya.S⁴,Srirenganayaki.V⁵

^{2,3,4,5} *UG Students, Electronics and communication Engineering,
Bharathiyar Institute of Engineering for women (Autonomous) Salem, TamilNadu, India*

¹ *Assistant professor, Electronics and communication Engineering &
Bharathiyar Institute of Engineering for women (Autonomous), Salem, Tamilnadu, India*

Abstract—Security of valuable assets such as jewelry, confidential documents, and digital data is a major concern in today's world. Traditional locker systems rely on single authentication methods like keys or passwords, which are vulnerable to theft, duplication, and hacking. To overcome these limitations, this paper proposes an AI-based smart locker security system using multi-authentication

The system integrates multiple authentication methods such as fingerprint recognition, face recognition, and password verification to ensure high-level security. Artificial Intelligence techniques are used for biometric verification, while IoT technology enables remote monitoring and real-time alerts. The system allows access only when all authentication layers are successfully verified. This approach significantly enhances security, reduces unauthorized access, and provides real-time monitoring through mobile or email notifications. The proposed system is reliable, efficient, and suitable for modern security applications.

Keywords: Smart Locker, Artificial Intelligence, Multi Authentication, IoT, Security System

1. INTRODUCTION

In traditional locker systems, security is limited because they rely on single authentication methods such as keys or passwords, which can be easily lost, stolen or hacked. As a result, there is a need for a more advanced and reliable security system to protect valuable items and sensitive data. To overcome these limitations, the proposed system integrates multiple authentication techniques such as password verification, face recognition, and OTP-based validation. These multiple layers of security ensure that only authorized users can access the locker.

Additionally, IoT technology is used to enable remote monitoring and real-time alert notifications. This improves the overall reliability, efficiency and security of the system, making it a modern and effective solution for smart security applications.

With the rapid growth of technology, security systems must to protect valuable assets from unauthorized access. Traditional locker systems use mechanical keys or simple passwords, which are prone to duplication, theft, and hacking. Modern security systems require intelligent solutions that can provide multiple layers of protection. Artificial Intelligence (AI) and Internet of Things (IOT) technologies offer advanced methods for improving security systems.

An AI-based smart locker system that uses multi-authentication techniques including fingerprint, face recognition, and password verification. The integration of AI ensures accurate identification, while IoT enables real-time monitoring and alerts.

2. RELATED WORKS

In recent years, several research works have focused on improving security systems using advanced technologies such as IoT, Artificial Intelligence, and biometric authentication. Many systems use RFID-based access control, password protection or fingerprint recognition to secure lockers and restricted areas. These methods provide basic security but are limited because they rely on a single authentication technique, which can be easily compromised or bypassed.

Some researchers have developed face recognition-based systems to enhance security by identifying authorized users. Others have implemented OTP-based authentication to add an extra layer of protection. Additionally, IOT-based smart security systems have been introduced to enable remote monitoring and real-time alert notifications. However, these systems often face challenges such as limited accuracy, higher cost, or lack of multi-level authentication.

To overcome these limitations, the proposed system combines multiple authentication methods including password, face recognition, and OTP verification along with IoT technology. This integrated approach provides higher security, better reliability, and improved protection compared to existing systems.

However, many of these systems still lack proper integration of multiple authentication techniques, which

reduces their effectiveness in preventing unauthorized access. Therefore, combining AI, IoT and multi-level authentication provides a more robust and secure solution.

Several researchers have proposed different methods to improve security systems using advanced technologies. Kumar et al. developed an RFID-based smart locker system that allows users to access lockers using RFID cards. While this method provides basic security, it is vulnerable to card duplication and unauthorized access. Similarly, Sharma et al. introduced a password-based digital locking system, but it suffers from security risks such as password leakage and hacking.

To enhance security, Reddy et al. proposed a face recognition-based system that uses image processing techniques to identify authorized users. This method improves authentication accuracy but may be affected by lighting conditions and facial changes. Additionally, Patel et al. implemented an OTP-based authentication system that provides an extra layer of security by sending a one-time password to the user's mobile device. However, relying on a single method is still not fully secure.

Furthermore, Singh et al. developed an IOT- based smart security system that enables remote monitoring and real-time alert notifications. Although this system improves accessibility and control, it lacks multi-level authentication for stronger protection. Therefore, the proposed system integrates password, face recognition, and OTP-based authentication along with IoT technology to provide enhanced security, reliability, and efficiency compared to existing methods.

3. PROPOSED METHODOLOGY

The proposed system operates using a multi- level authentication process to ensure high security for the smart locker. Initially, the user is required to enter a valid password as the first level of authentication. If the password is correct, the system proceeds to the next stage; otherwise, access is denied. In the second stage, face recognition is performed using a camera, where the captured image is compared with the stored data to verify the user's identity.

After successful face verification, the system generates a One-Time Password (OTP) and sends it to the registered mobile number using IoT technology. The user must enter the correct OTP within a specified time to complete the authentication process. If all the verification steps are successful, the locker opens; otherwise, access is denied and an alert notification is generated. This multi-layered approach improves security, reliability and protection against unauthorized access.

Implementation Algorithm

The implementation of the smart locker system is based on a multi-level authentication process to ensure high security and reliability. The system verifies the user through password, face recognition, and OTP authentication in a sequential manner. Each step must be successfully completed before proceeding to the next, ensuring that only authorized users can access the locker. The following steps describe the working process of the system.

Algorithm:

Step1: Initialize the system

→ Power ON all components and prepare the system for operation.

Step2: Enter password

→ The user inputs the password as the first level of authentication.

Step3: Verify password

→ The system checks the entered password. If correct, it proceeds; otherwise, access is denied and an alert is generated.

Step4: Activate face recognition

→ The camera is turned ON to capture the user's face.

Step5: Verify face

→ The captured image is compared with stored data. If matched, the system proceeds; otherwise, access is denied.

Step6: Generate OTP

→ A One-Time Password is created for additional security.

Step7: Send OTP

→ The OTP is sent to the user's registered mobile number using IoT.

Step8: Enter OTP

→ The user enters the received OTP.

Step9: Verify OTP

→ If the OTP is correct, the locker opens; otherwise, access is denied and an alert is generated.

Step10: End process

→ The system resets and returns to the initial state for the next user.

Thus, the implementation algorithm ensures a systematic and secure operation of the smart locker system through multi-level authentication.

Each step verifies the user's identity before granting access, reducing the chances of unauthorized entry.

The combination of password, face recognition, and OTP verification enhances the overall security, reliability and efficiency of the system.

Module List

1. User Authentication Module
2. Face Recognition Module
3. OTP Verification Module
4. IoT Communication Module
5. Alert and Notification Module
6. Locker Control Module

3.1ModuleDescription

User Authentication Module

This module verifies the user by checking the entered password. It acts as the first level of security and ensures that only authorized users can proceed to the next stage of authentication.

Face Recognition Module

This module captures the user's image using a camera and compares it with the stored database. It confirms the identity of the user using facial features, providing an additional layer of security.

OTP Verification Module

This module generates a One-Time Password (OTP) and sends it to the registered mobile number. The user must enter the correct OTP to complete the authentication process.

IOT Communication Module

This module enables communication between the system and the user's mobile device. It is responsible for sending OTPs and alerts through internet connectivity.

Alert and Notification Module

This module generates alerts when incorrect authentication attempts are detected. It helps in notifying the user about unauthorized access attempts, improving security.

Locker Control Module

This module controls the opening and closing of the locker. It unlocks the locker only after successful authentication and ensures proper system operation.

4. RESULTS AND DISCUSSION

The proposed AI-Based Smart Locker Security System was successfully implemented and tested to evaluate its performance in providing secure access.



Fig1.Flow Diagram

The system uses multi-level authentication, including password verification, face recognition, and OTP validation. During testing, the system accurately identified authorized users and prevented unauthorized access attempts. The face recognition module showed good accuracy under normal lighting conditions and the OTP verification process ensured an additional layer of security.

The system also demonstrated fast response time, as each authentication step was completed quickly without causing delays to the user.

The IOT module effectively sent OTPs and alert notifications to the registered mobile number, enabling real-time monitoring of the system. In cases of incorrect password, unmatched face, or wrong OTP entry, the system immediately denied access and generated alerts, improving overall safety. Furthermore, the integration of multiple authentication techniques significantly enhanced the reliability and robustness of the system compared to traditional single-level security systems. The system was able to detect and handle unauthorized access

attempts efficiently, reducing security risks. Over all, the results show that the proposed system is effective, secure, and suitable for real-time smart locker applications.



Fig. 2 Demonstrated Ouput

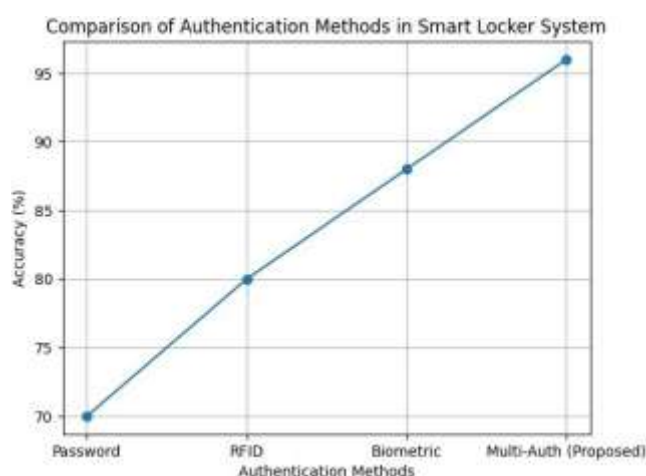


Fig.3.Comparisionof Authentication

5. CONCLUSION AND FUTURES COPE

We present a secure and efficient smart locker system using a multi-level authentication mechanism. By integrating password verification, face recognition, and OTP-based authentication, the system ensures a high level of security and minimizes unauthorized access. The use of IoT technology enables real-time communication and monitoring, making the system more reliable and user-friendly. Furthermore, the proposed system enhances safety by providing alert notifications during invalid access attempts. Overall, the implementation demonstrates improved security, accuracy, and flexibility compared to traditional locker systems, making it suitable for modern smart security applications. In future, the system can be enhanced by integrating advanced technologies such

as AI-based behavior analysis and fingerprint authentication for an additional layer of security. Cloud storage can be implemented to maintain access logs and enable remote monitoring from anywhere in the world.

Moreover, mobile application integration can be developed to control and monitor the locker system more efficiently. The system can also be expanded to support voice recognition and real-time video surveillance, further improving the overall security and usability of the smart locker.

REFERENCES

- [1] S. Sharma, A. Gupta, and R. Singh, "Smart Locker Security System Using IoT and Biometric Authentication," in Proceedings of the International Conference on Smart Computing, 2021, pp. 45–49.
- [2] M. K. Jain and P. Verma, "Multi-Factor Authentication Based Secure Locker System Using Embedded Systems," IEEE Access, vol. 8, pp. 102345– 102352, 2020.
- [3] R. Kumar, S. Patel, and N. Shah, "Face Recognition Based Smart Security System Using Artificial Intelligence," in IEEE International Conference on Artificial Intelligence and Signal Processing (AISP), 2022, pp. 1–5.
- [4] D. Lee and H. Kim, "IoT-Based Smart Home Security System with Real-Time Alerts," IEEE Internet of Things Journal, vol. 7, no. 6, pp. 5123– 5130, 2020.
- [5] P. Raj and K. Anand, "Design and Implementation of Smart Locker Using Fingerprint and OTP," in IEEE Conference on Communication and Electronics Systems (ICCES), 2019, pp. 678–682.
- [6] A. N. Khan, M. Ali, and S. Ahmed, "Secure Multi-Authentication System Using IoT for Smart Applications," IEEE Sensors Journal, vol. 21, no. 4, pp. 4567–4575, 2021.
- [7] A. A. Alzhrani et al., "Design and Implementation of an IoT-Integrated Smart Locker System utilizing Facial Recognition Technology," Engineering, Technology and Applied Science Research, 2024.
- [8] C. Bharatiraja et al., "An IoT based centralized smart locker using RFID technology," AIP Conference Proceedings, 2023.
- [9] Y. Wu et al., "A Design of Smart Locker System Based on IoT for Campus," IEEE CYBER Conference, 2023.
- [10] P. M. Sánchez et al., "Auth CODE: A Privacy-

preserving and Multi-device Continuous Authentication using Machine Learning,” 2020.

[11] S. AlJanah et al., “A Multi-factor Multi-level Authentication Framework for IoT Applications,” 2022.

[12] S. AlJanah et al., “Multi-Factor Homomorphic Encryption based Authentication for IoT Devices,” 2023.