INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VI, June 2025

Bank Locker Security System Using Machine Learning

Vaishnavi Gund, Samiksha Wagaj, Sonali Mane, Divya Sapkal, Prof. S.D. Pandhare, Prof. I.Y. Inamdar

SMSMPITR Institute of Technology, Akluj, India

DOI: https://doi.org/10.51583/IJLTEMAS.2025.140600032

Received: 18 June 2025; Accepted: 23 June 2025; Published: 05 July 2025

Abstract: This project presents a highly secure and intelligent Bank Locker Security System that integrates multiple layers of authentication, including face recognition, OTP verification, and traditional physical key access, to ensure maximum safety and reliability. The system aims to overcome the limitations of conventional bank locker mechanisms by introducing a multi-factor authentication model that minimizes the risk of unauthorized access and theft. The face recognition module, powered by AI, authenticates the customer using live camera input, while a one-time password (OTP) sent to the registered mobile number acts as a second layer of security. Only after successful verification of both digital steps is the customer allowed to use the physical key to access the locker, thereby creating a robust three-level authentication system. The solution also includes an admin dashboard for locker management, user access control, and real-time security logs. This modernized locker system enhances trust, improves security standards, and brings smart automation to traditional banking services.

Keywords — Bank Locker Security, Multi-Factor Authentication, Face Recognition, OTP Verification, Physical Key Access, Artificial Intelligence, Biometric Security, Secure Access System, Real-Time Authentication, Admin Dashboard, Smart Banking, Fraud Prevention, Surveillance System, User Verification

I. Introduction

In the digital age, the importance of security in the banking sector has grown exponentially. With increasing cases of data breaches, identity theft, and physical break-ins, traditional security methods for bank lockers—primarily dependent on manual operations and physical keys—are no longer sufficient to meet modern safety standards. There is a growing demand for more secure, automated, and intelligent locker access systems that can guarantee the identity of users and prevent unauthorized access.The Bank Locker Security System proposed in this research is designed to address these challenges by introducing a multi-level authentication mechanism, which combines the power of biometric verification (face recognition), dynamic OTP-based authentication, and physical key access. This combination ensures that even if one layer is compromised, the other layers continue to safeguard access. Each component plays a vital role: face recognition ensures that only the authorized person is attempting to access the locker, the OTP confirms identity via a secure mobile channel, and the traditional key provides a physical layer of control.The system is built using advanced AI and image processing techniques for real-time facial recognition, and Twilio API or similar services to handle secure OTP generation and delivery. An IoT-enabled hardware setup manages the locking mechanism. The admin panel provides an intuitive web interface for managing lockers, viewing logs, and controlling user permissions. All authentication activities are logged and monitored to enable complete transparency and traceability.Furthermore, the integration of AI and real-time monitoring allows for features like suspicious activity detection, fail-safe mechanisms, and alerts in case of unauthorized access attempts. This smart system not only enhances user trust but also significantly reduces human intervention and operational delays.The implementation of such a security system represents a major shift from legacy models to intelligent, technology-driven infrastructure in banking. It aligns with the goals of digital transformation in financial institutions, offering a scalable, secure, and user-friendly solution.The growing number of security breaches and unauthorized access incidents in financial institutions, particularly in bank locker facilities, has emphasized the urgent need for a more advanced and foolproof security system. Traditional lock-and-key systems are increasingly vulnerable, while biometric authentication offers a secure and intelligent solution. Our proposed system combines facial recognition technology with OTP-based two-factor authentication, creating a dual-layered security protocol that ensures only authorized individuals gain access to bank lockers.The system is designed to minimize human dependency while enhancing access control accuracy. Upon reaching the locker access point, the user's face is captured and matched against a secure database using deep learning-based face recognition algorithms. Upon successful recognition, an OTP is generated and sent via SMS to the user's registered mobile number. Only after the correct OTP is entered, the locker access is granted.

II. Literature Review

Persis Jessintha J [1] the author has told us that by taking a fuel sensor and GPS tracker, they

connect each other with the help of cloud and get information about the nearest fuel station through mobile.

Ganesh Kadam, Saurabh Lanke, Kavita Suryawanshi [2] the author has given the information how to provide the connection senser and gas tracker.

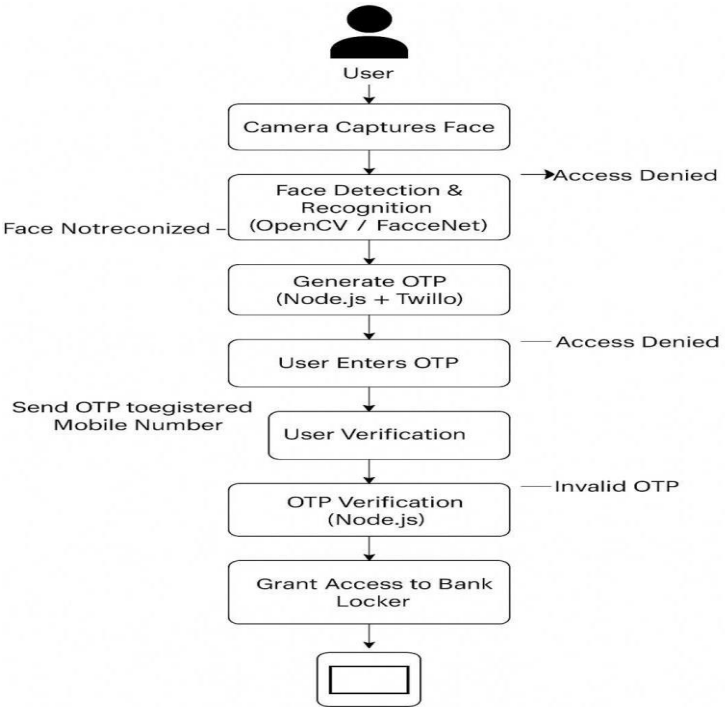
Vaishnavi Shinde, Saloni Pawar, Purva Patel, Sakshi Ghorpade, Nilesh Wankhede [3] proposed the author has said that our main objective is to reduce the crowd at the CNG station and save the user's time and provide him with live information of CNG station.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VI, June 2025

Prachi Jain, Rashid Ali [4] the author has given information about the model of CNG station, in which he has said that we have to calculate how many nodes we have and how much time we need to fill a car with CNG and accordingly we have to design the architecture of CNG.

III. Proposed Methodology

Methodology:



The proposed Bank Locker Security System employs a multi-level authentication mechanism to ensure only authorized individuals can access bank lockers. The methodology integrates biometric recognition, dynamic OTP verification, and physical key access to form a robust, secure process. When a user attempts to access the locker, the system initiates by capturing a real-time image using a camera connected to the terminal. This image is then processed using AI-based facial recognition algorithms, such as OpenCV with Haar Cascades or deep learning models, and compared with the stored database records. If the face is recognized successfully, the system generates a One-Time Password (OTP) and sends it to the user's registered mobile number using secure communication APIs like Twilio. The user must enter this OTP within a limited timeframe to proceed. Once both the face recognition and OTP verification are successful, the final step involves manual confirmation using a physical key to unlock the locker, thus completing a three-layer security process.The system also includes an intuitive admin dashboard developed using modern web technologies, which enables bank officials to manage user access, monitor locker activities, and track all authentication attempts in real-time. This dashboard provides features such as user record management, log monitoring, and alert notifications for failed or suspicious access attempts. All user interactions and system activities are logged into a secure database, ensuring full traceability and audit capabilities. The entire system is built to align with modern banking requirements, offering a reliable and scalable solution to prevent unauthorized locker access while maintaining user convenience and enhancing institutional trust.

Implementation:

The implementation of the Bank Locker Security System is carried out by integrating hardware and software components to ensure secure and reliable access. The system begins with the installation of a high-definition webcam or surveillance camera at the locker terminal to capture the user’s facial image in real time. This image is processed using facial recognition algorithms built using Python libraries such as OpenCV and face_recognition. The trained model compares the live image with pre-stored images in the database to authenticate the user. If the face is successfully recognized, the system proceeds to the next step, where an OTP is generated using a Python-based backend and sent to the user’s registered mobile number through an SMS gateway like Twilio or Fast2SMS. The frontend interface, developed using HTML, CSS, and JavaScript, prompts the user to enter the received OTP. Once verified, the system confirms the user's digital identity.The final step involves enabling the physical locking mechanism. After successful digital verification, a microcontroller such as Arduino or Raspberry Pi activates the relay to allow physical key insertion or locker door unlocking. This ensures that digital authentication is always followed by manual verification for added security. The admin dashboard, built using PHP or Node.js with a MySQL database, allows administrators to monitor user activity, manage authentication logs, and update locker assignments in real time. All modules communicate seamlessly through RESTful APIs and secure backend services. This implementation approach ensures high accuracy in user identification, real-time monitoring, and robust access control while keeping the system user-friendly and scalable for real-world deployment in banking environments.

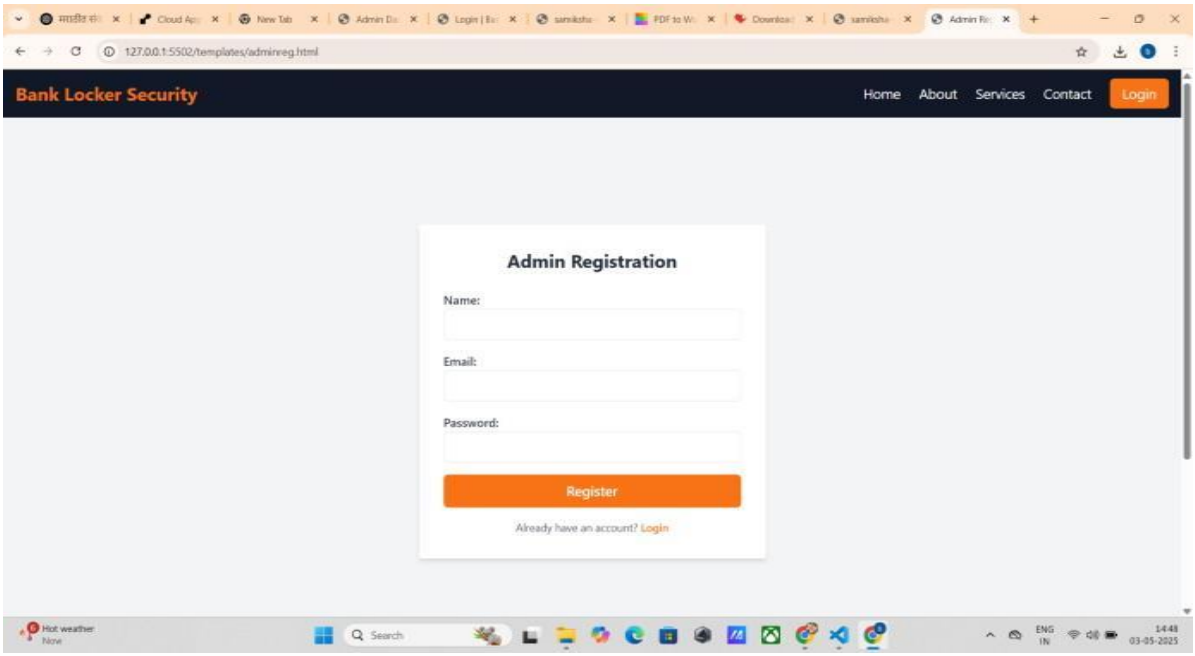
ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VI, June 2025

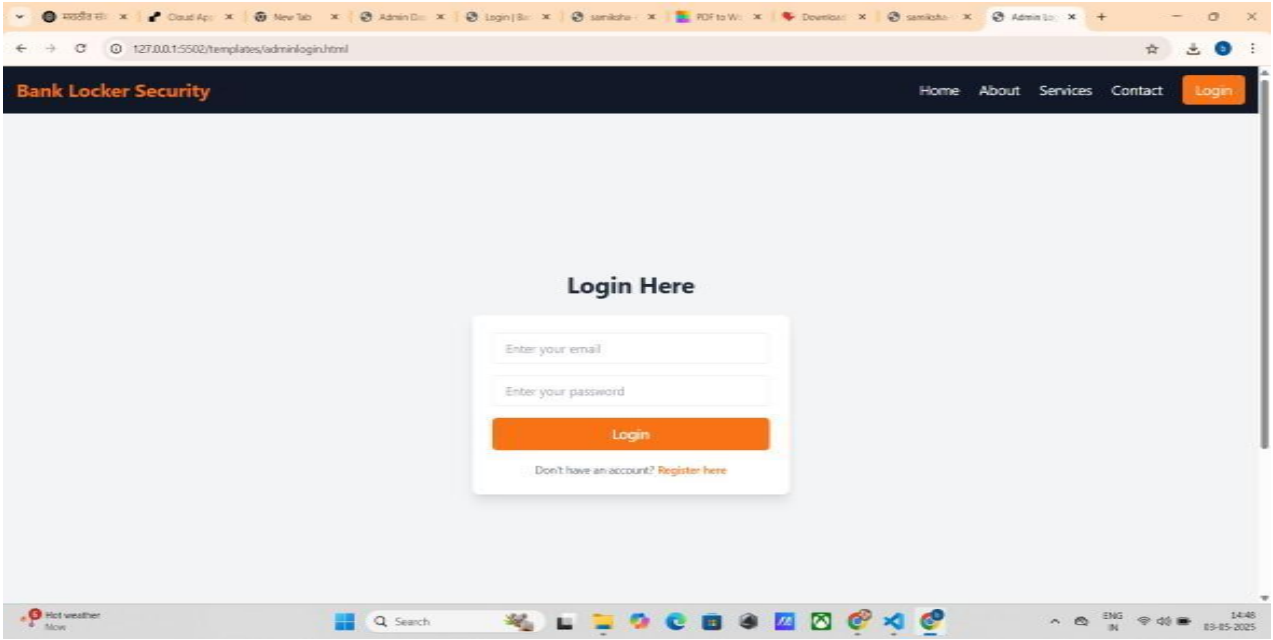
Overview

The Bank Locker Security System is designed to enhance the traditional locker access process by integrating advanced security technologies into a single, cohesive solution. This system introduces a three-layered authentication process—face recognition, OTP verification, and physical key access—to ensure that only verified users can access bank lockers. The core idea behind the system is to combine digital and physical security methods to prevent unauthorized access and potential security breaches.At the user level, the system offers a seamless and secure experience by allowing the customer to verify their identity through AI-powered facial recognition followed by a time-sensitive OTP sent to their registered mobile number. Only after successful digital verification can the user proceed to unlock the locker using a traditional key. This layered approach greatly reduces the chances of impersonation, theft, or unauthorized usage.On the administrative side, the system features a robust dashboard where bank officials can manage locker access, view real-time logs, monitor user activity, and receive alerts in case of suspicious behavior or failed authentication attempts. The use of AI and real-time monitoring also enables predictive analysis and system learning for future security improvements. Overall, this system offers a significant advancement in locker security by blending biometric authentication, digital communication, and physical control mechanisms to deliver a modern, scalable, and highly secure solution for banking institutions.

IV. Result and discussion

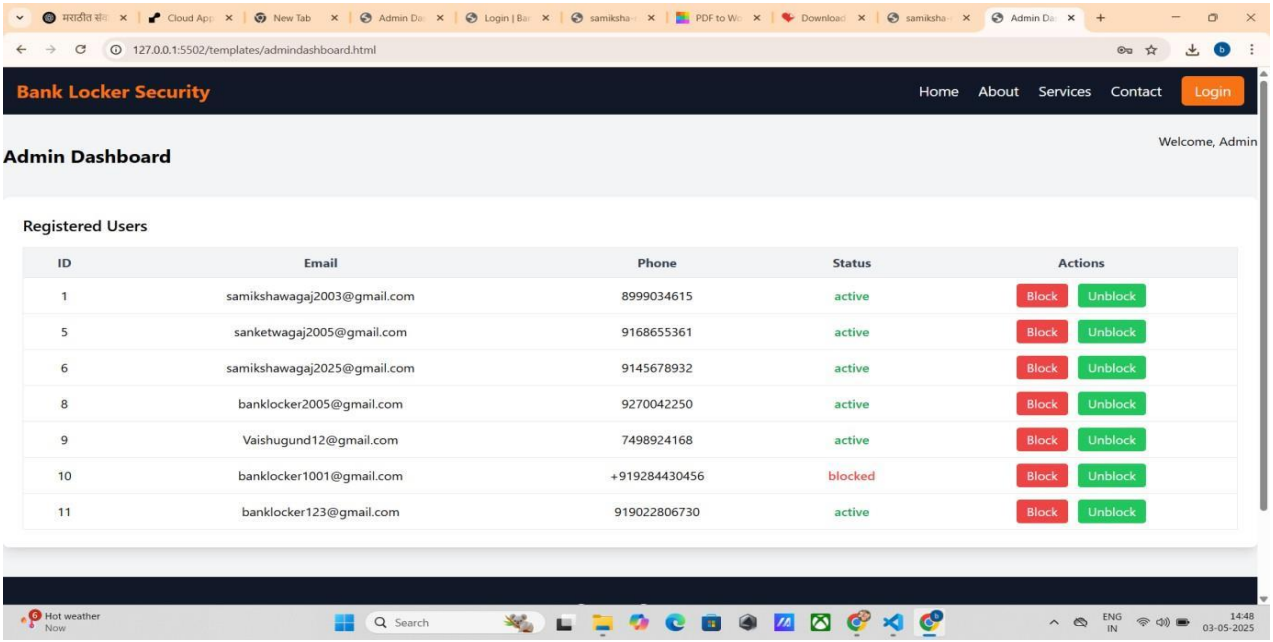
Registration Page and Login Page



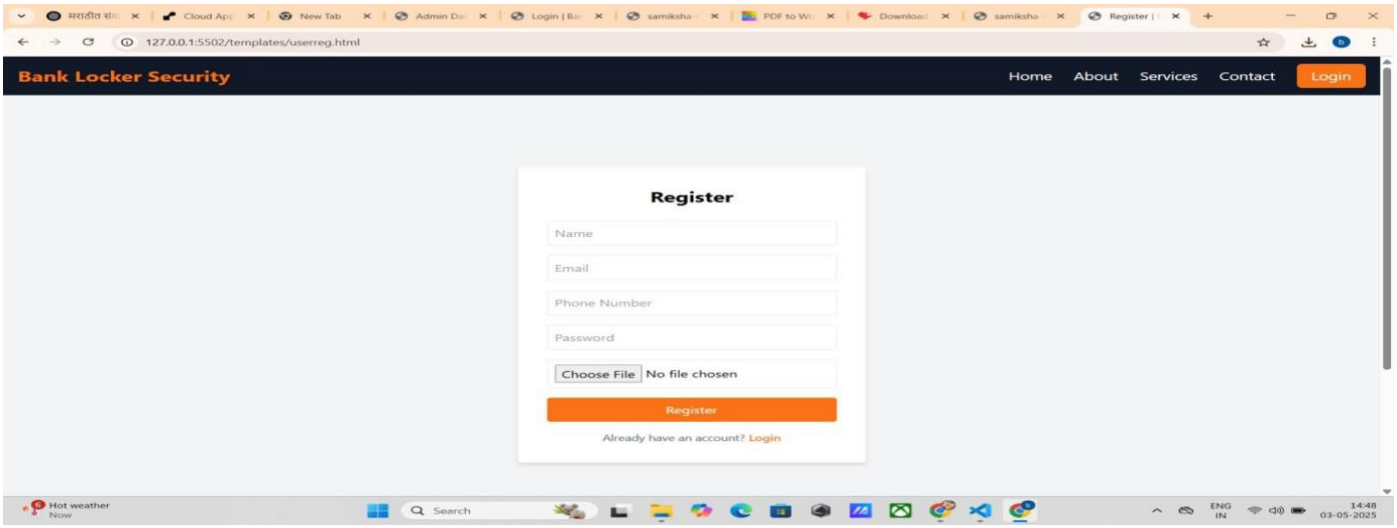


ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VI, June 2025

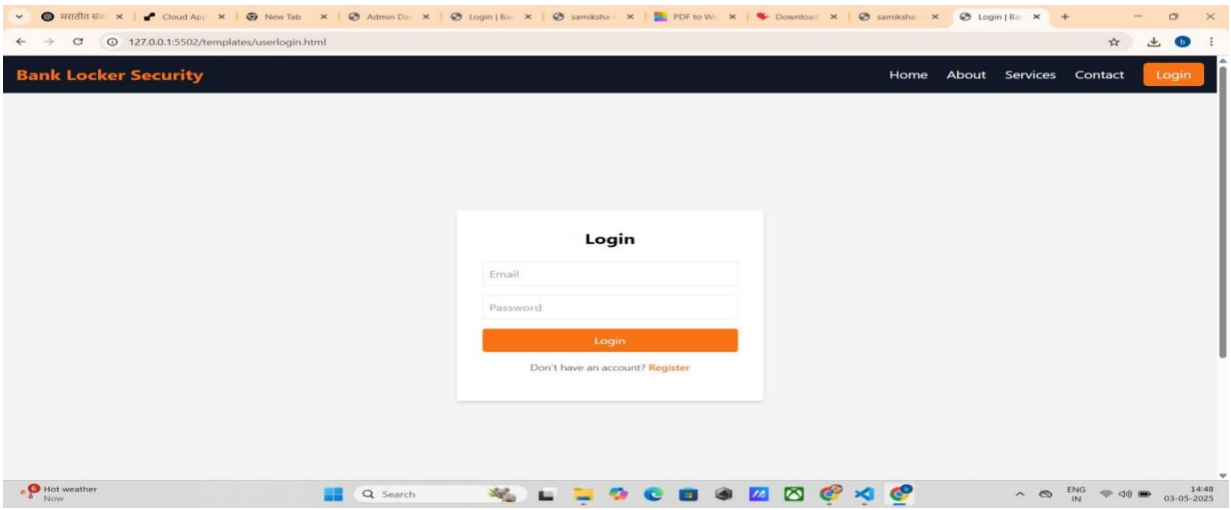
Admin Dashboard



User Register

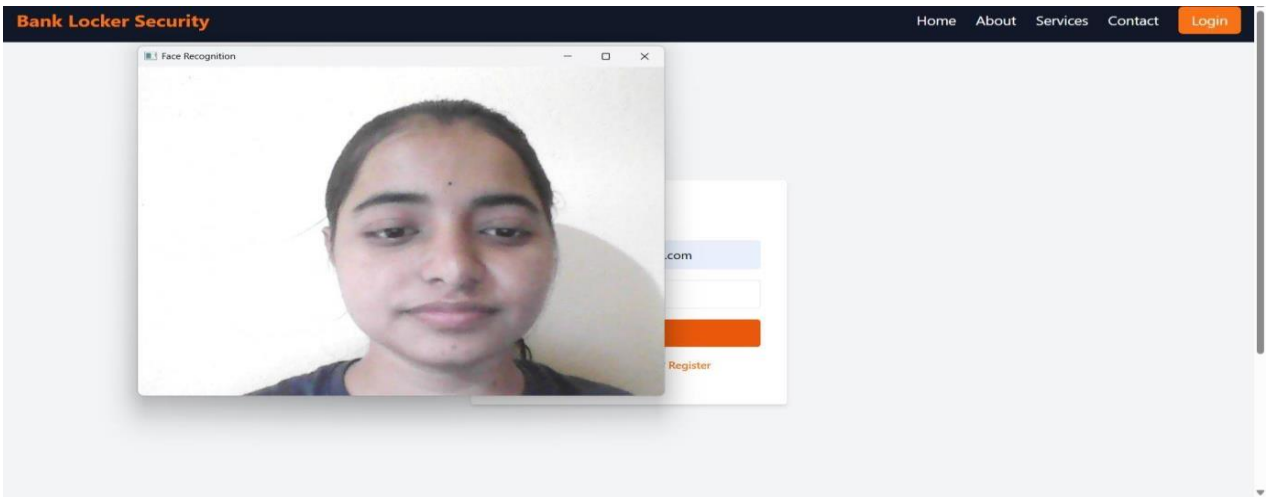


User Login

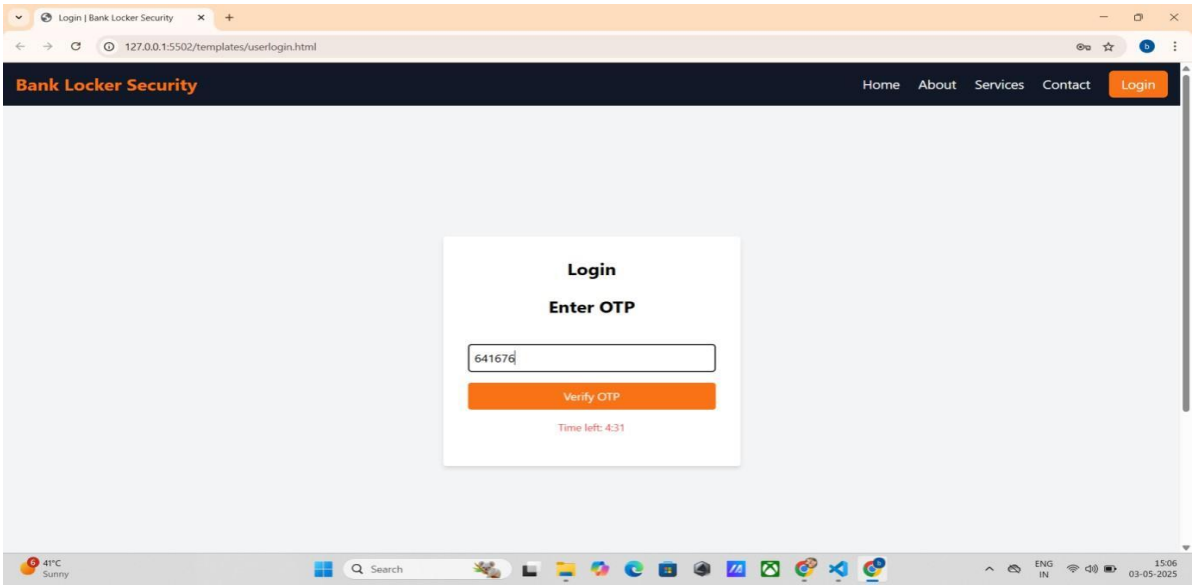


ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VI, June 2025

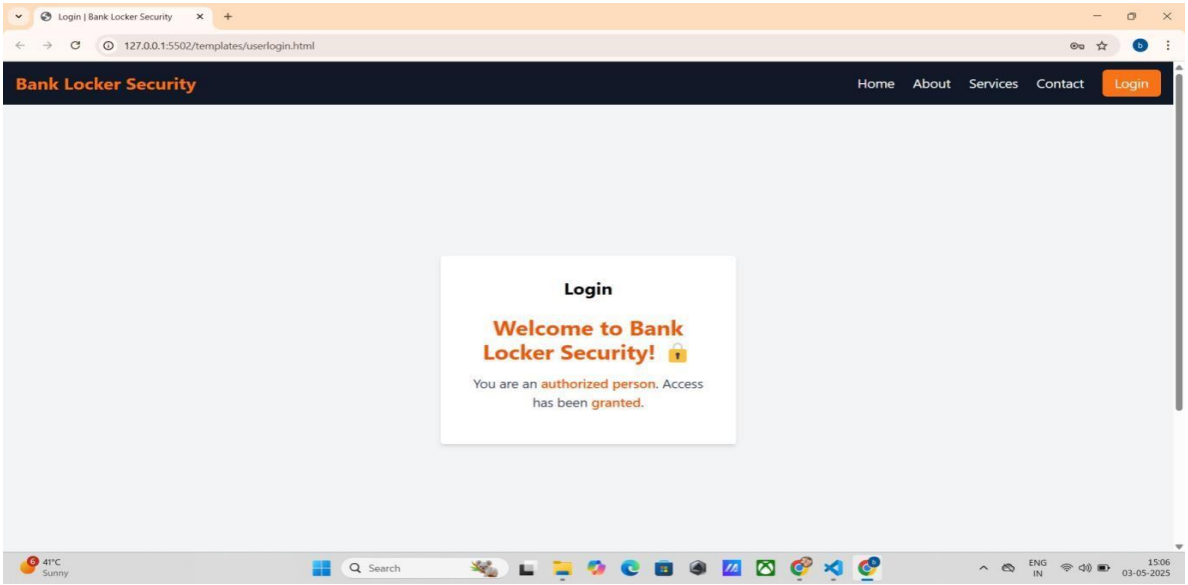
After User Login Then To detecting The Face and and generate the OTP:



Enter the OTP:



To match the OTP, access the locker:



ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VI, June 2025

IV. Conclusion

The proposed Bank Locker Security System integrates face recognition, OTP verification, and physical key validation to create a robust, multi-factor authentication system. This layered approach ensures high security by combining digital and physical methods. The system is developed using Python for face recognition and Node.js for backend API and OTP handling, leveraging built-in libraries and APIs to reduce development time. The modular structure of the system allows easy testing and debugging of each component. With minimal hardware requirements and efficient use of modern tools, this system demonstrates a practical and scalable solution for securing locker access in sensitive environments like banks.

References

1. R. Usain, H. Jain, dan S. Pratap, “Enhancing bank security system using Face Recognition, Iris Scanner and Palm Vein Technology,” 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT- SIU), Bimetal, pp. 1-5, 2018.
2. I. G. P. S. Wijaya, A. Y. Hosoda, and I. W. A. Ari Mbawa, “Real time face recognition based on face descriptor and its application,” Telkom Nika, vol. 16, no. 2, pp. 739–746, April 2018.
3. K. Patel, H. Han, and A. K. Jain, “Secure Face Unlock: Spoof Detection on Smart phones,” IEEE Trans. Inf.
4. Di Wen, Hu Han, and A. K. Jain, “Face Spoof Detection with Image Distortion Analysis,” IEEE Trans. Inf. Forensics Secure., vol. 10, no. 4, pp. 746–761, 2015.
5. Di Wen, Hu Han, and A. K. Jain, “Face Spoof Detection with Image Distortion Analysis,” IEEE Trans. Inf. Forensics Secure., vol. 10, no. 4, pp. 746–761, 2015.