International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 3, 2025

Smart Bank Locker Access with Multi-Factor Authentication

S Revathi, Ananya Mallepally, Deepthi Vaddagani, Navya Kolloju

[1]Assistant Professor, Department of IT Bhoj Reddy Engineering College for Women, India.

[2,3,4]B. Tech Students, Department Of IT, Bhoj Reddy Engineering College For Women, India.

ABSTRACT

Face Locker is an innovative facial recognition-based security system designed to modernize traditional bank locker access methods. In today's digital banking environment, conventional key and PIN-based systems face numerous security challenges and user inconvenience. This project introduces a sophisticated solution that combines facial recognition technology with secure cloud-based authentication to create a more robust and user-friendly locker access system. The system utilizes face-api.js for accurate facial detection and recognition, while Firebase provides secure backend services and user authentication. Face Locker's architecture ensures bank-grade security through encrypted data handling, real-time monitoring, and comprehensive access logging. The implementation of Next.js framework enables a responsive and intuitive user interface, making the system accessible across different devices. By replacing physical keys and PINs with biometric authentication, FaceLocker significantly reduces the risks associated with lost or stolen credentials while streamlining the locker access process. The system maintains detailed information and provides administrative controls for bank staff, ensuring both security and regulatory compliance. This modern approach to locker security represents a significant step forward in banking infrastructure, offering enhanced protection while improving the overall customer experience.

Keywords: *Facial recognition, face-api.js, Firebase, Next.js, secure locker access, cloudbased authentication, real-time monitoring, encrypted data handling, cross-platform user interface.*

1. INTRODUCTION

In recent years, the banking sector has experienced a significant transformation in security systems, driven by technological advancements and increasing security concerns. Traditional bank locker systems, which depend on physical keys and PIN codes, have shown vulnerabilities and often result in operational inefficiencies. Face Locker emerges as a modern solution to these challenges by integrating secure digital authentication and smart locker access management. The main objective behind Face Locker is to overcome the limitations of conventional methods while enhancing both security and user convenience. Utilizing advanced web technologies and a cloud-based backend, the system offers a streamlined, reliable approach to locker access. Technologies like Firebase ensure secure data storage and real-time synchronization, while the use of secure user credentials provides strong authentication. Face Locker's architecture features encrypted data transmission, centralized access control, and all designed to meet the compliance standards of modern banking. This innovative system strengthens locker security by eliminating the risks associated with physical key management and forgotten PINs, while also improving the overall user experience with a simplified, efficient process. Additionally, it supports efficient administrative oversight through real-time monitoring and secure. Through this combination of enhanced digital security, improved user experience, and efficient system management, Face Locker represents a forward- thinking solution for the evolving needs of financial institutions.

Existing System:

Traditional bank locker systems rely on physical keys, PINs, and manual identity checks. Customers must carry keys, remember PINs, and present ID proof, while staff manually verify identities and log entries in physical registers.

This approach presents several issues—lost or stolen keys, PIN theft, slow verification, outdated paper records, no real-time monitoring, and high management costs. As banking evolves, these limitations highlight the need for a more secure, efficient, and tech-driven solution.

Proposed System:

Face Locker is a modern digital locker access system that replaces traditional keys and PINs with secure, cloud-based authentication. It offers real-time identity verification, secure login, and encrypted data handling to ensure safe access management. The system is built on a reliable cloud infrastructure using Firebase for secure data storage, user management, and automated access logging. It supports digital user registration, multi-factor authentication, and role-based access control to enhance security and convenience.

2. RELATED WORK

A biometric locker system integrating facial recognition and fingerprint verification through machine learning techniques has been developed to enhance the security and reliability of access control. The system leverages multiple biometric modalities as part of a multi-factor authentication process, ensuring a more robust defense against unauthorized access[1]. Facial recognition is supported by real-time processing and liveness detection to verify the authenticity of the user, while fingerprint scanning provides an additional verification layer, significantly minimizing the chances of identity spoofing. The use of machine learning algorithms improves accuracy and adaptability in identifying users under varying conditions. Designed for secure physical access, particularly in banking and high-security environments, the system ensures secure data handling and fast, responsive operation. It utilizes a hardware-based authentication mechanism to further strengthen protection against tampering and fraud. The layered security model enables strong user verification by combining advanced biometric analysis with real-time responsiveness. Overall, this approach lays a solid foundation for implementing secure and intelligent locker systems that prioritize both safety and user convenience through a combination of AI-powered facial and fingerprint recognition technologies.

Secure cloud-based authentication and data handling play a crucial role in the architecture of modern applications like Face Locker[2].It enables real-time synchronization and secure login management, enhancing both responsiveness and user experience. The authentication module supports multiple sign-in methods, including email and password, while seamlessly integrating with advanced security models. Customizable security rules and end-to-end encryption ensure that user data remains protected from unauthorized access. This secure and responsive authentication framework aligns well with the objectives of smart bank locker systems, reinforcing system integrity and user trust.

Recent advancements in facial recognition technology have significantly enhanced security measures within the banking sector. Improved image processing techniques, combined with sophisticated machine learning algorithms, have enabled the development of more accurate and dependable authentication systems[4]. These systems now offer better performance even under variable lighting conditions and incorporate advanced spoof detection methods to prevent unauthorized access. Real-time recognition capabilities ensure swift identity verification, aligning seamlessly with the operational demands of banking environments. Furthermore, AI-driven models play a crucial role in minimizing false acceptance and rejection rates, thereby improving the overall reliability of customer authentication. Integration with existing banking infrastructure has also become more efficient, supporting the deployment of seamless and secure access control solutions like those envisioned in modern biometric systems.

3. REQUIREMENT ANALYSIS

Functional Requirements:

- **User Authentication:**
  Supports facial recognition enrollment and verification with user profile and access controls.
- **Security Operations:**
  Performs real-time face detection, biometric processing, access logging, and alerts on unauthorized access.
- **Administrative Functions:**
  Enables user registration, access monitoring, system configuration, and report generation.
- **Data Management:**
  Ensures secure storage of facial templates, maintains access records, and supports backup and recovery.

Non-Functional Requirements:

Performance
The system ensures face recognition in under 3 seconds with high accuracy and supports multiple users simultaneously without performance issues.

Security
The system ensures encrypted data transmission and secure biometric storage with strict access controls. Regular security audits help address vulnerabilities, maintaining compliance with banking regulations and standards.

Usability
The system features an intuitive, mobile-responsive interface for easy access across devices. Its simple design requires minimal user training and enables quick verification for efficient access.

Reliability
The system runs 24/7 with automatic recovery from failures, regular data backups, and strong error handling to ensure continuous, smooth, and reliable operation.

4. DESIGN

System Architecture:

The system architecture of the Face Locker application is designed as a modular, cloud- enabled facial recognition system for secure bank locker access. The architecture begins with the user, who interacts through a frontend interface built using Next.js. The user can perform registration, OTP entry, facial image upload, and locker access requests via this interface. Upon registration, an OTP is generated and sent to the user’s email through an integrated email server. The frontend triggers facial scan operations and communicates with the backend, which is developed using TypeScript. The backend handles core business logic including OTP verification, face-api.js invocation for facial matching and intruder detection, database handling, and locker access signaling. The facial recognition process uses the face-api.js library to match the user’s live scan with the images stored during registration. All user data, OTPs, and facial images are securely stored in the Firebase Realtime Database. If the face matches the enrolled template, the backend sends a signal to unlock the locker. In case of an unrecognized user, the system captures the intruder’s image and sends an alert with the image to the registered user’s email using the email server.

This architecture ensures real-time verification, secure data transmission, and automated alert mechanisms, making it suitable for sensitive environments like banking systems.

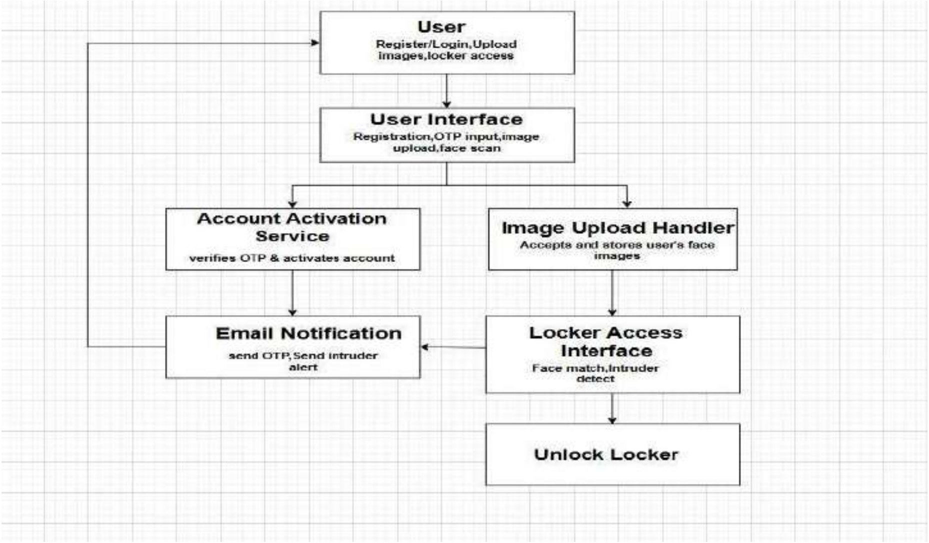

User
Register/Login,Upload images,locker access
User Interface
Registration,OTP input,image upload,face scan
Account Activation Service
verifies OTP & activates account
Image Upload Handler
Accepts and stores user's face images
Email Notification
send OTP, Send intruder alert
Locker Access Interface
Face match,Intruder detect
Unlock Locker

Fig. 4.1.1 System Architecture

Technical Architecture:

The technical architecture of the FaceLocker system defines a secure, modular, and scalable infrastructure for implementing facial recognition-based bank locker access. The frontend is developed using Next.js with Tailwind CSS to provide a responsive user interface for registration, OTP input, image upload, and access requests. It serves as the primary interaction point for users and triggers facial scanning when locker access is requested. The backend, written in TypeScript, handles all business logic, including OTP verification, communication with the database, and locker control. Facial recognition is powered by face-api.js, integrated into the backend to perform face detection, matching, and intruder identification. All user data—including personal information, uploaded facial images are stored securely in Firebase Realtime Database. Firebase also supports authentication, real-time syncing, and backup functionality. The backend communicates with an email server to send OTPs during registration and real-time alerts with intruder images if unauthorized access is attempted. This architecture ensures secure client-server communication, fast facial verification, robust data handling, and automated alerting, making it suitable for real-world deployment in banking environments that demand high reliability and security.

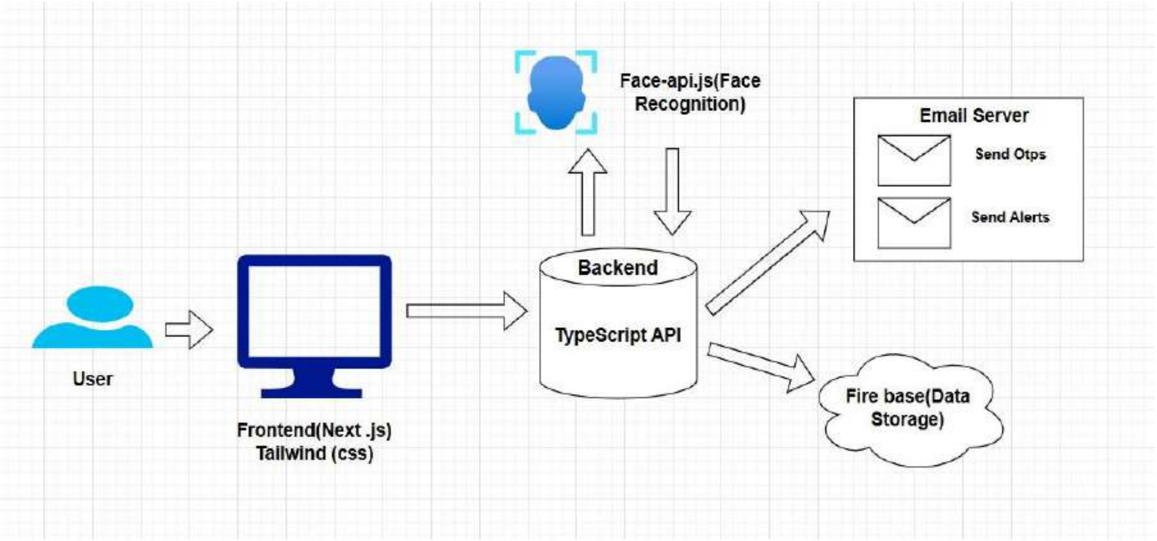


Fig. 4.1.2 Technical Architecture

5. IMPLEMENTATION

The implementation of the Face Locker system comprises multiple interconnected software components built using modern web technologies and advanced AI-powered facial recognition tools. Designed with a modular architecture, the system emphasizes scalability, maintainability, and seamless integration with cloud services and external APIs. Operating entirely within the software domain, Face Locker requires no additional hardware, enabling flexible deployment across various platforms. Below is a detailed breakdown of the system's core modules and their implementation.

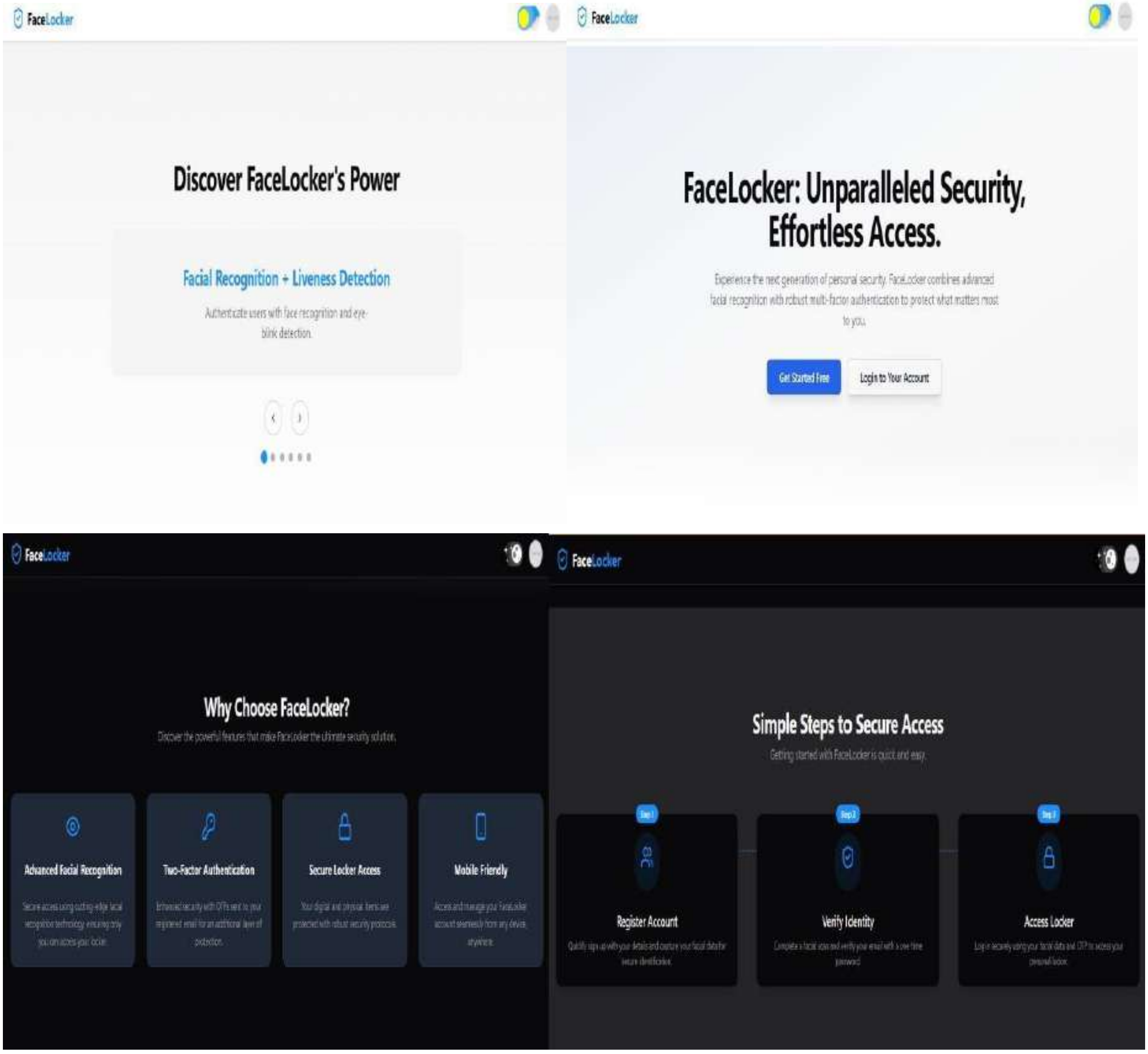
1. Frontend Implementation:

- The frontend of the Face Locker application is developed using Next.js, TypeScript, and TailwindCSS, bundled with Vite to enable fast development cycles and optimized production builds.
- The user interface features interactive components for seamless user authentication, real-time face capture and verification, administrative controls, and live monitoring dashboards.
- React-powered elements ensure smooth user experience with real-time updates and responsive design across devices.
- Visualizations for access history and system alerts are integrated to provide clear and actionable insights to users and administrators.

2. Backend Architecture and Security Integration

- The backend of Face Locker is powered by Firebase, managing user authentication, real-time database operations, and secure storage of biometric data.
- Firebase Cloud Functions provide serverless execution of security workflows, including face recognition triggers, access validation, and alert generation.
- API integrations handle communication between frontend components and backend services, orchestrating biometric processing and access control logic.

6. Screenshots



FaceLocker
Discover FaceLocker's Power
Facial Recognition + Liveness Detection
FaceLocker
FaceLocker: Unparalleled Security, Effortless Access.
Get Started Free
Login to Your Account
FaceLocker
Why Choose FaceLocker?
Advanced Facial Recognition
Two-Factor Authentication
Secure Locker Access
Mobile Friendly
FaceLocker
Simple Steps to Secure Access
Step 1
Register Account
Step 2
Verify Identity
Step 3
Access Locker

Authenticate users with face recognition and eye-blink detection.

Experience the next generation of personal security. FaceLocker combines advanced facial recognition with robust multi-factor authentication to protect what matters most to you.

Discover the powerful features that make FaceLocker the ultimate security solution.

Secure access using cutting-edge facial recognition technology, ensuring only you can access your locker.

Enhanced security with OTPs sent to your registered email for an additional layer of protection.

Your digital and physical items are protected with robust security protocols.

Access and manage your FaceLocker account seamlessly from any device, anywhere.

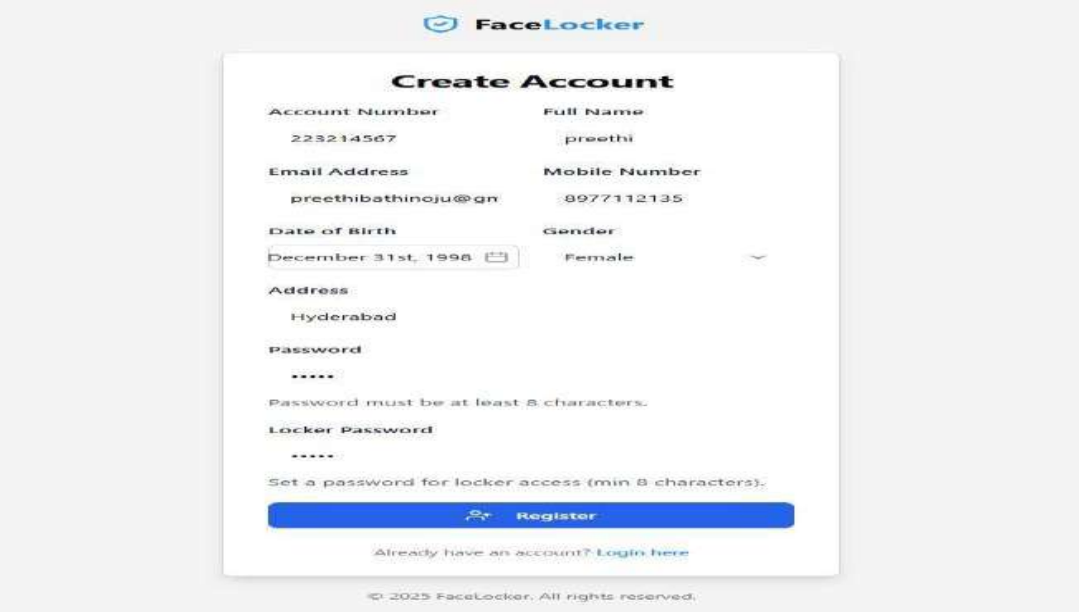
Getting started with FaceLocker is quick and easy.

Quickly sign up with your details and capture your facial data for secure identification.

Complete a facial scan and verify your email with a one-time password.

Log in securely using your facial data and OTP to access your personal locker.

Screenshot 6.1 From Signup to Secure Access – Here's How FaceLocker Works



FaceLocker

Create Account

Account Number
223214567

Full Name
preethi

Email Address
preethibathinoju@gn

Mobile Number
8977112135

Date of Birth
December 31st, 1998

Gender
Female

Address
Hyderabad

Password
•••••

Password must be at least 8 characters.

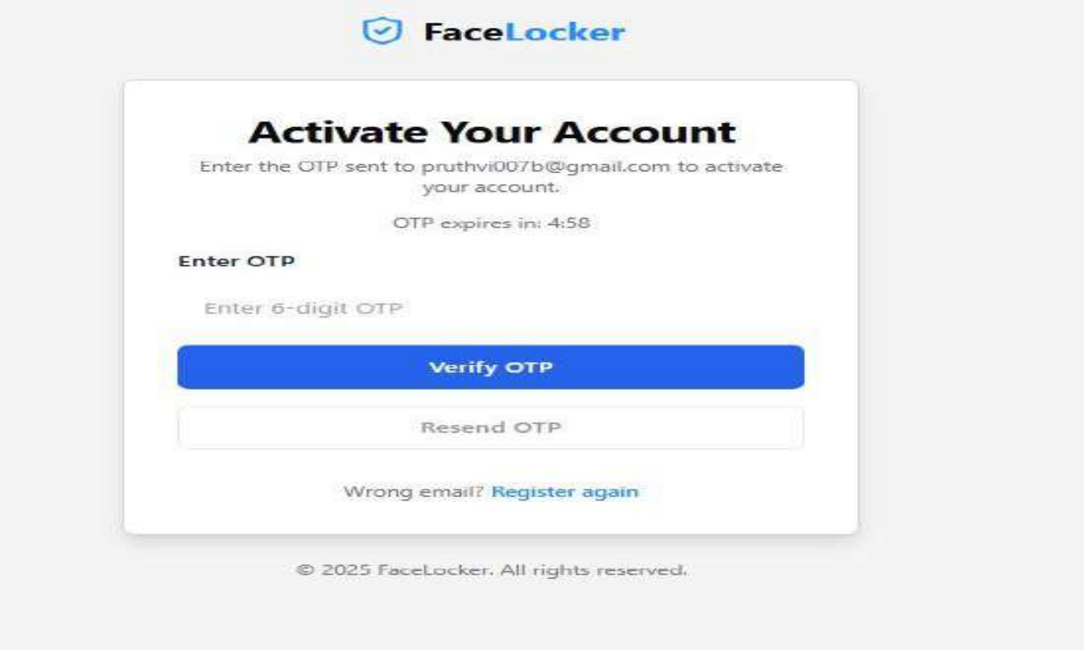
Locker Password
•••••

Set a password for locker access (min 8 characters).

Already have an account? Login here

© 2025 FaceLocker. All rights reserved.

Screenshot 6.2 User Registration Interface for Secure Access



FaceLocker

Activate Your Account

Enter the OTP sent to pruthvi007b@gmail.com to activate your account.

OTP expires in: 4:58

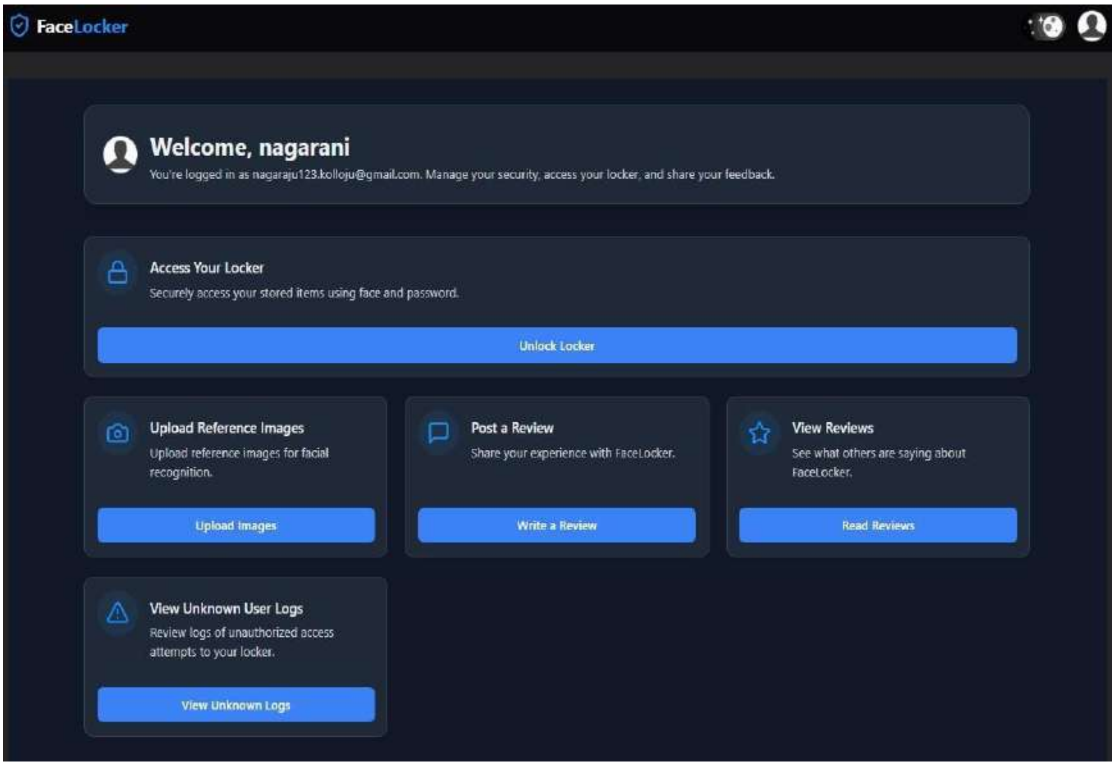
Enter OTP
Enter 6-digit OTP

Wrong email? Register again

© 2025 FaceLocker. All rights reserved.

Screenshot 6.3 OTP Verification Page for Safe User Activation

- Page 33



Welcome, nagarani

You're logged in as nagaraju123.kolloju@gmail.com. Manage your security, access your locker, and share your feedback.

Access Your Locker

Securely access your stored items using face and password.

Upload Reference Images

Upload reference images for facial recognition.

Post a Review

Share your experience with FaceLocker.

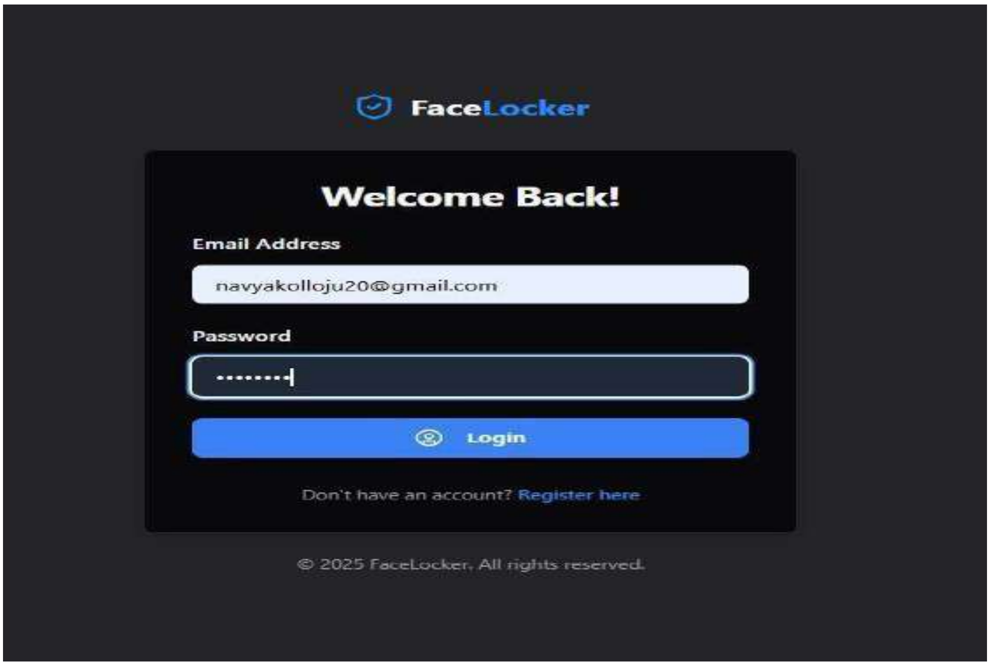
View Reviews

See what others are saying about FaceLocker.

View Unknown User Logs

Review logs of unauthorized access attempts to your locker.

Screenshot 6.4 Dashboard Interface



Welcome Back!

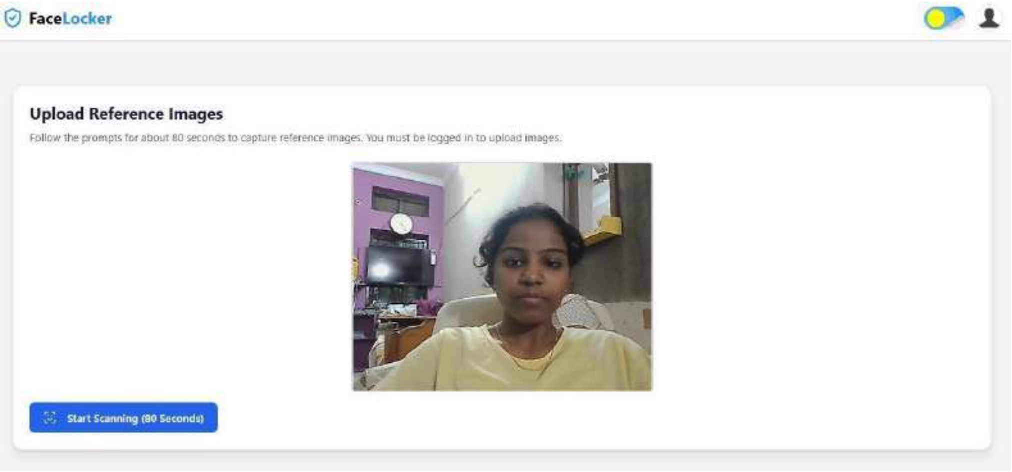
Email Address: navyakolloju20@gmail.com

Password: ••••••••

Don't have an account? Register here

© 2025 FaceLocker. All rights reserved.

Screenshot 6.5 Login Portal – Authenticate to Access Locker Dashboard

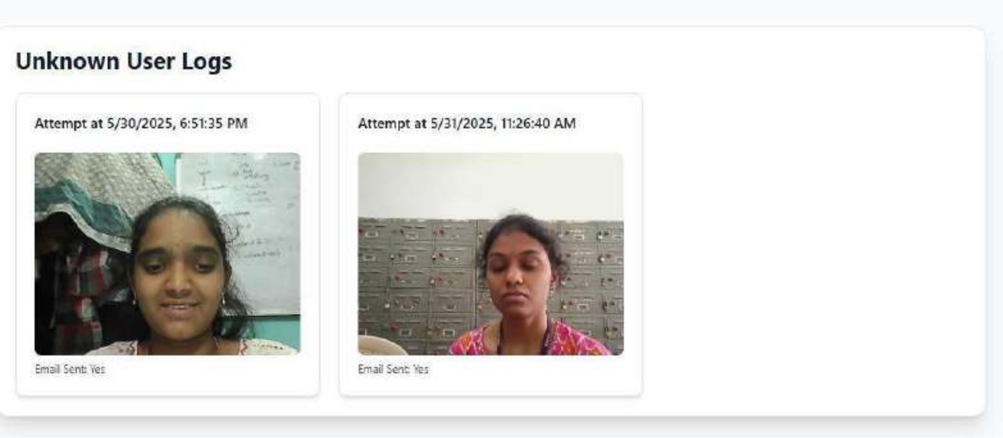


FaceLocker

Upload Reference Images

Follow the prompts for about 80 seconds to capture reference images. You must be logged in to upload images.

Screenshot 6.6 Reference Image Upload Interface



Unknown User Logs

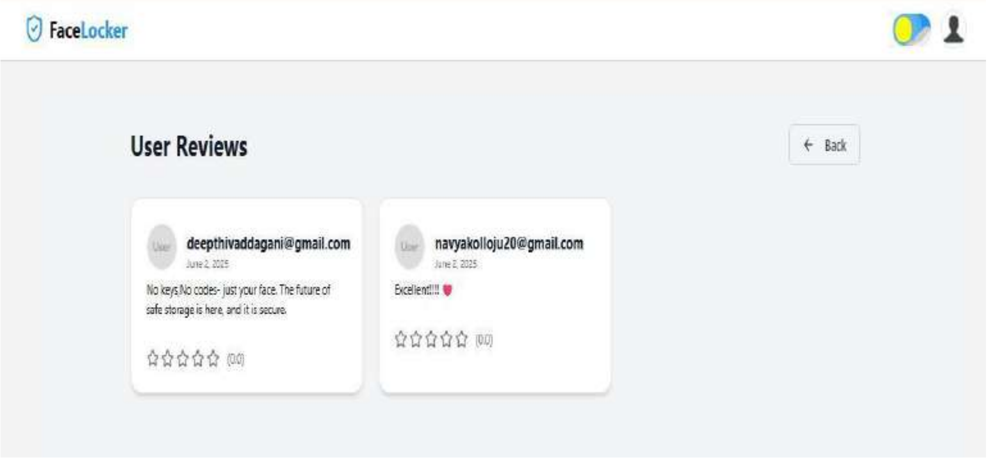
Attempt at 5/30/2025, 6:51:35 PM

Email Sent: Yes

Attempt at 5/31/2025, 11:26:40 AM

Email Sent: Yes

Screenshot 6.7 Intruder Detection – Logs of Unrecognized Face



FaceLocker

User Reviews

deepthivaddagani@gmail.com
June 2, 2025

No keys.No codes- just your face. The future of safe storage is here, and it is secure.

☆☆☆☆☆ (0.0)

navyakolloju20@gmail.com
June 2, 2025

Excellent!!! ♥

☆☆☆☆☆ (0.0)

Screenshot 6.8 Displaying Customer Feedback and Ratings

7-CONCLUSION

The Face Locker project represents a significant leap forward in banking security by replacing conventional locker systems with an advanced, facial recognition-based access solution that emphasizes both security and user convenience. Built using Next.js for a dynamic and responsive frontend, TensorFlow.js for real-time facial detection and liveness validation directly in the browser, and Firebase for robust, cloud-based backend operations, the system eliminates the dependency on physical keys, PINs, or manual verification. By performing biometric authentication entirely on the client side, Face Locker not only enhances speed and user privacy but also provides strong resistance to threats such as identity theft, key duplication, spoofing attacks, and unauthorized access. The platform offers an intuitive and user-friendly interface, enabling seamless operation for both users and administrators. Real-time alerts, encrypted data transmission, and comprehensive audit logs ensure complete transparency and traceability of locker access. Additional features such as secure session management, role-based access control, and compliance with industrystandard data protection protocols bolster the system's security posture. Its modular, maintainable, and scalable architecture is designed to accommodate future upgrades, including multi-modal biometric authentication and AI-driven anomaly detection. Face Locker thus delivers a forward-thinking, reliable, and secure solution that aligns with the evolving needs of modern banking infrastructure and biometric access control systems.

REFERENCES

[1] Baikerikar, J., D'souza, A. A., Patil, K., Sekar, V., Jadhav, A., and Naik, S. (2024). Machine Learning based Facial Recognition and Finger Print Identification for Secure
Locker Access. In Proceedings of the 2024 IEEE 9th International Conference for for ConvergenceinTechnology(I2CT),Pune,India..https://doi.org/10.1109/I2CT61223.2024.10 544254

[2] Firebase Documentation. (2024). Security & Authentication. Retrieved June 1, 2025, from https://firebase.google.com/docs/security

[3] Next.js Documentation. (2024). Next.js Official Documentation. Retrieved June 1, 2025, from https://nextjs.org/docs

[4] Smith, J., & Kumar, R. (2023). Advances in facial recognition for banking security. International Journal of Banking Technology, 15(2), 45–58.

[5] ISO/IEC 27001:2022. (2022). Information Security Management Systems.

[6] National Institute of Standards and Technology (NIST). (2017). Digital Identity Guidelines (Special Publication 800-63-3) https://doi.org/10.6028/NIST.SP.800-63-3

[7] PCI Security Standards Council. (2024). Payment Card Industry Data Security Standard v4.0. Retrieved June 1, 2025, from https://www.pcisecuritystandards.org/