Biometric Payment System with Two-Step Verification

Using Secure Authentication and Backend Intelligence

"NO PHONE. NO CARD. NO CASH. ONLY YOU."

Abstract

The rapid growth of digital payment systems has increased the demand for secure, fast, and user-friendly authentication mechanisms. Traditional payment methods relying on cards, mobiles, or some type of electronic gadget, are vulnerable to theft, duplication, and misuse. This project presents a **Biometric Payment System with Two-Step Verification**, combining fingerprint authentication and PIN verification to ensure enhanced security. The system is designed to operate across multiple environments such as ATMs, vending machines, grocery stores, shopping malls, and college canteens etc. A centralized backend using Spring Boot and a secure database enables real-time verification, transaction processing, and account management.

Introduction

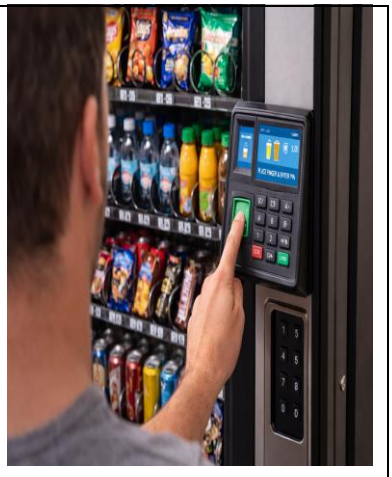
Digital payment systems have transformed financial transactions by offering convenience and speed. However, security remains a critical challenge due to increasing cyber threats and identity fraud. Biometric authentication has emerged as a reliable solution because biometric traits are unique, difficult to replicate, and permanently associated with an individual.

This project focuses on integrating **fingerprint-based biometric authentication** with a **secondary PIN verification step**, creating a robust two-layer security mechanism. By eliminating the need for physical cards and **reducing dependency on mobile phones**, the system enhances trust and usability in real-world payment scenarios.

Concept of Two-Step Biometric Verification

The proposed system follows a **two-step verification model**:

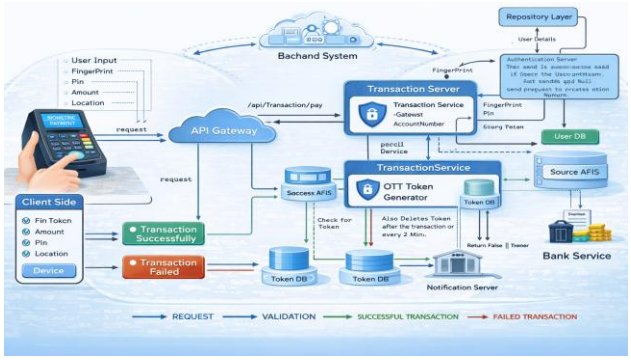
1. **Biometric Verification (Fingerprint)-** The user places their finger on the biometric sensor. The captured fingerprint is securely processed and matched against encrypted biometric data stored in the database.



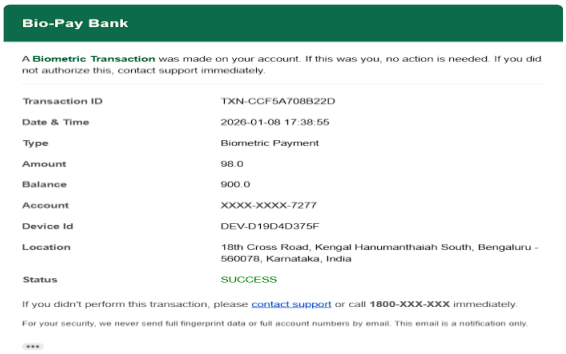
2. **PIN Verification-** After successful fingerprint matching, the user enters a personal identification number (PIN) to confirm the transaction.

This layered approach ensures that even if one factor is compromised, unauthorized access is prevented. The system aligns with modern authentication principles that combine something the user is (biometric) with something the user knows (PIN).

Working Principle



1. The user initiates a payment at the biometric terminal.
2. The fingerprint is scanned and converted into a secure digital template.
3. The backend system verifies the fingerprint against stored records.
4. Upon successful biometric authentication, the system prompts for PIN entry.
5. If both steps are verified, OTT token is generated for the associated account number and request the bank service for verifying the token and proceeding with the transaction.
6. If token is verified and balance>=debit amount transaction will be successful or else failed.
7. The user receives confirmation of payment completion or failure along with the LOCATION of the payment.



Bio-Pay Bank

A **Biometric Transaction** was made on your account. If this was you, no action is needed. If you did not authorize this, contact support immediately.

Transaction ID	TXN-CCF5A708B22D
Date & Time	2026-01-08 17:38:55
Type	Biometric Payment
Amount	98.0
Balance	900.0
Account	XXXX-XXXX-7277
Device Id	DEV-D19D4D375F
Location	18th Cross Road, Kengal Hanumanthaiah South, Bengaluru - 560078, Karnataka, India
Status	SUCCESS

If you didn't perform this transaction, please contact support or call **1800-XXX-XXX** immediately.

For your security, we never send full fingerprint data or full account numbers by email. This email is a notification only.

Applications

The proposed biometric payment system can be deployed in multiple real-world environments:

- **ATMs** – Cardless cash withdrawal and secure account access.
- **Vending Machines** – Quick and cashless purchases.
- **Grocery Stores** – Faster checkout without cards, cash or mobile phones.
- **Shopping Malls** – Secure retail payments.
- **College Canteens** – Student-friendly, wallet-free, phone-free, card-free transactions.

Its versatility makes it suitable for both commercial and institutional use.

Benefits and Advantages

- Enhanced security through two-step authentication.
- Eliminates the need for physical cards, cash and smart phone.
- Reduces fraud and identity theft.
- Fast and user-friendly transaction process.
- Scalable architecture for future expansion.

Limitations and Challenges

Despite its advantages, the system faces certain challenges:

- Initial cost of biometric hardware deployment.
- Privacy concerns related to biometric data storage.
- Dependence on sensor accuracy and environmental conditions.
- Requirement of strong encryption and secure backend management.

Proper data protection policies and secure implementation practices are essential to address these challenges.

Mithun Y

1CE22IS030

ISE 7th SEM

City Engineering College

https://github.com/mithun-y/FinalYearProject