

A Field Project Report on  
**Fingerprint Based ATM**

Submitted

*In partial fulfillment of the requirements for the award of the degree*

**BACHELOR OF TECHNOLOGY**

In

**COMPUTER SCIENCE and ENGINEERING**

By

K Rajesh	(231fa04023)
G Sri Vardhan	(231fa04523)
K Joshmajoy	(231fa04525)
P Vishnu Vardhan	(231fa04529)

Under the Guidance of

**Mr.G.Murali**

Assistant Professor, CSE



**VIGNAN'S**

FOUNDATION FOR SCIENCE, TECHNOLOGY & RESEARCH

(Deemed to be University) - Estd. u/s 3 of UGC Act 1956

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**

**SCHOOL OF COMPUTING AND INFORMATICS**

**VIGNAN'S FOUNDATION FOR SCIENCE, TECHNOLOGY & RESEARCH**

(Deemed to be University)

Vadlamudi, Guntur -522213, INDIA.

April, 2025



# VIGNAN'S

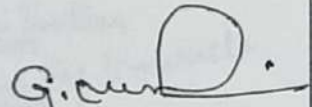
FOUNDATION FOR SCIENCE, TECHNOLOGY & RESEARCH

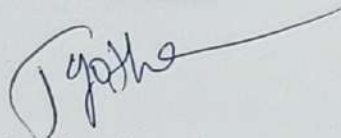
(Deemed to be University) - Estd. u/s 3 of UGC Act 1956

## CERTIFICATE

This is to certify that the field project entitled "FINGER PRINT BASED ATM" is being submitted by K Rajesh [231fa04023], G Sri Vardhan [231fa04523], K JoshmaJoy [231fa04525] and P Vishnu Vardhan [231fa04529] in partial fulfilment of the requirements for the degree of **Bachelor of Technology (B.Tech.) in Computer Science and Engineering** at Vignan's Foundation for Science, Technology and Research (Deemed to be University), Vadlamudi, Guntur District, Andhra Pradesh, India.

This is a bonafide work carried out by the aforementioned students under my guidance and supervision.

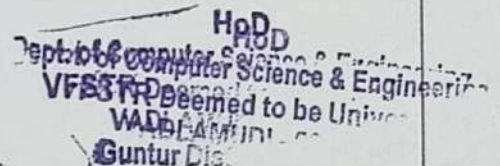
  
Guide



Project Review Committee



HoD, CSE

  
HoD  
Dept. of Computer Science & Engineering  
VFSFR Deemed to be University  
Vadlamudi  
Guntur Dist.



# VIGNAN'S

FOUNDATION FOR SCIENCE, TECHNOLOGY & RESEARCH

(Deemed to be University) · Estd. u/s 3 of UGC Act 1956

## DECLARATION

Date: 10-04-2025

We hereby declare that the work presented in the field project titled "FINGER PRINT BASED ATM" is the result of our own efforts and investigations.

This project is being submitted under the supervision of Mr . G . Murali, Assistant Professor in partial fulfillment of the requirements for the Bachelor of Technology (B.Tech.) degree in Computer Science and Engineering at Vignan's Foundation for Science, Technology and Research (Deemed to be University), Vadlamudi, Guntur, Andhra Pradesh, India.

K Rajesh (231FA04023)

*Rajesh K*  
Signature

G Sri Vardhan (231FA04523)

*G Sri Vardhan*  
Signature

K Joshmajoy (231FA04525)

*K Joshmajoy Kalimela*  
Signature

P Vishnu (231FA04529)

*P Vishnu*  
Signature

## TABLE OF CONTENTS

Chapter No.		Contents	Page No
1		Introduction	1
	1.1	Problem Definition	1
	1.2	Existing System	1
	1.3	Proposed System	1
	1.4	Literature Review	2
2		System Requirements	2
	2.1	Hardware & Software Requirements	2
	2.2	Software Requirements Specification(SRS)	3
3		System Design	3
	3.1	Modules of System	3
	3.2	UML Diagrams	4-6
4		Implementation	6
	4.1	Sample Code	7
	4.2	Test Cases	8
5		Results	8
	5.1	Output Screens	8-10
6		Conclusion	10
		References	11

# Fingerprint-Based ATM System Documentation

## 1. Introduction

**Fingerprint-based Automated Teller Machines (ATMs)** represent an evolution in user authentication for financial transactions. Leveraging biometric fingerprint recognition technology, these systems enhance security protocols by verifying user identity through the unique physiological characteristics of an individual's fingerprint. Upon initial enrollment, a user's fingerprint is digitally captured and securely stored as a template within the financial institution's database. Subsequent ATM access necessitates the user placing their finger on an integrated scanner. The system then performs a comparative analysis between the live scan and the stored template. Successful biometric matching authenticates the user, granting access to transactional functionalities. This modality mitigates vulnerabilities associated with traditional card-based systems, such as card skimming, PIN compromise, and unauthorized usage, thereby fostering a more secure and efficient banking environment. Furthermore, the elimination of physical cards and memorized PINs offers enhanced user convenience and accessibility..

### 1.1. Problem Definition

The prevalent reliance on traditional ATM authentication methods, predicated on magnetic stripe cards and Personal Identification Numbers (PINs), presents inherent security vulnerabilities and limitations in user convenience. These include susceptibility to card fraud (e.g., skimming, cloning), PIN compromise (e.g., shoulder surfing, data breaches), and the logistical burden of physical card management and PIN memorization for users. Furthermore, these methods may pose accessibility challenges for individuals with certain cognitive or physical impairments. Consequently, there exists a need for a more robust, secure, and user-centric authentication mechanism for ATM transactions that mitigates these existing risks and enhances the overall user experience.

### 1.2. Existing System

In the current ATM systems:

- Users **insert an ATM card** and enter a **PIN** to authenticate.
- **Security vulnerabilities** include PIN theft, card skimming, and shoulder surfing.
- Fraudulent activities like **card cloning** and **phishing attacks** are common.
- Customers often **forget their PINs**, causing inconvenience.

### 1.3. Proposed System

The **Fingerprint-Based ATM System** offers a **biometric authentication method**, which is:

- **More secure** since fingerprints are unique to each individual.
- **Convenient**, eliminating the need to remember passwords or PINs.
- **Prevents unauthorized access** because fingerprints cannot be stolen like PINs.
- **Enhances user experience** by reducing authentication time.



## 1.4. Literature Review

Several studies suggest that biometric authentication:

- **Reduces fraud and identity theft** in banking transactions.
- **Improves accessibility** for users who struggle with PIN-based authentication.
- **Has been implemented successfully** in modern banking security systems.

Biometric authentication is already used in smartphones, border security, and law enforcement, demonstrating its **effectiveness and reliability**.

## 2. System Requirements

- **Software Requirements:**
  - Frontend: **HTML, CSS, JavaScript**
  - Backend (optional for data storage): **Node.js, PHP, MySQL**
- **Functional Requirements:**
  - Authenticate users via **fingerprint scanning simulation**.
  - Allow users to **view account balance, deposit, withdraw, and check transaction history**.
  - Provide a **secure, user-friendly interface**.
- **Non-Functional Requirements:**
  - **Security:** Prevent unauthorized access.
  - **Efficiency:** Fast authentication process.
  - **Usability:** Easy to use for all customers.

### 2.1 Minimum Hardware Requirements:

These are enough to run simple websites and do basic web development.

- **Processor (CPU):** Dual-core processor (e.g., Intel Core i3 or AMD equivalent)
- **RAM:** 4 GB
- **Storage:** 64 GB (SSD preferred but not required)
- **Graphics:** Integrated graphics (Intel HD Graphics or similar)
- **Operating System:** Windows 10, macOS, or a lightweight Linux distro (like Ubuntu or Linux Mint)
- **Display:** 720p resolution
- **Browser:** Latest version of Chrome, Firefox, Edge, or Safari
- **Text Editor/IDE:** Lightweight editors like VS Code, Sublime Text, or Notepad++

## 2.2. Software Requirements Specification (SRS)

- **Functional Requirements:**
  - User places a finger on the scanner for authentication.
  - If fingerprint authentication is successful, the user accesses banking options.
  - Users can **view balance, withdraw money, deposit money, and check transaction history.**
- **User Interface Requirements:**
  - **Scanner animation** for user feedback.
  - **Buttons for account selection and banking transactions.**
  - **Real-time updates** on account balance and transaction history.
- **Performance Requirements:**
  - Fast response for authentication.
  - Smooth transition between different sections of the ATM interface.

## 3. System Design

The system is designed with the following components:

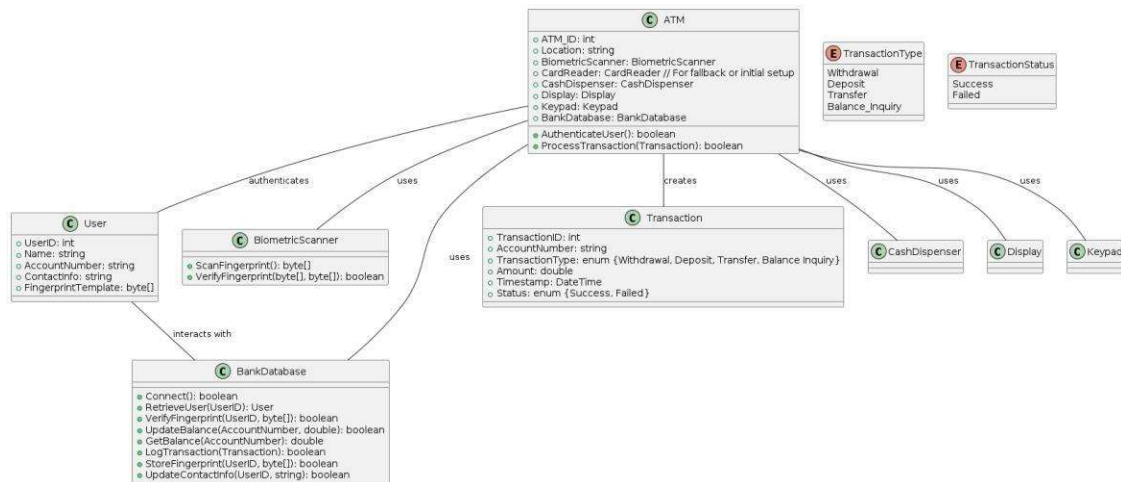
1. **User Interface (UI):**
  - Built using **HTML, CSS, and JavaScript.**
  - Includes a **fingerprint scanner simulation, account selection, and transaction buttons.**
2. **Logic Layer (JavaScript):**
  - Handles **fingerprint authentication.**
  - Manages **account selection and transaction processing.**
3. **Simulated Database (JavaScript Objects):**
  - Stores **account balances and transaction history** for different account types.

### 3.1. Modules of the System

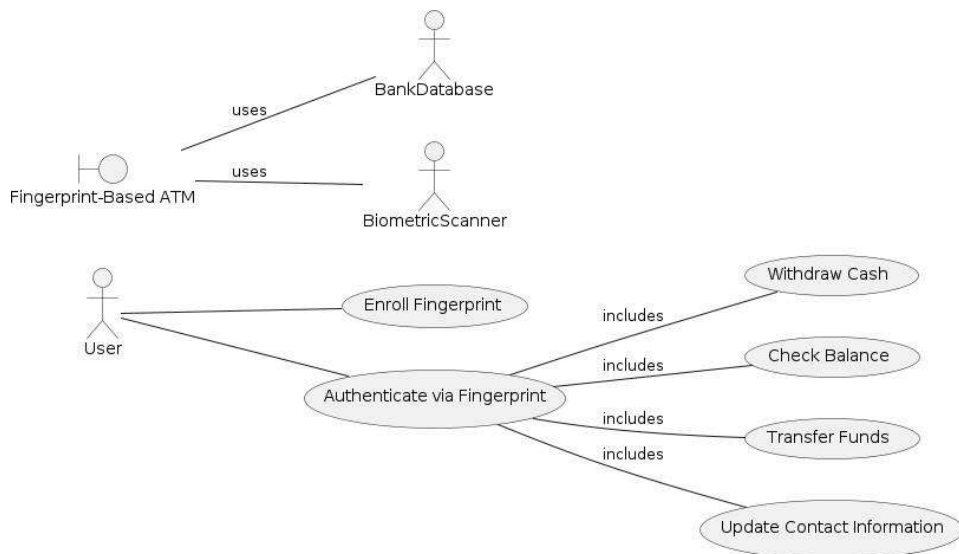
1. **Fingerprint Authentication Module:**
  - Simulates scanning and validating a fingerprint.
  - Displays authentication success or failure messages.
2. **Account Selection Module:**
  - Allows users to choose between **Current, Savings, and Fixed Deposit (FD) accounts.**
3. **ATM Functions Module:**
  - Provides options to **view balance, withdraw, deposit, and check history.**
4. **Transaction History Module:**
  - Stores and displays **user transactions** in a readable format.

## 3.2. UML Diagrams

- **Class Diagram:** Represents different components like User, ATM, and Transactions.

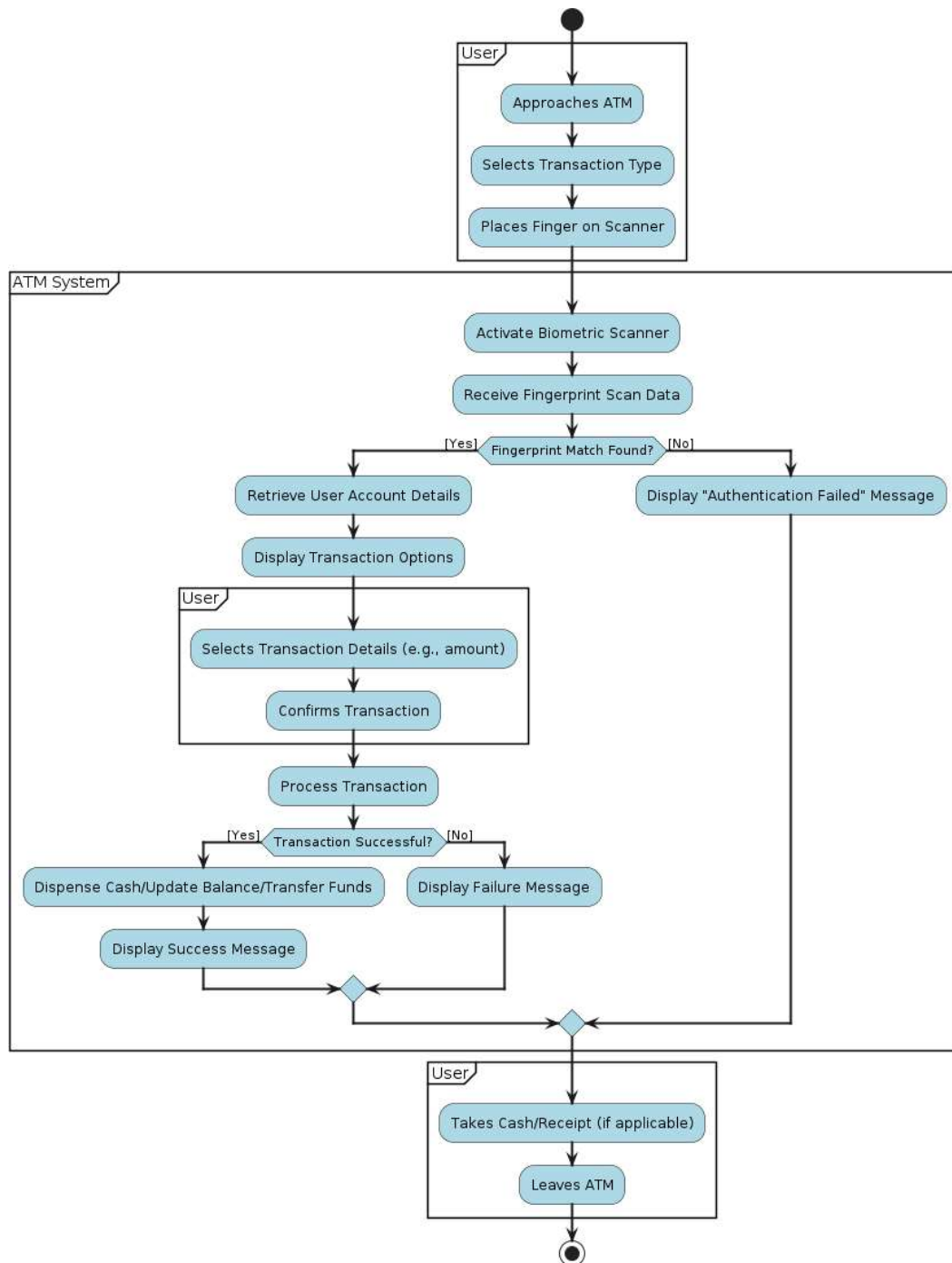


- **Use Case Diagram:** Shows user interactions with the system.

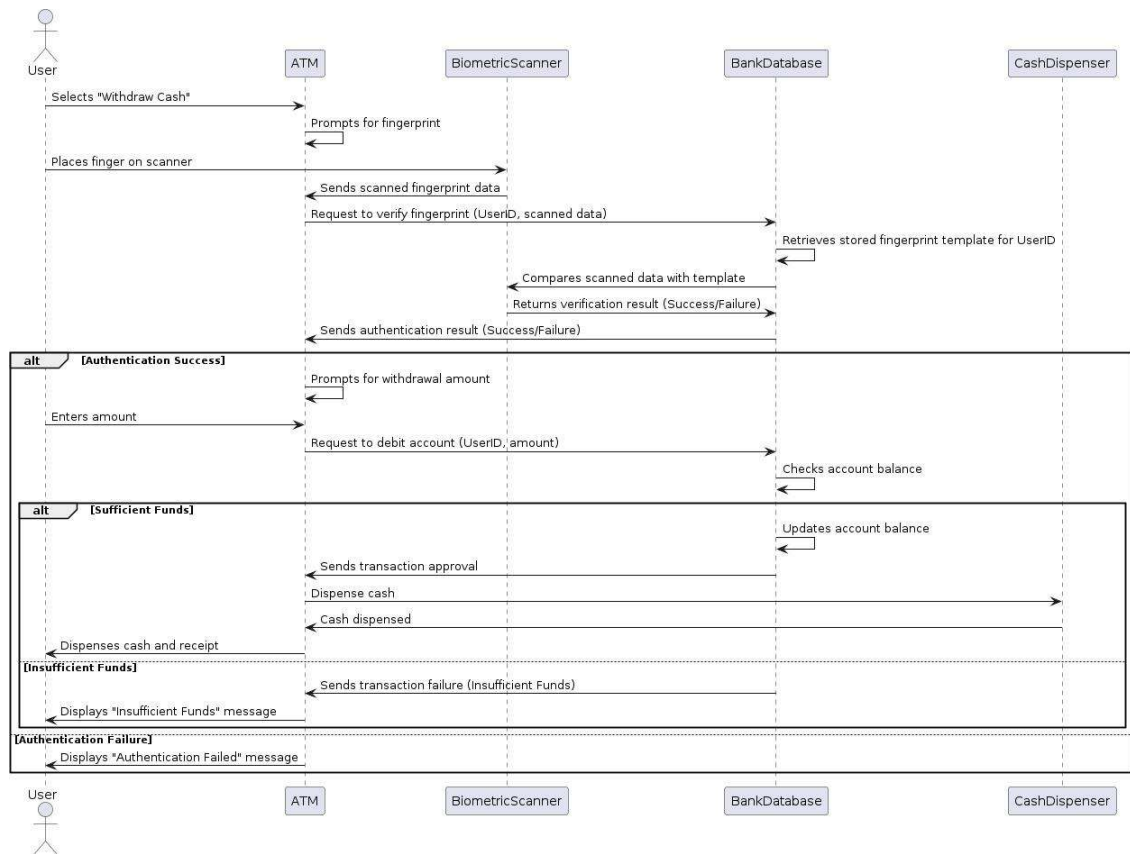




- **Activity Diagram:** Illustrates workflow from **fingerprint scanning** to **transaction confirmation**.



- **Sequence Diagram:** Explains the order of interactions, from authentication to transaction completion.



## 4. Implementation

- The system is implemented using **pure HTML, CSS, and JavaScript**.
- JavaScript handles authentication and account transactions.
- The fingerprint scanner is **simulated using a button with a scanning animation**.
- JavaScript objects **store user account details and transaction history**.

## 4.1. Sample Code

```
<html><body>

  <div class="fingerprint-scanner">

    <div class="scanner" id="scanner"></div>

    <p id="scanner-status">Place your finger on the scanner</p>

  </div>


<script>

document.getElementById("scanner").addEventListener("click", function () {

  let isAuthenticated = Math.random() < 0.7; // 70% chance of success

  let scannerStatus = document.getElementById("scanner-status");

  if (isAuthenticated) {

    scannerStatus.textContent = "Fingerprint Accepted!";

    scannerStatus.style.color = "green";

  } else {

    scannerStatus.textContent = "Fingerprint Rejected!";

    scannerStatus.style.color = "red";

  }

});

</script>

</body>

</html>
```

## 4.2. Test Cases

Test Case	Input	Expected Output
Fingerprint Authentication	Finger placed on scanner	Authentication <b>Accepted/Rejected</b>
View Balance	Click "View Balance"	Display correct <b>balance amount</b>
Withdraw Money	Enter amount and click withdraw	Deduct from balance if sufficient funds
Deposit Money	Enter amount and click deposit	Add amount to balance

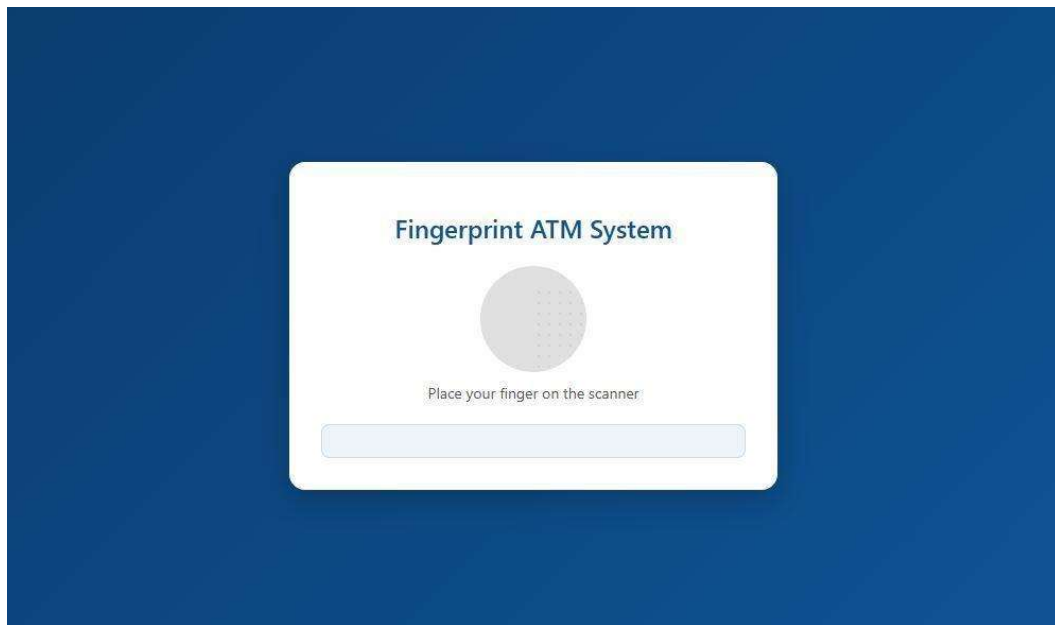
## 5. Results

- The **fingerprint authentication simulation works correctly**, with randomized success/failure.
- **Account selection and transactions operate as expected.**
- **Balance updates correctly** after deposit and withdrawal transactions.

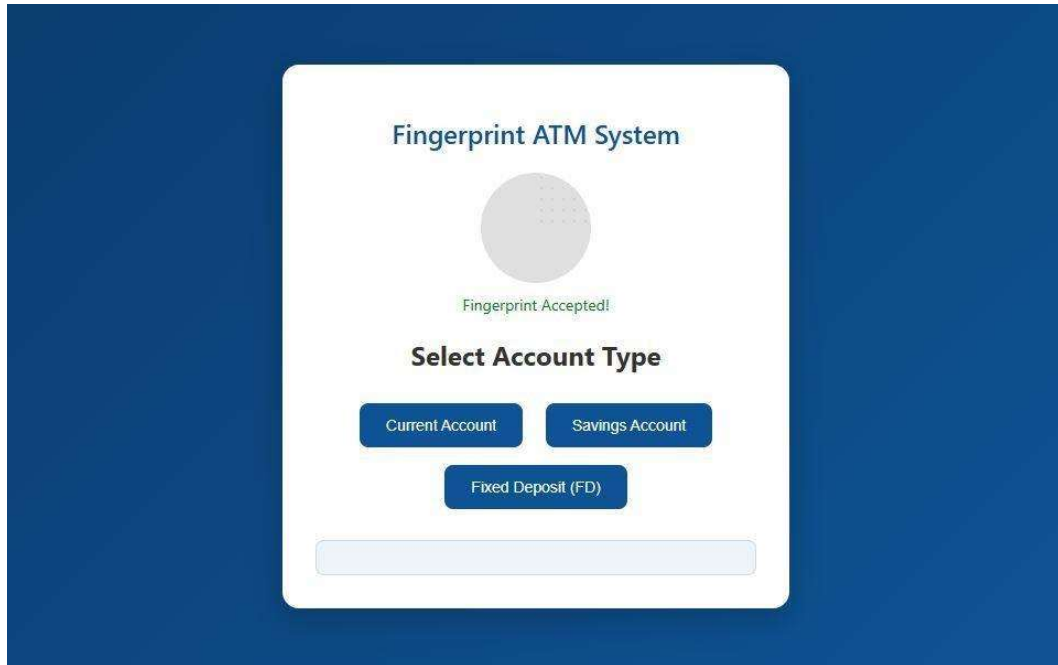
### 5.1. Output Screens

Screenshots include:

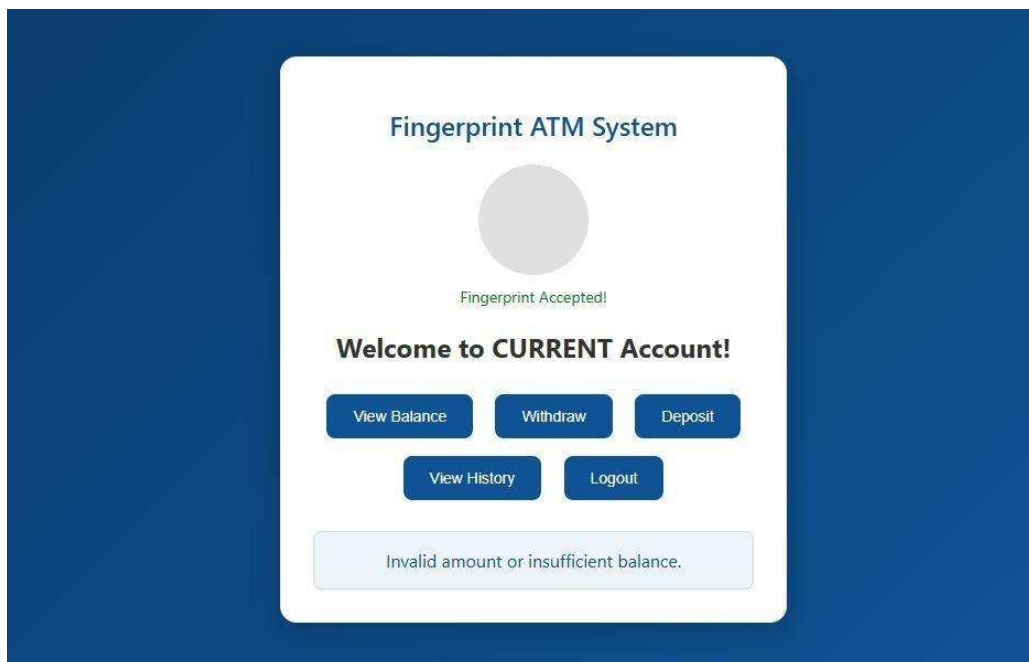
- **Fingerprint scanning interface**



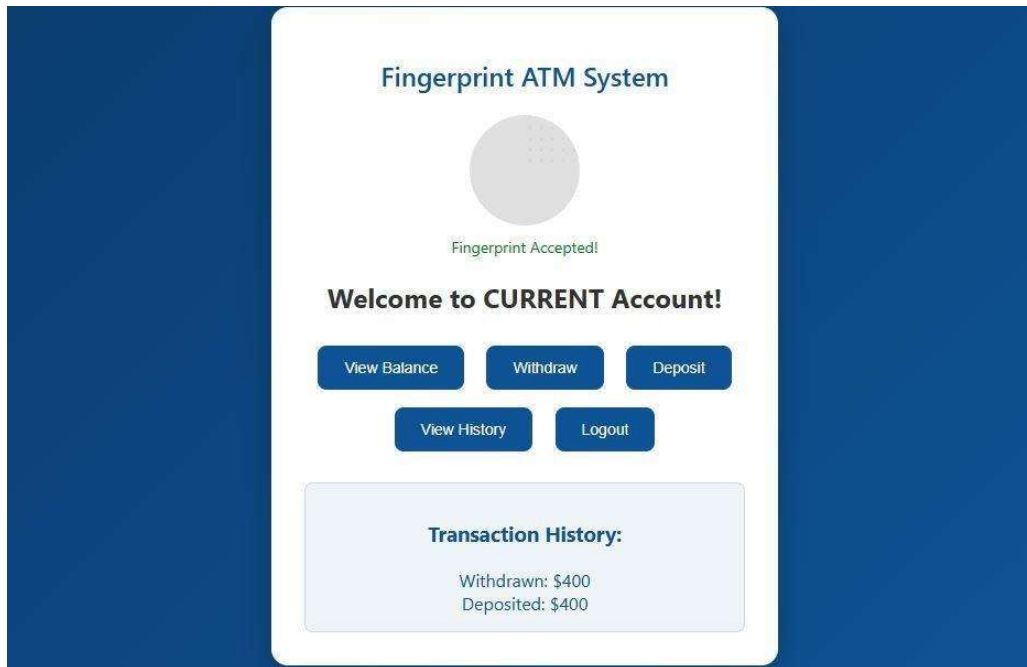
- **Account selection menu**



- **ATM transaction options**



- **Transaction history display**



- **When Fingerprint is rejected**



## 6. Conclusion

The **Fingerprint-Based ATM System** provides a **secure and user-friendly authentication mechanism** that eliminates the risks associated with **PIN-based ATM transactions**. The system demonstrates the feasibility of using fingerprint biometrics for banking security in a web-based environment.



## References

- Research papers on biometric authentication.
- Online resources for fingerprint scanning in web applications.
- JavaScript tutorials for ATM transaction simulations.

## GITHUB link:

<https://github.com/rajesh93471/Finger-Print-BasedATM>