**FINGERPRINT-BASED ATM SYSTEM**

A PROJECT REPORT

*Submitted by*

D.LOHITH CHOWDARI [RA2211003011384]

*Under the Guidance of*

Dr. Manju A

Assistant Professor, Department of Computing Technologies

*in partial fulfilment of the requirements for the course*

*21CSC303J Software Engineering and Project*

*Management*

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE ENGINEERING



DEPARTMENT OF COMPUTING TECHNOLOGIES COLLEGE OF ENGINEERING AND TECHNOLOGY SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR- 603 203

MAY 2025

Department of Computational Intelligence

##### SRM Institute of Science & Technology Own Work\* Declaration Form

This sheet must be filled in (each box ticked to show that the condition has been met). It must be signed and dated along with your student registration number and included with all assignments you submit – work will not be marked unless this is done.

To be completed by the student for all assessments

##### Degree/ Course : BTech / Computer Science and Engineering

**Student Name : Dupati Lohith chowdari**

**Registration Number : RA2211003011384**

**Title of Work : Fingerprint-Based Atm System**

I / We hereby certify that this assessment compiles with the University’s Rules and Regulations relating to Academic misconduct and plagiarism\*\*, as listed in the University Website, Regulations, and the Education Committee guidelines.

I / We confirm that all the work contained in this assessment is my / our own except where indicated, and that I / We have met the following conditions:

* Clearly referenced / listed all sources as appropriate
* Referenced and put in inverted commas all quoted text (from books, web, etc)
* Given the sources of all pictures, data etc. that are not my own
* Not made any use of the report(s) or essay(s) of any other student(s) either past or present
* Acknowledged in appropriate places any help that I have received from others (e.g. fellow students, technicians, statisticians, external sources)
* Compiled with any other plagiarism criteria specified in the Course handbook / University website

I understand that any false claim for this work will be penalized in accordance with the University policies and regulations.

|  |
| --- |
| **DECLARATION:** |
| I am aware of and understand the University’s policy on Academic misconduct and plagiarism and I certify that this assessment is my / our own work, except where indicated by referring, and that I have followed the good academic practices noted above.  D.Lohith Chowdari [RA2211003011384] |
| If you are working in a group, please write your registration numbers and sign with the date for every student in your group. |



SRM INSTITUTE OF SCIENCE AND TECHNOLOGY KATTANKULATHUR – 603 203

BONAFIDE CERTIFICATE

<

Certified that 18CSP107L - Minor Project [18CSP108L- Internship] report titled “**Fingerprint-Based Atm System**” is the Bonafide work of **“Dupati Lohith chowdari [RA2211003011384]”** who carried out the project work[internship] under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

**SIGNATURE SIGNATURE**

**Dr. Manju A DR. Niranjana G**

|  |  |
| --- | --- |
| **SUPERVISOR**  Assistant Professor Department of  CTECH | **PROFESSOR &HEAD OF DEPARTMENT**  Department of CTECH |

# ACKNOWLEDGEMENTS

We express our humble gratitude to **Dr. C. Muthamizhchelvan**, Vice-Chancellor, SRM Institute of Science and Technology, for the facilities extended for the project work and his continued support.

We extend our sincere thanks to **Dr. Leenus Jesu Martin M,** Dean-CET, SRM Institute of Science and Technology, for his invaluable support.

We wish to thank **Dr. Revathi Venkataraman**, Professor and Chairperson, School of Computing, SRM Institute of Science and Technology, for her support throughout the project work.

We encompass our sincere thanks to, **Dr. M. Pushpalatha**, Professor and Associate Chairperson - CS, School of Computing and **Dr. Lakshmi,** Professor and Associate Chairperson

-AI, School of Computing, SRM Institute of Science and Technology, for their invaluable support.

We are incredibly grateful to our Head of the Department, **Dr. Niranjana G**, Professor &Head, Department of Computing Technologies, SRM Institute of Science and Technology, for her suggestions and encouragement at all the stages of the project work.

We want to convey our thanks to our Project Coordinators, Panel Head, and Panel Members Department of Computational Intelligence, SRM Institute of Science and Technology, for their inputs during the project reviews and support.

We register our immeasurable thanks to our Faculty Advisor, **Dr. Nancy P** Department of Computing Technologies, SRM Institute of Science and Technology, for leading and helping us to complete our course.

Our inexpressible respect and thanks to our guide, **Dr. Manju A**, Department of Computing Technologies, SRM Institute of Science and Technology, for providing us with an opportunity to pursue our project under her mentorship. She provided us with the freedom and support to explore the research topics of our interest. Her passion for solving problems and making a difference in the world has always been inspiring.

We sincerely thank all the staff members of Department of Computing Technologies , School of Computing, S.R.M Institute of Science and Technology, for their help during our project. Finally, we would like to thank our parents, family members, and friends for their unconditional love, constant support and encouragement

# ABSTRACT

The Fingerprint-Based ATM System aims to enhance security and user convenience by integrating biometric authentication into the ATM process. The initiative replaces traditional PIN-based access with fingerprint recognition, eliminating the vulnerabilities associated with PINs, such as theft or forgetfulness. By utilizing fingerprint files for user authentication, this system ensures a more secure, user-friendly, and efficient banking experience.

The project focuses on creating a seamless ATM transaction environment, where users can withdraw, deposit, and check mini-statements through a secure fingerprint authentication process. The system also includes multi-language support to cater to users from diverse linguistic backgrounds, ensuring accessibility for a broad demographic. core aspect of the project is its emphasis on security. The fingerprint data is encrypted and stored securely, ensuring that sensitive information is protected. The system also incorporates a robust backend to handle transactions securely, reducing fraud risks. This project aims to modernize the traditional ATM system, offering a higher level of user trust and operational efficiency, while providing a smoother, more secure banking experience. With a goal to simplify and improve the ATM experience, the successful implementation of this system will bring a significant advancement in banking security and convenience, benefiting all users by reducing manual intervention and enhancing transaction reliability.

|  |  |  |
| --- | --- | --- |
|  | **TABLE OF CONTENTS** |  |
| **ABSTRACT**  **TABLE OF CONTENTS LIST OF FIGURES LIST OF TABLES**  **ABBREVIATIONS** |  | **iv v vii ix**  **x** |
| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |
| **1. INTRODUCTION** |  | **1** |

* 1. Introduction to Project 1
  2. [Motivation 1](#_TOC_250019)
  3. [Sustainable Development Goal of the Project 2](#_TOC_250018)
  4. [Product Vision Statement 2](#_TOC_250017)
  5. Product Goal 4
  6. Product Backlog (Key User Stories with Desired Outcomes) 6
  7. [Product Release Plan 7](#_TOC_250016)

1. SPRINT PLANNING AND EXECUTION 8
   1. [Sprint 1 8](#_TOC_250015)
      1. [Sprint Goal with User Stories of Sprint 1 8](#_TOC_250014)
      2. [Functional Document 13](#_TOC_250013)
      3. [Architecture Document 15](#_TOC_250012)
      4. [UI Design 18](#_TOC_250011)
      5. [Functional Test Cases 23](#_TOC_250010)
      6. Daily Call Progress 23
      7. Committed vs Completed User Stories 24
      8. [Sprint Retrospective 24](#_TOC_250009)
   2. [Sprint 2 25](#_TOC_250008)
      1. [Sprint Goal with User Stories of Sprint 2 25](#_TOC_250007)
      2. [Functional Document 32](#_TOC_250006)
      3. [Architecture Document 34](#_TOC_250005)
      4. [UI Design 37](#_TOC_250004)
      5. Functional Test Cases 41
      6. Daily Call Progress 43
      7. Committed vs Completed User Stories 44
      8. [Sprint Retrospective 44](#_TOC_250003)
2. RESULTS AND DISCUSSIONS 45
   1. [Project Outcomes 45](#_TOC_250002)
   2. [Committed vs Completed User Stories 46](#_TOC_250001)
3. CONCLUSIONS & FUTURE ENHANCEMENT 47

APPENDIX 48

1. [SAMPLE CODING 48](#_TOC_250000)
2. PLAGIARISM REPORT 60

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| CHAPTER NO | TITLE | PAGE NO. |
| 1 | Figure 1.1 – MS Planner Board of Fingerprint Based ATM systems | 8 |
| 1 | Figure 1.2 – Product Release plan | 9 |
| 2 | Figure 2.1 – User Story for withdraw cash | 11 |
| 2 | Figure 2.2 – User Story for OAuth | 12 |
| 2 | Figure 2.3 – User Story for Transfer money | 13 |
| 2 | Figure 2.4 – Architecture Diagram | 17 |
| 2 | Figure 2.5 – UI Design for Login page | 19 |
| 2 | Figure 2.6 – UI Design for Admin page | 19 |
| 2 | Figure 2.7 – Committed Vs Completed User Stories | 20 |
| 2 | Figure 2.8 – Monitoring | 21 |
| 2 | Figure 2.9 – Mini statement | 23 |
| 2 | Figure 2.2.3 – Architecture Diagram | 27 |
| 2 | Figure 2.2.4 – UI Design of Register page | 28 |
| 2 | Figure 2.3.1 – View Account Balance | 32 |
| 2 | Figure 2.3.2 – Log out | 33 |
| 2 | Figure 2.3.3 – Project scope | 34 |
| 2 | Figure 3.2 – commited vs completed user stories | 40 |

**LIST OF TABLES**

|  |  |  |
| --- | --- | --- |
| CHAPTER NO | TITLE | PAGE NO. |
| 1 | Table 1.1 – Product Backlog | 7 |
| 2 | Table 2.1 – Detailed User Stories (Sprint 1) | 10 |
| 2 | Table 2.2 – Authorization Matrix (Sprint 1) | 16 |
| 2 | Table 2.3 – Detailed Functional Test Cases (Sprint 1) | 20 |
| 2 | Table 2.4 – Detailed Sprint Retrospective (Sprint 1) | 21 |
| 2 | Table 2.5 – Detailed User Stories (Sprint 2) | 27 |
| 2 | Table 2.6 – Authorization Matrix (Sprint 2) | 28 |
| 2 | Table 2.7 – Detailed Functional Test Cases (Sprint 2) | 30 |
| 2 | Table 2.8 – Sprint Retrospective (Sprint 2) | 31 |

**ABBREVIATIONS**

|  |  |
| --- | --- |
| **Abbreviation** | **Full Form** |

|  |  |
| --- | --- |
| ATM | Automated Teller Machine |

|  |  |
| --- | --- |
| OTP | One-Time Password |

|  |  |
| --- | --- |
| UIDAI | Unique Identification Authority of India |

|  |  |
| --- | --- |
| Biometric | Biological Metric |

|  |  |
| --- | --- |
| FPGA | Field Programmable Gate Array |

|  |  |
| --- | --- |
| IoT | Internet of Things |

|  |  |
| --- | --- |
| AES | Advanced Encryption Standard |

|  |  |
| --- | --- |
| PIN | Personal Identification Number |

|  |  |
| --- | --- |
| GUI | Graphical User Interface |

|  |  |
| --- | --- |
| DBMS | Database Management System |

|  |  |
| --- | --- |
| RFID | Radio Frequency Identification |

|  |  |
| --- | --- |
| GSM | Global System for Mobile Communications |

**CHAPTER 1 INTRODUCTION**

## Introduction to Fingerprint-Based ATM System:

The **Fingerprint-Based ATM System** introduces a revolutionary approach to banking security by leveraging biometric authentication for ATM transactions. In contrast to traditional PIN-based systems, which are vulnerable to theft or forgetting, this system uses the unique biometric feature of fingerprint recognition to authenticate users. The fingerprint files are securely stored in the system, ensuring that they cannot be tampered with or stolen. During a transaction, users are prompted to place their finger on the scanner, where their fingerprint is captured and compared to the stored data for verification. If there is a match, the user is granted access to their account, enabling them to perform ATM services such as withdrawals, deposits, and viewing mini-statements. This transition to biometric-based authentication enhances the overall security of financial transactions by making it far more difficult for unauthorized individuals to gain access.

The integration of fingerprint biometrics into the ATM system is a key advancement in providing both security and convenience for users. Traditional ATM security methods, such as PINs or passwords, are vulnerable to various types of attacks, including card skimming and social engineering. By shifting to a fingerprint-based system, users are no longer required to memorize or share sensitive information. The fingerprint itself becomes the unique identifier, which is not transferable or replicable. Moreover, fingerprint biometrics offer a quick and efficient method of authentication, allowing users to complete transactions faster than ever before. This streamlined process not only improves user satisfaction but also reduces the chance of human error, offering a more foolproof method of ensuring that only the rightful account holder has access to their funds

## Motivation

The **Fingerprint-Based ATM System** aims to address security concerns in traditional banking systems,which rely on vulnerable PIN-based authentication. PINs are prone to theft, loss, and forgetfulness, leading to increased risk of unauthorized access. Biometric authentication, especially fingerprint recognition, offers a more secure and efficient alternative. Unlike PINs, fingerprints are unique to each individual and cannot be replicated, ensuring only authorized users can access accounts. This system not only enhances security but also improves user convenience by eliminating the need to remember PINs. The rise of financial fraud and identity theft further highlights the need for such advanced security measures. By adopting fingerprint recognition, the system ensures faster and safer transactions, promoting trust in the banking system. This solution aligns with the growing demand for more secure and efficient banking experiences. With the widespread adoption of biometric technology, the **Fingerprint- Based ATM System** seeks to set a higher standard for financial security. Ultimately, it aims to build a more secure, reliable, and user-friendly banking environment. Additionally, fingerprint- based authentication enhances the user experience by providing a faster, more reliable, and user-friendly method of authentication. Unlike PINs, which can be forgotten or compromised, fingerprint data is unique to each individual and cannot be shared or stolen. This system not only addresses the security concerns of traditional ATMs but also improves the convenience of banking transactions by eliminating the need to remember PINs. With the rise of digital banking, the demand for more secure and efficient authentication methods is increasing, making the adoption of fingerprint-based systems essential for the future of secure, user- friendly banking.

.

## Sustainable Development Goal of the Project

The **Fingerprint-Based ATM System** aligns with the United Nations' Sustainable Development Goal 16 (SDG 16), which focuses on promoting peaceful, just, and inclusive societies by enhancing the accessibility, security, and efficiency of financial systems. By incorporating biometric authentication, this system addresses critical security concerns and fosters trust in financial institutions. It promotes transparency and accountability in banking transactions, ensuring that only authorized individuals can access their accounts and perform financial activities. This enhanced security helps reduce financial fraud and identity theft, making the banking experience safer for everyone, regardless of their background or financial status.

Additionally, the system contributes to financial inclusion by offering a user- friendly and secure means of conducting transactions. Traditional ATM systems often present barriers such as forgotten PINs, security vulnerabilities, and limited access for individuals with disabilities or those unfamiliar with digital banking. The **Fingerprint-Based ATM System** eliminates these barriers by allowing individuals to authenticate using their unique fingerprint, ensuring a seamless and inclusive banking experience. This system empowers users, particularly those from underserved communities, to access financial services securely and with ease, promoting economic participation and personal financial growth. Through innovative biometric technology, the system helps bridge the gap in access to reliable, secure financial services, contributing to the sustainable development of communities and the overall goal of inclusive financial systems.

## Product Vision Statement

### Audience:

* + - * **Primary Audience**: Bank customers seeking secure, fast, and user-friendly ATM transactions.
      * **Secondary Audience**: Financial institutions and banks looking to integrate advanced biometric systems into their ATM infrastructure.

### Needs:

##### Primary Needs:

* + - * + Secure and foolproof authentication using fingerprint recognition to replace traditional PINs.
        + Quick and efficient transaction processing with minimal user interaction.
        + High level of reliability and security for financial transactions.

##### Secondary Needs:

* + - * + Seamless integration with existing ATM networks and banking systems
        + User-friendly interface for a smooth customer experience.
        + Privacy and data security protocols to protect fingerprint data and transaction details.

### Products:

* + - * **Core Product** : A **Fingerprint-Based ATM System** utilizing fingerprint recognition for secure and efficient authentication during ATM transactions.

##### Additional Features:

* + - * + Biometric data encryption to ensure the security and privacy of fingerprint data.
        + Integration with existing banking systems for seamless transactions.
        + Multi-language support for broader accessibility.
        + Real-time authentication feedback for faster transaction processing.

### Values:

##### Core Values:

* + - * + **Security:** Providing enhanced security by using fingerprint-based authentication to prevent unauthorized access.
        + **Convenience:** Streamlining the ATM transaction process for faster and more user-friendly experiences.
        + **Privacy:** Ensuring that all biometric data is encrypted and securely stored to protect user privacy.

##### Differentiators:

* + - * + **Biometric Authentication:** Replacing traditional PINs with secure fingerprint recognition to minimize the risks of identity theft and fraud.
        + **Seamless Integration:** Ensuring the system integrates easily with existing ATM infrastructure and banking systems.
        + **User Experience:** Offering an intuitive and simple interface, ensuring both tech-savvy and non-tech-savvy users can operate the system effortlessly.

## 1.4 Product Goal

The primary goal of the **Fingerprint-Based ATM System** is to revolutionize the banking experience by providing a secure, fast, and user-friendly alternative to traditional PIN- based ATM systems. By integrating biometric fingerprint authentication, the system aims to enhance security by ensuring that only authorized individuals can access their accounts, reducing the risks of fraud and identity theft. The system's goal is to provide seamless and efficient ATM transactions while ensuring that users can interact with their accounts without the need for remembering PINs, thus improving accessibility for all, including those who struggle with traditional methods of authentication.

In addition to enhancing security, the system seeks to make banking more inclusive by offering an intuitive, easy-to-use interface that is accessible to individuals from diverse backgrounds. The goal is to create a system where every user, regardless of technical proficiency, can confidently use the ATM. By offering multi-language support and ensuring ease of use, the system seeks to break down barriers and make banking services available to a wider population. This system also strives to create an ecosystem where users can have a smoother, more secure financial experience, promoting trust and confidence in digital banking systems.

Ultimately, the **Fingerprint-Based ATM System** aims to establish a secure, efficient, and inclusive banking environment that enhances user convenience, reduces the risk of fraud, and fosters greater trust in the financial system. By leveraging biometric technology, the system aspires to offer a safer, more accessible, and user-centered banking experience that promotes financial inclusion and security for all.

## 1.6 Product Backlog

|  |  |
| --- | --- |
| **S.No** | **User Stories of Fingerprint Based ATM Systems** |
| #US 1 | As a user, I want to easily register my fingerprint for the ATM system so that I can access my account securely. |
| #US 2 | As a user, I want to register my fingerprint securely so that I can eliminate the need for remembering a PIN. |
| #US 3 | As a user, I want to perform ATM transactions like withdrawals and deposits using fingerprint authentication to ensure security. |
| #US 4 | As a user, I want to access my account with fingerprint authentication at any ATM machine for convenience. |
| #US 5 | As a user, I want to check my mini-statements securely with biometric authentication to ensure privacy. |
| #US 6 | As an ATM provider, I want to ensure that the fingerprint recognition system works seamlessly with ATM machines. |
| #US 7 | As a user, I want immediate feedback when I authenticate my fingerprint to ensure the transaction process is fast and smooth. |
| #US 8 | As a user, I want to receive notifications on successful or failed transactions to keep track of my account activities. |
| #US 9 | As a user, I want the system to store my fingerprint data securely to protect my personal information from unauthorized access. |
| #US 10 | As a user, I want the fingerprint data to be encrypted and processed locally for privacy and security. |
| #US 11 | As a user, I want to provide feedback on the fingerprint authentication process so that improvements can be made to the system. |

The product backlog of Fingerprint Based ATM Systems was configured using the MS planner Agile Board which is represented in the following Figure 1.1. The Product Backlog consists of the complete user stories of Ai based E-learning Application

Each user story consist of necessary parameters like MoSCoW prioritization, Functional and non functional parameters, detailed acceptance criteria with linked tasks.

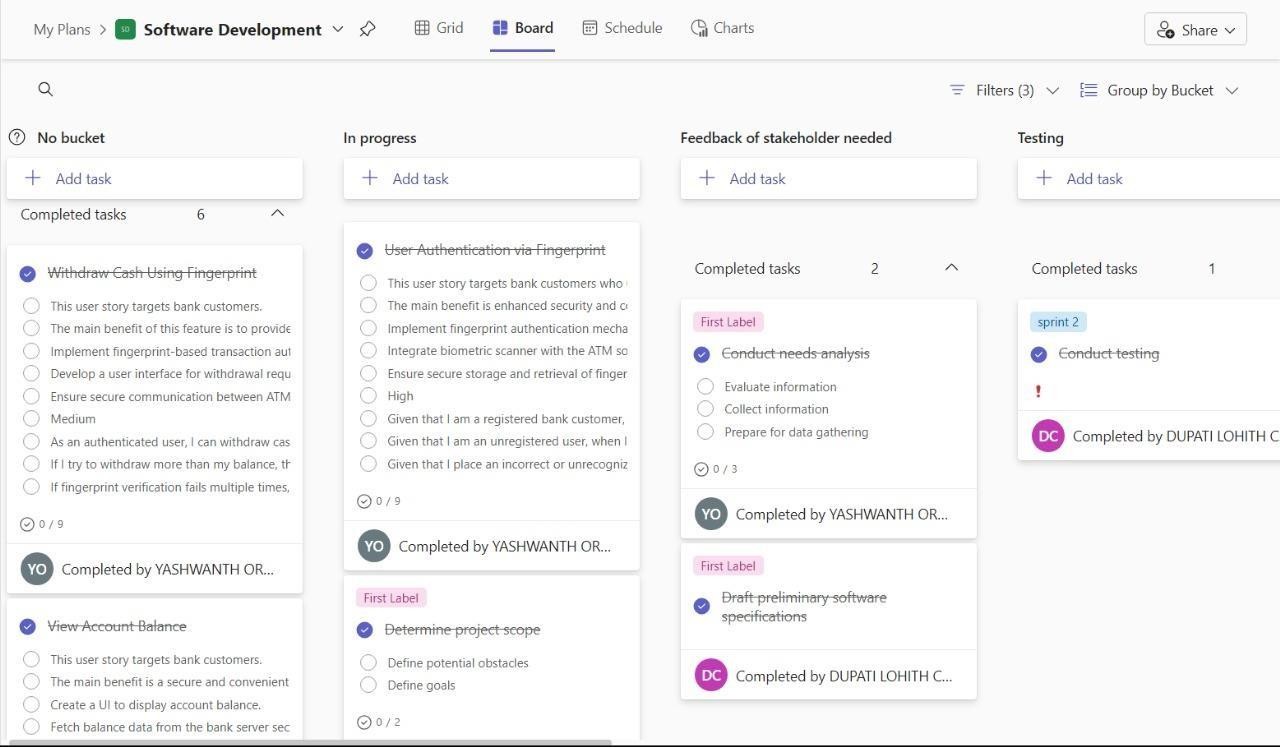


Figure 1.1 MS Planner Board of Fingerprint-Based ATM System

## 1.7 Product Release Plan

The following Figure 1.2 depicts the release plan of the project

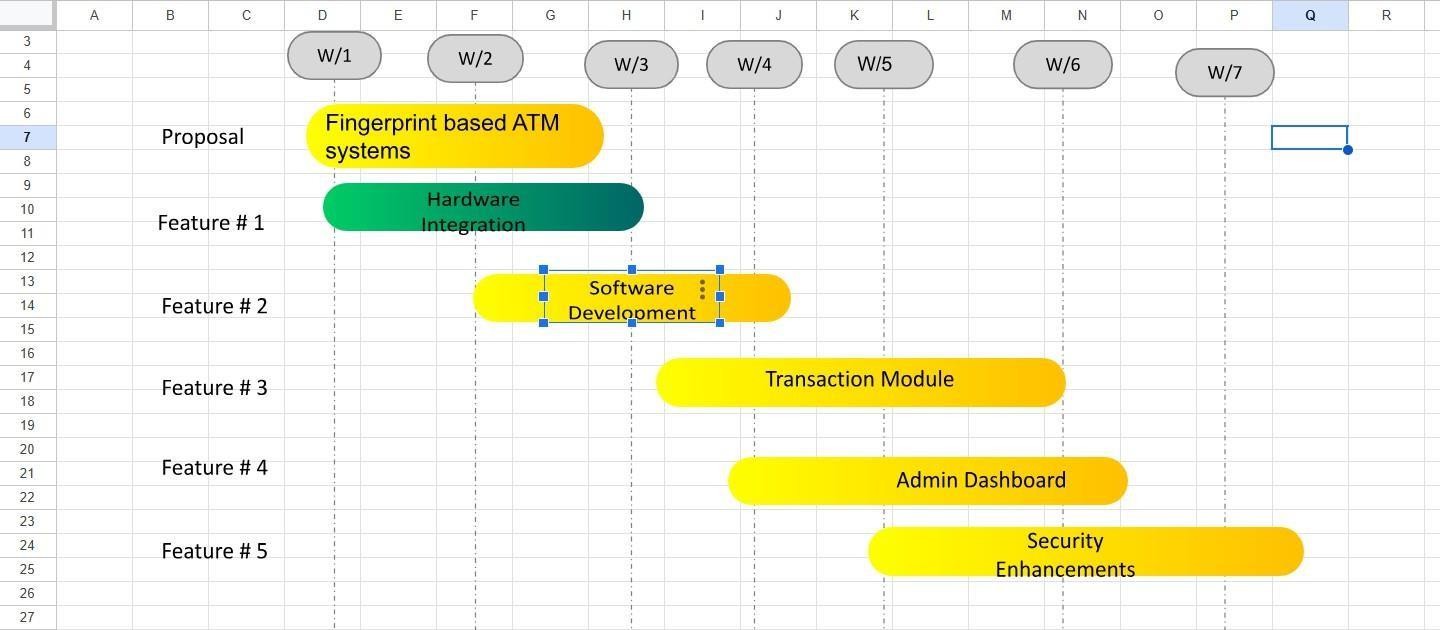


Figure 1.2 Release plan of Fingerprint-Based ATM System

# CHAPTER 2

**SPRINT PLANNING AND EXECUTION**

## Sprint 1

## Sprint Goal with User Stories of Sprint 1

The goal of the first sprint is to integrate fingerprint authentication into the ATM system, ensuring that only authorized users can access their accounts. The sprint will focus on developing the user interface, enrolling fingerprints, and allowing users to authenticate using biometric data.

The following table 2.1 represents the detailed user stories of the sprint 1

##### Table 2.1 Detailed User Stories of sprint 1

|  |  |
| --- | --- |
| **S.NO** | **Detailed User Stories** |
| US #1 | As a new user, I want to register my fingerprint for the ATM system so that I can securely  access my account without needing to remember a PIN. |
| US #2 | As a user, I want to verify my fingerprint at the ATM so that I can perform secure  transactions like withdrawals, deposits, and mini-statement retrieval. |
| US #3 | As a user, I want to authenticate my fingerprint at any ATM location to ensure  convenience and consistent access to my account across various machines. |

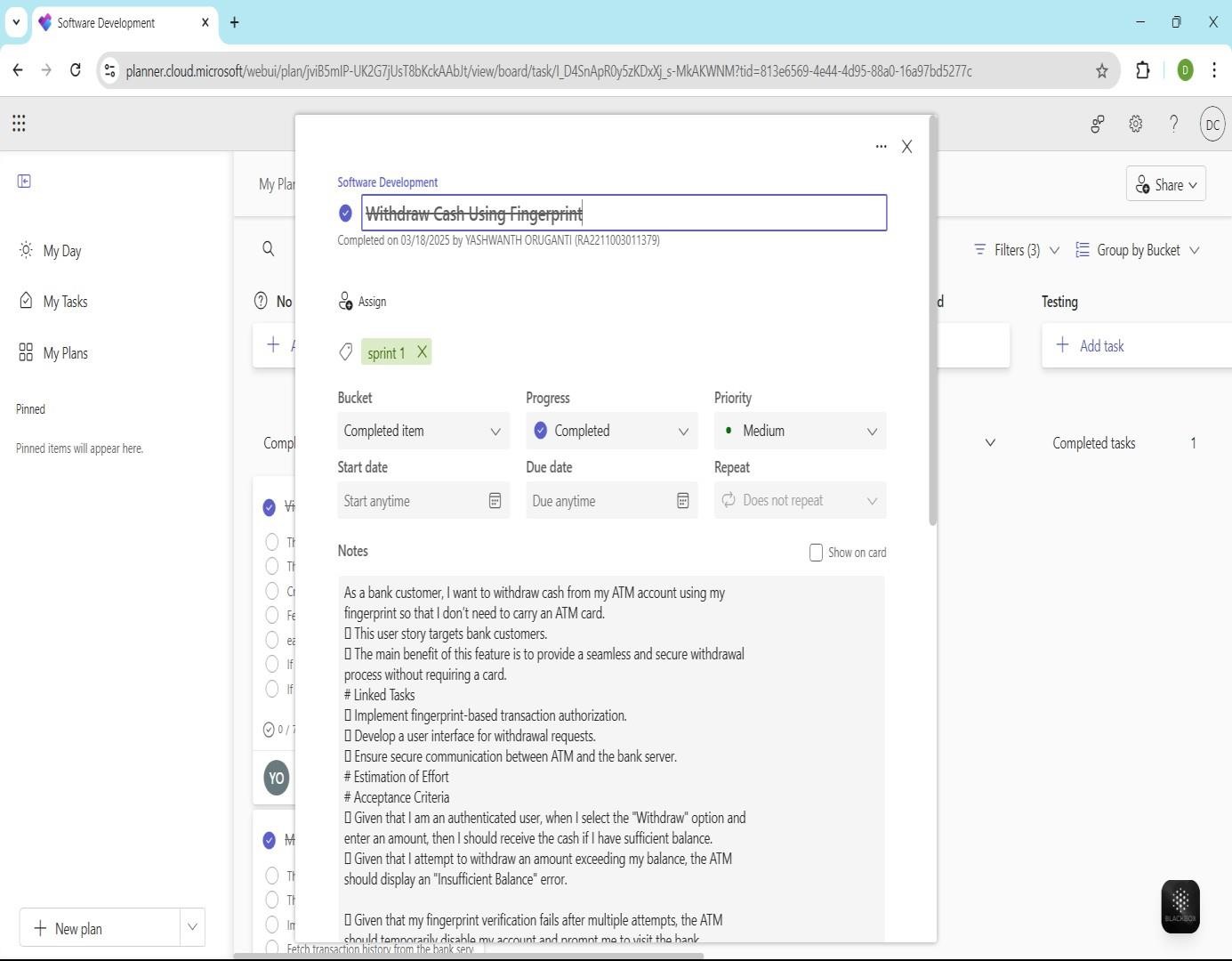
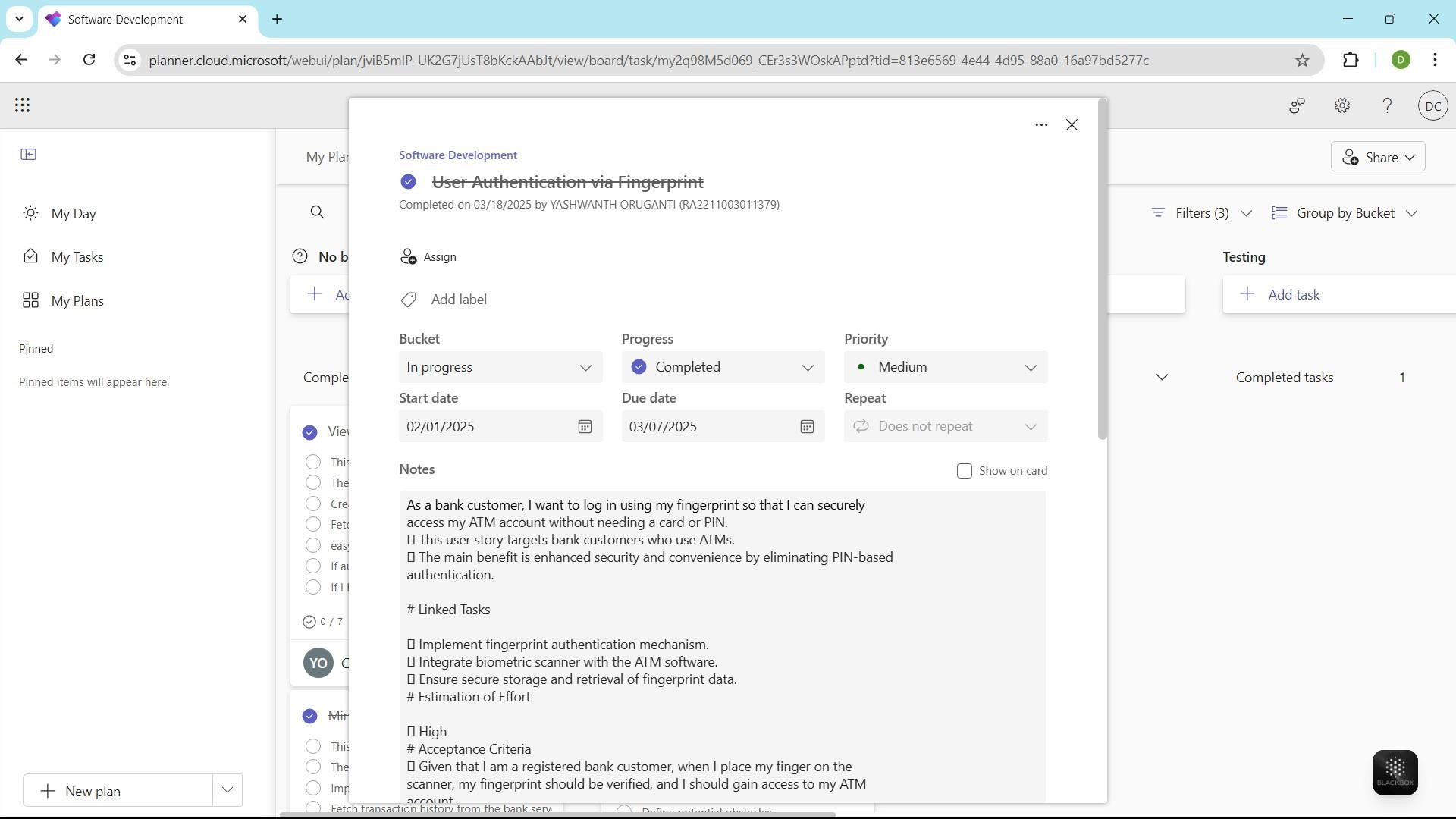
Planner Board representation of user stories are mentioned below figures 2.1,2.2 and 2.3

Figure 2.1 user story for Withdraw cash

Figure 2.2 user story Authentication

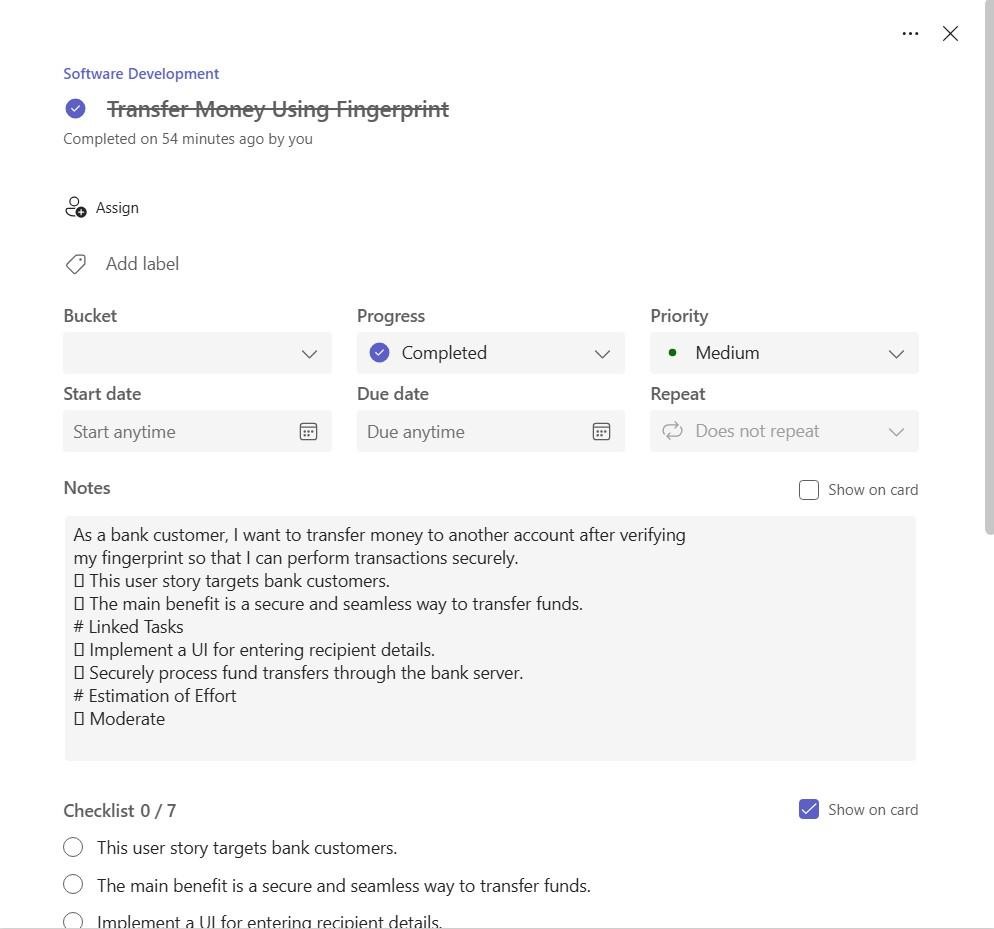


Figure 2.3 User story for Tranfer money

## Functional Document

* + - 1. Introduction

The **Fingerprint-Based ATM System** project aims to provide a secure, efficient, and user- friendly banking experience by integrating biometric fingerprint authentication into ATM systems. This system replaces the traditional PIN-based authentication with a secure and fast fingerprint recognition method, ensuring only authorized users can access their accounts. The

project focuses on enhancing ATM security while maintaining a smooth and convenient user

experience for all users, including those who may struggle with traditional methods of authentication.

* + - 1. Product Goal
         * The primary goal of this project is to develop an ATM system that utilizes fingerprint authentication to improve security, accessibility, and user experience. The platform aims to:
         * Provide seamless and quick ATM transactions for users.
         * Ensure ease of use and accessibility, regardless of the user's technical proficiency.
         * Integrate with existing banking systems to ensure smooth operation across all ATMs.
         * Create a secure, convenient, and efficient banking system for all users.
      2. Demography (Users, Location) Users:
         * Target Users: Bank customers, including individuals who are unfamiliar with traditional PIN-based systems or have difficulty remembering PINs.
         * User Characteristics: Varying levels of technical proficiency, with a focus on accessibility for elderly users or those unfamiliar with technology.

##### Location:

* + - * + Target Location: Global, with a focus on regions with high ATM usage, including urban and semi-urban areas, where security and convenience in banking transactions are a priority.

##### 2.1.2.4. Business Processes

The key business processes include:

##### User Registration and Authentication:

* + - * + Users can securely register their fingerprint for authentication through the ATM system.
        + The system ensures secure access by encrypting and storing the fingerprint data.

**Fingerprint Authentication for Transactions**:

* + - * + The system matches the user’s fingerprint to stored data during ATM transactions for secure access

##### Features

This project focuses on implementing the following key features:

##### Feature 1: User Registration and Fingerprint Enrollment

Description:

* + - * + Users can register their fingerprint for the ATM system to enable secure access to their accounts.

1. User Story:
   * As a user, I want to register my fingerprint so that I can access my ATM account securely without using a PIN.

Feature 2: **Secure ATM Transaction Authentication**

Description:

* + The system uses fingerprint authentication to grant access to ATM services such as withdrawals, deposits, and balance checks.

1. User Story:
   * As a user, I want to authenticate my fingerprint at the ATM so that I can securely perform transactions without needing a PIN.

Feature 3: **Multi-Language Support**

1. Description:
   * The system supports multiple languages to ensure accessibility for users from different linguistic backgrounds.
2. User Story:
   * As a user, I want the ATM system to support multiple languages so that I can easily navigate the interface in my preferred language.
     + 1. Authorization Matrix

##### Table 2.2 Access level Authorization Matrix

|  |  |
| --- | --- |
| Role | Access Level |
| Administrator | Full access to user management, system settings, and transaction oversight. |
| Educator | Access to transaction logs, user account details, and customer service features. |
| Learner | Access to perform transactions such as withdrawals, deposits, and mini- statements using fingerprint authentication. |
| Guest User | Limited access to view general ATM information but unable to perform transactions. |

* + - 1. Assumptions
* **Fingerprint system** will be trained on a diverse dataset for accurate authentication.
* **Continuous access** to ATM infrastructure will be available for testing and deployment.
* **User feedback** will be gathered during the pilot phase to improve the system.
* **Compliance** with global data protection and security standards to ensure privacy

## Architecture Document

##### Application Microservices:

The **Fingerprint-Based ATM System** is built on a microservices architecture, where different functionalities are encapsulated within independent services. Key services include:

* + - * + Authentication Service: Manages user fingerprint registration, fingerprint authentication, and account recovery.
        + Transaction Management Service: Handles transaction processing, including withdrawals, deposits, and balance checks.
        + User Role Management Service: Controls role-based access, ensuring (e.g., customers, bank employees, administrators) have appropriate permissions.
        + Notification Service: Sends real-time notifications for transaction updates, authentication status, and account activities.

2.1.3.2 System Architecture-

`

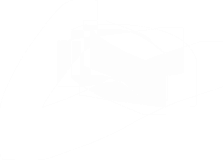
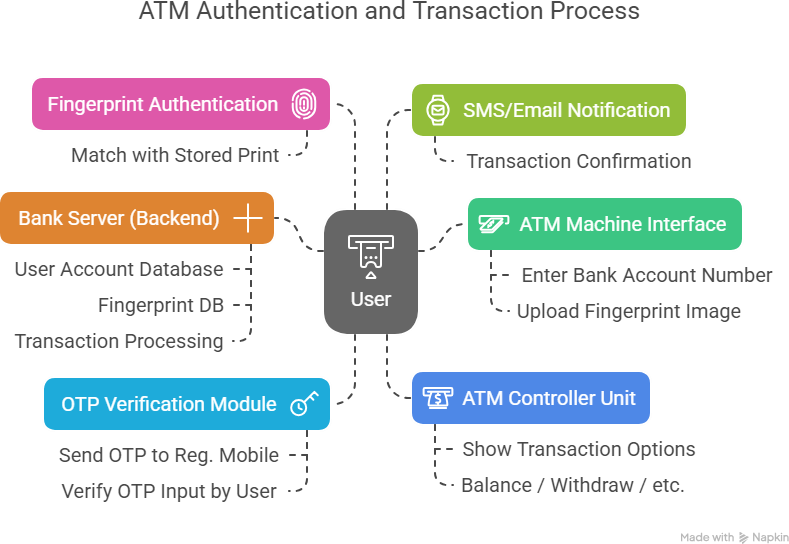


Figure 2.4 System Architecture Diagram

2.1.3.3. Data Exchange Contract:

##### Frequency of Data Exchanges:

Data exchanges in the **Fingerprint-Based ATM System** are managed based on the criticality of operations and performance requirements:

* Real-Time Exchanges: For critical operations such as fingerprint authentication and transaction processing, data is exchanged in real-time via APIs to ensure immediate feedback and validation.
* Periodic Syncs :Non-critical data, such as user activity logs and historical transaction data, is synchronized at scheduled intervals to optimize system performance .

##### Data Sets:

The platform handles several key data sets, each with specific exchange requirements:

* User Data: Includes personal details, fingerprint data, and account credentials. This data is exchanged during user registration, fingerprint enrollment, authentication, and account updates.
* Transaction Data : Includes transaction details such as withdrawal, deposit, and balance check records. This data is exchanged in real-time during transaction processing.
* Authentication Data: Tracks fingerprint authentication results, exchanged whenever users perform authentication actions at ATMs or through mobile apps.

##### Mode of Exchanges (API, File, Queue, etc.) :

Various methods are used for data exchange across the platform:

* API: RESTful are used for real-time data exchanges, facilitating communication between the front-end (ATM interface, mobile app) and back-end services (authentication, transaction management).
* Message Queues: Message queuing systems like RabbitMQ or AWS SQS handle asynchronous tasks such as processing background jobs, sending transaction alerts, or performing batch updates.
* File-Based Exchanges: Bulk data exchanges, like transaction history and backups, are handled via AWS S3.

### UI DESIGN

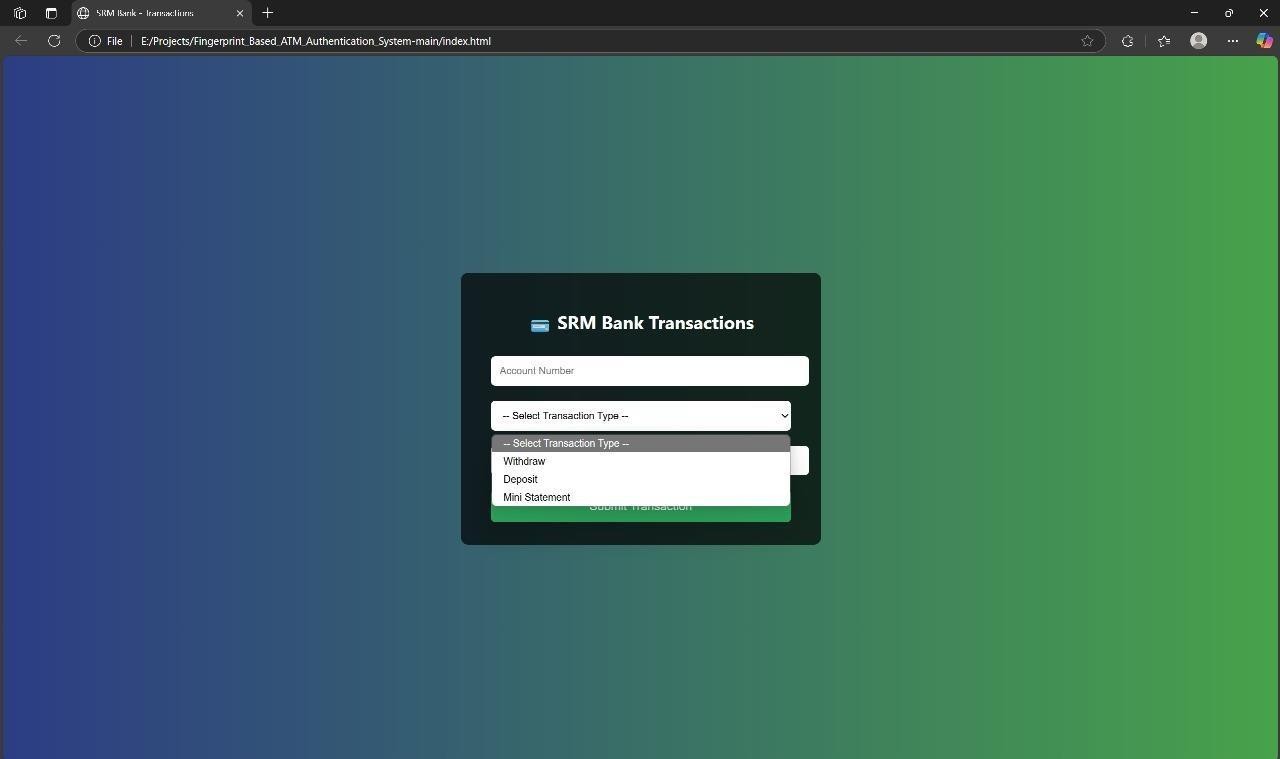
****

Figure 2.5 Login Page

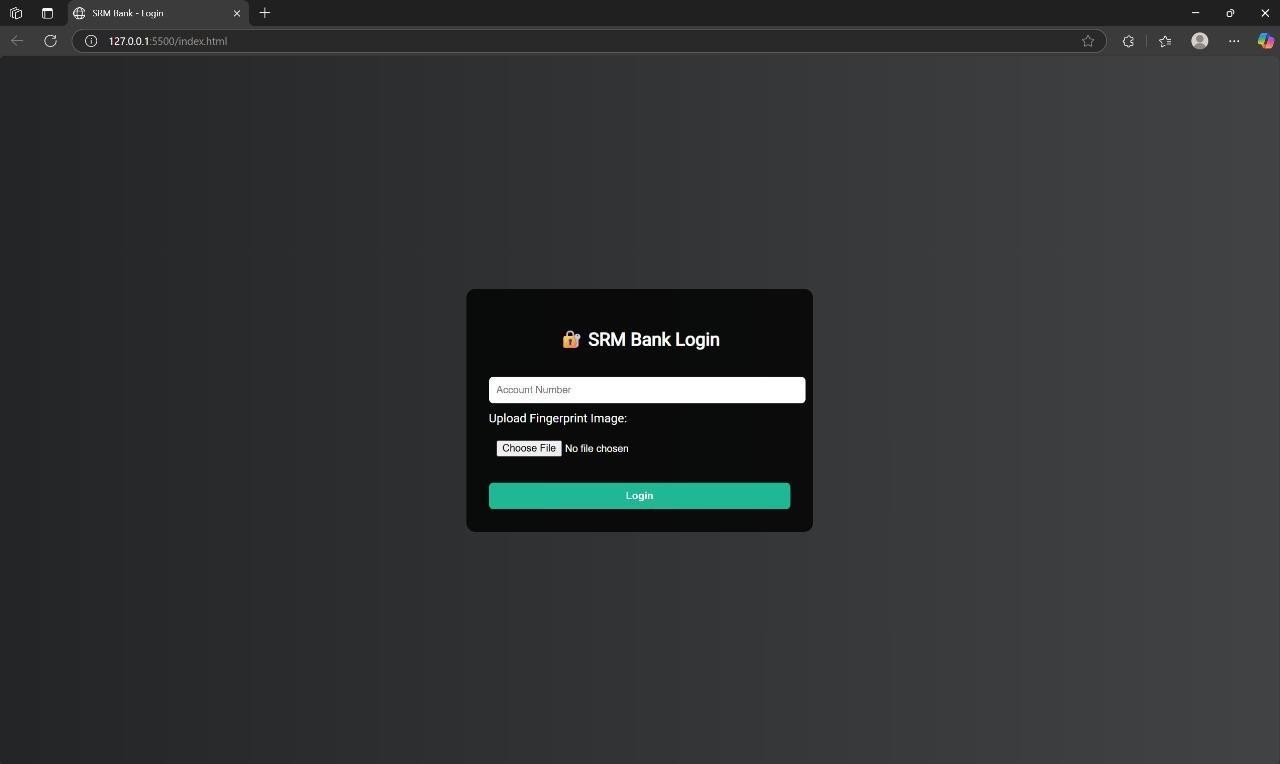


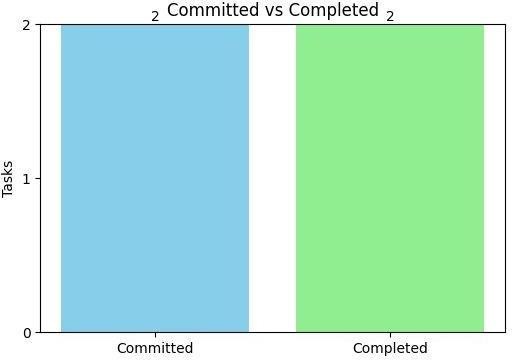
Figure 2.6 Admin Page

## Functional Test Cases

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Feature** | **Test Case** | **Steps to Execute Test Case** | **Expected Output** | **Actual Output** | **Status** | **More Information** |
| User Authentication | Login with fingerprint | 1. Place finger on scanner → 2. System captures fingerprint →  3. Match with DB | User logged in and dashboard shown | TBD | TBD | Use fingerprint module (e.g., R305) |
| Balance Enquiry | View current balance | 1. Login with fingerprint → 2. Select "Balance Enquiry" | Current balance displayed | TBD | TBD | Use encrypted API for data retrieval |
| Cash Withdrawal | Withdraw specific amount | 1. Login → 2. Select "Withdraw" → 3. Enter amount  → 4. Confirm | Cash dispensed, new balance shown | TBD | TBD | Validate min/max withdrawal limit |
| Mini Statement | View transaction history | 1. Login → 2. Click "Mini Statement" | List of recent transactions shown | TBD | TBD | Fetch from transaction DB |
| Fingerprint Retry | Retry on failed fingerprint scan | 1. Place incorrect/unclear finger  → 2. Retry prompt shown → 3. Re-scan | Retry message, successful login after valid scan | TBD | TBD | Add retry limit and timeout |
| Admin Access | Admin logs in to manage system | 1. Select “Admin Mode” → 2. Enter admin password/key | Admin dashboard shown | TBD | TBD | Secure admin- only access control |
| Session Timeout | Auto logout on inactivity | 1. Login → 2. Stay idle for X minutes | Auto logout with session ended message | TBD | TBD | Configure session duration |
| Logout | User logs out manually | 1. Click "Logout" after use | Session closed and login screen shown | TBD | TBD | Ensure secure  session termination |

**Table 2.3** Detailed Functional Test Case

## Committed Vs Completed User Stories

****

**Figure 2.7** Bar graph for Committed Vs Completed User Stories

## 2.1.8 Sprint Retrospective

|  |  |  |  |
| --- | --- | --- | --- |
| **Liked** | **Learned** | **Lacked** | **Longed For** |
| **Fingerprint sensor module integration was successful** | **How biometric authentication enhances security** | **Reliable fallback mechanism for failed fingerprint scans** | **Access to higher-quality fingerprint scanner SDKs** |
| **Node.js backend handled fingerprint data well** | **Importance of encryption and secure storage of biometric data** | **Better logging for failed login attempts** | **Pre-built biometric middleware for Node.js** |
| **UI for fingerprint scanning was intuitive and responsive** | **Designing event-driven flow with biometric input** | **Error feedback for invalid or unclear fingerprints** | **Sample datasets for biometric authentication testing** |
| **Hardware-software**  **interfacing worked without latency** | **Real-time data flow between hardware and server** | **Device compatibility documentation** | **More structured APIs for biometric services** |

**Table 2.1.8** Sprint Retrospective for the Sprint 1

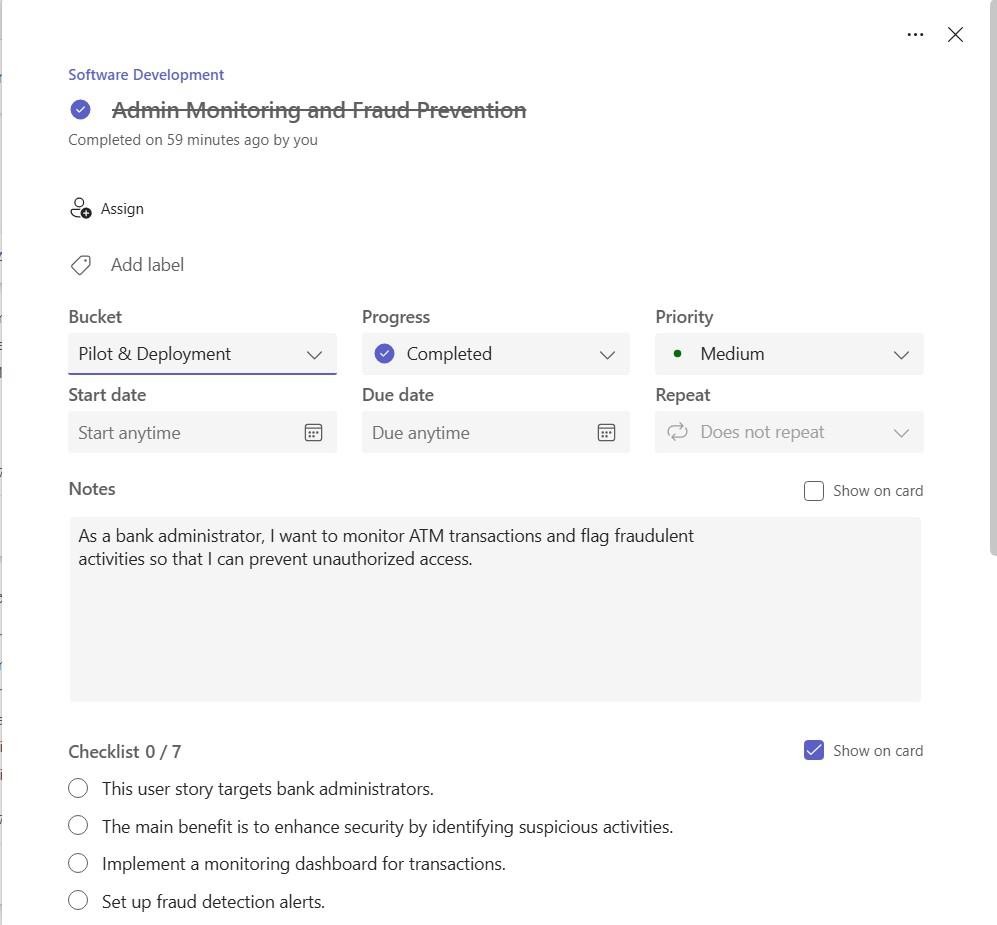
# SPRINT 2

##### Sprint Goal with User Stories of Sprint 2

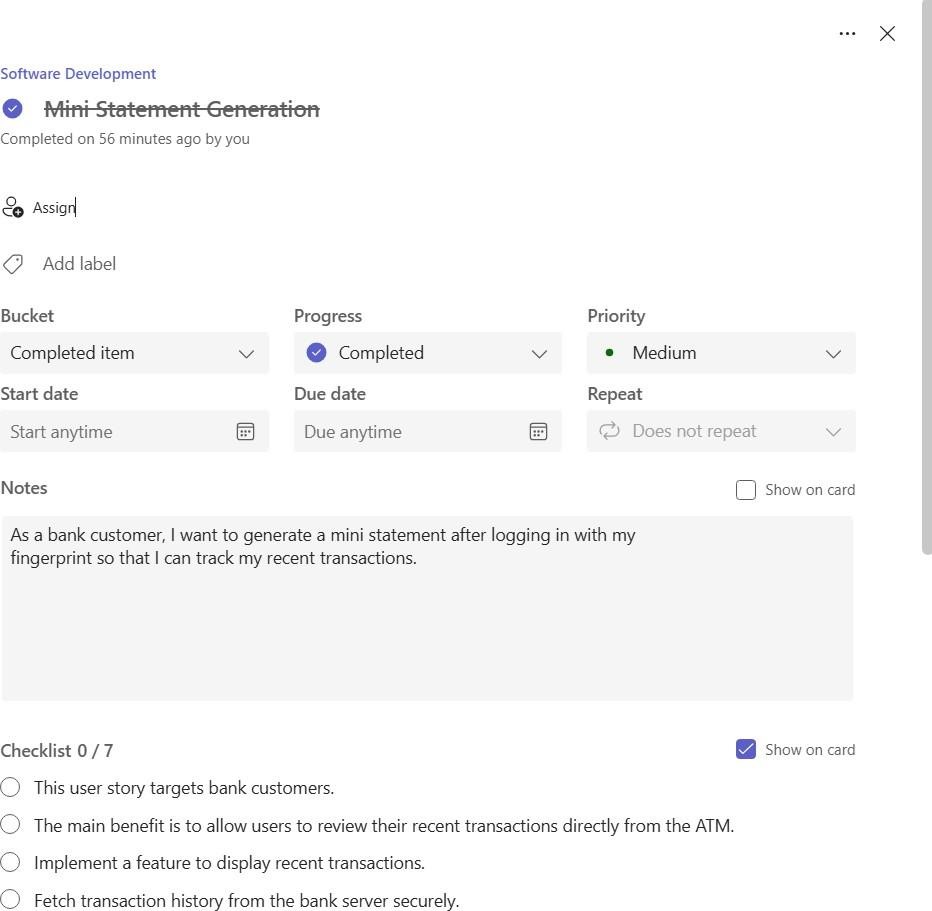
The goal of the second sprint is to assess the integration of fingerprint authentication, user feedback, and system performance to identify improvements for security, user experience, and transaction efficiency.

**Table 2.2 Detailed User Stories of sprint 2**

|  |  |
| --- | --- |
| S. No. | **Detailed User Stories** |
| US 3 | As a user, I want to receive real-time feedback on my fingerprint authentication status so that I can be sure the transaction process is going smoothly. |
| US 4 | As a user, I want to be notified if my fingerprint authentication fails so that I can take corrective action, such as re-registering my fingerprint. |
| US 5 | As an ATM provider, I want to monitor fingerprint authentication logs to ensure that the system is functioning effectively and securely. |



**Figure 2.8 Monitoring**

**Figure 2.9 Mini Statement Generation**

## Functional Document

* + - 1. Introduction

The CognitiveCare AI-driven project is designed to enhance the security and user experience of ATM transactions by replacing traditional PIN-based authentication with biometric fingerprint recognition. The system ensures secure and seamless access for authorized users, reducing the risks associated with PIN theft and forgotten credentials. By leveraging biometric authentication, the system provides users with an intuitive and reliable way to perform transactions at ATMs. A key focus is ensuring user privacy and data protection, making sure fingerprint data is encrypted and securely processed.

##### Product Goal

The primary goal of this project is to develop a **Fingerprint-Based ATM System** that provides secure, fast, and user-friendly access to ATM services through fingerprint authentication. The system aims to:Provide mood-based advice and coping strategies tailored to user input.

 **Provide secure access** to ATM services such as withdrawals, deposits, and balance checks through fingerprint recognition.

* **Enhance user convenience** by eliminating the need to remember PINs, offering a more reliable and seamless experience
* **Ensure data privacy** by securely storing and encrypting fingerprint data, protecting user information from unauthorized access.
  + - 1. Demography (Users, Location)

Users:

**Target Users:** Bank customers, including individuals who prefer biometric authentication over PINs for secure and easy access.

User Characteristics: Users of varying technical proficiency, with a focus on accessibility for older individuals or those unfamiliar with digital banking systems.

### Location:

**Target Location:** Global, with a focus on regions with high ATM usage, including urban areas with a strong focus on security and accessibility in banking services.

2.1.2.**4 Business Processes**

##### User Registration and Fingerprint Enrollment:

Users register their fingerprint for authentication at the ATM system.

The system ensures secure access by encrypting and storing the fingerprint data.

##### Fingerprint Authentication for Transactions:

The system verifies the fingerprint to grant access to ATM services like withdrawals, deposits, and balance checks.

Authentication is performed securely and quickly, reducing the risk of unauthorized access.

##### Monitoring and Logs:

Transaction logs and fingerprint authentication data are monitored to ensure the system’s performance and security.

Periodic reports are generated for security audits and performance analysis.

##### 2.2.2.5 Sprint Breakdown

🟦 Sprint 1: Security and UserRegistrationObjectives:

* Establish secure fingerprint data storage and communication protocols.
* Implement a registration process for fingerprint enrollment and user data collection.
* Provide Ensure compliance with privacy standards (e.g., GDPR) for biometric data

User Story:

* As a user, I want to know that my conversations with the chatbot are private and secure so that I can trust the platform.

Deliverables:

* Data encryption for storage and communication.
* User consent and privacy agreements for fingerprint data handling.
* Securecommunication protocols for fingerprint data transmission.
* Sprint 2: Mood Awareness and Personalized Coping Mechanism Objectives:
  + Enable users to authenticate via fingerprint for ATM transactions.
  + Implement real-time feedback for authentication success or failure
  + Provide transaction history logs and security notifications to users.

User Stories:

* + As a user, I want authenticate my fingerprint at the ATM so that I can perform secure transactions like withdrawals and deposits.
  + As a user, I want to receive real-time feedback when my fingerprint is authenticated or rejected so that I can take necessary actions.

Deliverables:

* + Fingerprint authentication system for ATM transactions.
  + Real-time feedback mechanism for users.
  + Transaction history and security alert system..

2.2.2.6 Authorization Matrix

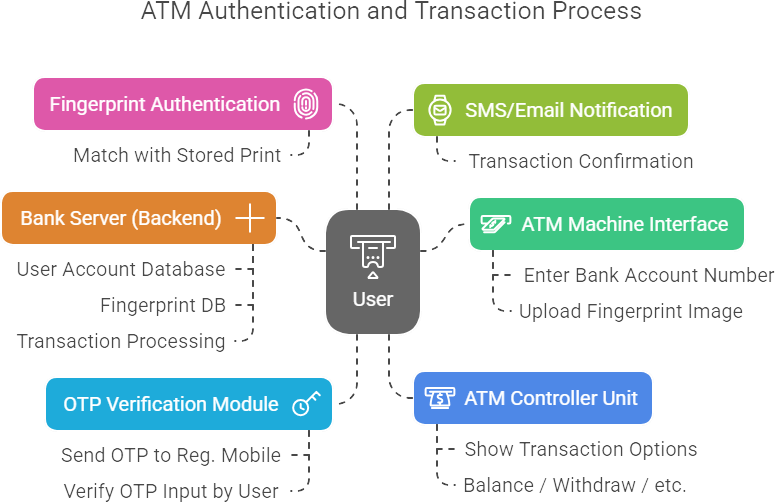
|  |  |
| --- | --- |
| **Role** | **Access Level** |
| Administrator | Full access to user data, transaction logs, fingerprint settings, system monitoring, and overall administration. |

|  |  |
| --- | --- |
| Bank Employee | Access to transaction history, user account details, and customer service tools. |
| ATM User | Access to perform transactions such as withdrawals, deposits, and balance checks using fingerprint authentication. |
| Guest User | Limited access to view general ATM information but unable to perform any transactions. |

**2.1.2.7 Assumptions :**

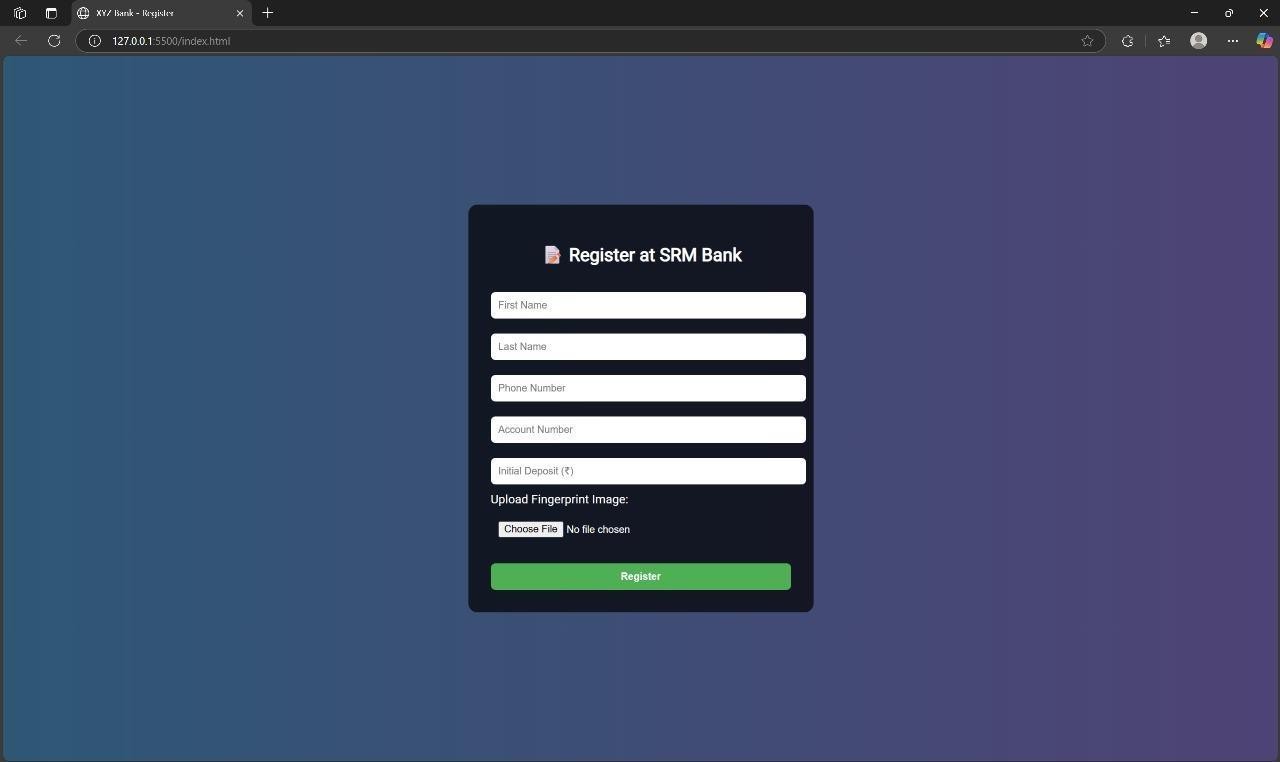
* Users will securely register and authenticate their fingerprints for smooth ATM transactions.
* Data security and privacy of biometric information are ensured throughout the system lifecycle
* The system is integrated with secure banking infrastructure and complies with industry standards.
* The product adheres to local and international data protection regulations, ensuring user privacy.

## Architecture Document

****

**Figure 2.2.3** Architecture Diagram

## UI Design

****

**Figure 2.2.4 UI Design**

## Functional Test Case

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Feature** | **Test Case** | **Steps to Execute Test Case** | **Expected Output** | **Actual Output** | **Status** | **More Information** |
| **Fingerprint Login** | **Login with registered finger** | **1. Click "Login with Fingerprint" → 2. Place registered finger on scanner** | **User successfully logged in** | **TBD** | **TBD** | **Integrate with biometric API** |
| **Fingerprint Login** | **Login with unregistered finger** | **1. Click "Login with Fingerprint" → 2. Place unregistered finger on scanner** | **Login failed with error message** | **TBD** | **TBD** | **Error: "Fingerprint not recognized"** |
| **Fingerprint Registration** | **Register new fingerprint** | **1. Login → 2. Navigate to "Settings" → 3. Click "Add Fingerprint" → 4. Scan finger** | **Fingerprint stored for future login** | **TBD** | **TBD** | **Store securely using encryption** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Fingerprint Removal** | **Remove existing fingerprint** | **1. Login → 2. Go to "Settings" → 3. Click "Remove Fingerprint"** | **Fingerprint removed** | **TBD** | **TBD** | **Confirm before removal** |
| **Fingerprint Retry Limit** | **Exceed retry limit** | **1. Attempt login with wrong finger multiple times (e.g., 5x)** | **Lockout message or cooldown** | **TBD** | **TBD** | **Prevent brute- force attempts** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Feature** | **Test Case** | **Steps to Execute Test Case** | **Expected Output** | **Actual Output** | **Status** | **More Information** |
|  |  |  | **triggered** |  |  |  |
| **Fingerprint UI Response** | **Scanner UI feedback** | **1. Attempt fingerprint scan (success/fail) → 2. Observe**  **UI response (LED, animation, etc.)** | **Proper visual feedback shown** | **TBD** | **TBD** | **Ensure accessibility and clarity** |

**Table 2.3** Detailed Functional Test Case

## 2.2.8 Sprint Retrospective

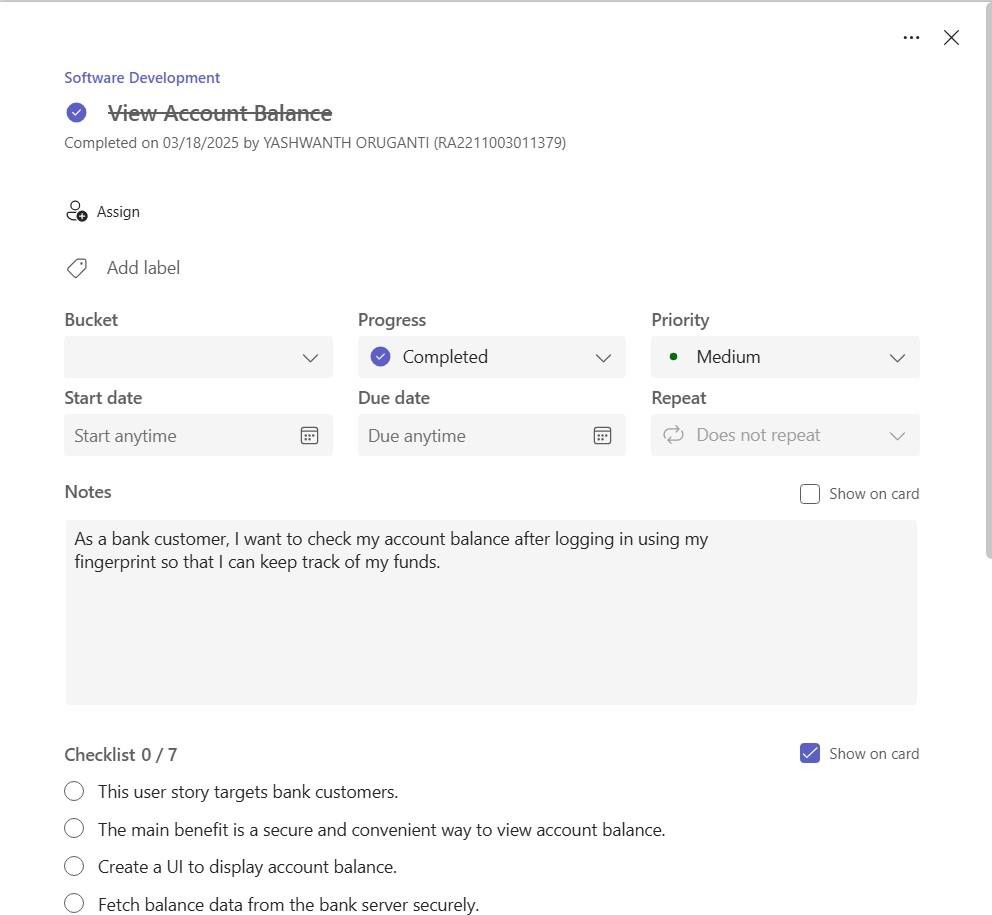
|  |  |  |  |
| --- | --- | --- | --- |
| **Liked** | **Learned** | **Lacked** | **Longed For** |
| **Fingerprint-based login added a secure and modern user experience** | **Real-time communication between biometric hardware and backend** | **UI feedback for partial or failed scans** | **AI-based fraud detection alerts** |
| **Clean component structure using React for user dashboard and status updates** | **State management using React context for session tracking** | **Better error boundaries around hardware- dependent components** | **Integration of biometric-based transaction logs** |
| **Smooth coordination between hardware and frontend team during sprint** | **Hardware abstraction and communication protocols (e.g., via Serial/USB)** | **Mock tools for fingerprint input testing** | **Biometric simulator for local development** |
| **Backend successfully handled authentication flow using fingerprint data** | **Encrypting biometric data before transmission and storage** | **Responsive UI scaling for ATM touchscreens** | **Custom themes and multi-language support** |

* 1. **Sprint 3**
     1. **Sprint Goal with User Stories of Sprint 3**

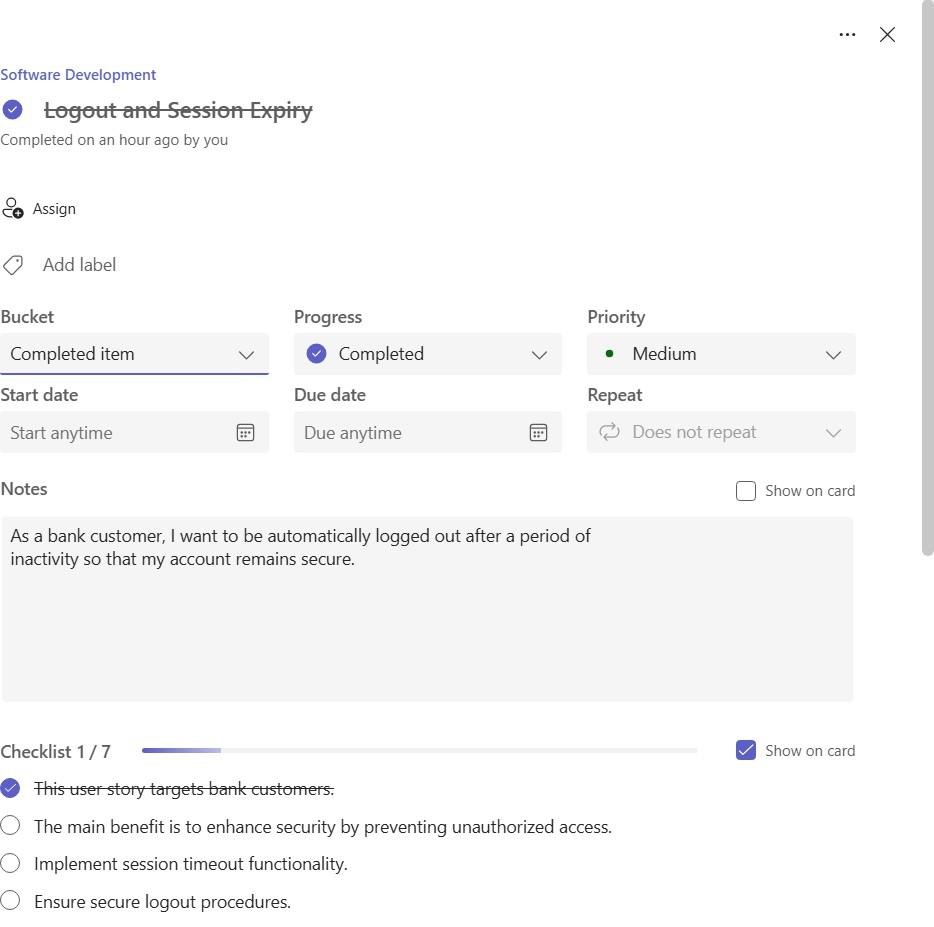
The goal of Sprint 3 was to implement and test the fingerprint authentication module, ensuring accurate user verification and secure access to ATM functionalities.

##### Table 2.3 Detailed User Stories of sprint 3

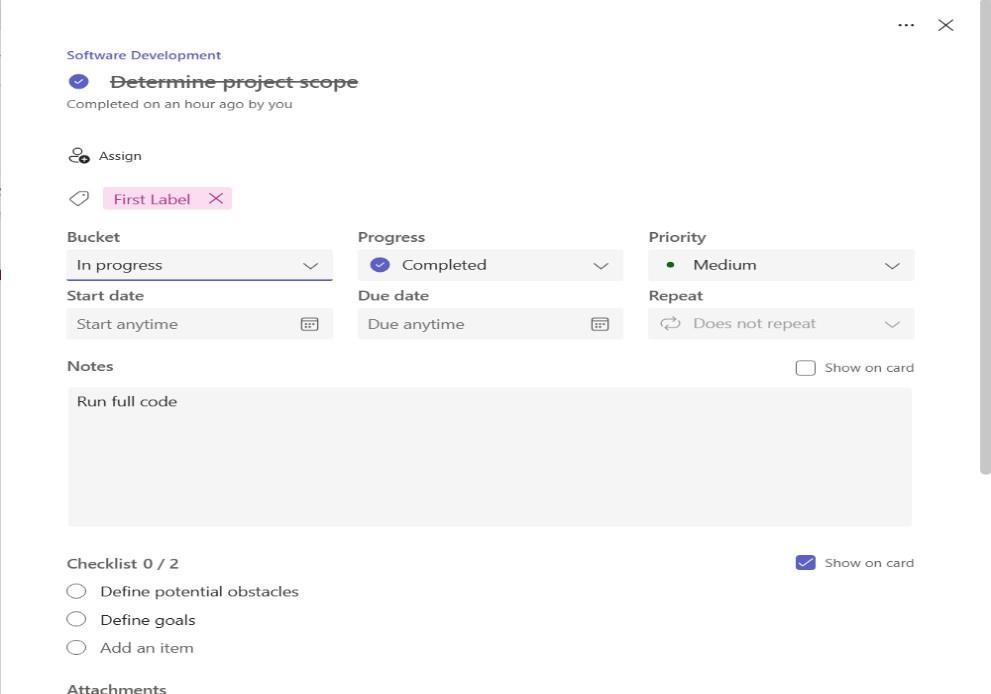
|  |  |
| --- | --- |
| **S.N**  **O** | **Detailed User Stories** |
| US 6 | As a user, I want to log in using my fingerprint so that I can securely access my account without needing a PIN. |
| US 7 | As a bank admin, I want to verify that fingerprint data is correctly stored and matched so that unauthorized users are prevented from accessing the ATM. |



**Figure 2.3.1 Account** Balance



**Figure 2.3.2** Logout



**Figure 2.3.3 project scope**

## Functional Document

#### Introduction

The Fingerprint-Based ATM System is designed to enhance the security of ATM transactions by replacing traditional PIN-based authentication with biometric fingerprint recognition. This system ensures only the rightful account holder can access ATM services, reducing fraud and increasing user convenience. The solution integrates fingerprint scanners with existing ATM software and databases to securely match biometric data during login and transaction processing.

#### Product Goal

The main goal of the project is to design and deploy an ATM system that uses fingerprint authentication to provide secure, fast, and user-friendly access to banking services. The objectives are:

* + - * + Provide fingerprint-based user authentication to eliminate the need for PINs
        + Improve ATM security by preventing unauthorized access.
        + Enable seamless integration with existing banking databases.
        + Ensure accuracy, speed, and reliability in fingerprint matching.

#### Demography (Users, Location)

##### Users:

* + - * + Target Users: Bank account holders who use ATMs.
        + User Characteristics: Adults aged 18–60 with basic banking knowledge and regular ATM usage.

##### Location:

* + - * + Target Location Urban and semi-urban areas with a high concentration of ATM usage and digital banking adoption.

#### Business Processes

Key business processes include:

* + - * + **User Registration:** Fingerprints are scanned and linked to the user’s ban account during in-branch registration.
        + **Authentication at ATM:** Fingerprints are scanned and matched against stored biometric data to authenticate the user.
        + **Transaction Processing:** Upon successful fingerprint match, the user can perform standard ATM operations (withdrawal, balance check, etc.).
        + **Admin Monitoring:** Upon successful fingerprint match, the user can perform standard ATM operations (withdrawal, balance check, etc.).

#### Sprint Breakdown

🟦 **Sprint 3: Chatbot Refinement and Emotional Responsiveness**

### Objectives:

* + - * + Integrate fingerprint scanner hardware with the ATM system.
        + Develop software to capture and match fingerprints against the user database.
        + Ensure secure storage of biometric data using encryption.

##### User Story:

* + - * + As a user, I want to log in using my fingerprint so that I can securely access my account without needing a PIN.

##### Deliverables:

* + - * + Fingerprint capture and verification interface.
        + Encrypted biometric database.
        + User login via fingerprint and fallback security mechanism.

**Sprint 4: Beta Release & Feedback Integration Objectives:**

* + - * + Enable secure ATM transactions post-authentication.
        + Implement fail-safe mechanisms for false rejections or scanner issues.
        + Collect feedback on usability and accuracy.

##### User Story:

* + - * + As a user, I want to withdraw money using fingerprint login so that I can avoid remembering a PIN.

##### Deliverables:

* + - * + Functional ATM transactions after fingerprint login.
        + Error handling and fallback authentication mechanism (e.g., OTP).
        + Usage logs and feedback interface.

#### Authorization Matrix

|  |  |
| --- | --- |
| **Role** | **Access Level** |
| Bank Admin | Full access to system configuration, biometric data, and transaction logs. |
| ATM Technician | Access to system diagnostics and maintenance tools only. |
| Registered User | Access to system diagnostics and maintenance tools only. |
| Guest User | No access – fingerprint registration required. |

* + - 1. **Assumptions**
         * All fingerprint data will be stored securely using industry-standard encryption.
         * The scanner hardware will function reliably under various environmental conditions.
         * Network connectivity is required to verify user details from the central bank database.
         * Users have already registered their fingerprint with the bank.

# CHAPTER 3 RESULTS AND DISCUSSION

## Project Outcomes

The development of the Fingerprint-Based ATM System adhered to core principles of Software Engineering Process Management (SEPM), ensuring that every phase from requirements gathering to deployment followed a structured and methodical approach. The main goal was to design a user-centric ATM system capable of providing secure and convenient financial transactions through fingerprint authentication.

The requirements engineering phase was crucial in defining the core functionalities of the system. The team conducted user interviews and stakeholder feedback sessions to identify the key expectations, which translated into the system’s functional and non-functional requirements. These were captured in the Software Requirements Specification (SRS), which served as the foundation for all subsequent development stages.

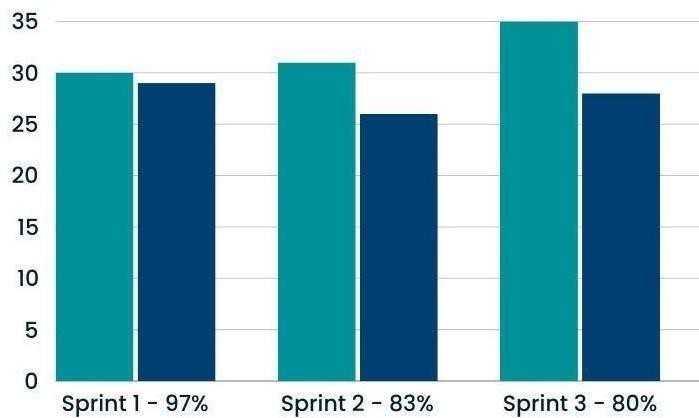
During the system design phase, architectural decisions focused on modularity and scalability. The decision to use microservices architecture ensured that the system would be flexible for future upgrades. The design separated concerns between authentication services, transaction processing, and security features, allowing for easy future integration and maintenance.

The system was developed using modern technologies, including ReactJS for the front-end and NodeJS/Flask for the back-end. Secure fingerprint authentication protocols were implemented to ensure data protection. Version control using Git ensured collaboration and traceability. Unit testing and integration testing were rigorous, confirming that each component functioned as intended and identifying any edge cases, such as user authentication failure scenarios or transaction discrepancies.

Upon deployment in a test environment, the system underwent evaluation for performance, security, and usability. Key performance indicators (KPIs) such as system uptime, average transaction processing time, and user satisfaction were measured. The system was found to be functionally stable and effective in performing its core functions, such as fingerprint authentication, transaction management, and real-time notifications. The integration of error handling, token-based authentication, and encryption mechanisms demonstrated the robustness and security of the system.

In conclusion, the Fingerprint-Based ATM System demonstrated the power of iterative development, requirement traceability, and continuous feedback in delivering a high-quality software solution. The project not only fulfilled its core mission of enhancing ATM security but also provided valuable insights into how disciplined software engineering processes can improve real-world systems.

## Committed Vs Completed User stories

****

**3.2 Figure Committed Vs Completed User stories**

# CHAPTER 4

**CONCLUSION & FUTURE ENHANCEMENTS**

### Conclusion

The **Fingerprint-Based ATM System** project represents a major advancement in leveraging biometric technology to enhance the security and convenience of ATM transactions. The system replaces traditional PIN-based authentication with fingerprint recognition, providing a seamless and secure user experience. Throughout the development and testing phases, the system demonstrated its potential to streamline ATM operations while offering enhanced protection against identity theft and fraud. By integrating modern security protocols and encryption techniques, the system ensures that users’ biometric data is protected, fostering trust and confidence.

The system’s user-centric design, which includes fingerprint enrollment, real-time authentication, and transaction processing, ensures a smooth and intuitive interface. Importantly, the solution’s modularity allows for future scalability, ensuring that additional features, such as multi-factor authentication or support for other biometric methods, can be integrated easily. Although not a substitute for more complex banking systems, the **Fingerprint-Based ATM System** acts as an efficient and secure alternative to traditional PIN- based systems, particularly useful for users seeking fast and reliable ATM services. Feedback during the testing phase highlighted the system’s effectiveness in delivering secure and quick transactions, with users appreciating the ease of access and reduced risk of PIN theft.

Overall, the **Fingerprint-Based ATM System** meets its core objective of providing a more secure and user-friendly banking experience. It demonstrates the potential for biometric technology in financial systems, offering a glimpse into the future of secure and seamless transaction systems that can be expanded to other banking and financial services.

### Future Enhancements

While the **Fingerprint-Based ATM System** has met its foundational objectives of enhancing security and convenience, there is significant room for improvement and expansion. One of the primary areas for future development is improving the fingerprint recognition technology by incorporating advanced machine learning models that can offer more accurate identification, even in cases of partial or worn fingerprints. By enhancing the accuracy of the fingerprint scanning process, the system can provide an even more robust and reliable authentication method.

Additionally, multimodal authentication could be integrated into the system to provide users with a choice of using fingerprints, voice recognition, or facial recognition for authentication. This would provide greater flexibility and ensure the system is accessible to a wider range of users, including those with conditions that may affect their fingerprints. Another possible enhancement is the integration of real-time fraud detection that monitors for unusual transaction patterns, offering an added layer of security by alerting users and banks to potential fraudulent activities.

The user experience could also be further improved by providing customized transaction summaries or account balance checks after each transaction. This feature could allow users to track their spending habits and receive personalized notifications about their financial status, promoting better financial management. Mobile integration could also be introduced to allow users to perform transactions or check their balance through a mobile app with fingerprint- based authentication, expanding the usability of the system.

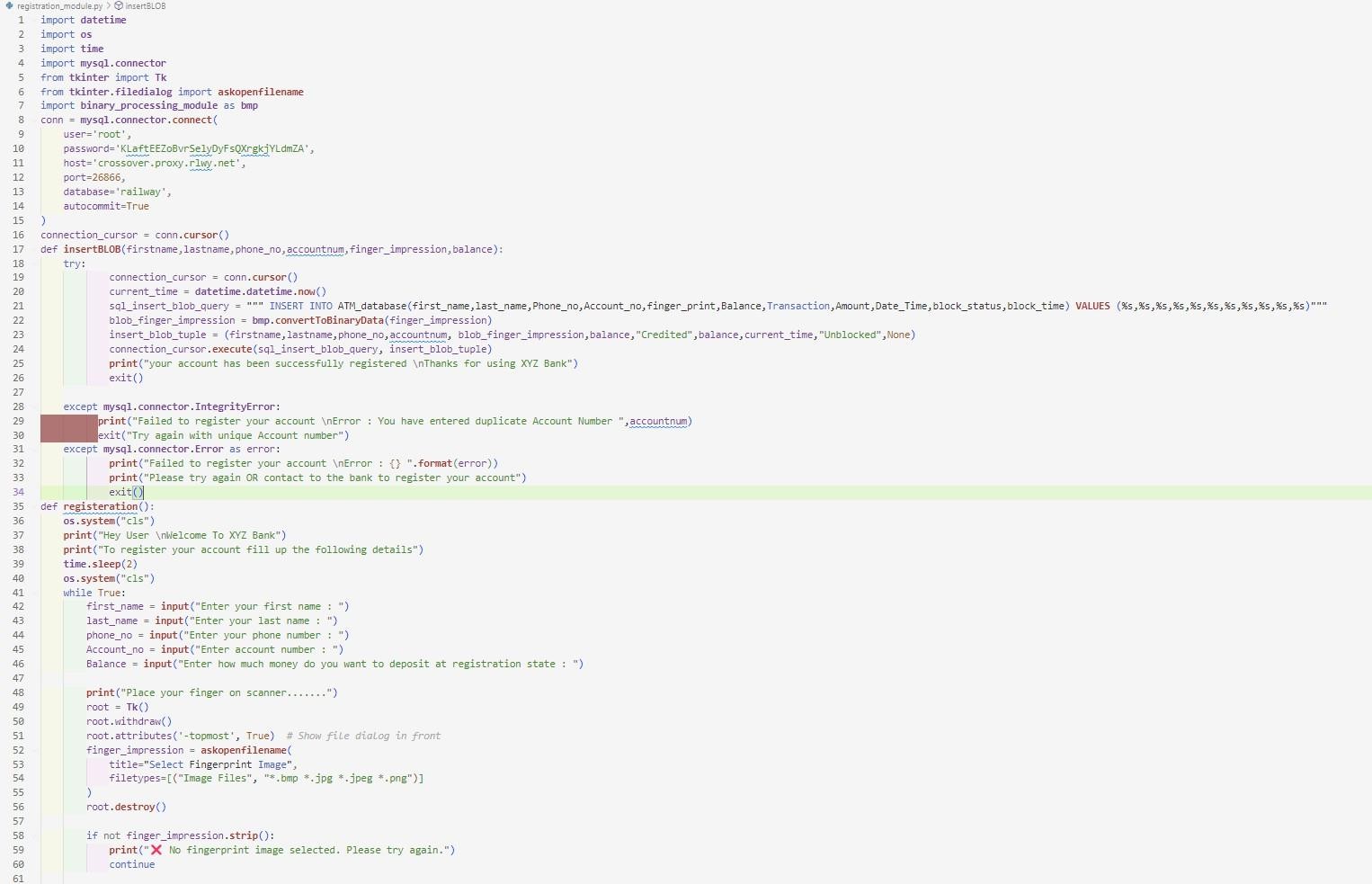
To further enhance the system’s functionality, it could be integrated with cloud-based analytics to monitor user interaction patterns and optimize the ATM interface. This data could help banks understand usage trends, allowing for more personalized services and the identification of high- demand features. Moreover, cloud integration could enable easier updates, ensuring that the ATM system remains up-to-date with the latest security patches and features without requiring physical upgrades at each ATM.

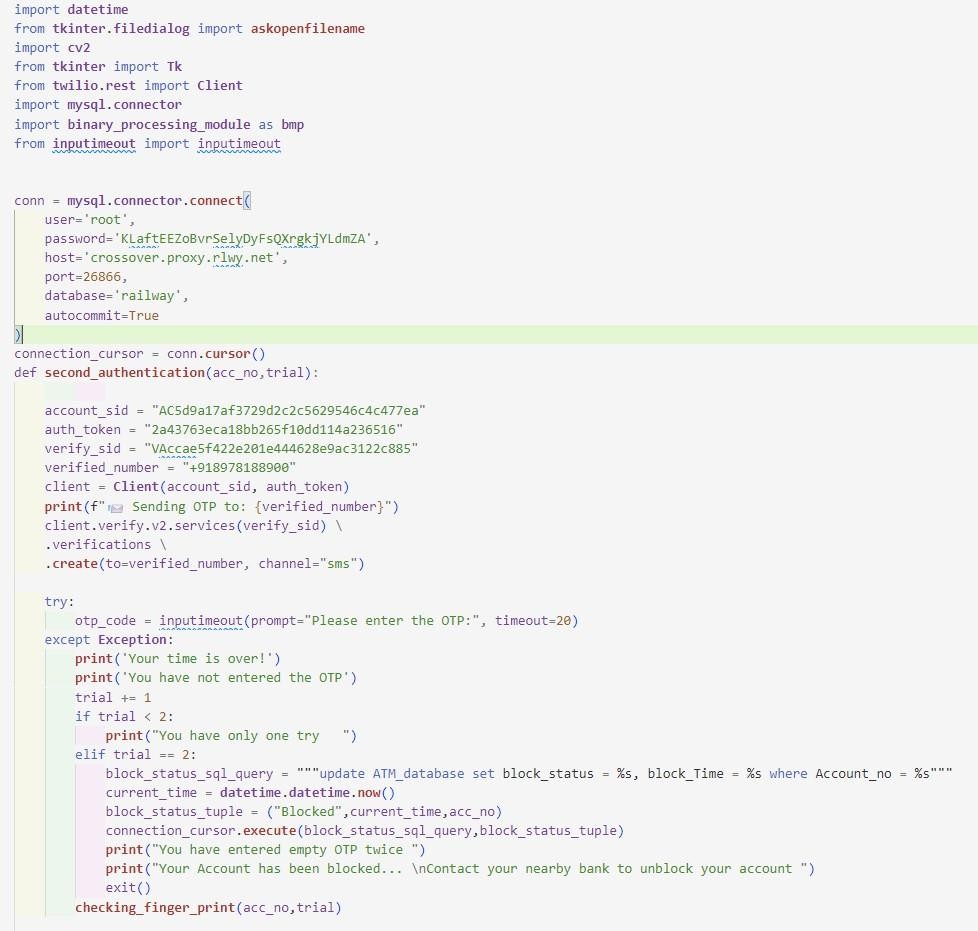
# A. SAMPLE CODING

**ATM.py**

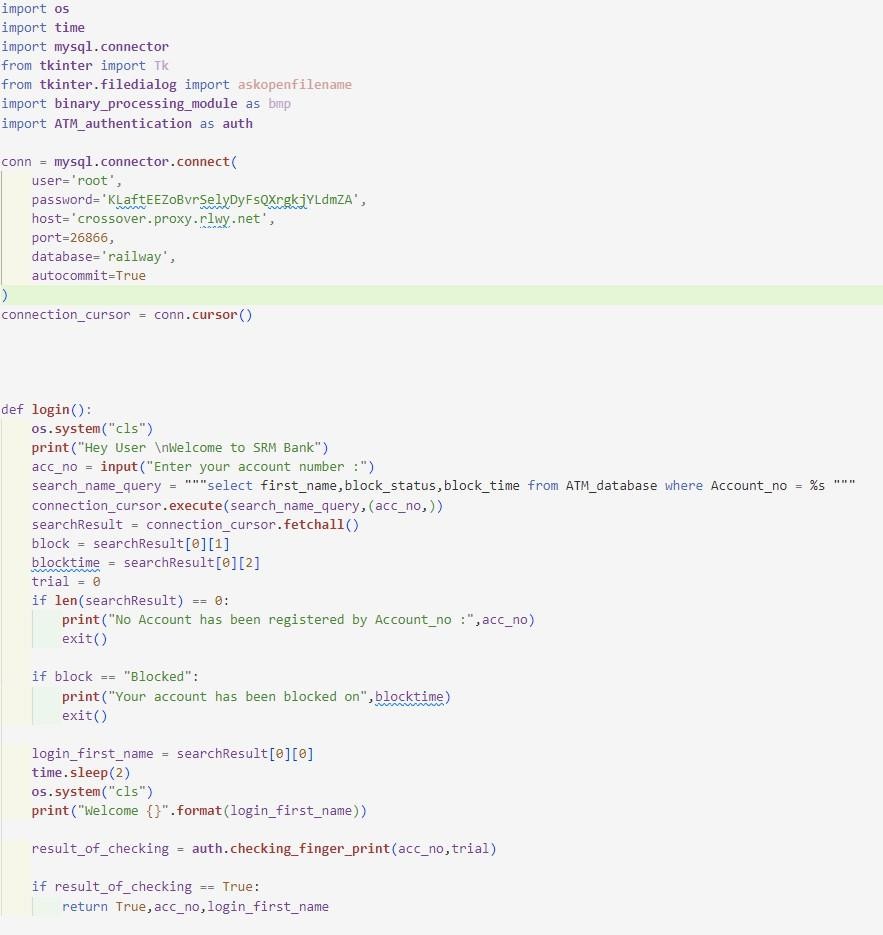
****

**registeration**.py



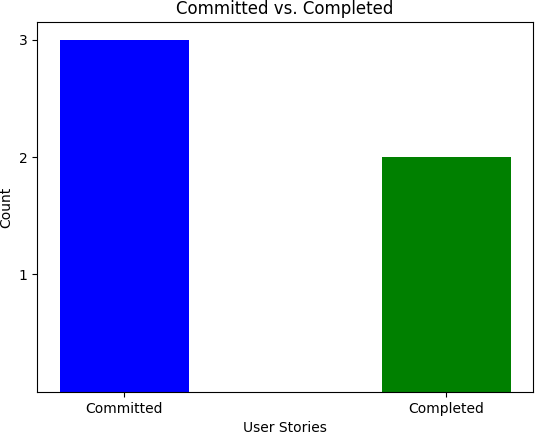
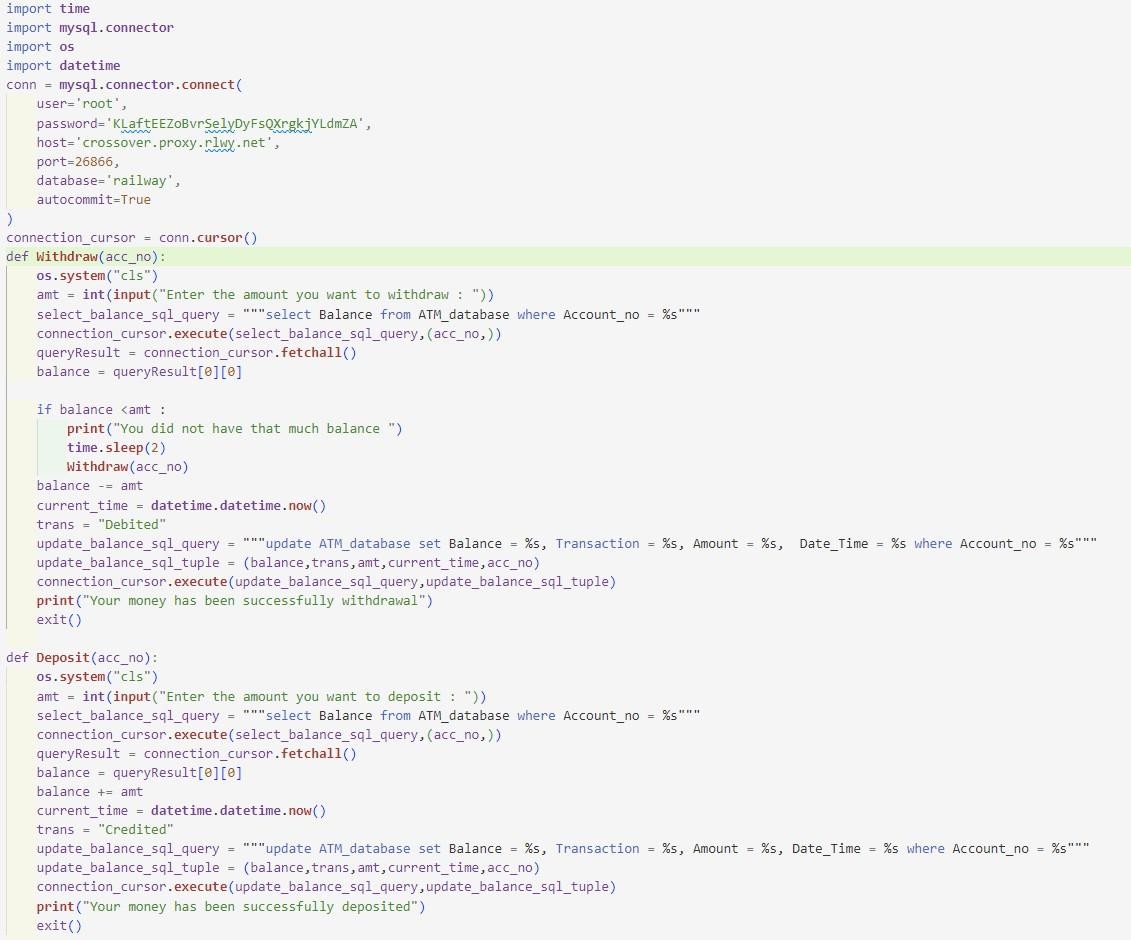
**Authentication.py**

**Login\_module.py**

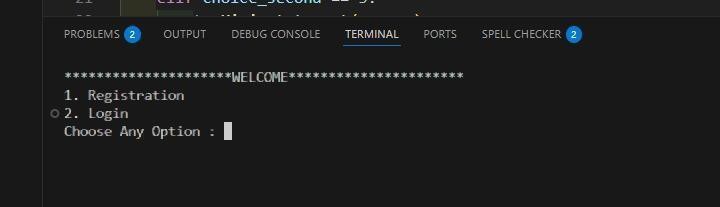
****

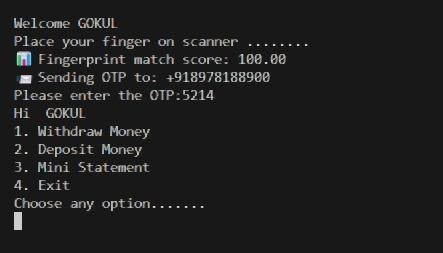
**Online database- Railwaydb**

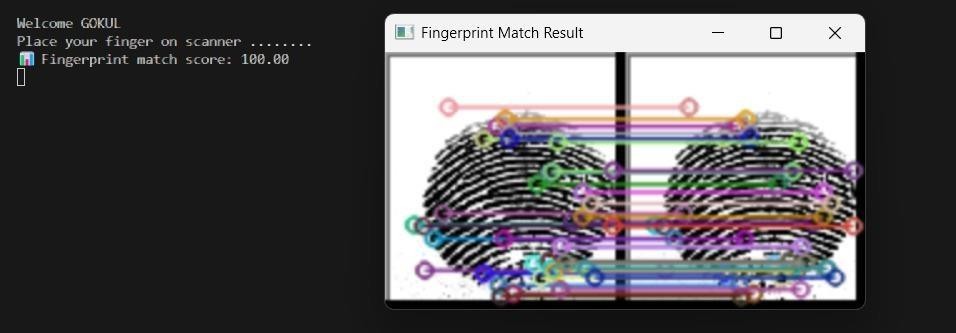
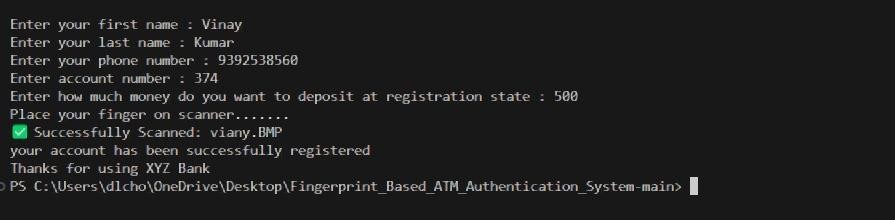
**Transaction**



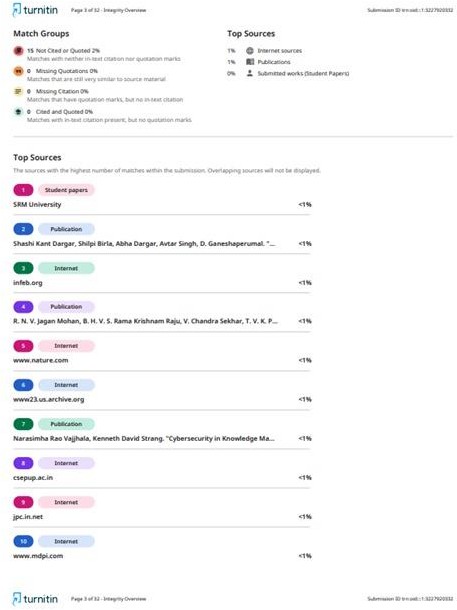
**Result :-**

****

****



**Plagiarism**

****