

Requirements Specification (SRS) Document

Fingerprint Based ATM System

1. Introduction

1.1 Purpose:

This is the Outlines the hardware and software requirements for implementing a fingerprint technology-based ATM system. It provides detailed specifications for both hardware and software components to ensure a secure and efficient system for managing financial transactions.

- **Actor**

1.User : The primary actor who interacts with the ATM system to perform financial transactions using fingerprint authentication.

2. System Administrator: Responsible for managing and maintaining the ATM system, including configuring system settings and managing user accounts.

3. Admin : Responsible for developing and implementing the software components of the ATM system, including the user interface and authentication softwareTest the functionality and usability of the ATM system to ensure it meets user requirements and expectations.

- **Hardware Actors:**

1. ATM Machine: The physical hardware device that dispenses cash and performs financial transactions. It includes components such as the card reader, cash dispenser, screen, keypad, and fingerprint scanner.

2. Fingerprint Scanner: A hardware device responsible for capturing and processing fingerprint images for authentication purposes. It interfaces with the ATM system to provide fingerprint authentication functionality.

1.2 Scope:

This document covers the following aspects of the fingerprint technology-based ATM system:

- Hardware components: fingerprint scanner, ATM machine, display screen, keypad, card reader, secure vault, connectivity modules (Wi-Fi or Ethernet), and printer.

- Software components: operating system, ATM software, database management software, authentication software, leave accounting software, reporting software, system administration software, and security software.

1.3 Objectives :

The objectives of the Fingerprint-Based ATM System project are to:

1. Enhance security through fingerprint biometrics.

2. Improve user experience by eliminating the need for cards and PINs.

3. Reduce fraud incidents at ATMs.
4. Ensure widespread adoption of secure authentication technology.
5. Enable efficient transaction processing.
6. Ensure scalability and interoperability with existing infrastructure.

2. User Requirements:

The following user requirements have been identified for the fingerprint technology-based ATM system:

- Fast and secure transaction processing
- Easy and intuitive user interface
- Multilingual support for international users
- Ability to handle multiple currencies
- Support for various payment methods (cash, debit cards, credit cards, mobile wallets, etc.)
- Real-time transaction monitoring and fraud detection
- Compliance with regulatory requirements and data protection laws

3. Functional Requirements:

The following functional requirements have been identified for the fingerprint technology-based ATM system:

- Fingerprint scanner: The fingerprint scanner should be able to capture and process high-quality fingerprint images, with a resolution of at least 500 dpi. It should be able to store up to 10,000 fingerprint templates and support multiple fingerprint matching algorithms.
- ATM machine: The ATM machine should be able to handle multiple transactions simultaneously, with a throughput of at least 30 transactions per minute. It should have a user-friendly interface, with a large and clear display screen and a keypad for inputting commands and numbers.
- Display screen: The display screen should have a resolution of at least 1280 x 768 pixels, with a brightness of at least 300 nits. It should support multiple languages and font sizes, and have a touch-sensitive interface for easy navigation.
- Keypad: The keypad should have a large and clear layout, with easy-to-press buttons and a backlight for low-light conditions. It should support multiple languages and input methods, including numeric, alphabetic, and symbolic characters.
- Card reader: The card reader should be able to read various types of cards, including debit cards, credit cards, and mobile wallets. It should support contactless and contact-based card reading, with a read range of at least 4 cm.
- Secure vault: The secure vault should be able to store large amounts of cash securely, with a capacity of at least 10,000 notes. It should have a locking mechanism that requires a unique key or biometric authentication to open.
- Connectivity modules: The connectivity modules should be able to provide high-speed and reliable connectivity to the ATM system, with a bandwidth of at least 10 Mbps. They should support multiple communication protocols, including Wi-Fi, Ethernet, and GPRS.

- **Printer:** The printer should be able to print receipts and transaction reports quickly and accurately, with a print speed of at least 150 mm/s. It should support multiple languages and font sizes, and have a paper capacity of at least 200 sheets.

4. Non-Functional Requirements:

The following non-functional requirements have been identified for the fingerprint technology-based ATM system:

- **Reliability:** The system should be highly reliable and available, with a uptime of at least 99.9%. It should have redundant components and backup systems to ensure uninterrupted service in case of failures.
- **Security:** The system should provide strong security features, such as encryption, access control, and fraud detection. It should be compliant with regulatory requirements and data protection laws, and have a secure communication protocol.
- **Usability:** The system should have an intuitive and user-friendly interface, with clear and concise instructions. It should support multiple languages and input methods, and have a simple and intuitive navigation structure.
- **Maintainability:** The system should be easy to maintain and upgrade, with clear documentation and support resources. It should have a modular and scalable architecture, with a separation of concerns between hardware and software components.
- **Performance:** The system should provide fast and efficient transaction processing, with a response time of less than 3 seconds. It should have a high throughput and a low latency, and support multiple concurrent transactions.
- **Compatibility:** The system should be compatible with various operating systems and software applications, and have a standardized interface for easy integration with other systems. It should support multiple currencies and payment methods, and have a flexible configuration and customization options.

5. Constraints:

The following constraints have been identified for the fingerprint technology-based ATM system:

- **Budget:** The system should be cost-effective and affordable, with a total budget of less than----. It should have a low total cost of ownership, with minimal maintenance and operating costs.
- **Space:** The system should be compact and space-efficient, with a footprint of less than 1 square meter. It should have a low power consumption and a low noise level, to minimize disturbance in the surrounding environment.
- **Environment:** The system should be able to operate in various environmental conditions, such as high humidity, low temperature, and vibration. It should have a rugged and durable design, with a long lifespan and a low failure rate.
- **Compliance:** The system should be compliant with regulatory requirements and data protection laws, such as PCI DSS, GDPR, and FCA. It should have a secure communication protocol and a strong encryption algorithm, to protect sensitive data and prevent fraud.

-

6. Verification and Validation:

The following verification and validation activities will be performed to ensure the compliance and effectiveness of the fingerprint technology-based ATM system:

- Functional testing: The system will be tested for its functional requirements, such as fingerprint scanning, transaction processing, and cash dispensing.
- Non-functional testing: The system will be tested for its non-functional requirements, such as reliability, security, usability, maintainability, performance, and compatibility.
- Regulatory compliance testing: The system will be tested for its compliance with regulatory requirements and data protection laws, such as PCI DSS, GDPR, and FCA.
- User acceptance testing: The system will be tested by actual users, to ensure its usability and effectiveness in real-world scenarios.
- System integration testing: The system will be tested for its integration with other systems, such as HRMS, payroll systems, and accounting systems.

7. Change Management:

The following change management processes will be followed to ensure the timely and effective implementation of the fingerprint technology-based ATM system:

- Change request: A change request will be submitted by the user or the system administrator, specifying the nature and the reason for the change.
- Change evaluation: The change request will be evaluated by the system architect, to determine its feasibility, impact, and priority.
- Change approval: The change request will be approved by the system manager, to authorize the change and allocate the necessary resources.
- Change implementation: The change will be implemented by the system administrator, following the standard change management procedures and documentation.
- Change verification: The change will be verified by the user or the system administrator, to ensure its compliance and effectiveness.
- Change closure: The change will be closed by the system architect, to document the change and update the system requirements and specifications.

8. Configuration Management:

The following configuration management processes will be followed to ensure the consistency and accuracy of the fingerprint technology-based ATM system:

- Configuration identification: The system components and their configurations will be identified and documented, using a configuration management tool.
- Configuration control: The system configurations will be controlled and maintained, using a configuration management process.

- Configuration status accounting: The system configurations will be tracked and audited, using a configuration management database.
- Configuration baselining: The system configurations will be baselined and versioned, using a configuration management methodology.
- Configuration audit trails: The system configurations will be audited and traced, using a configuration management audit trail.

9. Project Management:

The following processes will be followed to ensure the timely and effective implementation of this project :

- Project initiation: The project will be initiated by the project sponsor, to define the project objectives, scope, and resources.
- Project planning: The project will be planned by the project manager, to define the project schedule, budget, risks, and deliverables.
- Project execution: The project will be executed by the project team, to implement the project plan and deliver the project outputs.
- Project monitoring and controlling: The project will be monitored and controlled by the project manager, to manage the project progress, issues, and changes.
- Project closure: The project will be closed by the project manager, to evaluate the project outcomes, lessons learned, and recommendations for improvement.

10. Documentation:

The following documentation will be generated and maintained throughout the project lifecycle:

- System requirements specification (SRS) document
- Functional and non-functional requirements lists
- Change request forms
- Configuration management tool and database
- Project management plan and schedule
- Project status reports and issue logs
- User manuals and training materials
- Technical manuals and maintenance guides
- Security policies and procedures
- Regulatory compliance certificates and reports
- System architecture