“Project Report”

Course Code:	Course Title:
CSE321	System Analysis & Design

Submitted To : Ms. Most. Hasna Hena

Department of ‘CSE’
Daffodil International University

Submitted By :

Name :	SID:
Mahfujur Rahaman	221-15-4691
S.M. Sajjad Hossain Jim	221-15-5364
Fariha Rahman Aisharjo	221-15-5604

Section : J

Department of ‘CSE’

Submitted Date : 23/ 05/ 2024

Introduction:

The fingerprint is arguably a person's most unique physical characteristic. While humans have had the innate ability to recognize and distinguish different fingerprints for millions of years, computers are just now catching up… The twist of this software is that it can pick someone's fingerprint out of a crowd, extract that fingerprint for the rest of the scene and compare it with a database full of stored images. For this software to work, it must know what a basic fingerprint looks like. Fingerprint recognition software is based on the ability to first recognize fingerprints, which is a technological feat, and then measure the various features of each fingerprint. A fingerprint is the feature pattern of one finger. It is believed with strong evidence that each fingerprint is unique. Each person has his fingerprints with permanent uniqueness. So, fingerprints have been used for identification and forensic investigation for a long time. A fingerprint is composed of many ridges and furrows.

What is Fingerprint Authentication:

The fingerprint authentication problem can be grouped into two sub-domains. One is fingerprint verification, and the other is fingerprint identification. In addition, different from the manual approach for fingerprint authentication by experts, the fingerprint authentication here is referred to as FAA (Fingerprint Authentication in ATM), which is program-based. Fingerprint verification is to verify the authenticity of one person by his fingerprint. The user provides his fingerprint together with his identity information like his PIN-CODE. The fingerprint verification system retrieves the fingerprint template according to the PIN-CODE and matches the template with the real-time acquired fingerprint from the user. Usually, it is the underlying design principle of AFAS (Automatic Fingerprint Authentication System). Fingerprint identification is to specify one person's identity by his fingerprint(s). Without knowledge of the person's identity, the fingerprint identification system tries to match his fingerprint(s) with those in the whole fingerprint database. It is especially useful for criminal investigation cases. It is the design principle of AFIS (Automatic Fingerprint Identification System). However, all fingerprint recognition problems, either verification or identification, are ultimately based on a well-defined representation of a fingerprint.

Step in solution:

Biometrics can be used to identify physical and behavioural characteristics of user fingerprints. There are many biometric devices like iris detection, face recognition, and fingerprints. In our Project, we are using fingerprint biometrics. Users' fingerprints are scanned using biometric traits and stored in a database. All fingerprints have unique characteristics and patterns. A normal fingerprint pattern is made up of lines and spaces. These lines are called ridges while the spaces between the ridges are called valleys. Fingerprint biometrics are easy to use, cheap and most suitable for everyone. Characteristics of fingerprints vary from person to person. Fingerprints are the unique identity of the user. Data of a fingerprint is stored in a database using the enrolment process through the Bank. Banks provide authentication to the customer that can be accessed while performing the transaction process. If a fingerprint match is found in the database, then a transaction takes place. After verification, if the fingerprint does not match transaction will be cancelled. Using fingerprint-based ATM system user can make secure transaction. Fingerprint verification is to verify the authenticity of one person by his fingerprint and PIN code and Fingerprint identification is by matching the information of the user such as pin code and fingerprint matching. Basically, we can explain the complete Fingerprint based ATM system in two phases:

1) Enrolment Phase
2) Authentication phase.

Requirements Collection:

Security is a critical concern in modern life, particularly in the communication of sensitive information. Current ATM systems, which often use Triple Data Encryption Standard (3DES), face several issues such as vulnerability to differential attacks and performance limitations.

Problems with current ATM networks include card fraud, use of card duplicators, card sharing, and the potential for PINs to be shared or recorded by hidden cameras. This paper proposes a more secure and energy-efficient ATM banking system that addresses these issues by incorporating biometric authentication. The system requires three verifications: a unique 6-digit code, a fingerprint scan, and a 4-digit PIN. The fingerprint recognition, enabled by a fingerprint sensor, enhances security due to the stability and reliability of fingerprint characteristics.

The system uses embedded technology for improved safety, reliability, and user-friendliness. Key components include a fingerprint module, motor, motor driver, ATMEGA 16 microcontroller, LCD, and keypad. The LCD displays outputs and assists in debugging, while the keypad allows users to input data. The ATMEGA 16 microcontroller supports various features such as programmable flash memory, EEPROM, SRAM, and multiple I/O lines, making it suitable for this application. Fingerprint sensors capture and process fingerprint images to create biometric templates for secure matching. The system collects customer fingerprints and mobile numbers during account setup, ensuring only authorized users can access the ATM. This design leverages the robustness of fingerprint recognition to protect against card theft and unauthorized access, enhancing overall ATM security.

Study of the related system:

To design and implement a fingerprint-based ATM system, it's essential to study existing systems and technologies that have been successfully deployed in similar contexts. This includes understanding the components, architecture, security features, user interfaces, and operational challenges of current biometric authentication systems used in banking and other industries.

1. Existing Biometric ATM Systems

A. Citibank Biometric ATMs

Citibank has implemented biometric ATMs that use fingerprint and palm vein recognition for user authentication. Multi-factor authentication combining biometric data with card and PIN ensures high security. Enhanced security with user-friendly interfaces, reducing the need for memorizing PINs

B. Hitachi's Finger Vein ATMs

Hitachi's finger vein authentication system is used in ATMs primarily in Japan. Vein patterns are unique and difficult to replicate, offering high security against fraud. Fast and reliable authentication process, improving user satisfaction.

C. Wells Fargo Card-Free ATMs

Wells Fargo offers card-free ATMs that allow users to authenticate via their mobile banking app, often combined with biometric verification like fingerprint or facial recognition on the mobile device. Combines mobile banking app security with biometric verification. Convenient for users who prefer not to carry their ATM cards.

Stakeholder Identification:

To provide a detailed and specific stakeholder analysis for the fingerprint-based ATM system, let's break down the stakeholders into categories and address their specific roles, needs, and expectations.

Bank Management

Roles:

- Decision-makers who approve the project.
- Allocate budget and resources.
- Oversee strategic alignment with business goals.

Needs:

- Clear ROI and cost-benefit analysis.
- Detailed project plan and timeline.
- Risk assessment and mitigation strategies.

Expectations:

- Enhanced security measures leading to reduced fraud.
- Improved customer satisfaction and loyalty.
- Timely and within-budget project completion.

Regulatory Authorities

Roles:

- Ensure the system complies with data protection and privacy laws.

- Conduct audits and evaluations to enforce standards.

Needs:

- Detailed compliance reports and system documentation.
- Evidence of data security measures.
- Regular updates on system performance and security incidents.

Expectations:

- Full compliance with relevant laws and regulations.
- Regular audit reports and transparency.
- Prompt notification of any data breaches or security issues.

Vendors and Suppliers

Roles:

- Supply hardware (fingerprint sensors, microcontrollers) and software.
- Provide technical support and maintenance services.

Needs:

- Clear technical specifications and requirements.
- Timely payments and contracts.
- Long-term partnership and collaboration.

Expectations:

- Clear communication and timely feedback.
- Detailed specifications to meet project requirements.
- Continued business and support opportunities.

Gathering Information:

Use of Card:

Name	Number	Problem
Ajoad Abid	1745134332	Transection errors
Nazmul Islam	1845855388	Failed to get card back
Fardin Khan	1552406604	limited acceptance of card
Fuad naser	1777329456	Stolen and face financial loss.
siam shanto	1782380552	Transection errors
Fahim Zaman	17846281673	Failed to get card back
shoukhin Ahmed	1738684893	Failed to get card back

Use of OTP:

Name	Number	Problem
Saimul hossain	1750186215	Delivery Delay (SMS)
Fazle Rabbi	1911796578	Short Time

dipjoy baidda	1575466609	Limited Access (network)
shahed arefin	1533486163	Delivery Delays (SMS)
chandan Dash	1797334951	Device Dependency
Naimul Haque Tonmoy	1875954786	Security Risks
Jannatul Fardous	1614701496	Delivery Delays (SMS)
pollob Dey	1758911597	Dependency on service-provider

Requirement Specification and Finalize Requirement (Information Processing):

1. Functional Requirements

A. User Authentication

- Fingerprint Scanner Integration: Interface fingerprint scanner with ATMEGA 16.
- Enrolment Process: Enable users to enrol and store fingerprints securely.
- Verification Process: Match scanned fingerprints with stored templates.

B. ATM Transactions

- Balance Inquiry: Check account balance post-authentication.
- Cash Withdrawal: Withdraw cash after successful fingerprint verification.
- Mini Statement: Provide a summary of recent transactions.
- Pin Change: Allow users to change their PIN.

2. Non-Functional Requirements

A. Performance

- Response Time: Fingerprint verification within 2-3 seconds.
- Transaction Time: Complete transactions within 30 seconds.

B. Security

- Data Encryption: Encrypt fingerprint templates and transaction details.
- Secure Communication: Ensure secure communication with the bank system.

C. Usability

- User Interface: Intuitive interface for easy navigation.
- Accessibility: Design accessible features for users with disabilities.

D. Reliability

- Fault Tolerance: Handle hardware/software failures gracefully.
- Backup and Recovery: Regular backups and recovery mechanisms.

3. Hardware Requirements

A. Core Components

- ATMEGA 16 Microcontroller: Central processing unit.
- Fingerprint Scanner: Compatible sensor for fingerprint capture.
- LCD Display: User interface display.
- Keypad: For PIN entry and transaction selection.
- Card Reader: Fallback for traditional ATM cards.
- Cash Dispenser: Mechanism to dispense cash.
- Receipt Printer: For printing receipts.

B. Support Components

- Memory Module: External memory for storing data.
- Power Supply: Stable power with backup (UPS).
- Communication Module: Network interface for bank system connectivity.

4. Software Requirements

A. Embedded Software

Fingerprint Processing Library: For fingerprint data handling.

- ATM Application Software: Manages transactions, UI, and operations.

B. Backend Software

- DBMS: Stores user data, logs, and fingerprint templates.
- Banking Middleware: Interfaces ATM with bank's core system.

Feasibility Analysis:

To evaluate the feasibility of developing a fingerprint-based ATM system using the ATMEGA 16 microcontroller, focusing on technical, economic, legal, operational, and schedule feasibility.

1. Technical Feasibility

A. Hardware Compatibility

- ATMEGA 16 Microcontroller: Capable of handling the processing requirements for fingerprint scanning and basic ATM operations.
- Fingerprint Scanner: Ensure the selected fingerprint scanner is compatible with ATMEGA 16. Commonly used sensors like R305 or GT-521F32 can be integrated.

- Peripheral Components: LCD display, keypad, card reader, cash dispenser, and receipt printer can be interfaced with ATMEGA 16 using standard communication protocols (I2C, SPI, UART).

B. Software Requirements

- Embedded Software: Develop or integrate existing libraries for fingerprint processing and ATM operations.
- Security Software: Implement encryption algorithms (e.g., AES-256) within the microcontroller's capabilities.
- Development Tools: Utilize AVR Studio or Atmel Studio for programming the ATMEGA 16. Compatibility with C/C++ for firmware development.

C. Integration Challenges

- Interfacing Multiple Components: Adequate GPIO pins and communication protocols support is available in ATMEGA 16 to interface all necessary peripherals.
- Data Storage: External EEPROM or SD card module can be used to store fingerprint templates and transaction logs.

2. Economic Feasibility

A. Development Costs

- Hardware Costs: Estimate the cost of ATMEGA 16 microcontroller, fingerprint scanner, and other peripheral components.
- Software Development Costs: Include costs for development tools, libraries, and any third-party software.
- Prototyping and Testing: Budget for prototype development and iterative testing phases.

B. Operational Costs

- Maintenance Costs: Regular maintenance, software updates, and hardware replacements.
- Training Costs: Training for technicians and bank staff to operate and maintain the new ATM system.

C. Cost-Benefit Analysis

- Initial Investment: Compare the initial development and deployment costs with the anticipated benefits such as enhanced security and reduced fraud.
- Long-Term Savings: Potential reduction in ATM fraud and maintenance costs due to biometric authentication.

Based on the feasibility analysis, the fingerprint-based ATM system using the ATMEGA 16 microcontroller is technically and economically viable, with considerations for legal compliance and operational efficiency. The project is expected to be completed within 11-17 months, with a well-defined plan for development, testing, and deployment. The benefits of enhanced security and user convenience outweigh the initial costs, making it a worthwhile investment for the banking industry.

Budget and Time frame:

Creating a fingerprint-based ATM system is a complex project that involves hardware integration, software development, and thorough testing. Here is a suggested timeline to guide the project from initiation to deployment:

Phase 1: Planning and Requirements (2-3 weeks)

Project Kick-off Meeting (1 week)
- Define project scope, objectives, and deliverables.
- Identify stakeholders and form the project team.
- Conduct initial meetings to gather requirements.

Requirements Gathering and Analysis (1-2 weeks)
- Document detailed requirements (functional and non-functional).
- Analyse hardware and software requirements.
- Define project milestones and timelines.

Phase 2: Design (3-4 weeks)

System Architecture Design (2 weeks)
- Design the overall system architecture.
- Define hardware and software interfaces.
- Create detailed design documents.

UI/UX Design (1-2 weeks)
- Design user interfaces for the ATM screen.
- Develop user interaction flow diagrams.
- Create wireframes and prototypes.

Phase 3: Development (8-10 weeks)

Hardware Integration (3-4 weeks)
- Set up and test fingerprint scanners.
- Integrate fingerprint scanners with the ATM hardware.
- Develop drivers and middleware for hardware-software communication.

Backend Development (4-5 weeks)
- Develop core banking system integration.

- Implement authentication and authorization logic.
- Develop APIs for communication between the ATM and backend systems.

Frontend Development (2-3 weeks)

- Implement user interfaces based on the UI/UX design.
- Integrate frontend with backend APIs.
- Develop error handling and user feedback mechanisms.

Phase 4: Testing (4-6 weeks)

Unit Testing (1-2 weeks)

- Perform unit testing for individual components.
- Fix identified bugs and issues.

Integration Testing (2-3 weeks)

- Conduct integration testing of hardware and software components.
- Test communication between the ATM and backend systems.

User Acceptance Testing (1-2 weeks)

- Conduct user acceptance testing with a small group of users.
- Collect feedback and make necessary adjustments.

System Testing: 2-3 weeks

Pilot Testing: 1-2 weeks

Phase 5: Deployment and Rollout (3-4 weeks)

Deployment Preparation (1-2 weeks)

- Prepare deployment scripts and documentation.
- Train support and maintenance teams.

Pilot Deployment (1-2 weeks)

- Deploy the system in a limited number of ATMs.
- Monitor performance and gather feedback.

Full Rollout (2-3 weeks)

- Deploy the system in all target ATMs.
- Provide ongoing support and maintenance.

Phase 6: Maintenance and Support (Ongoing)

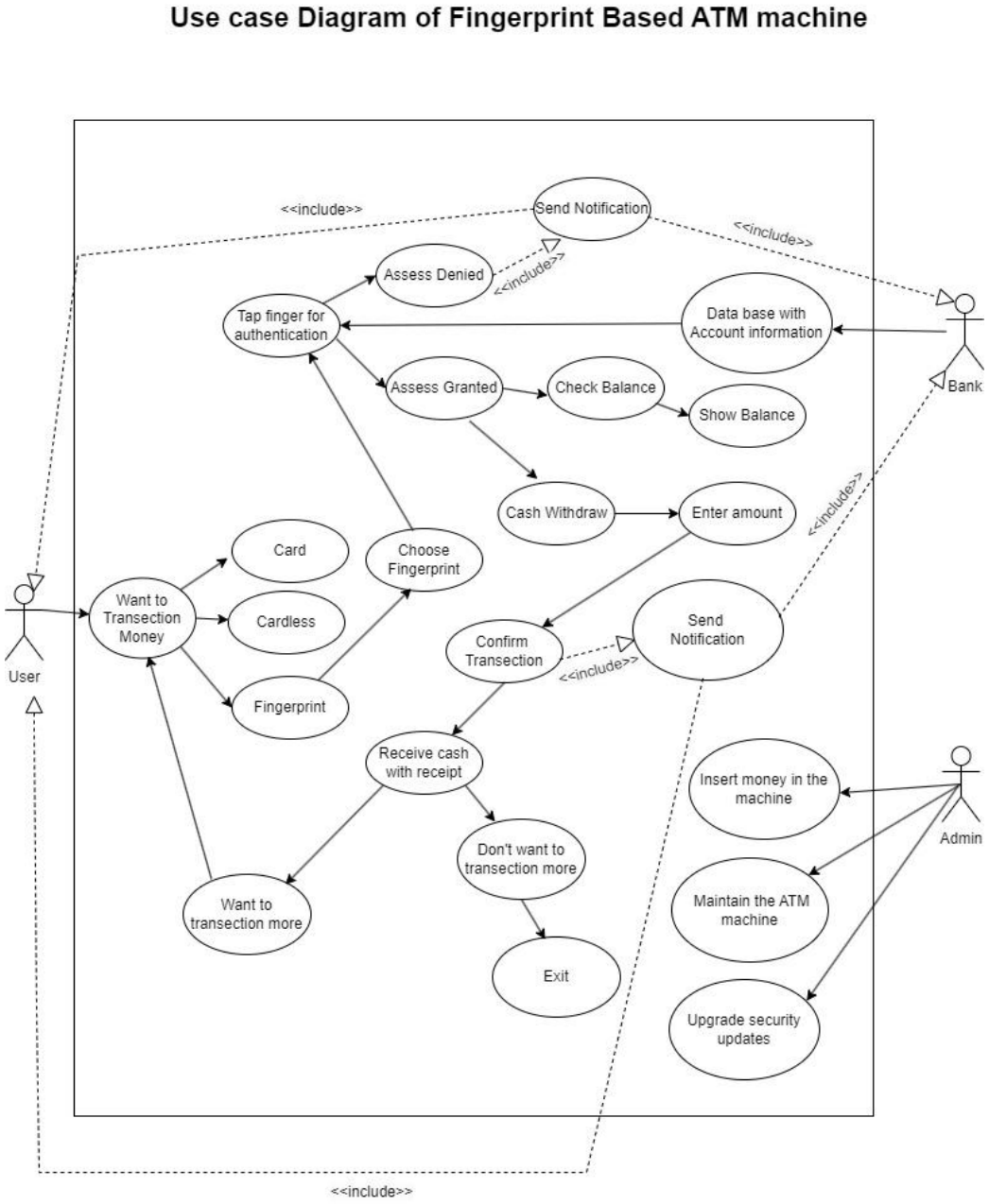
Post-Deployment Support

- Provide regular maintenance and updates.
- Address any issues or bugs reported by users.
- Monitor system performance and security.

Total Estimated Time: 20-27 weeks (5-7 months)

This timeline is a high-level estimate and can vary based on project complexity, team size, and other factors. Regularly reviewing progress and adjusting the plan as needed is crucial for staying on track.

UML Diagram:



DFD0

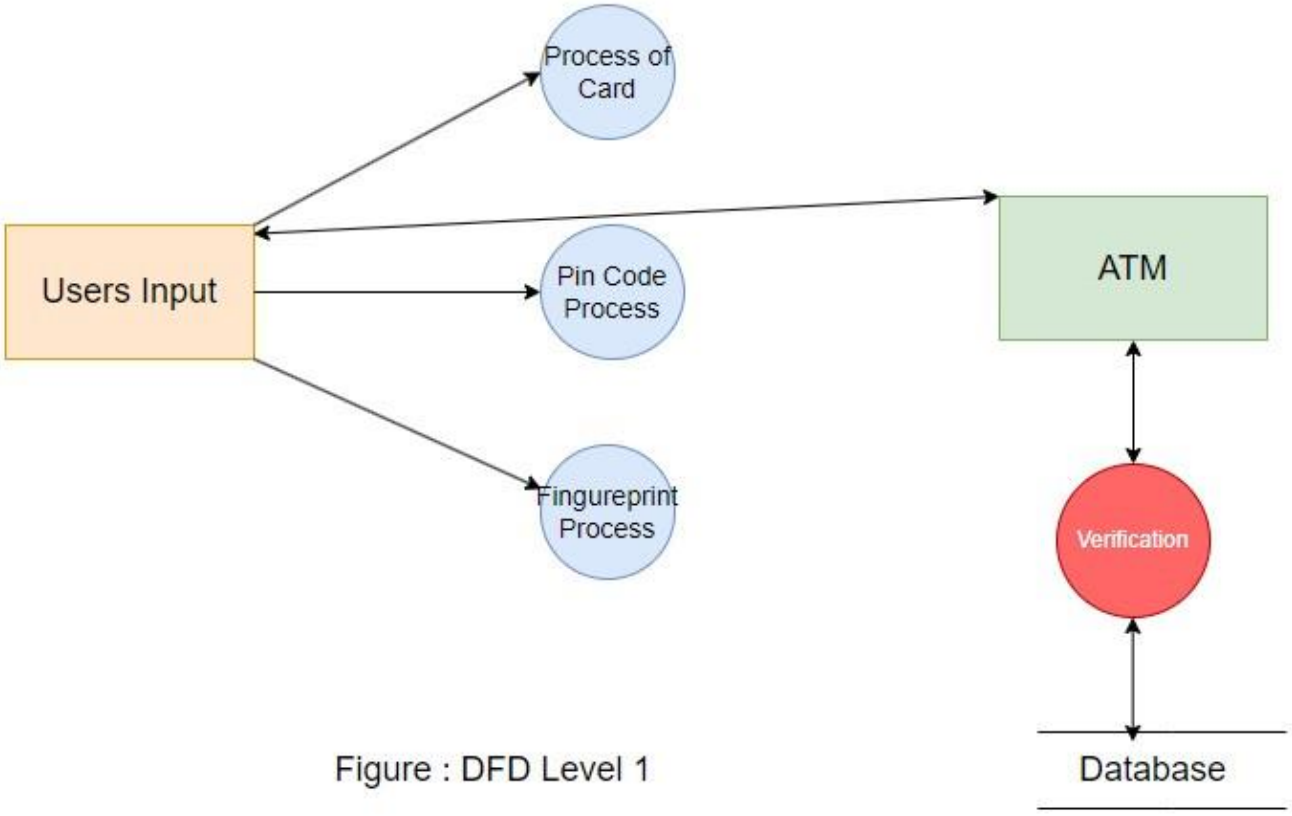


Figure : DFD Level 1

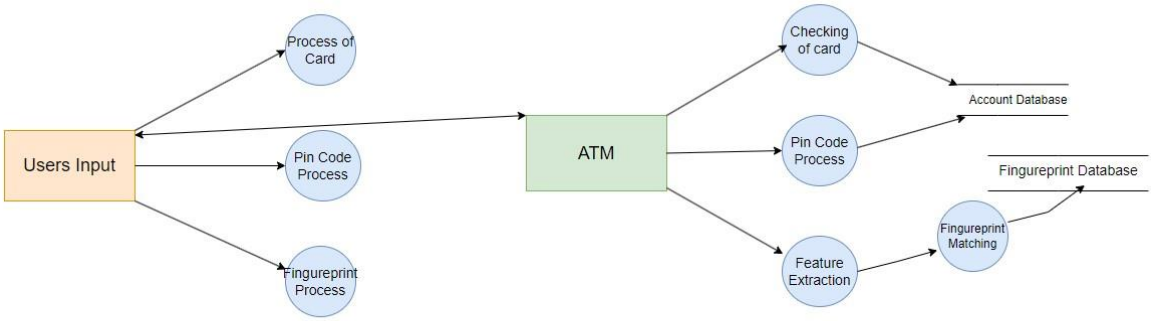
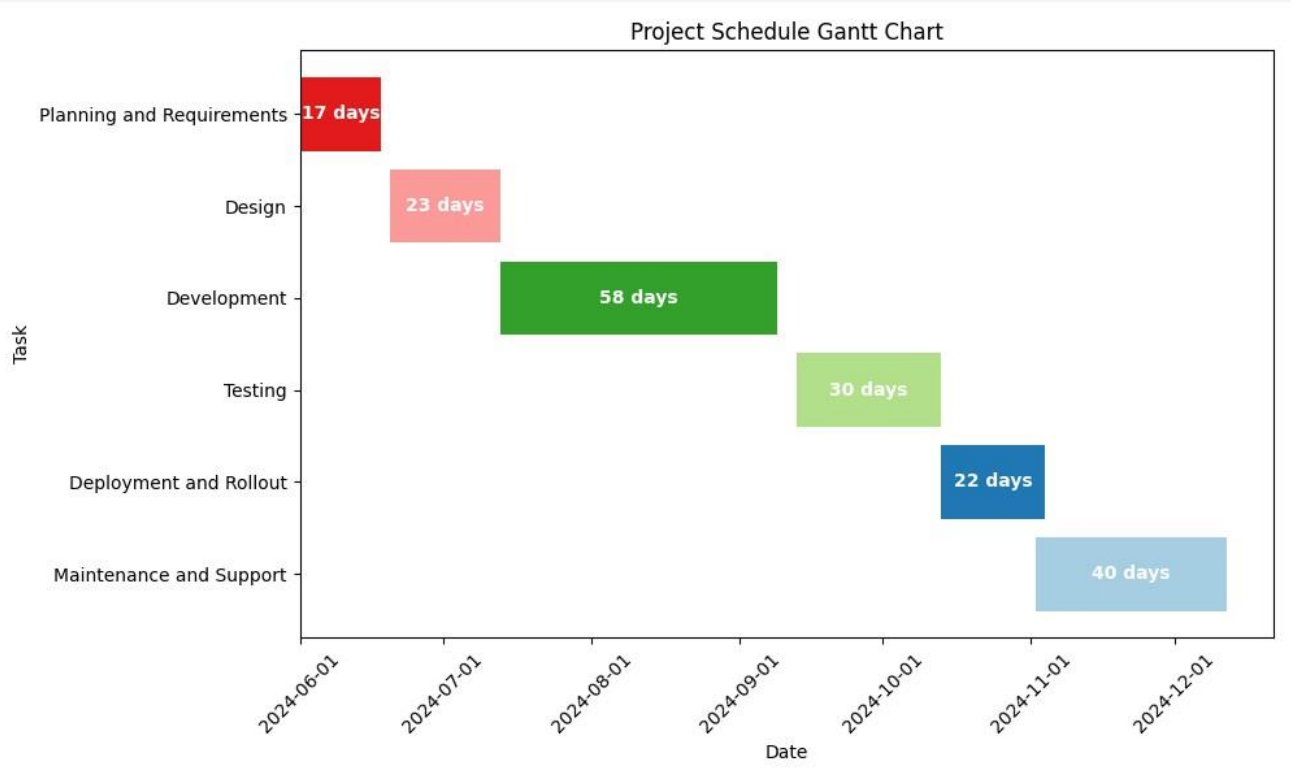


Figure : DFD Level 2



Implementation Procedures (Required h/w and s/w, security, authentication):

Implementing a fingerprint-based ATM system involves a detailed plan covering hardware and software requirements, security measures, and authentication processes. Below are the key steps and components needed for a successful implementation.

1. Required Hardware

A. ATM Machine Hardware

- Fingerprint Scanner: High-resolution fingerprint scanners with anti-spoofing technology.
- Touchscreen Display: High-quality, durable touchscreen interface for user interaction.
- Processor: High-speed processor to handle biometric data processing and transaction handling.
- Card Reader: For traditional card-based transactions as a fallback option.
- Receipt Printer: For transaction records.
- Cash Dispenser: Reliable and secure cash dispensing unit.
- Network Connectivity: Secure network interface (Ethernet/Wi-Fi) for communication with the central banking system.

2. Required Software

A. ATM Operating System

- Secure and reliable operating system, such as a customized Linux distribution or Windows IoT.

B. ATM Application Software

- Biometric Software: For capturing, processing, and verifying fingerprint data.
- Transaction Software: For managing ATM transactions like withdrawals, deposits, balance inquiries, and transfers.
- User Interface Software: Intuitive and accessible UI for user interactions.
- Communication Software: Secure protocols for communicating with banking servers (e.g., HTTPS, SSL/TLS).

C. Backend Systems

- Database Management System (DBMS): Secure and efficient database for storing transaction logs, user data, and biometric information.
- Banking Middleware: To connect the ATM network with the core banking system.
- Monitoring and Management Tools: For real-time monitoring, maintenance, and support of the ATM network.

3. Security Measures

A. Physical Security

- Tamper-Resistant Design: Ensure the ATM machine is built to resist tampering and physical attacks.
- Secure Installation Location: Install ATMs in well-lit, secure locations with surveillance coverage.
- Alarm Systems: Equip ATMs with alarms that trigger on tampering or unauthorized access attempts.

B. Data Security

- Encryption: Use end-to-end encryption (e.g., AES-256) for data transmission between the ATM and the banking server.
- Secure Storage: Encrypt sensitive data stored on the ATM, such as biometric templates and transaction logs.

C. Network Security

- Firewalls and IDS/IPS: Implement firewalls and intrusion detection/prevention systems to protect the network.
- VPNs: Use Virtual Private Networks (VPNs) for secure communication between the ATM and the bank's central system.

D. Software Security

- Regular Updates and Patches: Keep all software up to date with the latest security patches.
- Anti-Malware: Install anti-malware solutions to protect against viruses and other malicious software.

4. Authentication Procedures

A. Biometric Authentication

- Fingerprint Enrolment: Users need to enrol their fingerprints at the bank or during the initial setup. This involves capturing high-quality fingerprint images and storing them securely in the bank's database.
- Fingerprint Verification: During ATM transactions, the user's fingerprint is scanned and matched against the stored template for authentication.

B. Multi-Factor Authentication (Optional)

- PIN or Password: In addition to fingerprint authentication, users might be required to enter a PIN or password.
- One-Time Password (OTP): Send an OTP to the user's registered mobile number or email for added security.

5. Implementation Steps

A. Planning and Preparation

- Conduct a feasibility study and risk assessment.
- Define the project scope, objectives, and timeline.
- Procure the necessary hardware and software.

B. Installation and Configuration

- Install the hardware components at designated locations.
- Set up the operating system and application software on the ATMs.

- Configure network settings and security measures.

C. Integration and Testing

- Integrate the ATM system with the bank's backend systems.
- Conduct comprehensive testing, including functionality tests, security tests, and user acceptance tests (UAT).

D. Training and Deployment

- Train bank staff and support teams on using and maintaining the new system.
- Deploy the ATMs in a phased manner, starting with pilot locations.
- Collect feedback and make necessary adjustments before full-scale deployment.

E. Monitoring and Maintenance

- Establish a monitoring system for real-time tracking of ATM performance and security.
- Schedule regular maintenance activities and updates as outlined in the maintenance plan.

Testing:

Testing a fingerprint-based ATM system is critical to ensure its security, functionality, and user-friendliness. The testing phase can be divided into several key stages, each focusing on different aspects of the system.

Testing Phases and Activities

1. Unit Testing (1-2 weeks)

Test each software module, such as the fingerprint recognition algorithm, user interface components, backend services, and hardware drivers. Mock dependencies to isolate each unit. Write and execute unit tests using testing frameworks (e.g., JUnit for Java, pyres for Python). Fix identified bugs.

2. Integration Testing (2-3 weeks)

Test the integration between the fingerprint scanner and the ATM's software. Verify communication between the ATM and the backend banking systems. Check the interaction between the frontend (user interface) and backend services. Use integration testing tools and frameworks (e.g., Postman for API testing, and Selenium for UI testing).

3. System Testing (2-3 weeks)

Perform end-to-end testing of the entire ATM workflow, from user authentication via fingerprint to transaction completion. Test different user scenarios, including valid and invalid fingerprints, and successful and failed transactions. Verify system performance under load, ensuring it can handle multiple users simultaneously. Conduct security testing to ensure that the system is secure from unauthorized access and attacks (e.g., penetration testing, vulnerability scanning).

4. User Acceptance Testing (UAT) (1-2 weeks)

Engage a group of end-users to test the system in a real-world environment. Collect feedback on usability, performance, and any issues encountered. Address any defects or changes requested by users. Validate that the system meets all acceptance criteria defined during the planning phase.

5. Pilot Testing (1-2 weeks)

Deploy the system in a limited number of ATMs in a controlled environment. Monitor the system's performance and user interactions. Gather feedback from actual users and observe any issues or unexpected behaviour. Make necessary adjustments based on the feedback and observed data.

Maintenance:

Maintenance of a fingerprint-based ATM system is crucial to ensure its continuous and secure operation. Below are the key steps and considerations for maintaining the system and planning for further development.

1. Regular Maintenance Activities

A. Routine System Checks (Weekly/Monthly)

- Hardware Checks: Ensure fingerprint scanners, screens, and other hardware components are functioning properly.
- Software Updates: Apply patches and updates to the ATM software to fix bugs and enhance security.
- Log Review: Regularly review system logs for unusual activity or errors that may indicate potential issues.

B. Security Maintenance (Ongoing)

- Vulnerability Scanning: Perform regular scans to identify and address security vulnerabilities.
- Penetration Testing: Conduct periodic penetration tests to assess the security posture of the system.

- Access Control Reviews: Ensure that user access controls are up-to-date and enforce the principle of least privilege.

C. Performance Monitoring (Continuous)

- Load Testing: Regularly test the system's performance under different loads to ensure it can handle peak usage.
- Response Time Monitoring: Monitor the system's response time to transactions and fingerprint recognition.

D. Backup and Recovery (Daily/Weekly)

- Data Backup: Regularly back up transaction data, user information, and system configurations.
- Disaster Recovery Drills: Conduct drills to ensure quick recovery in case of system failure.