IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.1411141

THE DEVELOPMENT OF A UNIFIED, INTELLIGENT AND SECURE ATM CARD TO MANAGE MULTIPLE BANK ACCOUNTS.

Rashmi R[1], Swati[2], Thejaswini MB[3], Udeepa K[4], Mrs. Arathi HL[5]

BE, Computer Science Engineering, East West College of Engineering, Bengaluru, India[1-4]

Assistant Professor, Computer Science Engineering, East West College of Engineering, Bengaluru, India[5]

Abstract: The rapid expansion of digital banking has increased the number of customers maintaining multiple bank accounts, resulting in inconvenience and security challenges associated with carrying numerous ATM cards and remembering multiple PINs. This research proposes the development of a unified, intelligent, and secure ATM card capable of managing multiple bank accounts through a single authentication framework. Using RFID, fingerprint biometrics, Arduino-based embedded systems, and GSM-enabled OTP verification, the proposed solution enhances both convenience and security. This paper discusses the architecture, methodology, hardware integration, and performance assessment of the system that consolidates multiple bank accounts into one secure card.

Keywords: RFID, Biometrics, ATM Security, Multi-Account ATM Card, Embedded Systems, Arduino, OTP Verification.

I. INTRODUCTION

Automated Teller Machines (ATMs) have become an essential part of modern banking, enabling customers to withdraw cash, transfer funds, and check balances without the need for bank staff. As banking services expanded, many customers began maintaining accounts across different banks, resulting in the need to carry multiple ATM cards and remember several PINs. This not only creates inconvenience but also increases the chances of card misplacement and security breaches.

Traditional ATM systems rely heavily on PIN-based verification, which can be compromised through theft, skimming, or unauthorised access. With advancements in biometric and embedded technologies, there is a growing demand for a more secure and unified solution.

The concept of a single ATM card capable of managing multiple bank accounts aims to address these challenges. By integrating RFID technology, biometric fingerprint authentication, and OTP-based verification, banking transactions can become more secure, efficient, and user-friendly. The proposed system uses an Arduino-based embedded framework to authenticate users, allow selection between linked bank accounts, and verify each transaction through a mobile-based OTP.

This enhanced model not only reduces the burden of carrying multiple cards but also strengthens security through multi-factor authentication. The proposed approach represents a significant step toward smarter, safer, and more convenient banking for users who interact with multiple financial institutions.

II. LITERATURE SURVEY

[1] A study published in an IEEE conference (2025) presented a Smart ATM Card that integrates advanced security mechanisms to allow users to manage multiple bank accounts using a single card. The proposed system incorporated enhanced authentication and intelligent card management techniques, significantly simplifying user convenience. However, the work did not address real-time security monitoring or large-scale scalability challenges.

[2] Another study published in the IJRR Journal (February 2025) introduced a model for designing a Smart and Secure Single ATM Card supported by RFID technology and mobile application integration. This approach allowed users to link and manage several bank accounts directly through an RFID-enabled card, offering improved portability and easier account access. Despite these advantages, concerns regarding mobile application vulnerabilities and data security were not fully examined.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.1411141

[3] A similar approach was discussed in a Zenodo publication (April 2024), which combined RFID technology with biometric authentication to strengthen ATM security. The integration of dual-authentication methods enhanced system reliability and prevented unauthorised access. Although the approach increased overall security, the study lacked an in-depth analysis of biometric device failures and system redundancy requirements.

[4] Further contributions came from authors in the Journal of Microprocessor and Microcontroller Research (September 2024), who implemented a multi-account ATM card system using fingerprint-based embedded technology. Their model reduced the need for multiple cards and minimised interbank operational costs by allowing unified management through a single embedded system. While the system demonstrated practical benefits, the paper provided limited discussion on large-scale deployment and integration with existing banking infrastructures.

[5] Another work from the same journal (2024) focused on fingerprint-based ATM authentication for multi-account access. The solution addressed user inconvenience by eliminating multiple cards and improving transaction security. However, challenges related to practical deployment, system upgrading, and compatibility across diverse banking networks remained open research problems.

III. METHODOLOGY

This research paper employs a structured approach to design and implement a secure banking system. The methodology primarily focuses on defining a robust system architecture and elucidating the data flows that govern transactions and account management. The proposed system is characterised by a layered architecture and a clear definition of data interactions to ensure integrity, security, and efficiency.

1. System Architecture

The system architecture, illustrated in the provided diagram, is organised into several distinct layers to promote modularity and maintainability.

User Interface Layer: This is the presentation layer, facilitating interactions via various interfaces such as ATMs, web portals, and mobile applications. It serves as the primary entry point for all user requests.

Authentication Layer: Responsible for verifying user credentials and ensuring secure access to the system resources, sitting immediately behind the UI layer.

Card Management System: Manages the lifecycle of payment cards, including issuance, activation, deactivation, and updates to card information.

Bank Network Interface: This layer handles communication protocols required for interfacing with internal bank networks and external interbank switches/routers.

Secure API Gateway: All internal and external service communication is routed through a secure API gateway, which enforces security policies and manages access control.

Core Banking System (Bank-Specific): The central component that manages all core banking operations, including ledgers, deposits, loans, and primary account records.

Transaction Processing Layer: This bottom layer is dedicated to the execution, validation, and recording of financial transactions.

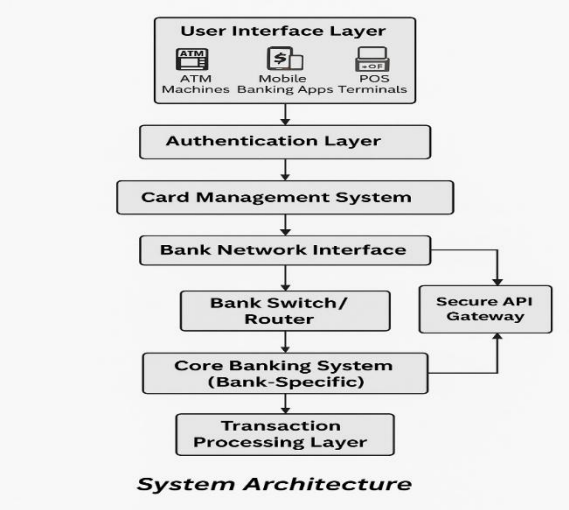


Fig.1 System Architecture

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.1411141

2. Data Flow Diagram (DFD)

The Data Flow Diagram details how information moves through the banking system, ensuring logical and secure processing of user requests and data updates.

User Interaction: A user initiates a request (e.g., transaction request) that flows into the Banking System. Simultaneously, the system receives or retrieves card information related to the user.

Validation and Account Management: The Banking System sends card details to the Card Validation process. Validated requests generate account data and are routed to the Account Management component.

Bank Interaction: The Account Management process interacts with the Bank entity to verify and update bank details.

Transaction Processing: The Banking System transmits the raw request data to the Transaction Processing data store, which holds the Transaction Data.

Record Generation: The Transaction Processing entity generates a transaction record and transaction details, which are passed back to the Banking System and ultimately provided as an output to the user.

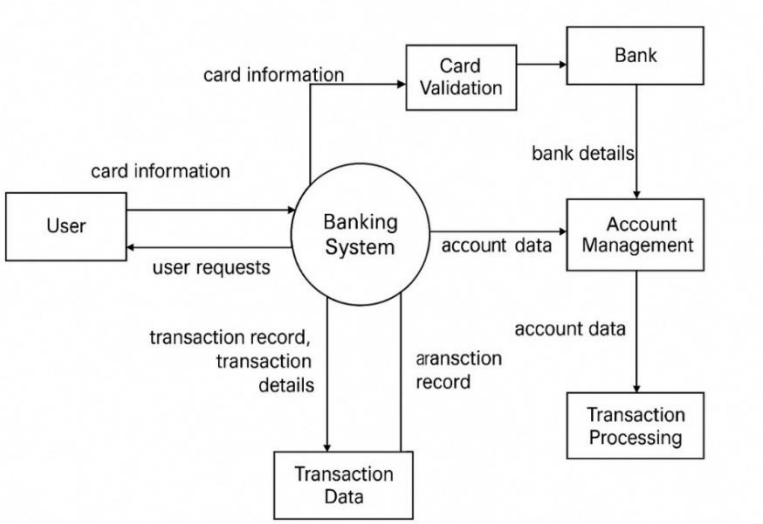


Fig.2 Data Flow Diagram

3. System Overview

System Name: Unified, Intelligent and Secure ATM Card System.

Purpose: To provide a secure and efficient platform for ATM card operations, including authentication, transactions, and administration.

Key Components: User, ATM Machine Interface, Authentication Module, Card Management System, Bank Switch/API Gateway, Bank Core System, and Transaction Processor.

4. Use Case Analysis

The use case diagram illustrates the interactions between actors (Bank Customer and Admin/System Operator) and the system.

Bank Customer Functions:

- Insert ATM Card
- Authenticate User (PIN/Biometric)
- Select Account
- Withdraw Cash
- Deposit Funds
- Transfer Funds
- Manage Account Preferences
- Admin/System Operator Functions:
- Update Card Security Settings

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.1411141

- Block Card

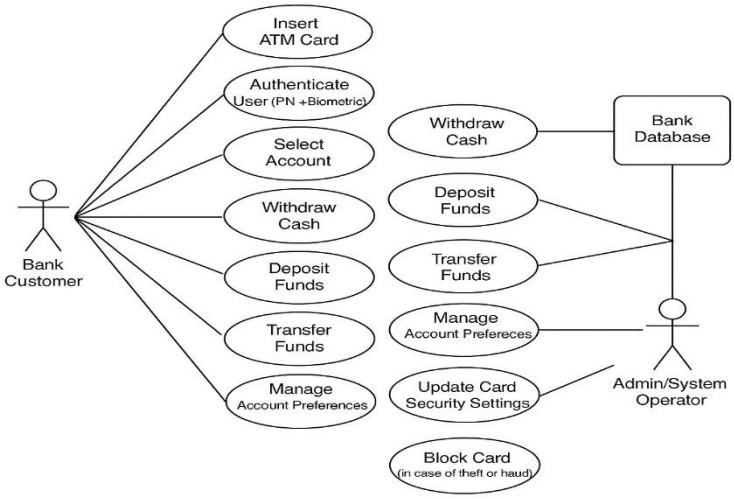


Fig.3 Use Case Diagram

5. Sequence Diagram Description

The sequence diagram details the flow of messages for an ATM transaction, likely a withdrawal or balance inquiry.

- A User inserts their card and inputs their PIN/biometric data into the ATM Machine Interface.
- The interface sends an Authentication request to the Authentication Module.
- The module validates the card and fetches linked accounts from the Card Management System.
- The interface displays options, and the user selects an account and requests a transaction.
- The request is forwarded to the Bank Switch/API Gateway and then to the Bank Core System/Transaction Processor.
- The transaction is logged, and a confirmation/status is sent back to the interface and user.

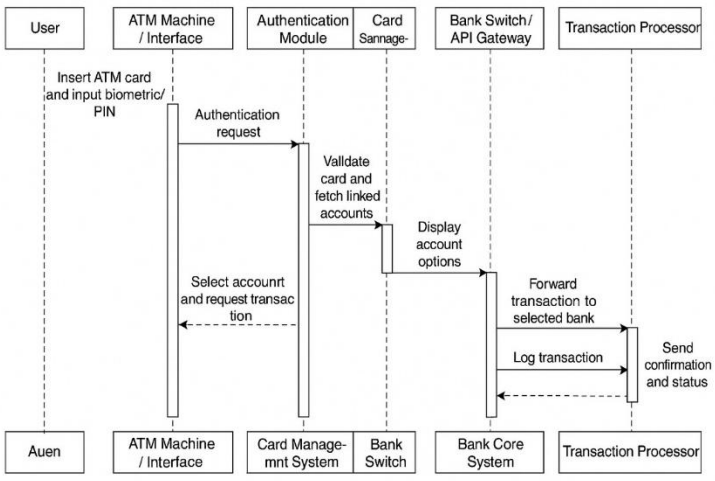


Fig.4 Sequence Diagram Description

6. Module Breakdown

The system is divided into several modules, each with specific functions:

Authentication & Security Module: Handles user authentication (PIN, biometric), card validation, and security settings.

Transaction Module: Manages various transactions like withdrawals, deposits, and transfers.

Admin & Monitoring Module: Provides tools for system administrators to manage cards, monitor system status, and handle security events.

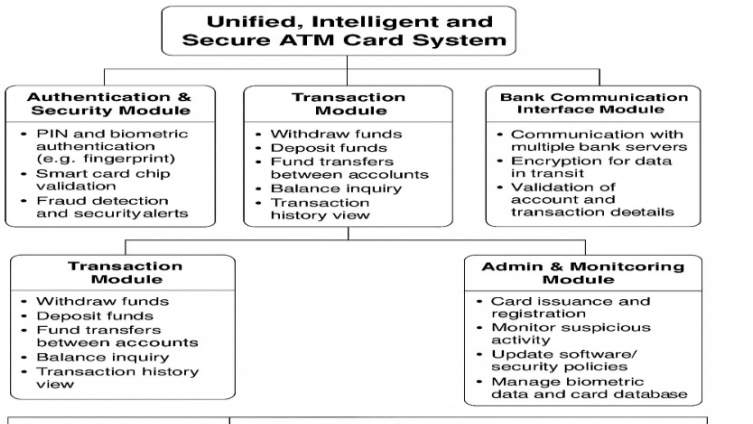
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.1411141

Card Management Module: Manages card details, linked accounts, and security information.



Module	Description
Authentication & Security Module	Handles user verification and system access concotrol
Account Management Module	Selection of bark/account from linked options
Transaction	View account details
Module	Manage linked accounts in case-account
Admin & Monitorring	Card issuance and registration
Module	Allows system admin to omanerates
Smart Card Management Module	Deals with smart card functiontiity operations and operations

Fig.5 Module -Wise Breakup

7. Entity-Relationship Diagram (ERD)

An Entity-Relationship Diagram (ERD) is a conceptual data model used to describe the inter-related information within a specific domain of knowledge, such as a banking system. It visually represents the structure of a database, helping to ensure efficient and accurate data access.

Entities: These are real-world objects or concepts about which data is stored. In the provided diagram, entities are represented by rectangles and include User, BankAccount, ATMCard, Bank, and Transaction.

Attributes: These are properties or characteristics of an entity, listed within the entity's rectangle. For example, the User entity has attributes like UserID, Name, Address, PhoneNumber, Email, and BiometricData.

Relationships: These describe how entities are associated with each other. They are represented by diamonds connecting entities. Examples in the diagram include:

- A User Owns a BankAccount.
- A User Owns an ATMCard.
- A BankAccount Has an ATMCard.
- A Bank Operates a Transaction.
- An ATMCard Initiated By a Transaction.

Cardinality/Multiplicity: While not explicitly labeled with notation in this specific diagram, ERDs typically define the number of instances of one entity that can be associated with the number of instances of another entity (e.g., one-to-one, one-to-many, many-to-many).

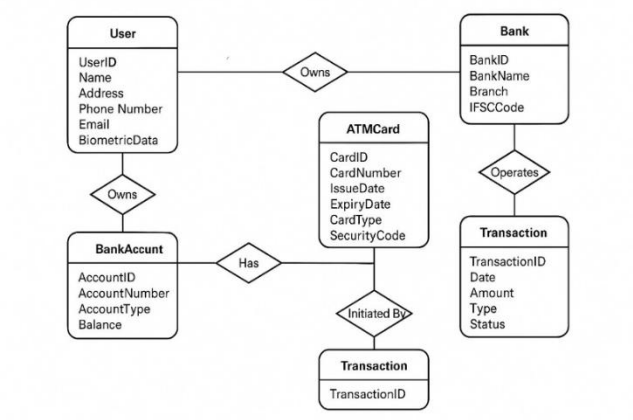


Fig.6 E-R Diagram

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025
DOI: 10.17148/IJARCCE.2025.1411141

IV. CONCLUSION

The "Smart and Secure Single ATM Card for Multiple Bank Accounts" project provides a practical and innovative solution to simplify banking access while enhancing transaction security. By combining RFID technology with GSM-based OTP verification, it ensures that only authorized users can access multiple linked accounts through a single card. This system reduces the need to carry multiple ATM cards, lowers the risk of misuse, and introduces a streamlined user experience. The use of Arduino Mega, along with cost-effective components like LCD display and buzzer, makes it highly feasible for educational, rural, or prototype applications.

This project not only demonstrates effective use of embedded systems and IoT in banking but also highlights a scalable framework for future enhancements. Its modular design makes it adaptable to advanced security mechanisms like biometrics, mobile integration, and real-time banking systems. Overall, the solution bridges a vital gap in multi-account accessibility and sets a strong foundation for secure, unified, and intelligent banking interfaces.

REFERENCES

[1] "Smart Card & Security Basics" - CardLogix, paper no.:710030 www.cardlogix.com
[2] "Smart card based Identity Card And Survey"-White Paper JKCSH (Jan Kremer Consulting Services).
[3] Chip-and-PIN: Success and challenges in reducing Fraud from Federal Reserve Bank of Atlanta"-Douglas King, Jan 2012.
[4] "Examining Smart-Card Security under the Threat of Power Analysis Attacks"- Thomas S.Messaerges member IEEE, Ezzat A.Dabbish member IEEE, and Robert H.Sloan senior member IEEE vol.51, No. 5, MAY 2002.
[5] "Secure Internet Banking Application"-Alain Hiltgen, Thorsten Kramp.
[6] Fingerprint Verification Using Smart Cards for Access Contol Systems, Raul Sanchez-Reilllo, IEEE AESS Systems Magazine , September 2002 [7] "Benefits Of Smart cards versus Magnetic Stripe Cards for Healthcare Application"-Smart card Alliance 2011.
[7] Katakam Swathi, Prof.M.Sudhakar "Multi Account Embedded ATM Card with Enhanced Security" IOSR Journal of Electronics and Communication Engineering IOSR Journal of Electronics and Communication Engineering, Volume 10, Issue 3, Ver. I (May- Jun.2015)
[8] Tahaseen Taj I S, Dr Suresh M B"AN EMBEDDED APPROACH: FOR HANDLING MULTIPLE ACCOUNTS WITH SMART ATM CARD" International Conference on Computer Science, Electronics & Electrical Engineering-2015
[9] Nair Vinu Uthaman, Pratiksha Shetty, Rashmi, Mr.Balapradeep K N "MAASC Multiple Account Access using Single ATM Card" International Journal of Science,Engineering and Technology Research (IJSETR), Volume 3, Issue 6, June 2014
[10] Youjung Ko, Insuk Hong, Hyunsoon Shin, Yoonjoong Kim"Development of HMM- based Snoring Recognition System for Web Services" 2016 IEEE