International Conference on Sciences, Engineering & Environmental Technology (ICONSEET), 17(17): 69-80, 2025
ISSN 0749-9650

www.repcomseet.org

Implementing Multifactor Authentication in Meeting Balanced Security in Automated Teller Machine Transactions

Fabiyi Aderanti Alifat*, Ramoni Tirimisiyu Amosa, Ileladewa Abiodun Adeoye, Olorunlomerue Adam Biodun, Ugwu Jennifer Ifeoma, Oluwatosin Adefunke Oluwatobi &Awosanmi Oluwatobiloba

Department of Computer Science, Federal Polytechnic Ede, Osun State, Nigeria.
adesunp@yahoo.co.uk,

Abstract: ***Cybercrime targeting Automated Teller Machines (ATMs) remains a critical challenge, particularly in developing economies such as Nigeria where traditional card-and-PIN authentication is highly vulnerable to fraud. This study explores the implementation of Multifactor Authentication (MFA) as a robust countermeasure against ATM-related attacks. A conceptual system prototype was designed using a client–server model and Unified Modeling Language (UML), integrating knowledge-based (PIN) and biometric (fingerprint) verification mechanisms. The proposed framework ensures dual-layer authentication, thereby mitigating threats such as skimming, cloning, and unauthorized withdrawals. Findings from literature and simulation indicate that MFA can reduce ATM fraud incidents by up to 60%, though challenges relating to infrastructure cost, maintenance, and user acceptance remain. The research concludes that MFA adoption provides a sustainable pathway for securing ATM transactions in Nigeria, provided it is complemented by customer awareness, regulatory enforcement, and future integration with AI-driven fraud detection systems.***

Keywords*: ATM Security, Biometric Verification, Cybercrime, Financial Technology, Multifactor Authentication, Nigeria.*

Introduction

Cybercrime is now considered a global threat, with its economic impact running into billions of dollars annually. According to the Internet Crime Complaint Centre (Abdullfatai, 2021), financial institutions remain one of the top targets. In the Nigerian context, the situation is worsened by rapid digitization coupled with limited cybersecurity awareness among customers. ATM fraud, in particular, has evolved from simple card thefts to sophisticated cyber-attacks involving malware and network infiltration (Yeboah et al., 2020; Jegede, 2020).While governments and financial regulators have enacted laws and guidelines, enforcement and compliance remain weak. This has created a pressing need for research-driven, technology-based solutions that balance security with user convenience. Multifactor authentication (MFA) represents one such approach, offering an opportunity to strengthen trust in Nigeria's financial systems. Cybercrime has become one of the most pressing challenges in the digital era, particularly in the financial sector. Automated Teller Machines (ATMs) revolutionized banking by enabling convenient, round-the-clock financial transactions, but they have also become targets of cybercriminals who exploit vulnerabilities in authentication mechanisms. Traditional card-and-PIN systems are increasingly inadequate against modern cyber-attacks (Gao et al., 2019; Adeoti 2021). In Nigeria, cybercrime is on the rise, with ATM fraud ranking among the most reported incidents. This study examines the potential of MFA as a viable solution to curb ATM-related crimes, focusing on its design, implementation, and feasibility within the Nigerian banking sector.

Table 1.1: Population and internet users and the internet crime rate in Nigeria and other countries.

S/n	Country	Population (2023 Est.)	Internet Users 31 Dec, 2000	Internet users, 31 Dec., 2021	Internet penetration	Internet crime victims	Facebook subscribers 2022
1	Nigeria	221,400,708	200,000	154,301,195	73.0%	16th	31,860,000
2	India	1,402,228,115	5,000,000	833,710,000	59.5%	3rd	515,800,000
3	Algeria	45,150,897	50,000	37,836,425	83.3%	20th	26,291,400

4	UK	68,468,662	-	65,045,228	95.0%	1st	555,891,100
5	Ghana	32,154,245	30,000	14,767,818	45.9%	25th	9,163,200

(Adapted from Internet Crime Report 2020 & Internet World Stats 2022)

Table 1.1: Showing Countries and Internet Stats number of Internet Crime Victims, the Internet Crime Report (2020) ranked Nigeria 16th in the world in terms of victim's loss, which is seen as a significant improvement to the Internet Crime Report (2010) that ranked the country 3rd after the United States and the United Kingdom with the highest prevalence of cybercrime in the world.

ATM cybercrime has become a significant threat to the security of financial transactions, posing risks to both financial institutions and customers (Adaramola, 2019). Criminals employ various techniques, such as skimming, card trapping, and cash-out attacks, to compromise ATMs and steal sensitive information or money. Traditional methods of ATM authentication, primarily relying on a single factor such as a card and Personal Identification Number (PIN), have proven inadequate in mitigating these risks. The problem addressed in this study is the need for effective security measures to curb ATM cybercrime. Single-factor authentication methods have demonstrated vulnerabilities, leading to an increase in fraudulent activities targeting ATMs. Financial institutions face the challenge of protecting customer information, preventing unauthorized access, and maintaining the integrity of ATM transactions in the face of evolving cyber threats (Abdullahi and Monsur, 2020).To address this problem, implementing multifactor authentication (MFA) has been proposed as a potential solution. MFA requires users to provide multiple factors to verify their identity, such as knowledge factors (passwords, PINs), possession factors (ATM cards, mobile devices), and inherence factors (biometric characteristics). However, the effectiveness of MFA in curbing ATM cybercrime and its practical implementation in the ATM environment remain open questions.

Literature Review.

Halder & Jaishankar (2021), defined cybercrimes as offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS).

Latha (2019) states that cybercrimes are nothing but crimes of the real world perpetuated in the medium of computer and hence there is no difference in defining a crime in the cyber world and real world. Cybercrime may threaten a person or a nation's security and financial health (Morgan, 2020).

Cybercrime has emerged as a significant threat in the digital age, affecting individuals, businesses, and governments worldwide, McQuade (2019). With the rapid advancement of technology and the widespread use of the internet, criminals have found new avenues to exploit vulnerabilities and perpetrate various illicit activities. This essay provides a comprehensive overview of cybercrime, exploring its types, motivations, impacts, legal frameworks, and the challenges faced in combating this complex phenomenon.

Cybercrime encompasses a diverse range of offenses, each exploiting the digital landscape for nefarious purposes, Gao et al. (2019). These include hacking and unauthorized access to computer systems, where malicious actors exploit security loopholes to gain unauthorized entry. Additionally, malware distribution involves the dissemination of viruses, ransomware, and spyware to compromise systems and extract sensitive information. Phishing and social engineering attacks trick individuals into revealing personal data, while online fraud encompasses credit card fraud, identity theft, and crypto currency scams. Cyberbullying and online harassment inflict psychological harm, and intellectual property theft and digital piracy undermine creativity and innovation.

One of the defining characteristics of cybercrime is its global reach, McQuade (2019). The borderless nature of the internet allows criminals to operate from anywhere in the world, often crossing international boundaries to evade detection and prosecution. This global reach poses significant challenges for law enforcement and legal authorities, as different jurisdictions may have varying laws and regulations regarding cybercrime. As a result, international cooperation and coordination are crucial to effectively combat cyber threats.

The impacts of cybercrime are far-reaching and multifaceted, World Economic Forum (2020). Financial losses resulting from online fraud and ransomware attacks can cripple businesses and individuals alike. Data breaches compromise sensitive information, leading to identity theft and potential exploitation. The dissemination of false information through social media can manipulate public opinion and destabilize societies. Moreover, cyberbullying and online harassment can cause severe psychological and emotional harm, especially among young individuals. Critical infrastructure such as power grids and communication networks are also at risk, with potential consequences for public safety and national security.

Governments and international organizations have recognized the urgency of addressing cybercrime and have developed legal and policy frameworks to combat it, Council of Europe, (2019). One significant example is the Council of Europe's Convention on Cybercrime, also known as the Budapest Convention. This treaty aims to harmonize laws and facilitate cooperation among participating countries in investigating and prosecuting cybercrime. Additionally, many countries have enacted their own cybercrime laws, empowering law enforcement agencies to take action against cyber offenders within their jurisdiction.

Despite efforts to combat cybercrime, numerous challenges persist World Economic Forum, (2020). The ever-evolving nature of technology means that cybercriminals constantly find new ways to exploit vulnerabilities. This demands a continuous effort from cybersecurity experts to stay ahead of the curve. Moreover, the anonymity offered by the internet makes it difficult to trace and identify cybercriminals, making prosecution challenging. Limited resources and the lack of international standardization in cybercrime laws and procedures also hinder effective global collaboration.

Cybercrime is a complex and ever-evolving phenomenon that demands comprehensive understanding and concerted efforts to combat effectively. Understanding the various types of cybercrime, the motivations behind it, and its far-reaching impacts is crucial in developing robust cybersecurity strategies. International cooperation, legislative frameworks, and awareness-raising initiatives are vital in safeguarding individuals, organizations, and societies from the threats posed by cybercriminals. A multi-faceted approach that involves collaboration between governments, private sector entities, law enforcement, and individuals is key to creating a secure digital environment for the future.

Methodology

The research followed a descriptive conceptual approach combined with a prototype design. First, secondary data was collected from scholarly articles, reports, and industry case studies. Then, a system prototype was designed using Unified Modeling Language (UML) to simulate ATM customer interactions. The choice of a client/server model was deliberate, as it allows scalability and secures data storage on centralized servers. Security mechanisms, including encryption and session management, were embedded in the database design. Evaluation of the model was conceptual, focusing on potential effectiveness, feasibility, and user experience implications. This research employed a client/server model to design and simulate a secure ATM system with MFA integration. Tools from Unified Modeling Language (UML), including use case diagrams and activity diagrams, were used to illustrate user-system interactions.

The system incorporated:

- PIN authentication (knowledge factor).
- Fingerprint recognition (biometric factor).
- Database integration using PHP/MySQL to store and verify user credentials.
- Interface design using HTML, CSS, and JavaScript.

The methodology focused on system design, database security, and feasibility assessment through conceptual modeling rather than physical deployment.

The Existing System

The current Automated Teller Machine (ATM) technology authenticates transactions using a card and PIN-based mechanism. Bank users can then access various services, including transfers, cash withdrawals and deposits, balance inquiries, top-up purchases, and utility bill payments. The PIN entered by each ATM user is compared to the authorized PIN maintained by the ATM system. If a match is found, the system authenticates the user and has access to all of the ATM's functions.

The user is given two more chances to input the proper PIN if there is a discrepancy, which results in the user authentication procedure failing. The Automated Teller Machine will be blocked if a wrong PIN is input.

The Proposed System

The initial interface a bank customer encounters on an Automated Teller Machine (ATM) requests that they enter their debit card, followed by a request for their PIN. This information is based on an analysis of contemporary ATMs. A notice window informing the user that their PIN is incorrect appears if they input one, and the system prompts them to enter a valid PIN. The consumer was led to the next stage of the authentication process, which asks for the enrollment of his or her fingerprint to be placed on a fingerprint reader or face the camera for facial recognition once the customer's PIN has been verified in our research and proposed prototype. After accepting the fingerprint, the fingerprint scanner compares the live sample to the previously enrolled templates in the bank's database. The consumer is taken to the transaction phase, where they must select from available transaction activities if the fingerprint or facial recognition technology is confirmed to be accurate; if not, access is denied. Following validation, the user is presented with a transaction menu from which they can choose which operation to perform in the following stage.

Client/Server Approach

Automated teller machines use client/server applications that rely on transactions. Requests are sent from the client to the server, like what a consumer would do with an ATM. The information provided to the server by the client determines the outcome of the information request, just as the type of information the user provides to the ATM when requested determines the outcome of the ATM transaction. The diagram below shows the client-server system relationship in the Automated Teller Machine.

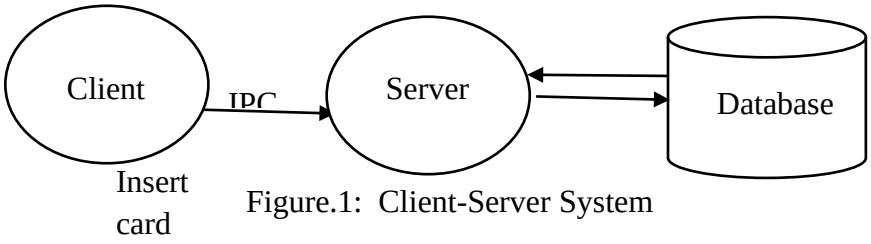


Figure.1: Client-Server System

The following is how the client-server approach can is applied to an Automated Teller Machine:

i. ATM Client: The client in the ATM context is the user who interacts with the ATM to perform various banking transactions. The client interacts with the ATM interface, which includes options for withdrawing cash, depositing funds, checking balances, transferring money, and other banking services.

ii. Banking Server: The server in the ATM context is the banking system or a network of servers that handle the user's requests and process the transactions. This banking server communicates with the ATM and interfaces with the bank's core banking system to perform the necessary actions and retrieve account information.

iii. Communication Protocol: The client (ATM) and the server (banking system) communicate using a secure and standardized communication protocol. Common protocols used in ATM systems include ISO 8583, a messaging standard for financial transactions, and TCP/IP for network communication.

iv. Request-Response Model: The client (ATM) initiates a request for a specific transaction, such as a cash withdrawal or balance inquiry. The request is sent to the banking server, which processes the request, verifies the user's identity, checks account balances, and performs the necessary transaction. The server generates a response with the requested information or the transaction status, which is then sent back to the ATM client.

v. Statelessness: The ATM client is generally stateless, meaning it does not store user-specific data between transactions. Each user interaction is treated independently by the ATM. The banking server, on the other hand, maintains state information about user accounts, balances, and transaction history.

vi. Security: ATM systems employ various security measures to protect user data and ensure secure communication. This includes encryption of data transmitted between the ATM and the banking server, user authentication through PINs or biometric authentication, and transaction authorization mechanisms to prevent unauthorized access to user accounts.

vii. Scalability: As the number of ATM users and transaction volume increases, the banking server infrastructure can be scaled up to handle the load efficiently. This may involve adding servers, balancing load, and optimizing network connectivity.

viii. Offline Capabilities: ATMs also have offline capabilities to provide basic services when the connection to the banking server is temporarily unavailable. In offline mode, the ATM can handle limited transactions, such as balance inquiries or cash withdrawals within predefined limits. Once the connection is restored, the ATM synchronizes with the banking server to update transaction records and account balances.

ix. Maintenance and Monitoring: The client-server approach allows for centralized maintenance and monitoring of ATMs. The banking server can monitor the status of ATMs, perform software updates, and collect transaction data for reporting and analytics purposes. The client-server approach in ATMs enables secure and reliable banking services, allowing users to perform a range of transactions conveniently while ensuring the integrity and confidentiality of their financial information.

Database phase

Implement security measures to protect sensitive data, especially customer and transaction information. Microsoft Access provides user-level security features. Apply data validation rules to ensure data integrity, such as enforcing PIN length or ensuring transactions don't exceed account balances.

S/N	Field	Data type	Description
1.	Fname	string	First name
2.	Mname	string	Middle name
3.	Lname	string	Last name
4.	DOB	String	Date of Birthday
5.	Address	string	Customer's Address
6.	Sex	string	Customer's Gender
7.	Acctype	string	Account Type
8.	AccNo	int	Account Number
9.	PhoneNo	int	Customer's Phone Number
10.	Nationality	string	Customer's Country

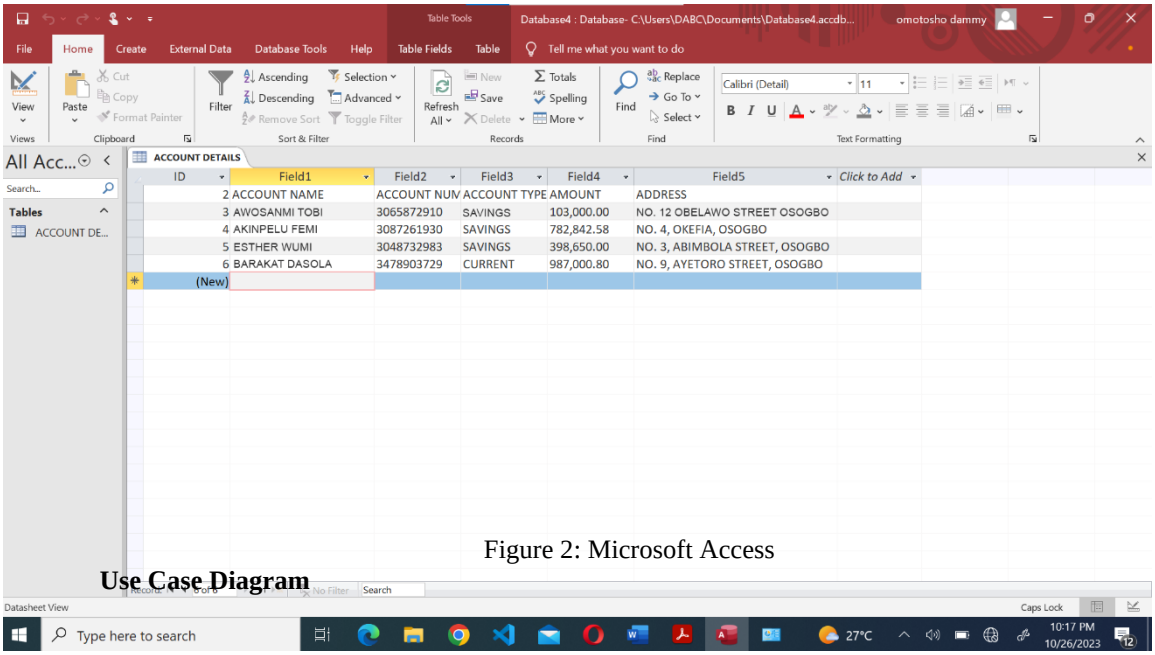


Figure 2: Microsoft Access

Use Case Diagram

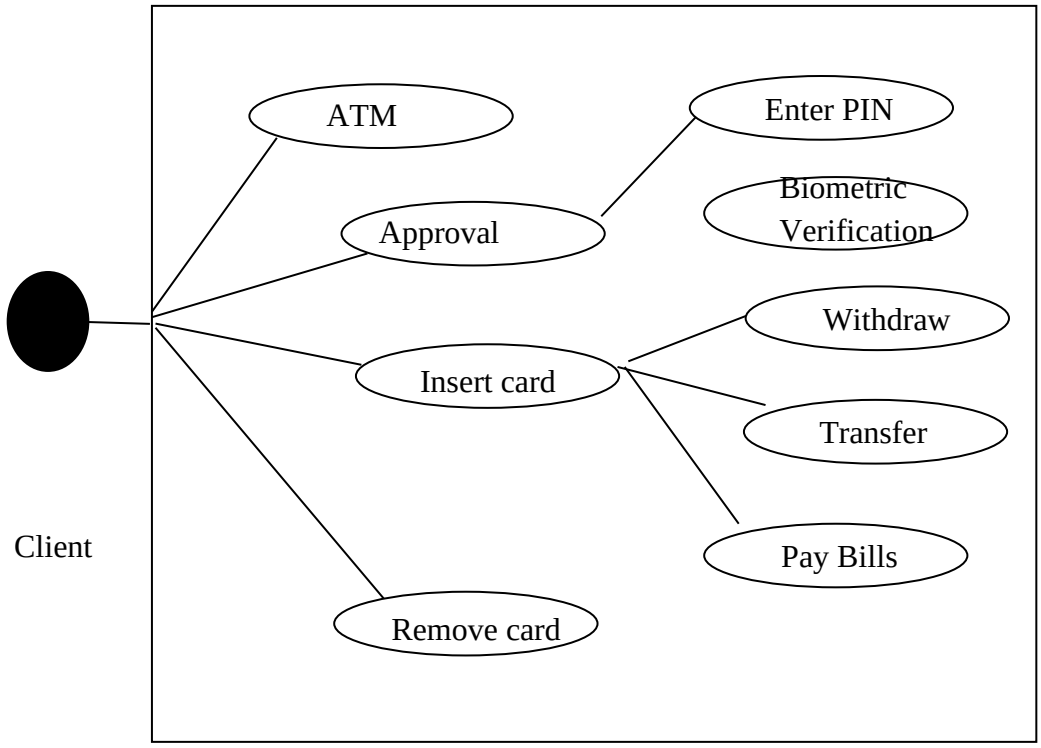


Figure 3: Use Case Model

Activity Diagram

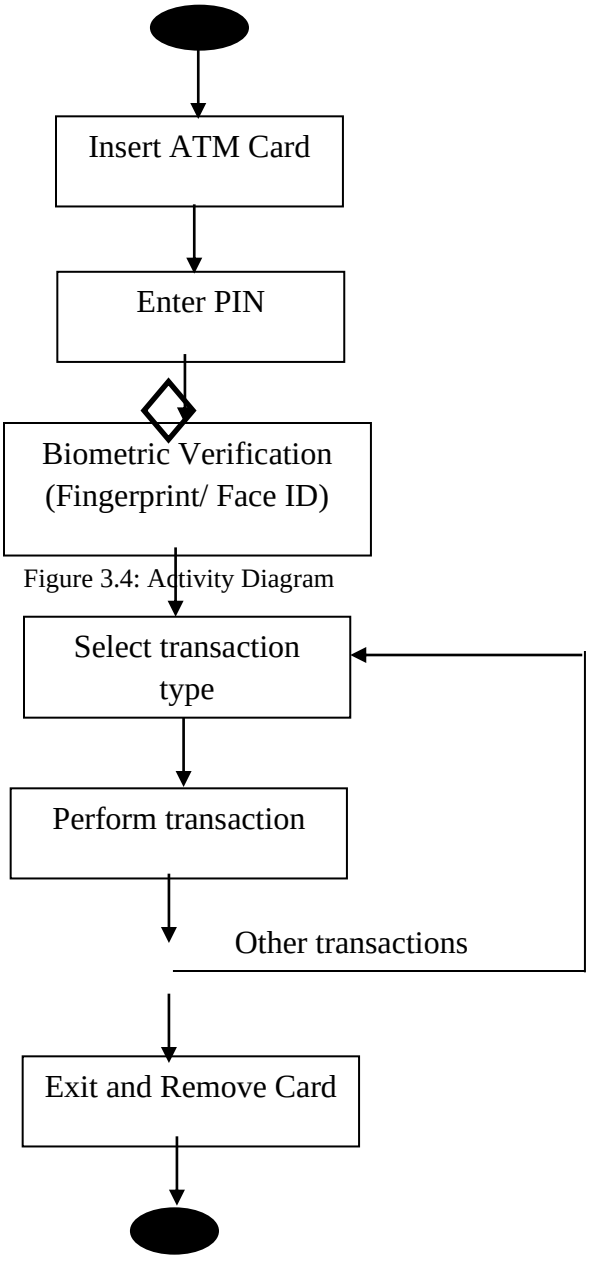


Figure 3.4: Activity Diagram

Class Diagram

The Bank class represents the bank that authorizes transactions. It has attributes like the bank's name and a list of accounts. It includes methods for verifying a PIN, authorizing withdrawals, and authorizing deposits. The Account class represents a customer's bank account. It has attributes for the account number, account name, balance, thumbprint and passport photograph. The Customer class represents a customer, with attributes like their name and a reference to their Card.

It includes a method to verify the PIN and the biometric verification. The ATM Card class represents the ATM card with attributes for the card number, expiry date, and a flag indicating whether the card is blocked. The Cash Dispenser class represents the ATM's cash dispenser and has an attribute to track available cash. It has a method to dispense cash.

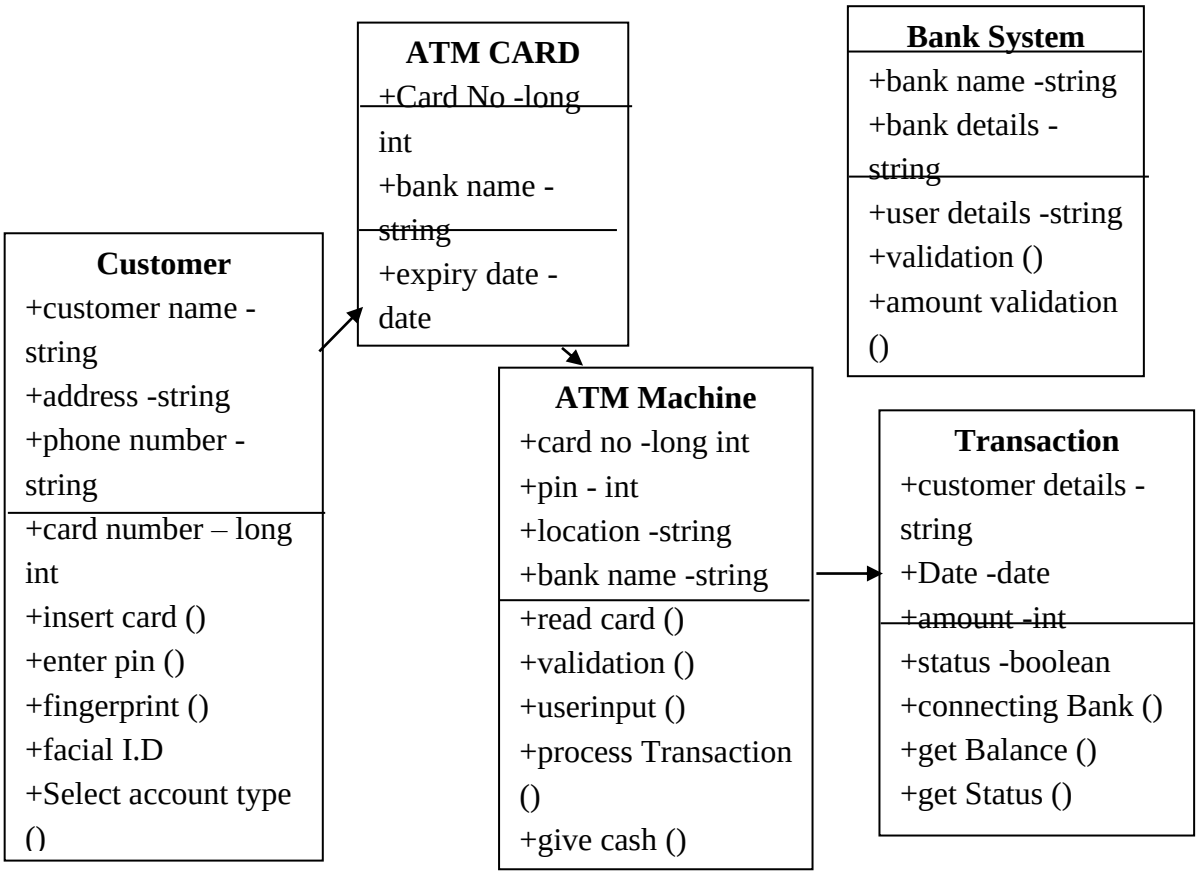
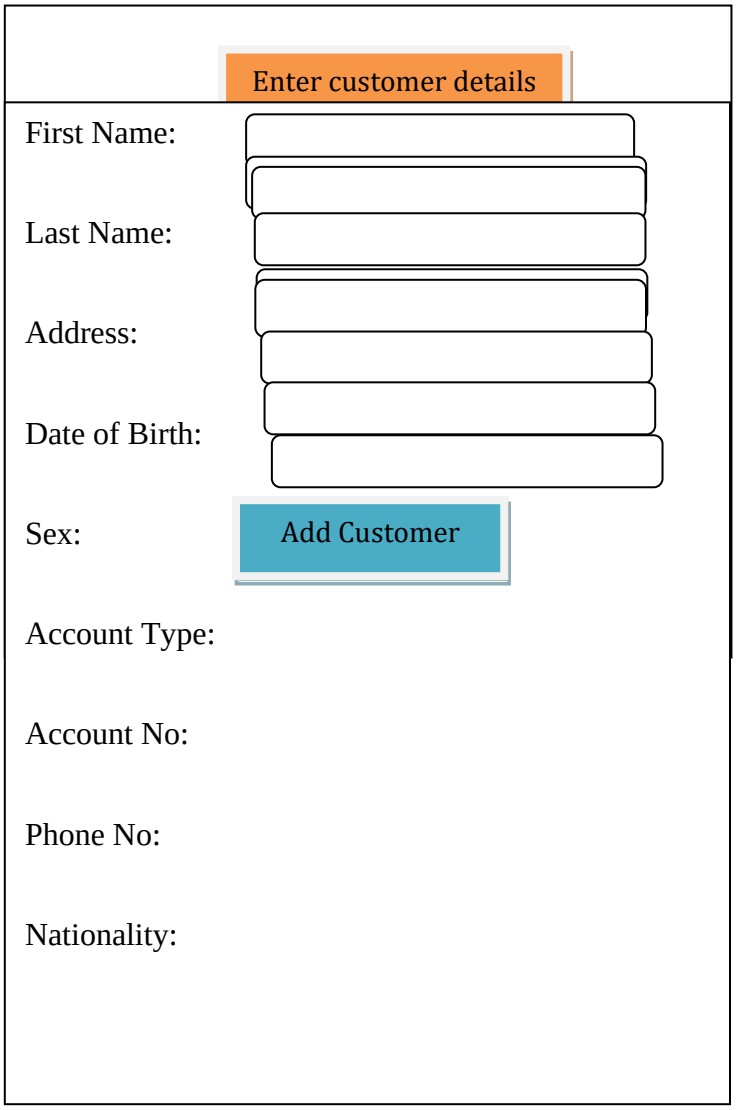


Figure 5: Class Diagram

Results and Discussion

Registration Page I

On the registration page, a form will be given to the customer, which contains their account name, account number and phone number. Also, the customer's thumbprint and facial verification were captured. The user's credentials will be entered into the database using this application. This module enters the user's phone number and email address into the database as the customer's first and last name. The diagram below illustrates the form to fill for the registration page.



Registration Page II

This is the second part of the registration; the Automated Teller Machine's built-in fingerprint reader will be used to scan the customer's fingerprint. The fingerprint was captured and added to the database. The diagram below (figure 7) shows how the biometric verification was captured.

Figure 7: Fingerprint Capturing

Registration Page III

This is the third part of the user's registration; the facial biometric data will be added to the database for authentication in this module. Multiple facial images were captured to ensure accuracy and adaptability to various lighting conditions and were added to the database. Below shows how the facial images is captured.

Figure 8: Sample of how the face will be captured

USER INTERFACE DESIGN

A system's user interface provides a user-friendly way for users to interact with the system to process inputs and get outputs. Through input/output devices and accompanying software, it also serves as a communication channel between the system and the human user. This particular ATM application is made up of 8 interfaces, which include the Welcome Interface, Enter Pin Interface, Enroll Fingerprint / Facial Verification Interface, Transaction Type, Withdrawal Interface, Enter Amount Interface, Transfer Page Interface and Balance Enquiry Interface.

Welcome Page Interface

This is the first interface the bank customer interacts with on the Automated Teller Machine (ATM). Creating a user-friendly and secure welcome page interface for an ATM is essential for a positive customer experience and ensuring financial transactions' safety. The primary input method should be a touchscreen display, making it easy for users to

navigate the interface. This interface prompts the customer to insert ATM card and proceeds with the entire authentication process, inputting the PIN. If the user enters an invalid PIN, a dialogue box prompts an invalid PIN or invalid card number, and the system returns to enter a valid PIN. A typical description of this is shown in the image below, using Temtop as the bank's name. Include a button for users to cancel the transaction if needed. After validating the customer's card and PIN, the customer is directed to the next phase of the authentication process via the authentication dialogue box for inputting the fingerprint.

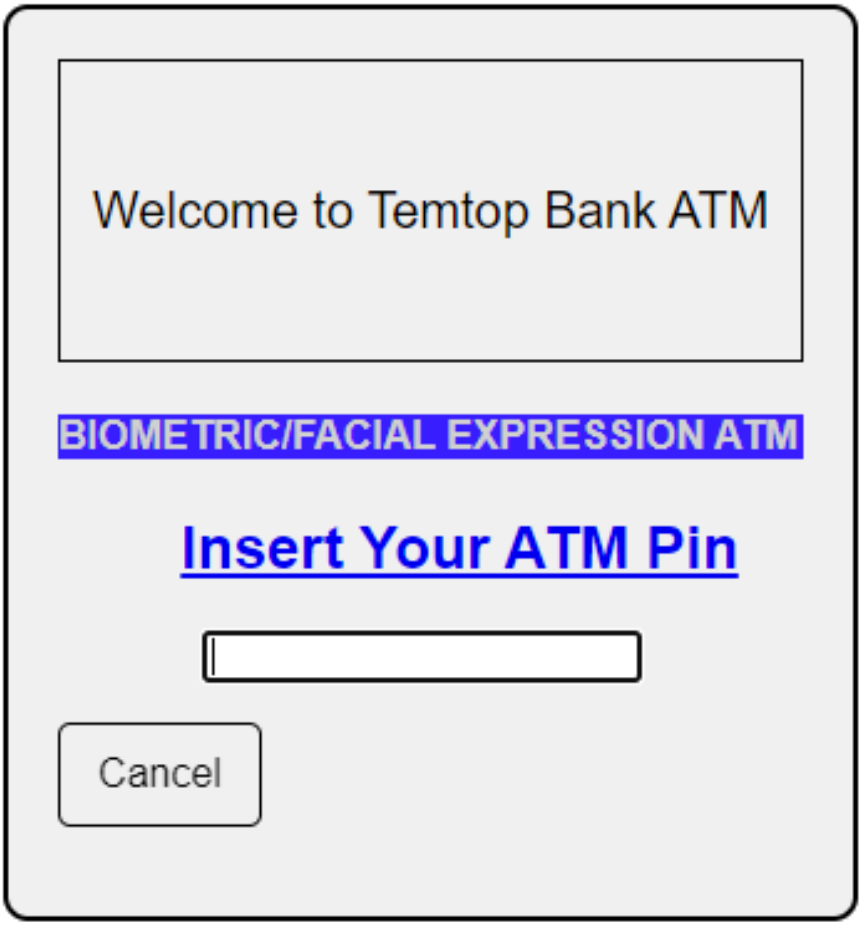


Figure 9: Interface design for Welcome Page

Conclusion and Recommendations

In conclusion, MFA provides a sustainable pathway for curbing ATM cybercrime in Nigeria. The study reinforces that a combination of knowledge (PIN) and biometric authentication is both practical and effective. However, success depends on more than just technology it requires a holistic strategy involving banks, customers, and regulators.

Recommendations for stakeholders:

1. Banks should pilot MFA-enabled ATMs in high-risk urban areas before nationwide rollout.
2. Regulators should introduce policies mandating MFA for ATM transactions above specific thresholds.
3. Customer education campaigns should highlight the ease and benefits of biometric security.
4. Further research should explore integrating MFA with AI-driven fraud detection systems.

REFERENCES

Abdulfatai, B. (2021). *Legislative Commitment and Cybercrime in Nigeria*. Paper presented at the Law Week of Faculty of Law of Lead City University Ibadan. Retrieved from http://nationalinsightnews.com/2017/03/08/legislative-commitment-cyber-crime-nigeria-sen-fatai-buhari-ph-d/

Abdullahi, R., Mansor, N. (2020). Concomitant Debacle of Fraud Incidences in the Nigeria Public Sector: Understanding the power of Fraud Triangle Theory. *International Journal of Academic Research in Business and Social Sciences,* 5(5), 312-326

Abubakar, A.S (2020) *Investigating Fraud Schemes in Nigeria.* Paper presented at International Conference on Cooperation against Cybercrime. Retrieved from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f2643

Adaramola, Z. (2019). Nigeria's cybercrime law and its 'loopholes'. *Daily Trust.* Retrieved 29 November, 2019, from https://www.dailytrust.com.ng/news/it-world/nigeria-s-cybercrime-law-and-its-loopholes/110593.html

Adeoti, J.O., (2021). Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out. *Journal of Social Sciences*, 27(1), pp.53–58.

Adesina and Charles. (2020). An Empirical Investigation of the levels of User' Acceptance of E-Banking in Nigeria. Journal of Internet banking and Commerce. Vol. 15, No. 1. April 2020.

Adesuyi, F.A. et al., (2019). A survey of ATM security implementation within the Nigerian banking environment. *Journal of Internet Banking and Commerce*, 18(1).

.

Gao J., J. Cai, K. Patel, and S. Shim: (2019), Wireless Payment, Proceedings of the Second International Conference on Embedded Software and Systems (ICESS05), China, pp. 367-374, December 2019.

Halder, A. B. Lass F. D. and Makinde J. (2018). *Cybercrime in Nigeria: Causes, Effects and the Way Out*, ARPN Journal of Science and Technology, vol. VOL. 2(7), 626 – 631.

Jegede C. A., (2020). "Effects of Automated Teller Machine on the Performance of Nigeria Banks". American Journal of Applied Mathematics and Statistics, 2.1 (2020): 40-46.

Latha O. B. and S. C. Chiemeke, (2018). "Cybercrime and Criminality in Nigeria: what roles is Internet Access Points Playing?" *European Journal of Social Sciences*, vol. 6, no. 4, pp. 132–139, 2018.

Morgan, D.S. (2019). The Internet as a Conduit for Criminal Activity. In A. Pattavina (Ed.), *Information technology and the criminal justice system (pp. 77-98). Thousand Oaks, CA: Sage.*

Wang, Y. (2018). On contemporary denotational mathematics for computational intelligence. *Transactions of Computational Science*, *2*, 6–29. doi:10.1007/978-3-540-87563-5_2

Wang, Y. (2020). Using process algebra to describe human and software system behaviors. *Brain and Mind*,*4*(2), 199–213. doi:10.1023/A:1025457612549

Yeboah-Boateng, E. O., & Kwabena-Adade, G. D. (2020). Remote access communications security: Analysis of user authentication roles in organizations. *Journal of Information Security*, *11*(3), 161-175.