International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2019.33580

Volume 5, Issue 10
October - 2019

SECURE ATM AND BANK TRANSACTIONS USING BIOMETRIC AND BLOCKCHAIN

ILODUBA SUSAN. C[1], MUHAMMAD SANUSI [2] and EBELOGU CHRISTOPHER UBAKA[3]

Research Scholar[1], Lecturer[2], Research Scholar[3]

[1-3]Department of Computer Science,

University of Abuja, Abuja,

Nigeria

Abstract

The conventional Automated Teller Machines in Nigeria have over the past few years been faced with inherent security challenges, which have mostly been attributed to the two-factor authentication structure (PIN and Card) of the ATM systems. The Nilson's report (2016) reveals that over 72% of ATM frauds within the period of the review were from card frauds, ranging from counterfeiting to card snatches. This record was able to soar so high since the identity thief is left with only one security clearance (PIN) to provide once the card is obtained. This work focuses on a multifactor approach to authentication which requires the presentation of three authentication factors: a knowledge factor ("something only the user knows"), a possession factor ("something only the user has"), and an inherence factor ("something only the user is"). After the presentation, the first factor and either of the next two factors must be validated by the other party for authentication to occur. This is to give room for exigencies and unforeseen circumstances such as loss/unavailability of mobile phones or lost or damaged fingers through accidents and aging factors. Although the proposed system does not promise a total eradication of ATM card frauds, and implementation of this design, it will to a large extent, reduce the occurrence and frequency of loss of money through ATM and card fraud since it provides an additional level of security. This translates to a more secure user identity, more secured funds and resources for the user and a more difficult and a less probable unauthorized access to an individuals' account.

***Key Words:** ATM Card Fraud, OTP, Bank Transaction, Blockchain Technology, Biometric Authentication.*

1. INTRODUCTION

Crimes at ATMs have become a nationwide issue that faces not only customers, but also bank operators which has risen repeatedly in recent years. This is mostly attributed to the little or no attention being paid to the card owner's level of education. A research conducted by [1] showed that one of the frequent causes of fraud is when customers are careless with their cards and pin numbers as well as their response to unsolicited e-mail and text messages to provide their card details. A lot of criminals tamper with the ATM terminal and steal customers' card details by illegal means either through illegal installation of skimmers or through the installation of fake and identical keypad overlays. Through these malicious activities, card and PIN details become available to the criminal. Furthermore, most identity thieves prey on the vulnerability of ATM card users through careful observation and monitoring. This vulnerability springs from a couple of factors ranging from the users' illiteracy level, age and in some cases trusting the wrong persons. A paper by [2] titled "Fraud vulnerability among ATM card users in Nigeria revealed the result of a survey on the growing trend of fraud, associated with ATM card usage as a result of disclosure of the four-digit pin by some ATM card users in some four randomly selected Nigerian cities: Abeokuta, Lagos, Port Harcourt and Kano. From the findings, 28%, 48%, 24% and 28% of card users are vulnerable to ATM card pin exposure respectively.

Despite several warnings, many people continue to choose easily guessed PIN's and passwords such as birthdays, phone numbers, social security numbers amongst others. Recent cases of identity theft have heightened the need for newer methods to improve the present method being adopted [2]. Biometric authentication technology may solve this problem since a person's biometric data is undeniably connected to its owner and is nontransferable and unique for every individual. The system can compare scans to records stored in a central or local database or even on a smart card. [3] defined biometrics as a measurable physiological and behavioral characteristic that can be captured and subsequently compared with another instance at the time of verification. It is an automated method of recognizing a person based on a physiological or behavioral characteristic. It is a measure of an individual's unique physical or behavioral characteristics to recognize or authenticate its identity. Common physical biometrics characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioral characteristics are signature and voice. Biometrics technologies are a secure means of authentication because biometrics data are unique, cannot be shared, rarely be copied and can be hardly lost. However, due to the possible challenges attributed to the biometric system, such as loss of biometric identifiers through accidents, aging and faulty biometric scanner, the proposed system will then implement an OR gate after the PIN verification which implies that at this point, an authentication of either the biometrics or the OTP, will result to a successful transaction. The OTP authentication approach then focuses on user validation based on something he has. Here, a one-time password that is valid for only one login session or transaction which is equally time bound is sent to the user's phone by SMS. As the OTP expires after one session it is immune to replay attacks (network attack in which a valid data transmission is maliciously or fraudulently repeated). OTP generation algorithms typically make use of pseudo-randomness and are mostly time based.

Hence an implementation of these two highly secured identity authentication approach in our ATM systems would provide users with a more secured ATM platforms and consequently amount to a reduced frequency and occurrence in ATM crime rate.

1.1 Problem Statement

The current ATM system has over the years faced the challenges of significant level of security loopholes, which is evident in the "two phase authentication approach" provided by all ATM systems within Nigeria. A research whose result was published in a paper presentation by [4], revealed that over 65.2% of ATM frauds in Nigeria were perpetrated through shoulder surfing, card snatching and skimmers. These lapses have been identified by identity thieves who have then taken maximum advantage of the unfortunate situation and implementation of an additional factor of authentication will raise the odds and make it less probable for perpetrators to commit ATM and card frauds. Research has shown that in 2015 alone, about $21.84 billion was stolen in ATM related crimes [5]. Although boggled ATMs constitute some part of the above result, however other means such as skimming, stolen cards, identity thefts, and in some cases maliciously obtained card details through receipts, bank statement and other documents containing card details equally made up the result of the above analysis. [5]

The financial hit one might take from the loss of funds through card fraud may just be the direct impact of this menace. The ripple effect that comes afterwards may be devastating ranging from loss of jobs, increased crime rates due to frustration, poverty, premature termination of child education and in some extreme cases may be life threatening. As we move deep into the century, the need for more technological advancement particularly in a more secured ATM fund transaction becomes a priority.

1.2 Aims and Objectives

The main objective of this project is to provide more security to the ATM system by using most trusted user friendly functionalities which are the One Time Password (OTP) and Biometric System. Other objectives include:-

- To evaluate the available system with the three-phase authentication system so as to create an avenue for the implementation of a more secured ATM card transaction.
- To introduce a new and well secured system which would improve the available system by at least 80%.
- Reduction by more than 85% the worrisome increasing crime rates in identity thefts and ATM frauds
- Produce a framework for maintaining huge and reliable, efficient and effective as well as easy to use but highly secured ATM transactions.

2. LITERATURE REVIEW

2.1 Overview of ATM Fraud Overview in Nigeria

The increasing number of ATM card users has been on a continuous growth within the last decade mostly as a result of more and more awareness on the e-payment system and the deployment of over 15000 ATM systems across the country with a whooping withdrawal of over 4.7 trillion Naira in 2016, [6]. As a result of the wide acceptance and usability of the ATM system, the activities of fraudsters have shown to be on the increase with even more sophisticated and technologically advanced fraudulent methods being applied. The menace and impact of ATM frauds have become so devastating on the victims and the state helplessness the banks portray most times has aggravated the panic among customers and victims. According to [7], reports have shown a continual increase in the number of victims of ATM frauds in Nigeria which contributed to a little below 10% of e-fraud in Nigeria and in 2015 over 46.6% of total monies lost through e-fraud were ATM frauds. Unfortunately, even with the level of awareness on e-fraud, very little attention is being paid to understanding the extent of its effect on the nation's financial structure and also its impacts on victims. ATM frauds have in recent years gone far beyond the cloning of ATM cards as noted by Mr. Michael Wona in 2016, a computer scientist. According to him, criminals may attach devices to ATM machines to record the account data stored on the magnetic stripe on the back of the card. This practice, according to him, is known as skimming. "The

DOI: 10.31695/IJASRE.2019.33580

card’s PIN can be spied with a secret camera or a fake number pad overlay [8]. The following fraudulent techniques mostly applied by fraudsters were outlined in a paper presentation by [9] titled “ATM frauds and security”

2.4 Types of ATM Frauds in Nigeria

According to [6] the numbers of ATM card holders have been on the increase so as to commensurate with the over 15000 deployment of ATM terminals across the country in 2016. As a result of this, fraudsters have deduced several techniques in robbing users of their resources due to the identified vulnerability in both the ATM system and users. Some of these techniques are highlighted below:

2.4.1 Skimming Devices: These are the most widely used method to illegally obtain people’s card details. The skimmers are usually installed on top of the actual card reader so that it is able to read the data stored in the metallic chip of the ATM card. Afterwards, the device is retrieved allowing the download of the information already stored in its memory. Reading and deciphering the information on the magnetic stripes of the card can be accomplished through the application of small card readers in close proximity to, or on top of, the actual card reader input slot, so it is able to read and record the information stored on the magnetic track of the card. The device is then removed, allowing the downloading of the recorded data.

2.4.2 Card Theft: Here, a couple of techniques have been applied in maliciously obtaining users’ card on of those is a card trapping device. Usually, this is placed at the card reader slot whose presence can hardly be noticed. This then prevents the card from returning to the owner at the end of the transaction. Mostly, the criminal who is in close proximity may show concern and offer to help and in the process may ask the card owner to renter the PIN. After much effort, his activities will now prove abortive and the card owner may leave in frustration. A phishing device is now used to extract the card. Having viewed the user’s PIN, the criminal now has control over the unsuspected user’s resources.

2.4.3 Fake PIN Pad Overlay: Usually an identical fake PIN pad is placed over the original keypad. This overlay captures the PIN data and stores the information into its memory. The fake PIN pad is then removed, and recorded PINs are downloaded. An additional type of overlay that is more difficult to detect is a thin overlay that is transparent to the consumer. This method used in conjunction with card trapping devices can give the criminal total control of consumers’ bank resources.

2.4.4 Shoulder Surfing: Here, the criminal places himself in close proximity to the card owner while making use of the ATM to covertly watch the user as he/she enters the PIN. In other cases, a mini camera is placed facing the machine’s keypad so as to monitor users as they enter their PIN while transacting.

2.4.5 PIN Interception: Most perpetrators of this fraudulent act usually have an insider or gain malicious access inside the ATM terminal particularly to the communication cable inside the terminal connecting to the PIN pad. Once access is secured, the criminal then installs a fishing device that would read all PIN information and card details of the users while the PIN is being transmitted to the host computer for the online PIN check. The information is captured in electronic format through an electronic data recorder.

2.5 E-Fraud Statistical Overview in Nigeria

Over the past few years the use of electronic means such as Internet banking, Mobile banking, ATMs, POS and the Web to transact businesses, transfer funds and perform other financial activities has gradually become a part of our livelihood due to its convenience, speed and efficiency and has continued to experience significant growth. According to NIBSS 2015 annual fraud report, transaction volume and value grew by 43.36% and 11.57% respectively compared to 2014. Although e-fraud rate in terms of value reduced by 63% in 2015, due, in part, to the introduction of BVN and improved collaboration among banks via the fraud desks; the total e-fraud volume increased significantly by 68.3% in 2015 compared to 2014. Similarly, data released in 2015 by NITDA (Nigeria Information Technology Development Agency) indicated that Nigeria experienced a total of 3,500 cyber-attacks which constitutes of attacks through Web, ATMs, Internet banking and Mobile transactions with 70% success rate, and a loss of $450 million within the last one year. Due to steady growth and rapidly evolving banking system by means of technological advancements, cyber criminals have over the years developed more schemes and innovations in perpetrating frauds. The popularity of the e-system has equally been a major attraction.

As we continue to witness growth and advancement in e-commerce and ATM transactions, fraudsters continue to advance in techniques of fraudulent activities. According to [11], if fraud prevention techniques do not rapidly evolve, an estimated sum of $5 to $15 billion would have been lost through card fraudulent activities by the tear.

2.6 Counter Measures in Curbing ATM Fraud in Nigeria

DOI: 10.31695/IJASRE.2019.33580

Many bank transactions ranging from deposits, to withdrawals to account opening and even enquiries are beginning to deviate from the usual physical channels to more technologically advanced methods by means of improved speed, conveniences, security and ease of use. As a result of this, financial institutions must optimize these digital means so as to meet up with the evolving trend. As the aforementioned witnesses these evolution, fraud on the other hand has become a co-benefactor of these technological improvements and so the financial institution are then tasked with striking the balance between preventing fraudulent activities and providing the customers with exceptional experience, an approach to identity proofing that accounts for the channel, product, customer, and threat environment is absolutely critical. Below are a few highlights on countermeasures to be undertaken by both banks and ATM users in curbing the already uprising ATM fraudulent activities.

2.6.1 Financial Institutions roles

- Requests for additional authentication information such as OTP, biometrics, security questions, personal information etc.
- The banks should conduct security awareness trainings by Informing users and employees about information security safety measures.
- Conduct regular visual inspections of ATMs through the use of video surveillance cameras inside and outside the ATM top box. A few ATM monitoring systems could also be employed so as to implement organizational and technical measures to protect the ATM top box and external communication lines and also conduct regular physical ATM security assessments.
- Monitor card users' pattern using threat intelligence applications that will be able to identify deviation and unusual behavior in the regular pattern of a card user and then flag likely fraud when identified

2.6.2 Card holders' roles

- Observing necessary security measures while at the ATM.
- Immediately report stolen cards or unauthorized transactions.
- Ensure that PIN is saved only in his/her memory and not disclosed to anyone.

2.6.3 Government's roles

- Monitor the situation in the black market so as to identify perpetrators hide-outs and locations of the manufactures of skimming devices.
- Set and execute strict legislation against offenders. This will discourage intending and existing fraudsters from venturing or continuing fraudulent activities.
- Ensure presence of law enforcement agents at major ATM terminals.

2.7 The Blockchain Technology

Blockchain is a growing list of records, called blocks that are linked using cryptography. It is digital information known as blocks stored in a public database. Here, the ATMs will use biometric scanners to scan the face of each account holder as part of the authentication process secured by a block chain app. Biometric ATMs will scan your face and verify ID through blockchain tech, eliminating passwords and card fraud. The traditional method of memorizing four digit PIN codes will be eliminated, thereby combating the ever present threat of credit card fraud.

The ATMs use blockchain technology to confirm the identity of each user without actually accessing the database of their bank. ShoCard tech is designed to protect user privacy during the authentication process, allowing for true-digital signature with non-perishable audit trails, transaction authorization, and frictionless login with no username or password required.

Implementing blockchain technology into cash ATMs would bring about faster, more efficient, and traceable transactions, according to a report by Finance Magnets. ATMs today are restricted to communicating with their particular financial institution as they run on the bank's operating system. Blockchain technology will eliminate this problem by easing these communication issues and tracking transactions more efficiently. Customers from varying banks can use these ATMs and the back-end processes will be far more efficient for banks. It will record all cash transactions including deposits and withdrawals on the blockchain in real-time. Customers of different banks can use an ATM even if it's dedicated to one particular bank. They also use ATMs for purposes beyond just cash withdrawal.

Blockchain does not store the user's data or information. Instead, the transactions made between identity holders and companies will only be recorded on the blockchain. Suppose there is a person named Alex, who needs to authenticate himself to apply for study abroad programs. Thus, the education centre can validate his identity faster because of the blockchain-enabled identity management app.

DOI: 10.31695/IJASRE.2019.33580

The use of blockchain technology is at a very early stage right now in Nigeria, but it is increasing at a rapid pace. Aside the Banking sector, blockchain is useful in many other sectors like retail, voting, insurance etc. One such aspect is the use of blockchain as an authentication provider, [12].

2.8 Concepts of One Time Password (OTP)

The OTP technology makes use of what is termed pseudorandomnes, which basically makes the generated codes appear random but are actually not random which makes code prediction very difficult. To add to the pseudorandomnes security technology, the concept equally makes use of what we call the hash function which equally makes it difficult to predict OTP as one who carefully observes previous pattern will still not be able to predict next code due to the hash function.

2.8.1 Various types of OTP Code Generation Approach

- The OTP code is based on time-synchronization which allows the client a short period of time to use the generated code

- It equally uses mathematical algorithm where a seed value is used to generate an infinite series of pseudo-random passwords.

- Another approach is the challenge-response authentication where a family of protocols in which one party presents a question ("challenge") and another party must provide a valid answer ("response") to be authenticated. The fourth is the lockstep-synchronization in which at every time a password is requested, the internal counter value is increased by one. On the server, each time you successfully authenticate, the server also increments its counter value by one. In this way the token's and the server's counter values stay synchronized in lock step and always will generate the same one-time password.

2.8.2 Various Media through Which OTP is Delivered

In a bid to ensure a secure channel between users and the resource database, a couple of media are recommended and have been employed and tested over the years and proven to be seldom prone to intrusion. The most widely used medium to deliver OTP is the Short Message Service (SMS). This section highlights some of the widely used media to disseminate OTP.

- **Short Message Service (SMS):** This is the commonest medium of delivering OTP to the user, majorly because of its granularity and universality since practically everyone requiring a service that necessitates an OTP generation is likely to have a phone. Here, once the user gets to the point where OTP is required, the system generates the password and sends to the users mobile number which must have been provided by the user in the registration phase. The OTP is usually time-bound and expires as soon as the time bound to it expires. The pitfall here are firstly, once an intruder gets hold of your phone, the communication channel can be easily breached and secondly the delivery of the OTP is dependent of on the availability of the user's mobile network provider.
- **Email delivery:** Just as in the SMS delivery method, the recipient email address must have been provided in the account opening/registration phase. The password is then sent to the email address of the user. As long as the user does not disclose the passcode to his email address, the OTP security and authenticity is somewhat guaranteed. A few of the disadvantages observed with this medium is that the user must have access to the internet at that particular time; secondly, this is dependent on the mail server host. Lastly, it may not be as ubiquitous as the SMS.
- **Token:** This is a security hardware device or software program that is capable of producing a single-use password or PIN passcode. Just as some financial institutions have employed, tokens are being issued to users based on requests. The tokens then contain passwords which change at interval. The password on display at a particular time will be valid for input for as long as it remains on the token screen. Since this is a hardware device, it is likely to get lost or fall into the wrong hands.

2.9 The Biometric Authentication Approach

Biometrics is unique in the sense that it is based on the inherent characteristic of the individual. It authenticates the user based on who they are as opposed to what they know or what they have. Another advantage of biometric identifiers is they cannot be guessed, forgotten, misplaced or easily forged unlike the knowledge-based and the possession-based identification schemes.

[3] described a biometric system is a technology which takes an individual's physiological, behavioral, or both traits as input, analyzes it, and identifies the individual as a genuine or malicious user. The vast use of information Technology in the banking sector and also the increasing rate of frauds have necessitated the immense need to safeguard consumers' properties and resources. Below are some highlighted uses of biometrics.

DOI: 10.31695/IJASRE.2019.33580

2.9.1 How Biometric Authentication works

For a Biometric authentication to be successful, the scanner must compare two sets of data. One of which in some cases is stored in a database which the scanner can access for comparisons, while the second is provided by subject to be authenticated. The scanner is set such that the match between the subject and a file in the database reaches an identical percentage. This cannot be a 100% match so as to give room for exigencies such as a sweaty finger, scar, and health anomaly.

2.9.2 Types of Biometric Authentication Technologies

There are several methods of biometric authentication and each of them have a unique quality or feature that makes it stand out and so it will be difficult to say a particular form of biometric authentication is the best. The choice of a particular biometric authentication technology is chosen based on the consideration of certain factors such as the target users, environment, convenience and so forth. A few of the authentication technologies are highlighted below:

Fingerprints Identification: This is has been identified as the most widely used method of biometric authentication based on its usability, acceptability and uniqueness as research has shown that in over 140 years of fingerprint comparison worldwide, there has been no same match for two different persons. In fingerprint identification, the scanner compares the furrows and minutiae (This is a point on the finger where a ridge splits in two or terminates) at the finger tips with what is stored in the database. Access will be granted only when a match is found. The pitfall here is that dirty fingers may alter the readings and so it may not be easily applicable in industries.

Facial recognition: This is best employed in crime investigation as a suspect can be scanned even without his/her knowledge, it can equally search through a crowd of faces within minutes. The facial recognition scanner systematically analyses some facial features such as the width of the nose, distance between the two eyes, and position of the cheek bone which are then converted in codes and stored in a database.

Retina Scan: This is mostly used in the military. Just like other biometric technologies, the retina scan is equally highly unique as this makes use of the pattern of blood vessels behind the eye which is unique for everybody. The pitfall here is that the subject will have to remain in a state of careful concentration for about 20 seconds for a good reading.

Voice recognition: This can be used for both voice authentications by comparing the subject’s voice to an already existing data in the repository for access control and voice identification by attempting to determine an unknown speaker where his voice is being matched to a number of samples mostly for investigative purposes. The challenge here is that the voices could be faked through recorders making it difficult to identify.

3. SYSTEM METHODOLOGY, ANALYSIS AND DESIGN

3.1 Sources of facts finding

In the investigation of the existing system, oral interview with ATM fraud victims and general ATM users was conducted, review of relevant literature and publications, and also distribution of questionnaires formed the sources from which the facts on the analysis of the existing system were obtained. In order to comprehensively study the existing system to be sure that the pitfalls and weaknesses the investigation covered a wide area with a random selection of respondents and interviewees. Some of the methods employed in information gathering are:

3.1.1. Personal Interview

The deductions from the interviews conducted revealed that a number of factors such as illiteracy, trust and issues of vulnerability have contributed in making theft through ATMs successful.

Deduction from personal Interview on contributors to ATM theft

Illiteracy of card Users: Some card holders who have no idea on how to use the ATM sometimes depend on people to make their transactions for them. In the process card and PIN details maybe compromised. One of the interviewees replied: “*I received the ATM from the bank and nobody told me how to use it. I met a man at the ATM stand and asked him to help me withdraw five thousand Naira and gave him my PIN. It was when I got home I realized he had switched my card.”*

Trust: The interview sessions equally revealed that trusting the wrong persons has equally been a major contributor to this menace. The story of a young man during the interview session helps illustrate this. He gave his ATM card and PIN to a friend to make a withdrawal on his behalf, the friend never returned and had parted away with all he had at the time.

The Coercion Factor: Some of the interviewees reverted that they have lost their resources through ATM by forceful means, ranging from armed robbery, to forceful compulsion and then to bag snatches. In this case, the perpetrators mostly track the most vulnerable victims in areas of less security.

From the above findings, I have discovered that most or all of these incidences can be averted if there were a third phase of verification most especially through inherent factors.

Figure 3.3 below shows more explicitly the flow of activities in the current ATM structure in the form of an activity diagram. This illustrates all stages of operation from card verification to PIN authentication up to cash payment.

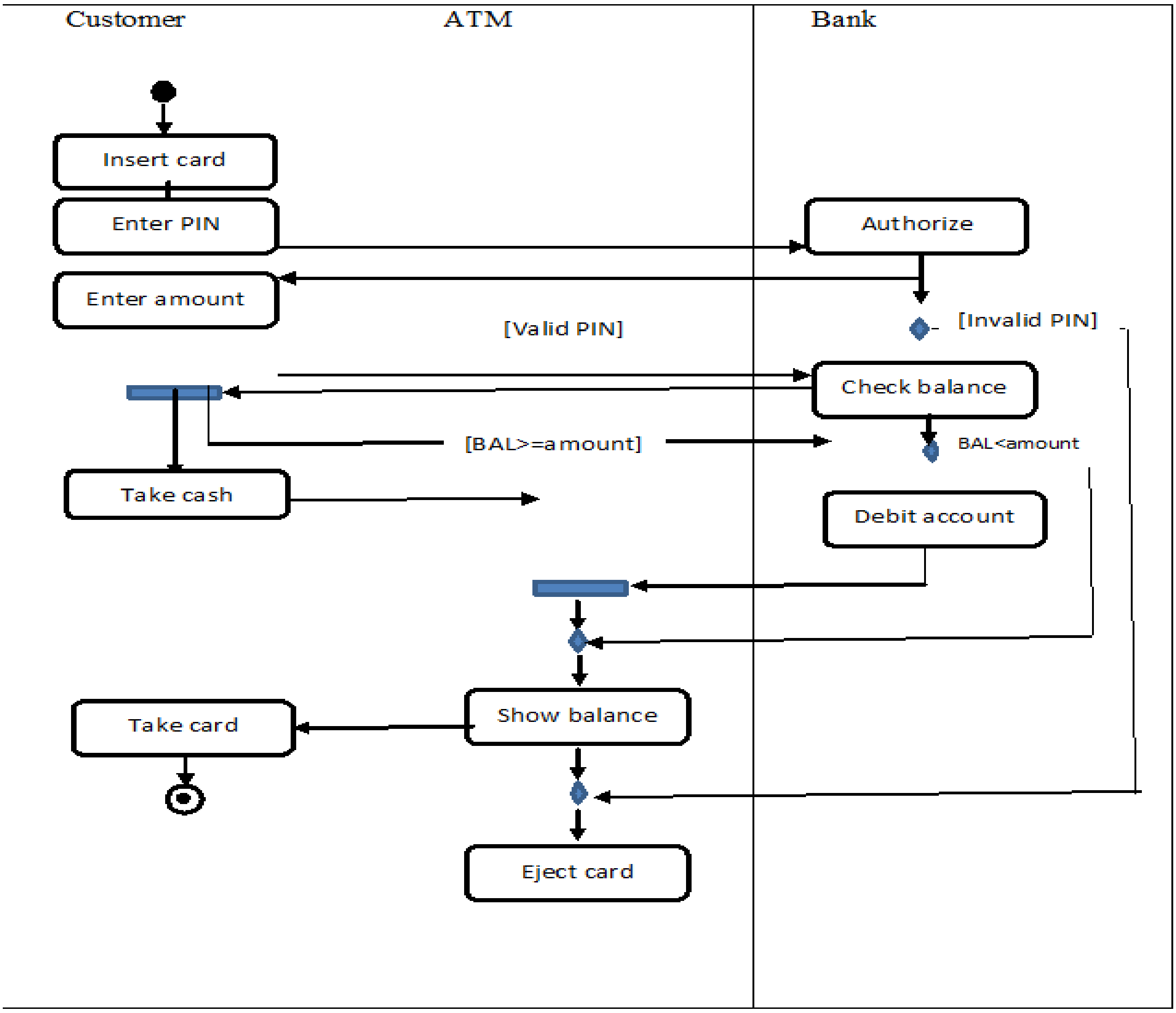

Figure 3.1: An activity diagram for the existing system

3.1.2 Distribution of questionnaires.

In order to comprehensively study the existing system to be sure that the capabilities and weakness of the existing system are fully explored, randomly selected areas within the Abuja metropolis were selected and the locals were interviewed in a bid to obtain their perception of the current ATM structure with regards to its security. Below are details of the facts deduced from some of the methods of information gathering.

Table 3.1: Results from questionnaire distribution

Variables	Categories	Frequency	Percentage (%)
How convenient ATM is to	Convenient	22	88

DOI: 10.31695/IJASRE.2019.33580

respondent	Not convenient	3	22
Observe ATM security measures	Yes	18	72
	No	2	14
	No answer	2	14
Perception on ATM security	Secured	9	36
	Somewhat secured	12	48
	Not Secured	4	16
Disclosed PIN to another	Yes	23	92
	No	2	8
Perception on biometrics/OTP for ATMs	More secured	16	64
	Will be difficult to use	3	12
	Indifferent	6	24
Ever been a victim of ATM fraud	Yes	16	64
	No	9	36

From the interaction made at the course of the questionnaire distribution and personal discussions, we can see that most cases of ATM frauds are successful due to the nature of the various authentication layers. More so, the answers received after the distribution of the questionnaires equally suggests that the proposed framework for the new system has a high acceptability rate and so deployment and integration may not be much of a challenge.

3.2 Analysis of the Proposed System

The proposed system is a web based application which provides two additional layers of authentication in the ATM authentication process in which one can be used in place of the other. The idea is to maximise ATM security while also considering users' convenience and comfortability. The proposed system intends to leverage on the platform and security of the existing system while also accommodating all the solutions to the problems of the existing system which are listed above. The following stage outlines the steps involved in the proposed ATM withdrawal process.

3.2.1 Card Verification.

Here the user is prompted to insert his card inside the ATM's card reader for verification and authentication through the card's metallic strip. If the card is considered valid, the machine then asks the user to provide PIN information.

3.2.2 Pin Authentication.

After the user inputs his PIN, the system then matches the newly provided PIN to what it has as the PIN in the data base which is tagged to the already inserted card. Once the information matches that in the database, the ATM then prompts the user with the option of either proceeding with OTP or with biometrics. Else, the system rejects the PIN and asks user to re-enter the PIN. After 3 failed trials, the system blocks the account from further transactions, withholds the card and advises user to contact his/her bank.

3.2.3 OTP/Biometric Authentication.

The OTP and biometric authentication options are displayed at the same time, where the user can choose either of the two provided options. A successful verification of either of the two authentication layers (OTP/Biometric) gives the user full access to the account. What happens at the back end just like we had in the PIN verification is that the system compares either the provided OTP or biometric information depending on which is provided with what it already has in the database. When an OTP is sent, the system registers the same number in the database which lasts only as long as the OTP is valid through. On the other hand, upon account registration process, the user is asked to provide biometric information which is stored in the database and tagged to the user's card. Therefore, when the user provides the biometric information, the biometric identifier then collects the information and sends to the database for verification. Once the biometric information matches that which is tagged to the ATM card, the user is given a go-ahead. Should there be an OTP mismatch, the transaction is then. After 3 consecutive failures, the account is blocked, ATM card withheld and user is advised to contact the bank.

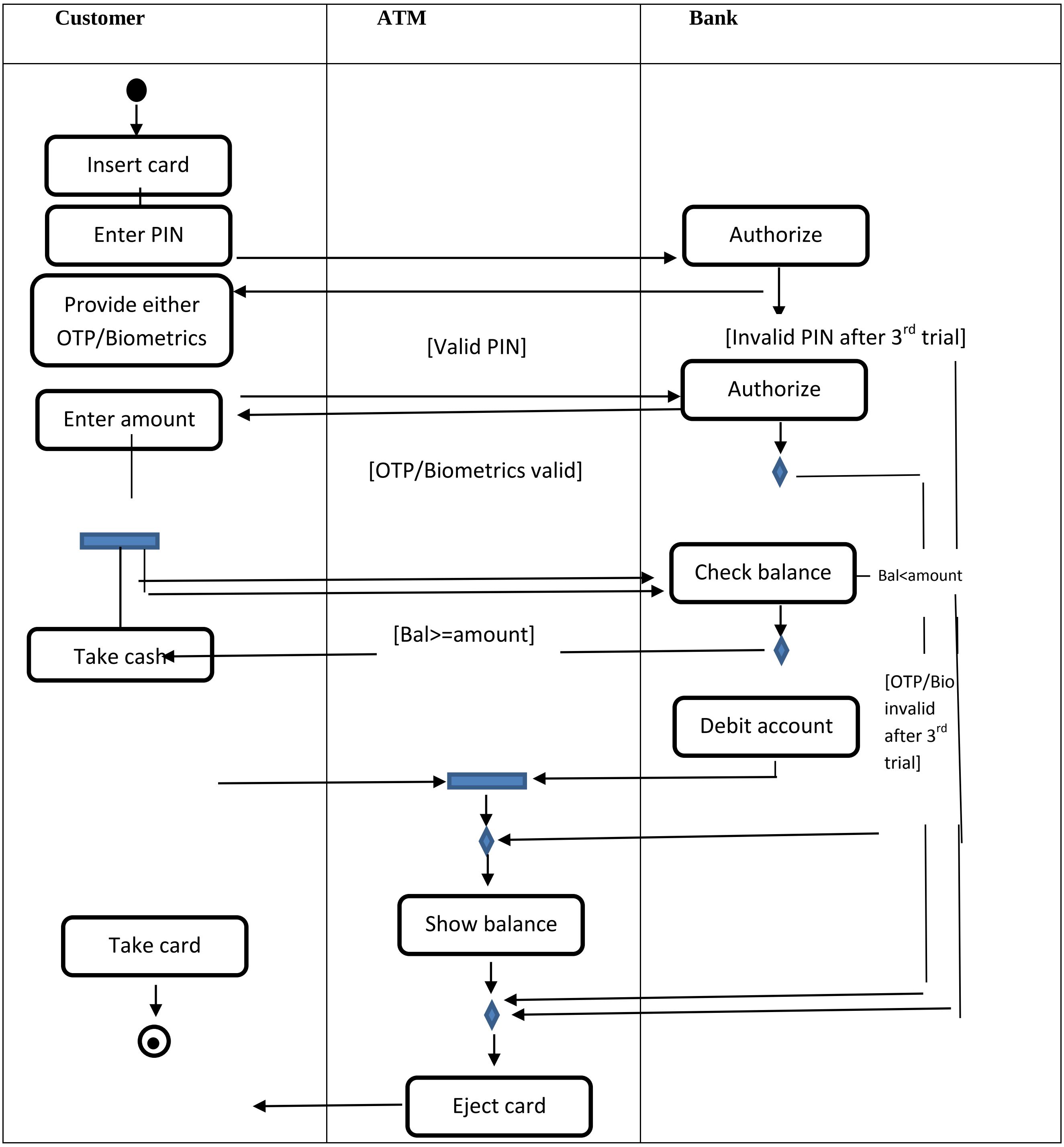

Figure 3.2: An activity diagram for the proposed system

Figure 3.2 above shows the flow of activities in the new system for the ATM transaction processes starting from the point the user inserts his card to the point the transaction is ended and card ejected.

3.3 System Flowchart

DOI: 10.31695/IJASRE.2019.33580

Figure 3.3 below shows the flow of transactions for the proposed system. The flow chat starts with the ATM user inserting his card and providing PIN details. These inputs are then verified by the system and if authenticated, the system then allows the user to proceed to other verification processes. Else, the user is prompted to re-enter required detail

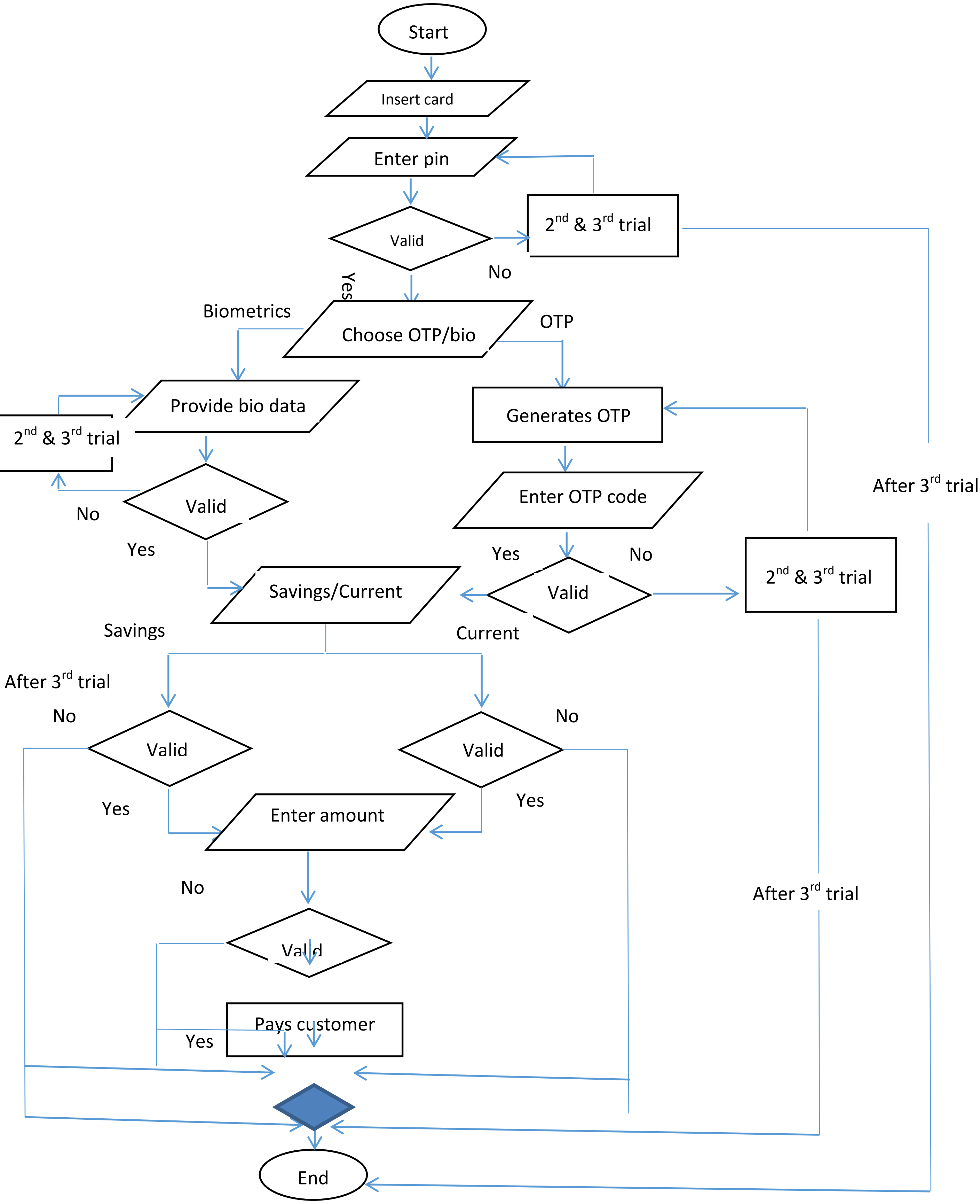

Figure 3.3 Proposed system flowchart.

DOI: 10.31695/IJASRE.2019.33580

Figure 3.4 below shows the general use case overview of the proposed system, illuminating explicitly the various jurisdiction of each actor in the use case. The system contains two actors which are the ATM user and the system. The use case diagram below highlights all the user access and privileges. It equally highlights entities that are common to both actors and those that are unique to only one actor. This implies that such entities will be restricted to the actor who does not have a relation with the entity.

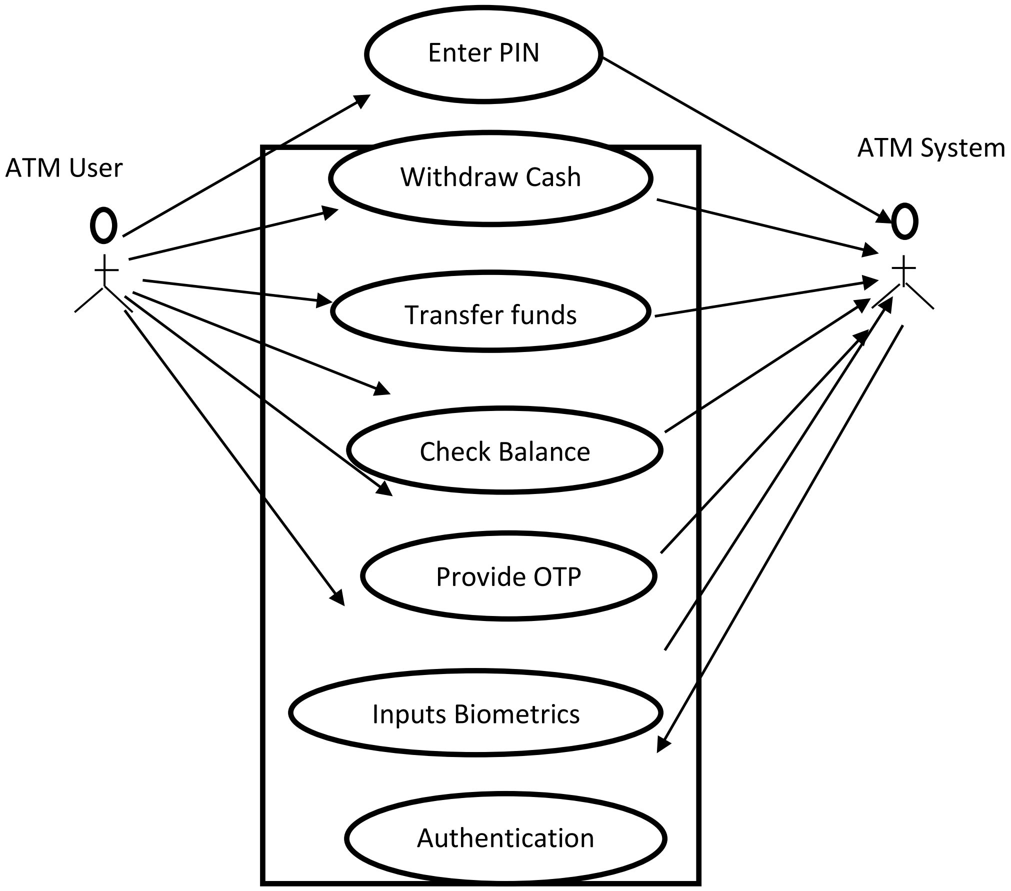

Figure 3.4: A use case diagram for the proposed system

4. SYSTEM IMPLEMENTATION SCHEDULE

An implementation period of about one year is proposed for this research work. This is putting into cognizance the newness of the proposed system which will then require and necessitate a structured sensitization programme so that the intending users may better appreciate the need for the change. Furthermore, the financial institutions will then commence biometric information collection and finally the deployment of biometric enabled ATM systems and installation of the developed software into the ATM's operating system.

Table 4.1: System Implementation Schedule

Phase One	Training and sensitization	2 months
Phase Two	Data collection	4 months
Phase Three	Infrastructural deployment	6 months

4.1 System Testing Scenarios

The following test cases will be carried out prior to the deployment of the proposed system. This is in a bid to achieve a seamless implementation process.

DOI: 10.31695/IJASRE.2019.33580

Table 4.2: System Testing Scenarios

Use Case	Test function	Initial system state	Input	Expected Output
OTP Verification	Customer is asked to provide OTP code.	Displays OTP code request	Provides incorrect code	Error message displays. User is asked to renter code. Terminates transaction after 3rd trial.
OTP Verification	Customer is asked to provide OTP code.	Displays OTP code request.	Provides correct code.	Transaction proceeds to next phase.
Biometrics authentication.	Customer is asked to provide biometric information.	Ready to accept biometric information.	Provides unrecognized biometric details.	Error message displays. User is asked to renter bio data. Terminates transaction after 3rd trial.
Biometrics authentication.	Customer is asked to provide biometric information.	Ready to accept biometric information.	Provides recognized biometric details.	Transaction proceeds to next phase.

5. SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Summary

This project is developed on the basis of the increasing need for a secured interaction with the ATM systems. With the advancing technology, modalities to hack/crack ATM PIN or ATM card are becoming more sophisticated. It is only imperative that a counter and even more sophisticated measure be put in place to secure our ATMs. The use of OTP and Biometric has proved to be very efficient measures against these security threats. This project employs the use of SHA-1 hash string algorithm to generate OTP with more randomness provided in the proposed system. The OTP will be sending authentication code to the user's registered mobile. The biometric scanner on the other hand serves as an alternative option to the OTP at the occurrence of unforeseen circumstances such as loss of phone, poor network coverage etc.

5.2 Conclusion

The development of this work springs from the need to bring to the barest minimum occurrences of theft through ATMs which has in recent years, emerged with sophisticated ways to hack and crack ATM PINs. To achieve the above stated, this work employs the use of two highly secured authentication factors: The biometrics and OTP. At the point of sale, the user is expected to provide either of this information based on his preference after the PIN verification.

The implementation of this work would require a total overhaul of the ATM transactions structure, ranging from the sensitization of users to changes in the ATM system algorithm and even down to physical changes on the ATM hardware.

5.3 Recommendation

The aim of this work is geared towards securing ATM users' resources. However, there is a limit to how much security this work can provide as this cannot ensure physical security on users. With that being said, it is highly recommended that the government pays critical attention to this emerging menace by setting strict legislations against perpetrators so as to discourage to a large extent further occurrence. More so, this work proposes that surveillance cameras and police patrol be installed within the vicinity of certain strategic busy ATM sites.

REFERENCES

[1] Obiano, W. (2009). How to fight ATM fraud. Lagos, Nigeria: Online Nigeria Daily News.

[2] Ahmed et al. (2015). Fraud vulnerability among ATM card users in Nigeria. Dutse, Jigawa: Dutse journal of pure and applied sciences.

[3] Ashbourn, J. (2000). Biometrics: Advanced Identity Verification: The Complete Guide. Verlag, London: Springer

DOI: 10.31695/IJASRE.2019.33580

[4] Adeoti, J. (2011). Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out. Ojo, Lagos: Journal of Social Sciences, Lagos State University.

[5] The Nilson's report. (2016). Credit card and Debit card fraud statistics. Washington: Robertson

[6] Emeka A. (2017) Fraud Alert - Banks Raise Fresh Alarm on ATMs. Lagos: Vanguard Newspaper.

[7] Akintunde A. (2017). "How Nigerian ATM fraud Victims are swindled" REUTERS, University of Ibadan, Oyo State Nigeria.

[8] Olakunle O. (2016). "ATM Fraud: More Nigerians lose Money to Scammers" Sun Newspaper, Lagos.

[9] Diebold I. (2002). "ATM frauds and security": White Paper, New York, USA.

[10] Emeka A. (2007). "Fraud Alert – Banks Raise Fresh Alarm on ATMs, Vanguard Newspaper, Lagos.

[11] Tej P.B., Vikram, P. and Amit D. (2003). "Understanding Credit Card Frauds", Cards Business Review#2003-01, Tata Consultancy Services 2002.

[12] Gupta. R (2018). "Hands-on cybersecurity with blockchain: Implement DDoS protection, PKI-based identity, 2FA, and DNS security using blockchain.

DOI: 10.31695/IJASRE.2019.33580