**OPTIMIZING PLASTIC CARD FRAUD PREVENTION USING ONE TIME PASSWORD**

**BY**

**OGUIBE GOD’SALVATION FECHUKWU**

**UJ/2012/NS/0401**

**DECLARATION**

I, OGUIBE GOD’SALVATION FECHUKWU with the matriculation number UJ/2012/NS/0401, hereby declare that this project work was carried out by me and every other external work used in this project has been duly acknowledged.

**APPROVAL**

This project has been read and approved as having satisfied the requirements of the Department of Computer Science, Faculty of Natural Sciences, University of Jos, Nigeria for the award of Bachelor of Science (B.Sc.) Degree in Computer Science.

**DEDICATION**

This project work is dedicated to Almighty God, who is my Author and Finisher, for providing guidance, wisdom and grace throughout the entire period of this research work. To my family chiefs, I really love and appreciate you all beyond words.

**ACKNOWLEDGEMENT**

I wish to acknowledge my Almighty God for the gift of life, his direction, grace and inspiration that made this research a success.

My sincere gratitude goes to my Project Supervisors, Mr. Ndukwe Ifeanyi and Miss MaryJane for their guidance and input in the achievement of this work. Also to all my lecturers, God bless you all.

To my Father, Fidelis Oguibe, whose constructive discipline gave me the patience to embark on exploration research that formed this project, my dear mom, Mrs. Agnes Oguibe, her unending love, support, ceaseless prayers and encouragement were strength to me all the way, my siblings, Foundation and Ada; My mentors, Professor John Mawak, Dr Owoeye and Pastor Ikechukwu, I appreciate all your support and encouragement. May God bless and be with you always.

My thanks to the entire 2016 graduating class of Department of Computer Science, all my friends in the school and business space; who were a very huge and constant source of strength and encouragement to me; I pray they find favor in their different fields of endeavors

**DEFINITION OF TERMS**

**Cyber Crime**: also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy.

**Cyber security**: also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction

**Plastic Payment Card**: A payment card is a device that enables its owner (the cardholder) to make a payment by electronic funds transfer. The most common types of payment cards are credit cards and debit card. Payment Cards were introduced into Nigeria some years ago but suffered low acceptability at the initial stage due to a number of factors which included amongst others: lack of shared network, epileptic services, limited ATM and Point of Sales (POS) Terminals and high cost of operations. The Central Bank of Nigeria in an attempt to promote the use of cards for making secured payments in Nigeria, issued relevant guidelines on e-banking in Nigeria in 2003, 2009, 2010 and 2011.

**Fraud**: can be described as deceit or trickery deliberately practiced in order to gain an advantage over someone dishonestly.

**Plastic card fraud**: This is defined as using plastic payment cards, such as ATM, debit, credit or store cards to take money without permission or prior knowledge from a bank, building society or credit card account owner.

**One- Time Password**: It is a unique 6-character **code** that can only be used once and is sent only to your registered mobile number.

**Vulnerability**: In information technology (IT), is a flaw in code or design that creates a potential point of security compromise for an endpoint or network.

**Transaction:** This is the electronic exchange or transfer of money from one account to another.

**Debit:** This is an accounting entry that results in either an increase in assets or a decrease in liabilities on a company's balance sheet.

**Automatic Teller Machine (ATM):**

This is a computerized machine that permits bank customers to gain access to their accounts with a magnetically encoded plastic card and a code number. It enables the customers to perform several banking operations without the help of a teller, such as to withdraw cash, make deposits, pay bills, obtain bank statements, effect cash transfers. Also called automated Banking machine, automatic till machine, or remote service unit

**ATM card:** This is a PIN-based card. That means that in addition to using it at ATMs, you may also be able to use it to make purchases (by entering your Personal Identification Number) if the merchant is using one of the same electronic ATM networks that’s listed on the back of your card.

**Debit card**  
A debit card looks just like a regular ATM card, and you can use it at ATMs. The difference is that a debit card has a Visa® or Mastercard® logo on its face. That means you can use a debit card wherever Visa® or Mastercard® debit cards are accepted, for example, department stores, restaurants, or online.

****

**Credit card**  
A debit card is **not** a credit card. When you use a debit card, the money is deducted from your checking account. With a credit card, you’re borrowing money to be repaid later  
****

**Introduction**

1.1 **BACKGROUND TO THE STUDY**

The vertical and intensive growth of technology has led to strong emergence of internet banking, intra bank/interbank transfer using plastic cards, web pay or other online related services that ranges from electronic mails, instant messaging, blogging to that of computing and other admirable benefits of technology.

Several innovative services such as Automatic Teller Machine (ATM), internet banking, smart cards, credit cards, mobile banking, phone banking, Anywhere-Anytime baking have provided a number of convenient services to the customer. As the service quality improves, the customer satisfaction has witnessed substantial growth. Increase in customer satisfaction in turn increases the mutual understanding, customer retention and a bond of trust between the customer and the bank. Among all these incremental advantages which have consistently redefined technology from a simple spectrum to be a new or better way of doing something, the internet/technology comes with disadvantages with the major one called “Plastic Crime”, “Cyber Crime” or “Internet Crime”.

Cybercrime is the term used to describe criminal activities committed online or in cyberspace that take advantage of vulnerabilities in the target system. (Report from the Internet Crime Complaint Center (IC3), 2009

The pervasiveness of the internet, the flaws in both man and technology, the struggle against time and the market, and greed have all led to problems that must be resolved. These difficulties have taken many different forms, including collusion, system failure, compromised passwords, compromised data, knowledge gap, backdoors, identity theft, session/credential hacking, surfing, Lebanese loop, using stolen cards, skimming, card swapping, SIM card cloning, and phone hacking, among others, which have led to cybercrimes or card frauds. The emergence of the Internet Banking lead to the introduction of Plastic payment cards that provide a suitable and secure medium which people conduct a variety of financial transactions. This has overly lessened the risky burden of carrying lot of money by individuals, and therefore, the risk of being attacked by armed robbers or malicious folks. It also solves the problem of money laundering and unchecked swap of funds.

Amist this mind blowing innovation of E-banking and plastic payment cards lie the propagation of new crime opportunities called “plastic fraud”.

Plastic fraud is defined as the use of plastic payment cards such as Debit card, Credit card or store card information to perform transactions without the prior knowledge or the permission of the owner, or the issuer. (Moon et. al, 2010).

Doing business in cyberspace or electronically therefore need informed, conscious and calculated management of risk. Due to the abstract, technical and pervasive nature of the internet, organizations need services of Information Security, Technology, Risk and Compliance experts to manage risk. They all need proactively gather and analyze information on security gaps, vulnerabilities, challenges and incidences to track and counter security threats making cyber intelligence a must.

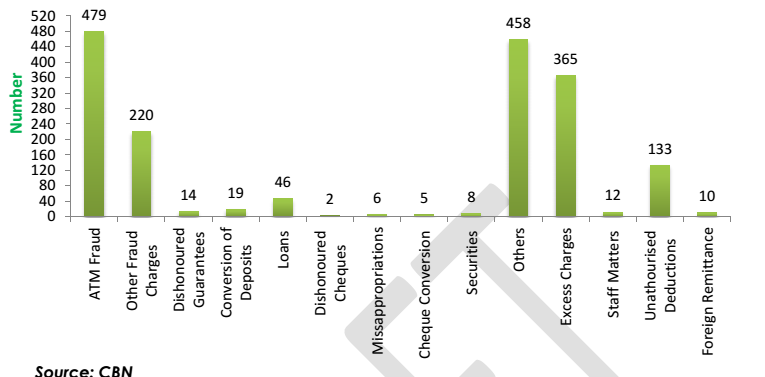
In November 2013, more than 40 million customers had their credit card and personal information stolen as a result of a data breach at a major retail outlet in the US. The estimated cost of this incidence was close to $150 million.

**1.2 STATISTICAL REPORT ON FRAUD CASES**

The Nigerian baking sector recorded 12,279 fraud cases involving the sum of N18.02bn in the 2015 financial period. Nigeria Deposit Insurance Corporation. This represents an increase of 15.71 per cent over the 10,612 recorded in 2014. The study show that 15.71 per cent increase in the incidence of fraud for 2015, hat amount decreased by N7.59bn or 29.63 per cent from N25.6bn in 2014 to N18.02bn in 2015. The reported stated that actual loss sustained in respect of internet banking fraud was N857m, representing 27 per cent of the total actual loss of the industry.

There was an increase in frequency of ATM/card-related cases from 7,181 in 4014 to 8,039 in 2015, an increase of 11.95 per cent.(Nigeria Deposit Insurance Corporation (NDIC) annual report in 2015).

According to Annual Economic report – 2014, The number of reported cases of fraud



In collaboration with key stakeholders, the bank and other fraud management agencies have deployed anti-fraud features, based on predefined rules with strong ability to checkmate suspicious card transactions. Some of these security features on E-products include the introduction of two factor authentication (Token), one Time Password capabilities, limit based transfer, MasterCard InControl, ScoreBridge, PinGuard, Anti-Skimming Device and lot more.

Once a transaction fails an authentication process and is pinged as suspicious, the system ends a request to the card issuer to confirm the validity of the transaction so as to take incorporate on ground means to abort any suspected ills.

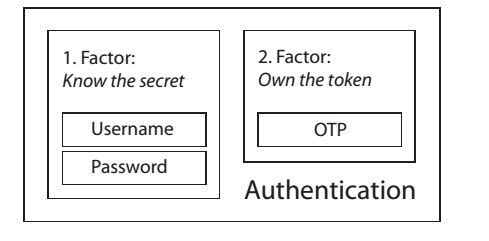
**1.3 Authentication**:

the method a system uses to confirm and authenticate a system user's identification using information like their user ID and password. (Parameswari D., 2011). It is a technique of confirming that a claimed identity is accurate in order to make sure that users are who they say they are when they access a system at a specific time. One or both of the three forms of information—something one knows (such as a user password or pin), something one owns (such as tokens (soft or hard) or smartcards), or something one is—are required for authentication (e.g., Biometrics, Finger prints or Iris scan).

**1.4 One Time Password**: A one-time password (OTP) is an automatically generated numeric or alphanumeric string of characters that authenticates the user for a single transaction or session.

An OTP is more secure than a traditional or static password, especially a user-created password, which is typically weak. OTPs may replace the knowledge based authentication or may be used in addition to it, to add another layer of security. This is a two factor authentication, a strong optimum security methodology to significantly elevate the safety level of the authentication process. (<http://searchsecurity.techtarget.com/definition/one-time-password-OTP>­­)

The traditional method of authentication using a username, password, and personal identification number (PIN) is insufficient. Personal information can frequently be obtained, for example, through phishing, social engineering, packet sniffing, or because of weak protocol. A higher level of security was therefore required. A hardware (or software) secure token that acts as an addition to current user IDs generates an OTP. The token creates a valve that can only be used once and, in some cases, for a brief amount of latency. It uses a knowledge factor and a possession factor-based two-factor (2FA or TFA) authentication system. Prior to using an ATM, the user must first be familiar with the traditional logon information (PIN) as in the case of using an ATM credit or debit card or the username and password as in the case of internet banking or mobile banking app platform and inclusively has to own the token or receive a soft token on registered SIM to successfully validate any transaction.. The OTP is usually derived based on timestamps, usage counters, secret key stored on the token by, eg., hashing or encrypting the valves.



(Young, 2010) stated there are two popular model of OTP solutions. The time-based OTP (TOTP) and HMAC-based OTP (HOTP) which can also be called the event based. The HOTP algorithm is based on a secret key and counter shared by the device and the server, and uses standard algorithms such as SHA-1 and HMAC (Jose et. al, 2011) defined security token is a physical device that an authorized user of computer services is given to aid in authentication. He also referred it to as an authentication token or a cryptographic token. He investigated the two formats of token: hardware and software. Hardware tokens are portable, compact devices that are easy to carry. A PIN that varies over time is displayed on some of these tokens, while others store cryptographic keys or biometric information. When a user wants to log in, or authenticate, at any given time, he needs both his regular account password and the PIN that is displayed on the token. Software tokens are computer applications that offer a PIN that changes over time. These applications use the One Time Password (OTP) algorithm. The security of systems using OTP algorithms is essential since unauthorized users shouldn't be able to predict the next password in the series. As there has been an exponential growth of smartphone usage nowadays, software-based OTP generators have been developed and integrated on Smartphones as software apps. As a result of the acceptance of smartphone usages, the software-based OTP solutions bring no extra burden to the users and are economical to use. (Kun et al., 2014)

**1.5 Motivation**

To say that we have made significant progress do not mean that the work has been completely done. The fight to checkmate cybercrime and plastic card fraud is a war between the fascinating technology propellers and intelligent criminals. Every common Nigerian has witnessed account compromise either by own or by a loved one.

Though for the purpose of this research, I will narrow my scope to only ATM- Plastic card frauds as I would not go into internet banking/E-banking cases. However, I will still site some potential defaming criminal activities including cybercrimes which has poised harm to both the users and the country at large.

Being someone that loves to explore the media, I have read about much cases of ATM fraud in Nigeria. According to a Nairalander who once withdraw from an Eco bank ATM at Alaba before making some number of stops down to Ikorodu. On getting home, he discovered his ATM card is missing. Though not worried at first, on getting to his bank or account verification and loss of card complaint, he was told a total of N135,000 has been moved from his account the previous night. (<http://www.nairaland.com/1251926/atm-card-stolen-money-withdrawn>, 2013). This particular case combines the ability of the criminal to obtain the user PIN and to successfully move his money out of his account without being detected immediately as there are no watchdog to check authenticity of customers or confirm unauthorized transactions.

I got an alert on my phone that a transaction of N490,000 was made. I didn’t understand the text because I never withdrew any money. Immediately, I called my account officer to inform him. As I finished talking to him, a new text came in that another N490,000 had been withdrawn. I called the account officer back and told him the latest development. He asked if I had misplaced my ATM card, and I said no because the card was with me,” Mr. Awe narrated. He said that the bank officer immediately promised to notify Interswitch, the ATM service provider, so that the card could be blocked.

He said further: “About 10 minutes later, another alert came in that N80,000 had been withdrawn. In total, N1,060,000 was withdrawn from my account on the same day. Initially, the bank acknowledged the case after writing through my lawyer, but for several months now nothing has been done on the matter. When I went to the bank in Apapa to challenge them, they used armed security men to force me out of the bank premises. I’ve gone to human rights activists and the EFCC for help but nothing has been done till date.” (<http://thenationonlineng.net/horror-stories-from-your-atm/>, 2016).

A personal friend of mine had his whole money transferred out by his own cousin owning to the fact that he had access to his plastic debit card and PIN as they live in the same apartment. This, I blame to the single authentication process of completing money transfer using ATM plastic cards. It could happen to anyone as your own spouse could move money out of your account due to ability to hold onto your ATM card and Personal Identification number.

A graduate of pure mathematics from the University of Maiduguri on, 20th March, 2017 attempted to withdraw N110,000 from another customer’s account after stealing his transfer slip, then forging the victim’s signature on a bank withdrawals slip right there in the bank before proceeding to carry out the fraud (Vanguard, 2017). Though, caught and arrested by the local authorities, this type of fraud could be successfully carried out.

In a study, researchers say that the widespread usage of dates of birth as PIN codes is primarily to blame for the weakness. Based on this number of cases and more undocumented or unreported once, I was overly motivated to focus this project in integrating the OTP in ATM human teller and transfer services.

This will help in educating the public and thereby strengthening the economic security in the banking space.

**1.6 Problem Statement**:

From my motivation above, it is significant, the threat plastic card fraud poises to the society at large and the purpose of this work is to optimize the various fraud prevention processes using one time password as a stronghold. Hence, this software will checkmate illegal interbank transfer by integrating an extra layer of security for card users. This software, when implemented, will provide the user with a more secure platform so as to avoid successful unauthorized transfer of fund. This work intend to identify and evaluate

1. The challenge single authentication method poise in the Banking system
2. The role multiple factor authentication plays in securing the economy
3. OTP and its usefulness in checkmating plastic card fraud.

**1.7 RESEARCH QUESTIONS**

In the course of implementing this project work, the following questions might need to be addressed

1. Is the plastic card fraud-fund transfer software deliverable or achievable
2. Is it an efficiently working study
3. Is the research implementable
4. Can further recommendation from this research be integrated
5. Can further evaluation techniques be carried out based on existing benchmark

**1.8 AIMS AND OBJECTIVES OF STUDY**

**1.8.1 AIM**:

The primary aim of this work is to design a system with significant implementable deliverables for preventing plastic card fraud in an ATM fund transfer platform.

**1.8.2 OBJECTIVES**:

1. To carry out thorough research and obtain sufficient knowledge of fraud related issues in Nigeria.
2. To develop a model and an algorithm for the proposed system
3. To develop a fraud prevention software using One Time password and integrating such model for proposed fund transfers using plastic card.
4. To interpret and make recommendation to ensure adequate crack down of plastic fraud.

## 1.9 METHODOLOGY

The proposed methods for achieving the above objectives are as follows;

1. Observational Studies
2. Documentation Review
3. Interviews
4. User report

Here, the source of data, collection and evaluation of data that are presented

The proposed system will be designed using Object Oriented Programming (JAVA to be specific). This language is the best fit in developing this software that will

**1.10 SCOPE AND LIMITATIONS OF STUDY**

The design of this software is limited to only the integration of One Time Password in the course of making fund transfer using ATM. The ATM will only be eligible to perform human teller activities, print mini statement, view account balance, pay bills. This ATM, therefore does not allow cash deposit nor cash withdrawal. Hence, the One Time Password does not apply to electronic transfer either by using mobile smartphone applications or using the conventional bank dialing codes which varies.

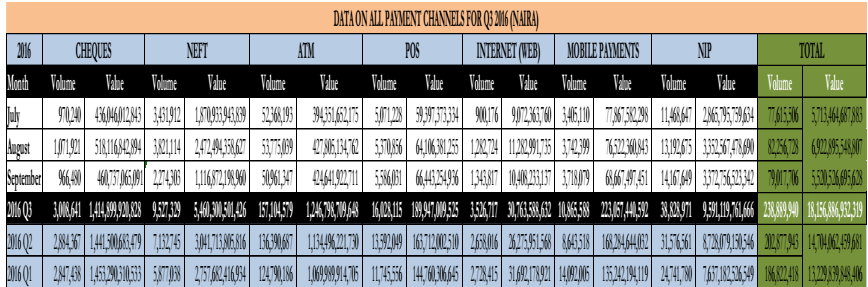
1. A user inserts a valid debit plastic card;
2. Types the correct card Personal Identification Number;
3. Selects account type;
4. Select Interbank Transfer
5. Chooses beneficiary’s Bank name
6. Selects beneficiary’s account type
7. Enters amount to be transferred
8. Confirms the amount and account Number
9. OTP is sent to user’s registered phone number
10. User authorizes transaction using supplied OTP
11. Transaction is completed, if One Time Password is correct.

Therefore we aim a using commercial smartphone to achieve a secure one time password solution with the same security level as hardware OTP tokens.

**CHAPTER TWO**

**2.1 Literature Review**

The ATM concept is relatively dated and has undergone constant development on a global scale. Since there have been so many ATMs installed around the world, many theoretical, empirical, and unbiased studies have been conducted in an effort to turn the global economy into a cashless one. (Saxena, 2011). The ATM is a cutting-edge method of service delivery that provides a range of economical and financial services, including cash deposits, withdrawals, fund transfers, utility payments, balance inquiries, and other financial enquires. (Khan, 2010). Rose (1999) described ATM as follow: an ATM combines a record keeping system, computer terminal and cash vault in one unit, permitting customers to enter the bank’s record keeping system with a plastic card containing a Personal Identification Number (PIN) or by punching a specific code into the computer terminal linked to the bank’s computerized records 24-hours a day. A user has access to an ATM machine by using an ATM card.

 Source: CBN

An ATM card is a card that allows the bank account holder to do same things at an ATM as he or she would do at a bank (Woelfel, 1994). Islam et al., (2007) also referred to ATM as a type of innovation that can mechanically accepts deposits, issue withdrawals, transfer funds between accounts, collect bills and make account enquiries. An optimal ATM is a sure bet of improving service quality in the banking industry.

Semore (1992) advised that the ATM in the advanced countries has been programmed to perform varieties of functions.

Therefore, the advancement of ATM technology may be viewed as both a benefit and a curse. The same technology that increases the effectiveness and profitability of trade is also systemically opening up opportunities for fraud, which results in losses of varying severity. In fact, the economic rift is so profound that organized criminality has grown up around ATMs.

Plastic card fraud is a form of identity theft in which an individual uses someone else’s credit card to charge purchases, to transfer or to withdraw funds from the account. Credit card fraud also includes the fraudulent use of a debit card, and may be accomplished by the theft of the actual card, or by illegally obtaining the cardholder’s account and personal information, including the card number, the card’s security number, and the cardholder’s name and address.

A range of anti-fraud strategies and tactics, including card activation, card verification codes, consumer education, address verification services, OTP integration, and real-time POS authorisation, can be used to prevent fraud. Etc. It depends on being able to prove that the card is an authentic one, issued by an actual bank for a certain amount given the growing issue of card counterfeiting, and that the person presenting the card is the rightful cardholder.

Like the fight against Ebola Virus Disease, cooperation and collaboration, among peers, professionals, organizations, and sharing of cyber intelligence is key to fighting the menace. Work must be done to develop and implement effective security, compliance and anti-fraud structures, which are absolutely necessary to handle the speed and complexity of transactions and exchange of information on the internet, and effectively tackle cyber incidents, ATM fraud, plastic card crimes and fraud losses.

Alao (2009) reported the colossal amount of money lost in Nigeria to ATM fraud through ATM card cloning, PIN theft among others and government had resorted to removing ATM from public places as well as installing security cameras at the ATM locations to track the activities of fraudsters. However, the level of ICT usage notwithstanding, the level of adoption of e-Banking by the citizen is still very low. Therefore, appropriate considerations must be given to these categories so that the most suitable e-Payment system can be adopted. Nigeria has remained the fastest growing mobile phone country in Africa and the third in the world where over 60% of the populace are connected (Akwaja, 2010). Thus, Nigeria has great potential for mobile commerce implementation besides the electronic commerce that is gradually gaining momentum. Hence, the challenging problem to economic activities and business growth are corruption and financial misappropriation or crimes. In Nigeria, the most serious problem to economic activities and business are financial crimes and corruption in higher offices that averages to 75% and 71% respectively)(Business Survey on Crime & Corruption and Awareness of EFCC in Nigeria, Summary Report, 2009-2010)

Adeoti J.O, (2011) in his paper entitled “Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out” emphasize the objectives of the paper as to (scrutinize various ATM frauds in the country and to provide solutions to mitigate the fraud in the banking industry, the methodology that is been used to carry out the research was sampling 5banks randomly from the 25 banks.

Cybercrime is any crime that is committed or enabled online. Any illegal behavior involving computers or networks is considered a cybercrime. It can include things like fraud and unsolicited emails (spam). It may also involve criminal trespass into distant systems throughout the world to steal corporate or government secrets. Anything from downloading illicit music files to stealing millions of dollars from online bank accounts is considered a kind of cybercrime. Cybercrime also involves non-financial violations like infecting other computers with viruses or publishing private company data online. The absence of a uniform and legal description for the behaviors that may be considered cybercrime is a major issue for the analysis of cybercrime. (PJCACC, 2004; Yar, 2005).

According to Smith et al. (2004), defining cybercrime raises conceptual complexi-ties. Varied definitions of cybercrime do exist. In addition to the difficult of definition, it is also called by variety of terms such as computer crime, computer-related crime, digital crime, information technology crime (Maat, 2004), Internet crime (Wall, 2001), virtual crime (Lastowka and Hunter, 2004; Grabosky, 2001 ), e-crime (AIC, 2006) and net crime (Mann and Sutton, 1998).

British Prime Minister, according to Reuter's media briefings from Cameroon, cybercrime costs the British economy some 27 billion pounds per year. On the other side, Nigeria is ranked third among the top ten global sources of cybercrime in the Economic and Financial Crimes Commission Report. According to estimates, Nigeria has the second-largest concentration of cybercriminals in the world, after the United States, which accounts for 65% of such activity, and the United Kingdom, which accounts for 9.9%. The popularity of online banking has increased the opportunity for cybercriminals. Using a wire transfer or account takeover, money can be stolen. (Wala & Odulaja, 2012). Criminals may submit fraudulent online applications for bank loans; disrupt e-commerce by engaging in denial of service attacks, and by compromising online banking payment systems. Identity takeover can also affect online banking, as new accounts can be taken over by identity thieves, thus raising concerns regarding the safety and soundness of financial institutions.

**2.2 Laws checking Fraud in Nigeria**

Though there is presently no law that is specifically checking cyber crime in Nigeria. However, this is not to say that cyber criminals are motivated to operate in the country. However, cybercrime proactive control measures that are relatively inexpensive and more sustainable may be better than reactive measures (McQuade, 2006). According to McQuade (2006) cybercrime can be minimized through public enlightenment campaigns, formal education, and professional training. There are general laws that are not specifically related to cyber crime but are being enforced to eradicate crime. Some of these laws are: the Nigeria criminal code, Economic and Financial Crimes Commission (EFCC) (Establishment) Act 2004, and the Advance Fee Fraud and other Related Offences Act 2006. The establishment of the Economic and Financial Crimes Commission (EFCC) in 2002 and it’s subsequently take off in 2004 under the Chairmanship of Nuhu Ribadu was a demonstration of the fervor with which the Obasanjo Administration wanted to stamp out corruption. (Nwaodu, 2014). The Commission is charged with enforcement and administration of the provisions of the Economic and Financial Crimes Commission Act – investigating all financial crimes, including advanced free fraud, money laundering, counterfeiting, illegal cash transfer, credit card fraud contract scams, etc. The Agency immediately took corruption head-on in its fight against the social menace and has recorded some degree of successes in this respect.

Owolabi (2010) examined that the problem of fraud in the banking industry is not limited to any economy, nation, and environment. Fraud and fraudulent activities can ultimately result to bank and total economy failure. Ojigbede (1986) attributed the cause of fraud in Nigeria’s economic space as the aftermath of general dishonesty and lack of morals in the society. He also evaluated the relationship between standing corrupt practices and fraudulent motivations.

Wada et al., (2012) studied the impact of cybercrime on Nigerian banking institutions and the methods used to obtain it. In order to address the effects of cybercrime on e-banking from a Nigerian viewpoint, they also investigated the effectiveness of the institutional responses and reviewed the current policy framework. With the aim of advising policy makers on behavioral issues that should be taken into consideration when formulating policies to address cyber crimes, they also analyze the influence of technology and its reaction to problems with cyber crime while incorporating social theories in explaining the causation.

Oluwaseyifunmitan et al., (2009) in their article titled “Towards Ameliorating Cybercrime and Cyber Security” The fundamental method integrated by the authors in performing the research includes, informed data collection, personal interviews, Observation, questionnaire and so on. They evaluated the obtained information and made some recommendations on how to improve the cyberspace at large.

According to Erhabor (2008), cybercrimes are described as one of the fastest growing criminal activities on the planet. He repeated the fact that it covers a large range of illegal activity including financial scams, computer hacking, downloading of pornographic images from the internet, virus attacks, stalking and creating websites that promote hatred. In recent time, young students in the tertiary engage in forgery of all kinds ranging from false admission paper to school fees receipts, certificates racketeering and examination malpractice that is, accessing useful information during examinations through the handset and other electronic devices. Ajao (2008) said Nigeria, Ghana and South Africa top cybercrime in Africa.

Meridien Research estimates that the credit card industry loses $1.5 billion in fraud each year, of which $230 million is thought to come from online purchases. Worldwide fraud increased by 33.7% between 1998 and 1999, according to MasterCard. Fraud losses climbed 35.3% from the previous quarter of 1999 to the first quarter of 2000. VISA notes comparable patterns. Online transaction fraud losses may top $500 million in 2000, according to estimates. The use of fake, stolen, and never-received credit cards, account takeover, mail-order, and online card-not-present transactions are only a few examples of 8 illegal credit card operations.

**2.3 Problems confronting law enforcement agencies and governmental cyber security agencies in combating cybercrime in Nigeria**

Odumesi (2006), studied the challenges hampering the involvement of law enforcement agencies from eradicating cybercrime from Nigeria.

1. Lack of adequate data on the reported level and extent of cybercrime damages in the country.

2. The Nigerian law enforcement agencies do not possess sufficient knowledge of how computer and ICT works and thus lacks an up-to-date computer forensic laboratory across her branches in the country. These, therefore retard there strength in properly investigating cyber-crime or plastic card fraud related cases.

3. Nigeria law enforcement agencies does not posses an accredited centralized government backed body that research and publish cybercrime and plastic card fraud statistical reports unlike in the UK or United States of America.

4. The lack of national policy framework and infrastructure for the prevention, avoidance and management of electronic payment fraud and other cybercrimes.

5. National Internet gateway’s absence has made it challenging to isolate, evaluate and determine the real criminal activity that could be ascribed to Nigeria on the internet.

**2.4 Study on OTP authentication Integration**.

Pathak et al., (2016) investigated the drawbacks of password reuse which led to the development of one-time password. They also proved the implementation and validity process of One-time password. The generation algorithm of OTPs where also studied as he proved the sequential and time synchronization approaches for generating OTP. An OTP is a generated password which only valid once. The user is given a device that can generate an OTP using an algorithm and cryptographic keys. On the server side, an authentication server can check the validity of the password by sharing the same algorithm and keys.

Jenifer R.S (2012) in his paper entitled “A Five Way Fuzzy Authentication for secured banking” proposed to combine the use of Pin Number along Keypad ID, RFID Tag, and Fingerprint. Image, One Time Password generated to users phone. Some security issues are also related to multi factor authentication protocol as another One Time Password given by the user to the server for authentication to secure Banking, this was related to the security issues associated with the existing three factor authentication protocols, which makes use of the RFID, Pin number and Biometrics.

**2.3 ALGORITHM OF SYSTEM**:

The suggested system's pseudo-code provides an easy approach to write programming code in English. There is no real programming language used in pseudo-code. Before you actually write the code for the program in a certain language, it employs brief sentences to do so. Once you understand the purpose of the program and how it will operate, you may use pseudocode to build statements that will cause your program to produce the desired results.

**2.3.1 Pseudo-code or Algorithm of proposed system is**

Step one: Insert the card

Step two: Interface prompt for Pin

Step three: Input card’s pin. If PIN is accurate, Skip to step five. If PIN not correct, go to the next step.

Step four: Abort transaction and eject card.

Step five: User navigates through to perform desired transaction. If fund transfer,

Step Six: User selects Account type and third party Merchant Bank,

Step Seven: User input recipient account number

Step Eight: User confirms recipient account details.

Step Nine: System Generates OTP, and sends to the user’s phone (2nd factor Authentication)

Step Ten: Interface Prompt for OTP

Step Eleven: Input OTP, if accurate skip to step thirteen. If OTP is wrong after three trails, proceed to the next step.

Step Twelve: Flag transaction as fraudulent, Abort transaction and Eject Card.

Step Thirteen: If transaction is less or equal to Balance, Complete Transaction, Else, Display message prompt “Insufficient fund” and Repeat action.

Step Fourteen: Interface prompt for another Transaction, if yes, go to step 9, Else Proceed to Next step

Step fifteen: Display transaction completed and Eject Card

**2.4 Model**

Passwords and PINs, the single factor authentication method used by banks, are no longer effective in securing online and offline banking transactions. Since people occasionally utilize their names, dates of birth, or other personal information for encryption operations, the majority of conventional passwords and PINs are simple to guess. Either social engineers or algorithms that automatically gather passwords might easily compromise this. Cybercrime and efforts at credit card fraud have routinely been defeated by multi factor authentication. Bank transfers should also incorporate the multifactor authentication process to protect user accounts from being compromised. A one-time password is delivered to the user's phone when starting a transfer process because many bank customers own mobile devices. Thee ATM in use for this study only allows account management system, fund transfer and bill payments. This paper focuses on the implementation of two-factor authentication methods using mobile phones during fund transfers. It provides the reader with an overview of the various parts of the system and the capabilities of the system.

**CHAPTER THREE**

**SYSTEM ANALYSIS AND SOLUTION DESIGN**

**3.1 INTRODUCTION**

The selection of platforms and their use in the building of this system as a remedy for the issue in chapter one are based on their dependability, expense, adaptability, and accessibility. Due to its superior suitability for the solution in light of the factors, the Arduino platform was chosen above competing options like the Raspberry Pi. The waterfall model, which was chosen as the project's methodology, is used to develop the system, and design models like use cases, sequence diagrams, activity diagrams, and class diagrams were used to record the system's requirements. Design decisions regarding the type of platforms, effective processing, transmission, and display were made, along with their justifications.

**3.2 ANALYSIS OF EXISTING SYSTEM**

The financial industry is dominated by transactions made through an ATM, a POS, or online banking. OTP has long been incorporated into platforms for online shopping, bill payment, and financial transactions. It is crucial to include OTP in fund transfers when using a debit card at an ATM since it will help protect the user from unauthorized transfers of client funds.

**3.3** **STRUCTURE OF THE PROPOSED SOLUTION**

This system consists of a mix of hardware and software elements that have been specifically created to carry out the required functions.

The system's input devices gather information about the user and the transaction before the micro controller generates a one-time password and sends it to the mobile devices for verification.

**3.4 FUNCTIONAL SYSTEM REQUIREMENTS**

Functional requirements define the function of a system or its components. They may be calculations, technical details, data manipulation, processing and other specific functionality that define what the system is to accomplish.

The system should be able to;

1. Accurately collect user and transaction details during financial transactions
2. Correctly display the necessary data collected
3. Generate a onetime password to validate transaction
4. Transmit the onetime password to the registered user number using a suitable and safe means of transmission
5. Receive the verified one time password
6. Verify, Validate and Permit the transaction

**3.5 NON FUNCTIONAL SYSTEM REQUIREMENTS**

The non-functional requirements are those requirements that impose constraints on the design or implementation

1. Transmission of onetime password in the shortest possible time to prevent delay in transfer
2. The system should operate with minimal power consumption
3. The system should operate with minimal human interference.

**3.6 SYSTEM DESIGN MODELS**

This accurately depicts the waterfall model's second stage. The system's design is a description of the architecture, data models, and structural elements that will be used to implement the system. In order to express the "blueprints" of a system, the display system is modelled using UML (Unified Modelling Language), a modeling language or graphical/diagrammatic notation for object-oriented programming. The sequence diagram and class diagram are examples of UML diagrams.

**3.6.1 SEQUENCE DIAGRAM**

In the UML, sequence diagrams are generally used to model interactions between individual objects as well as interactions between actors and objects in a system. A sequence diagram, as the name suggests, depicts the interactions that happen in the order they do during a specific use case or use case instance. A dotted line is created vertically from the list of the involved items and actors at the top of the graphic. Annotated arrows show how items interact with one another. The rectangle on the dotted lines indicates the lifeline of the object concerned (i.e., the time that object instance is involved in the computation). Interactions are read from top to bottom, while annotations on the arrows indicate the calls to the objects, their parameters, and the return values.

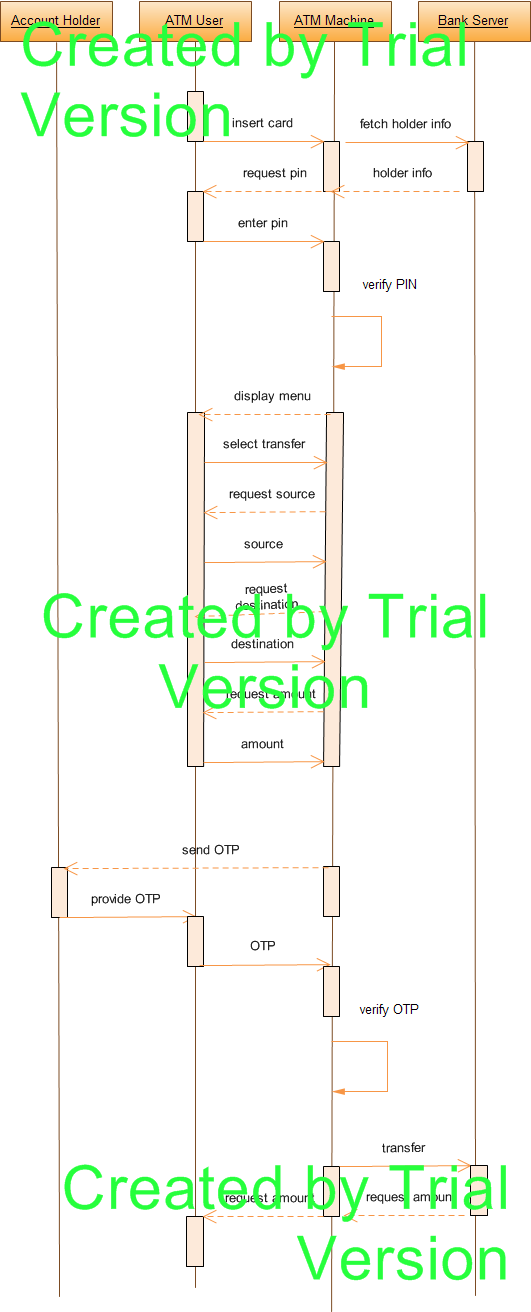
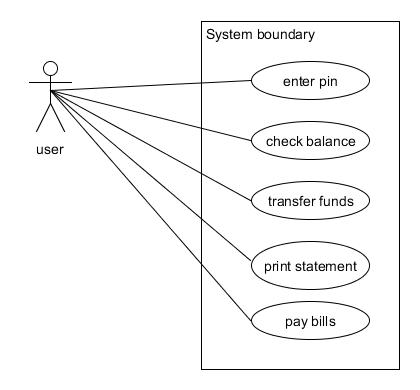
****

Figure 3.1: Showing sequence diagram of the designed system

**3.6.2 USE CASE DIAGRAM**:

Typically, behavior diagrams are used to explain a series of actions that a system or systems should or could carry out in coordination with one or more external users of the system (act). Each use case should produce a tangible benefit for the system's actors or other stakeholders.

****

**Fig 3.2** Interaction between User and System

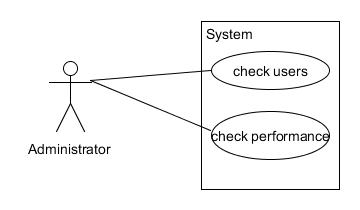
****

Fig 3.3 Interaction between Administrator and system

**3.5.3 CLASS DIAGRAM**

In software engineering, a class diagram in the Unified Modelling Language (UML) is a form of static structural diagram that depicts the classes, their characteristics, actions, (or methods), and relationships between objects to explain the structure of a system.

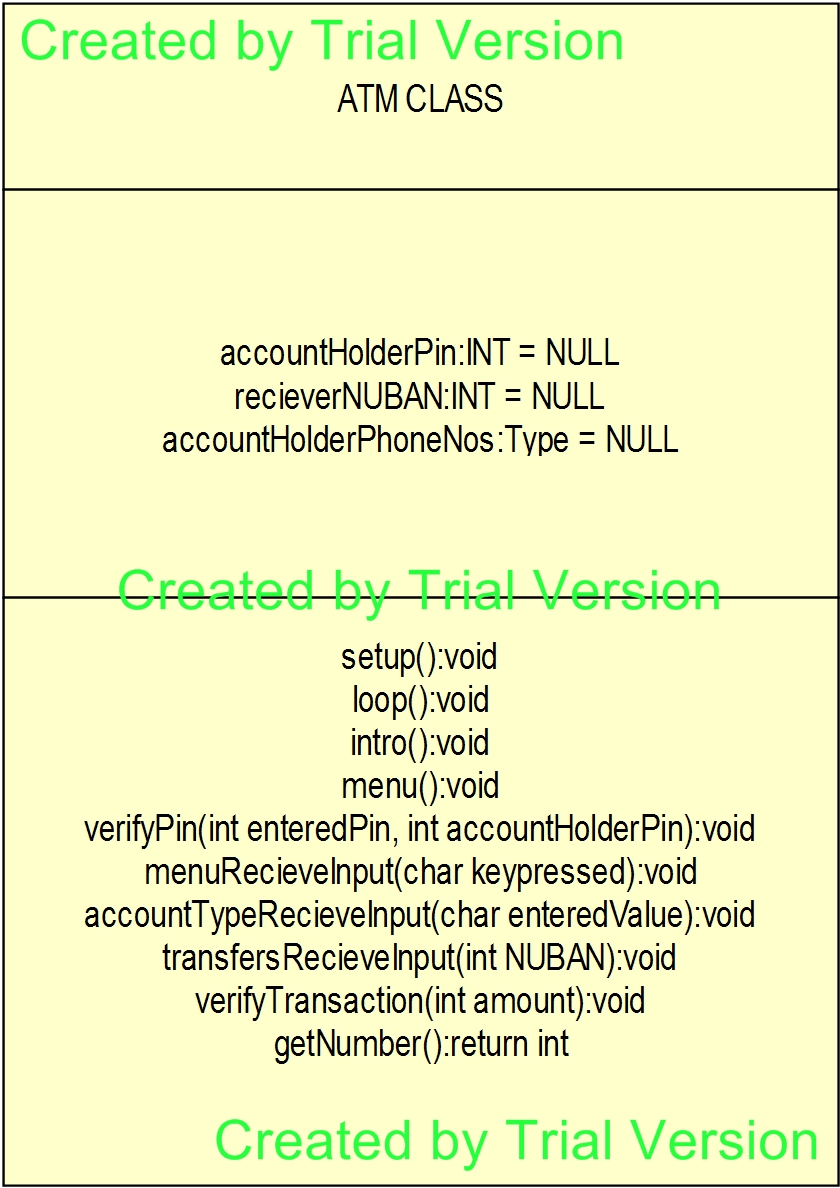
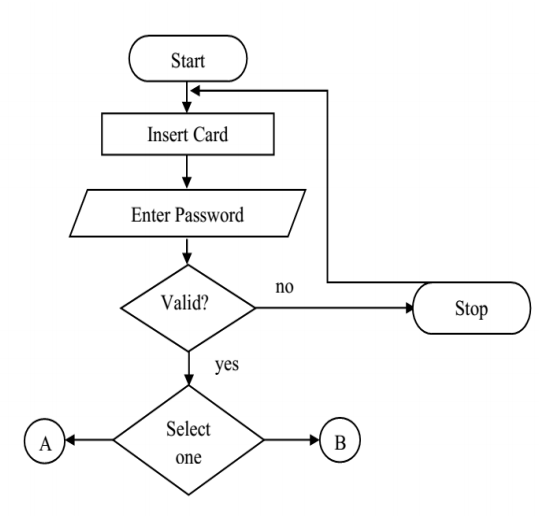


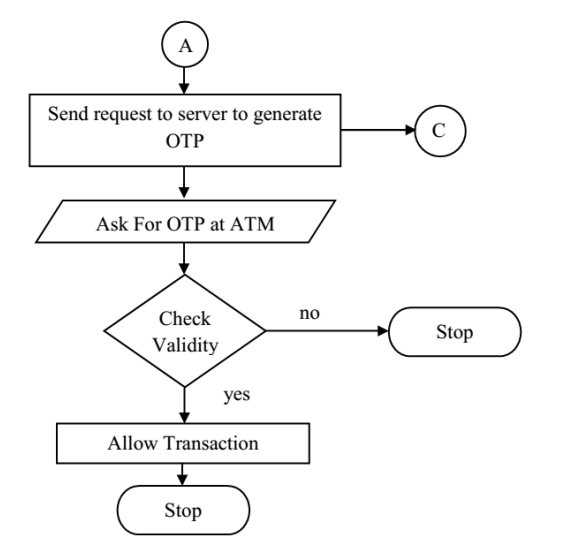
Fig 3.4: Class Diagram of the designed system

**3.4 Flowchart**

The first flow chart shows the initial state of inserting the card and entering the PIN to bypass the first layer of the security. If the PIN is correct, user will be permitted to explore transactions and initiate the next transaction.



Flow chart 1



Flow chart 2

CHAPTER FOUR

**DESIGN AND IMPLIMENTATION**

**4.1 INTRODUCTION**

The selection of platforms and their use in the building of this system as a remedy for the issue in chapter one are based on their dependability, expense, adaptability, and accessibility. Due to its superior suitability for the solution in light of the factors, the Arduino platform was chosen above competing options like the Raspberry Pi. The waterfall model, which was chosen as the project's approach, is used to create the system, and design models such use cases, sequence diagrams, activity diagrams, and class diagrams were used to record the system's requirements. Platform type, effective processing, transmission, and display were the design decisions that were made, along with their reasoning.

An executable software system is developed at the design and implementation phases of the software engineering process. Design and implementation frequently go hand in hand. The creative process of identifying software components and their connections based on client needs is known as software design. The process of making the design into a program is called implementation.

This solution's design involves mounting a number of hardware components and testing at various implementation stages. Some of the testing approaches used in testing include:

1. Unit integration and system testing: This involves testing implemented every time a new module is implemented. Integration test is run together with the unit testing.
2. Major component in the system are tested earlier, this is to minimize the problem resulting from the component that could necessitate the revision of the lower level modules.

Debugging is made easy as test failure on addition of a new module is either due to bug in the module or at the interface between the already tested working system and the new module.

**4.2 SYSTEM REQUIREMENTS**

For complete functionality, computer software requires specific hardware elements or other software resources. These prerequisites, also referred to as (computer) system requirements, are frequently employed as a general norm rather than an unbreakable law. The majority of software specifies the minimum and recommended system requirements as two separate sets of criteria.

System requirements tend to change over time due to the rising demand for more processing power and other resources in newer versions of software. According to industry observers, this trend more than technological improvements is what is pushing changes to current computer systems.

**4.3 HARDWARE REQUIREMENTS**

For a successful implementation of a system, hardware requirement must be specified. For this work, the following are some of the hardware requirements needed for the successful and efficient implementation of this system:

1. Arduino Platform.
2. GSM Module.
3. Keypad input
4. LCD Screens.
   1. **SOFTWARE REQUIREMENT**

Software tools needed to successfully run the system include:

1. Linux or windows operating system
2. Arduino IDE 1.5.8

**4.5 SYSTEM MAINTENANCE**

Dadik (2016) defined software process as computer programs with associated documentations.  In this phase of the system, documentation is done in order to guide the user on how to operate the new system effectively. Software upgrade and update guidelines are specified and implemented here to ensure accurate performance of the system. The system maintenance involves two stages; Hardware Maintenance and Software Maintenance

* + 1. **HARDWARE MAINTENANCE**
  1. Provision of cooling system to reduce over heating on the hardware components.
  2. Steady power supply to avoid break in transmission by the GSM module.
  3. Provision of moisture free environment to prevent damage to electrical components and subsequent risk of electrical shock.
     1. **SOFTWARE MAINTENANCE**

In software engineering, this is the modification of a software product after delivery to correct faults, improve performance or other attributes. A common perception of maintenance is that it merely involves fixing defects. However, one study indicated that the majority, over 80% of maintenance effort is used for non-corrective actions (Pigosky, 1997). Software maintenance processes includes the following:

* + - * 1. **The implementation processes**:

This contains software preparation and transition activities such as the conception and creation of maintenance plan; the preparation for handling problems identified during development; and the follow up of product configuration management.

* + - * 1. **The problem and modification analysis process**:

This is executed once the application has become the responsibility of the maintenance group. The team responsible for maintenance must; analyze each request, confirm it (by reproducing the situation) and check it validity, investigate it and process a proposed solution.

The process considering the implementation of the modification itself.

The process acceptance of the modification, by confirming the modified work with individuals who submitted the request in order to make sure the modification provided a solution

1. The migration process (platform migration):

Though necessary but it is not part of daily maintenance tasks. If the software must be ported to another platform without any functionality, this process will be used and a maintenance project team is to be assigned to this task.

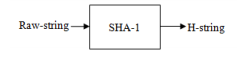
1. Finally, the last maintenance process, also an event which does not occur on a daily basis, is the retirement of a piece of software.

**4.6 Algorithm for Generating the One Time Password**

The OTP must be challenging to guess, obtain, or compute in order to protect the user against unauthorized transactions. Therefore, it is crucial to create a secure OTP generating method to calculate and provide a challenging permission code. The security of systems using OTP algorithms is essential since malicious users shouldn't be allowed to figure out or guess the next password sequence. Therefore, the combinatory sequence should be as random, unpredictable, and irreversible as feasible. Thus, some criteria are taken into account when creating this randomly generated six-digit One Time Password..

* Card Name: This identifies the card bearer’s name. Names could be shortened I some occasions.
* PIN: This is required to verify the authenticity of the human behind the transaction authorization. It is needed in the verification process and also use once mechanism in the generation of OTP
* Plastic Card Number: This is a 16 digits number which is also the card holder account number embossed on the card. It also includes the Card Verification Value (CVV), which is a unique check valve, generated using a secure cryptography process which helps in transaction authorization.
* Time Stamp or slot: In order to minimize the cost of computation power we need to separate the time into slots so that each token calculation will be generated to be valid for period of time and not just a moment in time. This is used to uniquely generate the OTP and its only valid for a short amount of time.

These factors are then computed and hashed into a unique one time password. The SHA-1 is used to compute the message and return the string. The calculation of the hash string of about 16 bits long, a Six digit OTP is sent to the user’s registered mobile phone.



Example of how it works:

|  |  |
| --- | --- |
| Card Name | Oguibe Godsalvation |
| PIN | 2607 |
| Card Number | 5399831623425001 |

|  |  |
| --- | --- |
| String | Hash Valve |
| Oguibe Godsalvation | 539980dkadd078g0dvv9 |
| 2607 | I9dk3408496050t06kgpp |
| 5399831623425001 | 948kjvd094llfjlodh93045 |

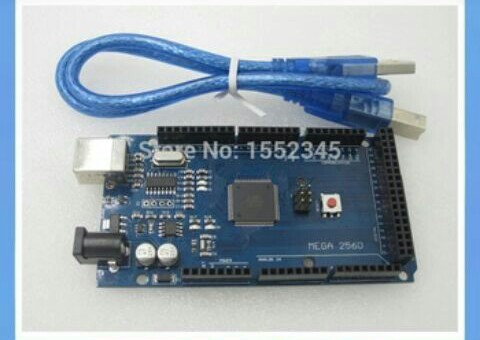
Therefore, when the Hash Valve is computed, the random selector will pick from the 6th position till six counts which serves as the OTP.

**4.7 PROPOSED SYSTEM COMPONENTS**.

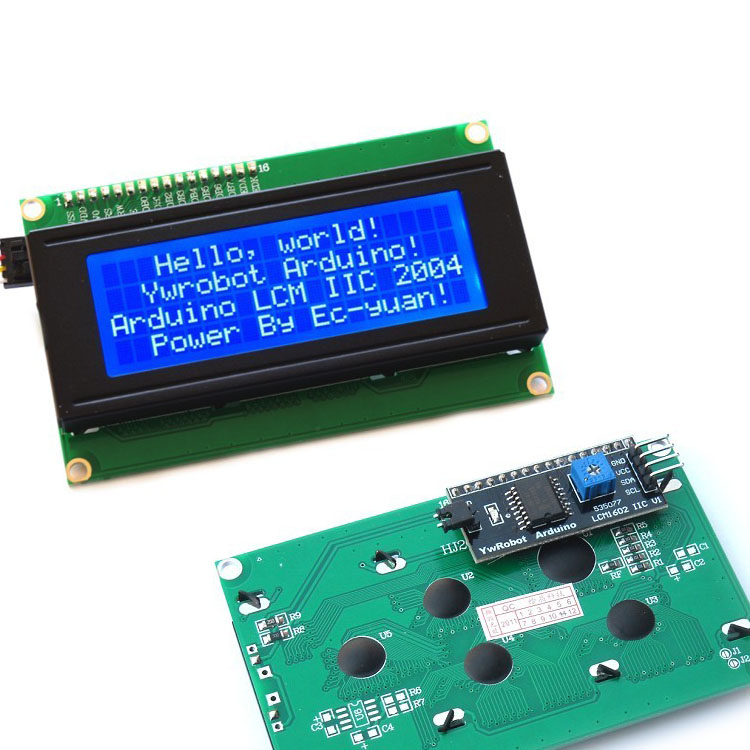
The One Time Password will be generated by the system used to avoid plastic fraud based on a variety of factors.

**Card:** The customer slips their card and PIN into the ATM. The first security layer is passed if accurate, and if a fund transfer is started, the information retrieved will also be used to create the One Time Password.

**One Time Password Generator (Micro Controller**): This



**Arduino LCD display:** The Arduino communicates with the LCD through the four lines. We use the digital pins on the Arduino to talk to the LCD and display what we want on it.



**GSM Module**: The GPRS Shield is based on SIM900 module from SIMCOM and compatible with Arduino and its clones. The GPRS Shield provides you a way to communicate using the GSM cell phone network. The shield allows you to achieve SMS, MMS, GPRS and Audio via UART by sending AT commands (GSM 07.07 ,07.05 and SIMCOM enhanced AT Commands).



**Latency:** On delivery of the One Time Password, there is a latency period in which the generated OTP must be used else it will be invalid when used to authorize a transaction.

**CHAPTER FIVE**

**EVALUATION AND TESTING**

**INTRODUCTION**

This chapter gives detail system testing and evaluation process carried out on the developed system solution. Prototype evaluation is a process that critically examines the prototype. It involves collecting and analyzing information about a prototype‘s activities, characteristics and outcomes. Its purpose is to make judgments about a prototype, to improve its effectiveness and/or to inform programming decisions (Patton, 1987).

**5.1 System Evaluation**

System evaluation is the process of analyzing a system to see whether it satisfies the objectives set forth in order to provide effective/required service to its intended audience. The system will next need to be evaluated to make sure it is effective and efficient in its operational state after being planned and constructed in accordance with the established requirement collection. The major goal of conducting this evaluation is to comprehend and verify how effectively the system achieves its intended goal.

* 1. **System Evaluation Criteria**

The criteria involved in the evaluating this system includes;

* **Functionality criterion:** This criterion entails evaluating how correct the system meets it stated functional requirement goals. Referring back to the functional requirements and evaluating, a user should able to insert a valid plastic card, type in his/her PIN, view account balance, pay bills, make fund transfers and print mini statement. In general, this criterion should ensure that the system perform its functions as intended in fulfilling its objectives.
* **System reliability:** This criteria ensure the reliability of the system in performing it operations efficiently and effectively under any presented condition. This should be dependent on the individual components of the system in ensuring the reliability of the developed solution. The reliability of the system should be measured by checking the correctness of the PIN, checking the validity of the ATM card and retrieved and also how easy the system gives feedback to the users, it describes the ability of a **system** or component to function under stated conditions for a specified period of time.
* **Performance criterion:** The algorithm employed by the system in building the decision tree and making decision based on the given location should be evaluated. It is extremely important that the system does not fails in performing it functions accurately.
* **Ease of Installation and Setup:** The system should be easy to setup and install within the work zone, power supply should be ready for use for the period of time. The system should take lesser time to be set up.
* **Operation and Maintenance:** The operation and maintenance of the system is an important factor that needs to be considered during evaluation. The system, once setup and installed at a work zone, should be easy to operate and maintain. All operations that need to be performed should be simple and obvious. Basically, the system should be user friendly, uncomplicated, and designed such that mistakes cannot be made often.
* **Cost:** The cost of the system as a whole, as well as its operation and maintenance costs, will be a very important factor in adopting the system for use. The use of low powered system components such as sensors and other components that make up a system and a 5v battery power for operation of these components may help reduce operation costs of the system.

**5.2 LIMITATIONS OF THE SYSTEM**

* The system cannot function when there is power failure.
* Some of the system components are fragile and so need to be handled with extreme care.

CHAPTER SIX

**SUMMARY CONCLUSION AND RECOMMENDATION**

**6.1 SUMMARY**

For in-person, ATM, point of sale, and internet purchases, plastic payment cards are increasingly used as the principal mode of payment. This adoption of payment cards has led to a steady increase in the market for credit and debit cards. More so than in the past, consumers today favor electronic payment options. E-payment is now accepted thanks to technology and innovation. Customers can utilize cards easily and effectively. Theyy are gradually replacing cash and check to a great extent. Studies estimated that there are about 10,000 payment card transactions initiated every second the world,. On the other hand, innovations and new technologies also created more complexity and introduced new risks factors presented by new products, new providers, and new technologies. Sadly, as cards have taken over as the major method of payment in retail purchases, they have also turned into a tempting target for thieves.

Since the introduction of cards into the payment system, payment card fraud has been a problem. The rate of payment card fraud has increased in tandem with the card market's recent rapid expansion. Card fraud costs billions of Naria annually, and the numbers keep rising.

**6.2 Conclusion**

Information technology initiatives are becoming totally dependent on Nigerian banking. The advent of computer-aided systems has replaced the large work force that would have been required to manage the massive volume of financial transactions that occur today. Any financial institution that wants to succeed in the current, intensely competitive and demanding business environment must find a way to use creative electronic tools to help her service delivery. Today's banking operations increasingly use computer-oriented technological solutions and packages to manage tasks like ATM (Automatic Teller Machine), Internet Banking, Mobile Banking, Tele-banking, Web Purchases, and Human Teller activities. Therefore, the transaction is further protected thanks to the second factor authentication. Adding 2FA to all card services and financial applications will be recommended practice. This control primarily serves to prevent identity theft from financial institution employees and their use to post fraudulent transactions. This type of fraud scheme was very rampant in the Nigerian Banking space a few years back and substantial sums of funds were lost to fraudsters who perfected the act of using hard/soft devices to capture the login credentials of unsuspecting users and using same to process transactions on either their core banking application or on the other funds transfer platforms.

**6.3 RECOMMENDATION**

Without reservation, it can be said that since the introduction of plastic cards and debit cards, the rate of e-payment fraud in the Nigerian banking system has dramatically increased, having a negative impact on the development and success of electronic banking in Nigeria. Additionally, it has been discovered that, like any other product, electronic banking products have had a significant impact on customers' preferences for banking convenience. However, the solutions for halting the ugliness of fraud demand rapid attention through cooperation among banks, users, and switching businesses. In addition, CBN needs to keep checking for and enforcing violations of the various Electronic Banking System standards.

**6.3.1 RECOMMENDATION TO BANKS**

The following advice are provided to financial institutions or card issuing institutions in an effort to lessen or perhaps even combat plastic card fraud.

* Banks should constantly remind their clients to use ATMs with caution and with security in mind.
* Banks should inform CBN of their fraud status for advice on establishing procedures for ATMs and electronic banking.
* Banks shouldn't be reluctant to deactivate or hot-list suspected compromised cards.
* When issuing cards, banks should follow the KYC (Know-your-customer) regulations.
* Adherence to established corporate regulations and procedures on ATMs should be strictly enforced.
* Banks should offer campaigns to educate cardholders about the freedom to independently enable and disable their cards as desired.
  + 1. **RECOMMENDATIONS TO CUSTOMERS**

A lot of the responsibility for protecting personal card information is on the client, even though some advice are offered to banks and other financial institutions. The following suggestions are provided to card users to assist protect their financial transactions from nefarious intruders.

* Avoid responding to prospective social engineers by phone or mail by disclosing Personal Identification Numbers, Token Codes, passwords, or login information.
* Make sure to use complex passwords for ATM PINs and internet banking logins rather than easily guessed date of birth or name combinations.
* Customers should notify the proper authority about any fraud attempt made using their cards so that proactive measures can be taken.
* To improve swift card blocking, customers should not hesitate to report lost plastic payment cards to financial or issuing organizations.
* Without official authorization from bank authorities, customers shouldn't comply with cold-callers or scam text message requests for account updates or upgrades.
* Why Users shouldn't record their PIN or passwords on paper. Typically, it is best for it to
* Customers should not lend out their credit card to someone.
* Customers should resist keeping PIN together with the card

**6.4 RECOMMENDATIONS FOR FURTHER RESEARCH**

One Time Password appears to hold promise in the effort to protect users' financial information and shield them from attacks involving plastic card fraud. It might offer a long-term answer to checkmating E-crimes if correctly incorporated. Multi-factor authentication should be incorporated into all financial projects in order to completely combat fraud, including that committed by family members, close friends, and acquaintances, and as such serve as a gateway for authorized users to successfully complete a transaction. There should be swift implementation of more study on the full use of these authentication modalities.

**REFERENCE**

Nigeria Deposit Insurance Corporation (2012) “*Annual Reports”,* Nigeria, December 2012

Wada, F. and Odulaja, G.O. (2012);*Assessing Cybercrime and its Impact on EBanking* *in Nigeria using Social Theories*. African Journal of Comp & ICTs.Vol 5.No.1.pp 69-82.

Ehimen, O. R. andBola, A. (2009): *Cybercrime in Nigeria*. Business Intelligence Journal- January 2010 Vol3 No.1 pp 93-98.

Olasunkanmi, O. O (2010): “*Computer Crimes and Countermeasures in the Nigeria Banking Sector”* journal of internet bankingand commerce. 15(1) pp 1-10

National Fraud Authority (2012); *Annual Fraud Indicator,* United Kingdom, March2012

Pahwa, M.S., Saxena, K., (2011). Analytical study of customer satisfaction at ICICI Bank with special reference to ATMs. 3rd International Conference on Information and Financial Engineering IPEDR, IACSIT Press, Singapore.

Nwagwu, E. J. (2012) .“An Appraisal of Economic and Financial Crimes Commission (EFCC)and the War Against Corruption in Nigeria (1999-2007)”, International Journal of Research in Arts and Social Sciences.

Mohammed Hamid Khan, Apr 15 Volume 3 Issue 4, “***OTP Generation using SHA***”, International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), ISSN: 2321-8169, PP: 2244 - 2245, DOI: [10.17762/ijritcc2321-8169.1604104](http://dx.doi.org/10.17762/ijritcc2321-8169.1604104)

Parameswari, D., & Jose, L. (2011). SET with sms otp using two factor authentication. *Journal of Computer Applications (JCA)*, *4*(4), 4.

Lee, Y. S., Lim, H., & Lee, H. (2010, February). A study on efficient OTP generation using stream cipher with random digit. In *Advanced Communication Technology (ICACT), 2010 The 12th International Conference on* (Vol. 2, pp. 1670-1675). IEEE.

Khan, M. A. (2010). An empirical study of automated teller machine service quality and customer satisfaction in Pakistani banks. *European journal of social sciences*, *13*(3), 333-344.

Ada, L. (2005). *About Us: MIT engineer, Limor "Ladyada" fried*. Retrieved 2015, from Adafruit: [www.adafruit.com](http://www.adafruit.com)

Dadik, G. (2016). Fundamental of software engineering. Student Lecture Note.

Massimo, D. D. (n.d.). *About Us: Arduino*. Retrieved from Arduino web site: [www.arduino.cc](http://www.arduino.cc/)

**APPENDIX**

**Sample Source Code**

//COMPLETE CODE

#include <virtuabotixRTC.h>

virtuabotixRTC myRTC(10, 11, 12);

//include a library for the GSM module

#include "SIM900.h"

#include <SoftwareSerial.h>

#include "sms.h"

//declare necessary constants

SMSGSM sms;

//import libraries for LCD

#include <Wire.h>

#include <LiquidCrystal\_I2C.h>

//instantiate library class

LiquidCrystal\_I2C lcd(0x27,2,1,0,4,5,6,7,3, POSITIVE);

//import keypad library

#include <Keypad.h>

//set keypad constants

const byte numRows= 4; //number of rows on the keypad

const byte numCols= 4; //number of columns on the keypad

//these constants represent customer data that would normally be in the banks Database

int customerpin = 1234;

int recieverNUBAN = 0;

//Holds the current status of the gsm module ON/OFF

boolean started=false;

//keymap defines the key pressed according to the row and columns just as appears on the keypad

//This maps the keys to the keypad buttons

//NOTE: use the #key as your Enter BUTTON

char keymap[numRows][numCols]=

{

{'1', '2', '3', 'A'},

{'4', '5', '6', 'B'},

{'7', '8', '9', 'C'},

{'\*', '0', '#', 'D'}

};

//Code that shows the the keypad connections to the arduino terminals

byte rowPins[numRows] = {9,8,7,6}; //Rows 0 to 3

byte colPins[numCols]= {5,4,3,2}; //Columns 0 to 3

//initializes an instance of the Keypad class

Keypad myKeypad= Keypad(makeKeymap(keymap), rowPins, colPins, numRows, numCols);

//====================================================

//This method starts up the Device, it is the the first FUNCTION that is executed

void setup()

{

//start up the lcd screen

lcd.begin (20,4);

lcd.backlight(); // backlight on

//Start up the CGSM module

//if (gsm.begin(2400)) {

//started=true;

//}

}

//i for keeping track of while loop

//it make the whole code run only once till re boot

int i=0;

//holds keypad value pressed for each keypad entry

int key;

//====================================================

//this is a continuous loop that keeps the system running

void loop()

{

while(i==0)

{

//run the introductory screen once

intro();

}

}

//====================================================

//function that displays the first logon screen

//with PIN request, and account user details

void intro(){

lcd.setCursor(0,0);

lcd.print("Hello, Ayo Okeke");

lcd.setCursor(0,2);

//Request user pin

lcd.print(" ENTER PIN: ");

lcd.setCursor(0,3);

lcd.print(" [then press #]");

//call the method to validate customer pin

//i.e is user pin entered the same as what is in banks database

verifypin(GetNumber(),customerpin);

i=1;

}

//====================================================

//function that displays the options available to the User

void menu(){

lcd.setCursor(0,0);

//Press 1 to make fund transfers

lcd.print(" Press 1 : TRANSFER");

lcd.setCursor(0,1);

//Press 2 to make For other bank transactions

lcd.print(" Press 2 : OTHERS.");

lcd.setCursor(0,2);

//Press zero to cancel operations

lcd.print(" Press 0 : CANCEL");

lcd.setCursor(0,3);

lcd.print(" [then press #]");

//call the method to recieve user selection from menu

menuRecieveInput(GetNumber());

i=1;

//end loop

}

//====================================================

//function that verifies if Pin entered matches Pin stored on system

void verifypin(char enteredpin, char customerpin){

if(enteredpin == customerpin){

//login was successful

lcd.clear();

lcd.setCursor(0,0);

//display confirmatory message

lcd.print(" PIN ACCEPTED ");

delay(1000);

//return to main menu

menu();

}

else

{

//login failed

lcd.clear();

lcd.setCursor(0,0);

//display error message

lcd.print(" INVALID PIN ");

delay(1000);

//go back to introductory screen

intro();

}

}

//====================================================

//method to recieve user selection from menu

void menuRecieveInput(char keypressed){

if(keypressed == 1){

//if user selected 1 as an option i.e funds transfer

lcd.clear();

lcd.setCursor(0,0);

lcd.print(" FUND TRANSFERS");

delay(1000);

lcd.clear();

lcd.setCursor(0,0);

lcd.print("Loading menu...");

delay(1000);

lcd.setCursor(0,0);

lcd.print(" RECIEVER ACCT TYPE");

lcd.setCursor(0,1);

//Press 1 for current account

lcd.print(" Press 1 : CURRENT");

lcd.setCursor(0,2);

//Press 2 for savings account

lcd.print(" Press 2 : SAVINGS");

lcd.setCursor(0,3);

//Press zero to cancel

lcd.print(" Press 0 : CANCEL");

delay(1000);

//recieve option from user for account type selection

accounttypeRecieveInput(GetNumber());

delay(1000);

}

if(keypressed == 2){

//user selected 2 i.e other transactions

lcd.clear();

lcd.setCursor(0,0);

lcd.print("OTHER TRANSACTIONS");

delay(1000);

lcd.setCursor(1,2);

lcd.print("Not Available");

delay(1000);

lcd.setCursor(2,3);

lcd.print("Exiting to menu...");

delay(1000);

menu();

}

if(keypressed == 0){

//user opts to exit or cancel

lcd.clear();

lcd.setCursor(0,0);

lcd.print("THANK YOU, GOODBYE...");

delay(1000);

menu();

}

}

//====================================================

//method to recieve user choice on account type

void accounttypeRecieveInput(char enteredvalue){

if(enteredvalue == 1 || enteredvalue == 2){

//if user selectected Savings or Current account, take them to NUBAN input screen

lcd.clear();

lcd.setCursor(2,0);

lcd.print("RECIEVER NUBAN: ");

lcd.setCursor(2,3);

lcd.print("[then press #]");

//recieve account number of reciever

int NUBAN = GetNumber();

transfersRecieveInput(NUBAN);

delay(1000);

}

if(enteredvalue == 0){

lcd.clear();

lcd.setCursor(2,0);

lcd.print("Exiting to menu...");

menu();

}

}

//====================================================

void transfersRecieveInput(int NUBAN){

recieverNUBAN = NUBAN;

//check if account number was entered

if(recieverNUBAN != 0){

lcd.clear();

lcd.setCursor(3,0);

lcd.print("Please Wait...");

lcd.setCursor(3,1);

lcd.print("Accepted!");

lcd.clear();

lcd.setCursor(3,0);

lcd.print("ENTER AMOUNT:");

//collect amount to be transfered

int AMOUNT = GetNumber();

//authenticate transaction

verifyTransaction(AMOUNT);

delay(1000);

}

}

//====================================================

//this FUNCTION does 3 things

//1. Generates the OTP

//2. Sends the OTP to the account holder

void verifyTransaction(int AMOUNT){

//generate OTP

//OTP generation code comes here

//hard coded OTP is 1212

//send OTP to the registered account holders number

if(started) {

sms.SendSMS("2349065068907", "1212");

}

lcd.clear();

lcd.setCursor(6,0);

lcd.print("OTP Sent");

delay(3000);

lcd.clear();

lcd.setCursor(3,1);

lcd.print("Enter the OTP: ");

//enter the OTP recieved on your mobile device

int recievedOTP = GetNumber();

lcd.clear();

lcd.setCursor(3,0);

lcd.print("Verifying...");

delay(3000);

//test to see if the recieved OTP is the same with the OTP that was sent by the system

if(recievedOTP == 1212){

//The user entered the Correct OTP sent to the account holders number

//display confirmatory message

lcd.clear();

lcd.setCursor(4,0);

lcd.print("Verified!");

delay(3000);

lcd.setCursor(2,2);

lcd.print("Transfering...");

//Banks fund transfer process comes here, funds transferred to Reciever NUBAN

delay(5000);

lcd.clear();

//Notify user if transfer is complete

lcd.setCursor(2,0);

lcd.print("Transfer Complete!");

delay(2000);

lcd.clear();

//return back to main menu i.e introductory screen

intro();

}

else

{

//the entered OTP does not match the OTP sent to the User

//Display Error notification the ATM user

lcd.clear();

lcd.setCursor(4,0);

lcd.print("Transaction");

lcd.setCursor(3,1);

lcd.print("Not Verified!");

delay(2000);

lcd.setCursor(1,3);

lcd.print("Exiting to menu...");

delay(2000);

lcd.clear();

//Take the User back to the Main menu

menu();

}

delay(1000);

}

//====================================================

//this method is for the key pad it processes all keypad entries

int GetNumber()

{

int num = 0;

char key = myKeypad.getKey();

while(key != '#')

{

switch (key)

{

case NO\_KEY:

break;

case '0': case '1': case '2': case '3': case '4':

case '5': case '6': case '7': case '8': case '9':

lcd.setCursor(19,3);

lcd.print(key);

num = num \* 10 + (key - '0');

break;

}

key = myKeypad.getKey();

}

return num;

}