Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY
Vol. 9. No. 2, June-December, 2021

Article Citation Format
Onamade, A.A., Adediran, A.A. & Adepegba, O.A. (2021): ATM Model for a Trusted Third Party System. Journal of Digital Innovations & Contemp Res. In Science., Engineering & Technology. Vol. 9, No. 2. Pp 81-86
DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V9N2P7

Article Progress Time Stamps
Article Type: Research Article
Manuscript Received: 17th October, 2021
Review Type: Blind
Final Acceptance: 20th December, 2021

ATM Model for a Trusted Third Party System (TTPs)

[1]Onamade, Akintoye Abraham, [2] Adediran, Abiodun Adedayo, [3]Adepegba, Oluwafunmilola Aderannibi
Department of Computer Science,
Adeleke University
Ede, Osun State, Nigeria.
E-mails: [1]onamadeakintoye@adelekeuniversity.edu.ng, [2]adediranabiodun364@gmail.com,
[3]Adepegbafunmilola@adelekeuniversity.edu.ng
Contacts: +234 703 066 7893[1], +234 803 633 4835[2], +234 706 736 8960[3]

ABSTRACT

The history of banking transaction has been with the use of cheque books, which direct the bank to pay or transfer specific amount to the bearer – third party on behalf of account owner. Identity card (ID) is the means of authentication and the third party is asked to append his or her signature and address on the back of the cheque for the bank to grant the request. Therefore, human beings cannot do without the help of third party, for their daily activities as nature can call for such service at any time. Even today, may be as a result of sickness, people do give their ATM card and PIN to third party to withdraw money on their behalf. The negative effect of involving third party to withdraw money with an ATM card on behalf of an account owner is at alarming rate. This action to say the least is prone to many security risks which must be avoided at all costs. Therefore, a system is designed in this study to recognize the use of third party in an ATM bank transaction in order to alleviate the negative effect of using the third party. An algorithm was designed for third party ATM transaction using Bracket IDE and Xampp as programming tools. The developed system, allows a trusted third party to have access to ATM card and to withdraw money on behalf of an account owner. The account owner initiates the process through the platform created in this study by registering the third party details and the transaction to be carried out on behalf of an account owner. The system generates an OTP that allows the third party to perform a restricted transaction on behalf of the account owner. The amount to be withdrawn is embedded in the OTP generated for the third party, such that there is no checking of account balance, no withdrawal of an amount less or above amount specified in the OTP, and no money transfer. Therefore, since the system allows restricted transactions to be performed by the third party, it becomes very difficult for third party to use the privilege of performing ATM transaction against the account owner.

Keywords: ATM, One Time Password (OTP), Trusted Third Party (TTP), Third Party

1. INTRODUCTION

An Automated Teller Machine (ATM) is a self-service machine that dispenses cash and performs some human teller functions like balance enquiry, bills payments, mini statements, Fund Transfer, Cash Deposit and so on. ATM is an electro mechanical machine that allows customers to complete their transaction without the help of a bank representative [1]. ATM transactions are conducted through the use of a debit/credit card, which allows card holders

to access and conduct bank transactions without a counter, the strip contains an identification code that is transmitted to the bank's central computer via modem.
To prevent unauthorized transactions, the user must also use a personal identification number (PIN) through the keyboard. The computer then allows the ATM to complete the transaction. Automated teller machines (ATMs) have been introduced worldwide and are still being introduced by banks. They offer significant benefits to both banks and their depositors; the machine allows depositors to withdraw cash at more convenient times and locations than during business hours.

In Nigeria, the introduction of ATMs by banks and their use by bank customers is on the rise and has increased significantly in recent times. This happened in particular after the recent bank consolidation, which has in all likelihood allowed more banks to afford ATMs or at least to become part of common networks [2]. ATMs emerged as the most popular with an awareness level of 96 percent, just behind savings accounts [3]. Therefore, there is a clear need to study ways in which third party system can be legalized in the act of perfuming cash withdrawal on behalf of account owner. According to [4] implementation of information technology and communication networking has brought revolution in the functioning of the banks and the financial institutions. It is argued that dramatic structural changes are in store for financial services industry as a result of the internet revolution. Arguably, the most revolutionary electronic innovation in this country and the world over has been Automated Teller Machine (ATM) and the introduction of card-less ATM withdrawal policy.

A bank's effectiveness in providing these services depends to a large extent on whether they are aligned with customer needs in terms of ease of use, customer satisfaction and the time required to provide the services. In an attempt to please their customer's, banks have deployed ATMs to replace human intervention, reduce costs, and increase corporate profits and customer satisfaction [5]. It is usually possible for someone to legitimately access the customer's account with their permission. The exact agreement depends on the type of your account and the account provider to check what agreements are available. Customers should be advised that setting up third party access may take some time. Under no circumstances will the customer pass on his personal identification number (PIN) to third parties in order to give them access to his account [6].

1.1 Problem Statement

The history of banking transaction has been with the use of cheque books, which direct the bank to pay or transfer specific amount to the bearer – third party on behalf of account owner. Even today, as result of circumstances that are beyond human control, for instance sickness, third party is being engaged to perform ATM transaction on behalf of account owner. The trust placed in the third party or total ignorance make account owner to give ATM card and pin to third party to withdraw money on his or her behalf. Hence, there have been reported cases of fraudulent transactions and retention of customers' cards and or PIN by the third party. This action to say the least is prone to many security risks which must be avoided at all costs because its negative effect is at alarming rate. Therefore, the aim of this research is to develop a model for a trusted party for a secured ATM transaction on behalf of account owner.

2. REVIEW OF RELATED WORK

The current third party system in use in the banks is in the form of issuing of cheques and ID is the means of authentication, the third party is asked to append his or her signature and address on the back of the cheque for the bank to grant the request. Today we are the era of ATM machine; ATM cards, ATM machine and PIN are being used for the same purpose. This act is a form of security risks that opens the account owner to different fraudulent vulnerabilities. There are various frameworks in existence to fortify the ATM machine. For instance a card less multi banking ATM system services using biometrics and face recognition was developed by [8]. It portrays a framework that replaces the ATM cards with Personal Identification Number (PIN) by using unique physiological biometrics validation and facial acknowledgement.

Python face recognition API is used to capture and verify the user's facial features, MFA application to check if the OTP authentication is successful, Java was used to implement the system which makes it easy to understand. The implementation was in phases: registration phase which capture the fingerprint of the user using MFS100 device, captured image is compared to the one stored in the database and it sends 6 digit OTP to the user's registered mobile number. Obscured during imaging by moisture, dirt or wear can be challenging when using fingerprint for authentication, hackers could use the stolen fingerprint easily to break into the security system.

The implementation of a biometric (finger) using multispectral imaging biometric authentication measures for enhancing ATM security in Nigeria was carried out by [9]. To design the system, a one factor authentication metric (biometric feature) which plays a dual role for identification and authentication. Client server architecture and visual studio 10.0 software tools are used to design the interface. The fingerprint image of the customer is enrolled and scans transmit to the central server via secured channel. The proposed system can still be hacked because its authentication is only on who you are; account ownership is not verified before performing transaction.

3. RESEARCH METHODOLOGY

The system is designed to eradicate any form of illicit transactions involving third parties for an account holder. As shown in figure 1, there are three user groups namely the bank, account holder and the third party. Using the administrator platform, the third party is registered through the account owner. The account owner can edit or delete the profiles of the third party as needed from time to time; the bank will be notified about the full details of the third party (name, gender, date). One time password (OTP) is generated based on the details of the third party. The OTP which can last for hours is given to the third party as a means of authentication, during ATM transactions on behalf of account owner.

The OTP generated has the following features: i) it carries the amount to be withdrawn from the ATM by the third party; ii) it limits the third party to withdraw money only, there is no checking of account balance, transfer of money or any other ATM transaction iii) the OTP can last for about an hour (this allows the third party to have enough time to get the ATM machine).

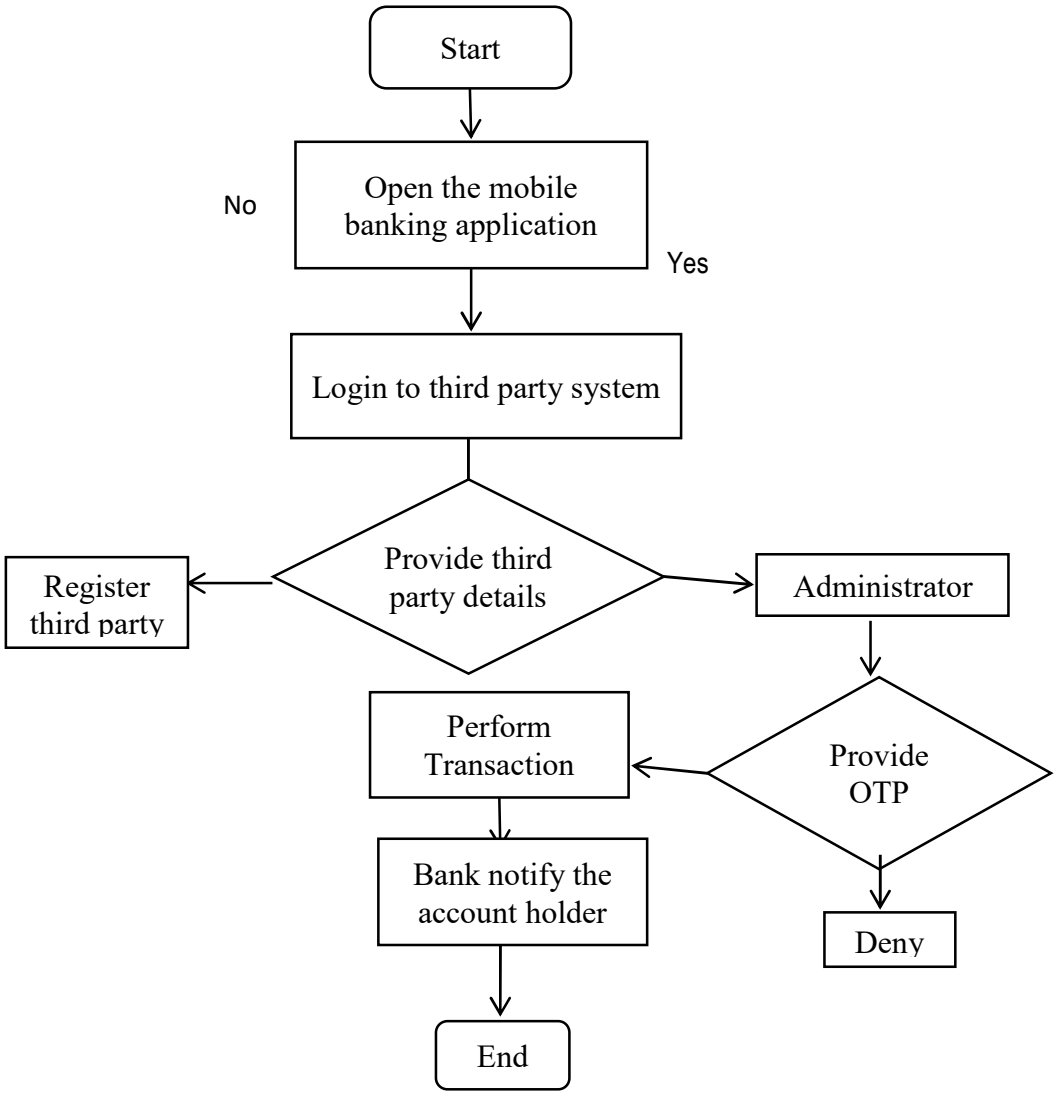

Figure 1: Block Diagram for Account Owner Authentication Process

3.1 System Design and Modeling

In order to achieve the goal of this research, some functional requirements are placed on the application platform. The user (account holder) based on the permission assigned by the bank to perform the task for the third party by using the mobile app. Users (account holder) register the third party via the administrator (mobile banking application) and provide the amount to be withdraw by the third party, add new users to the system database, view existing items in the application and manage their account on the platform (application) and delete or block them if necessary. Administrator via (Mobile banking apps) is the only user group that can set a one-time password (OTP) for security and send the amount to be withdrawn embedded in the OTP to the account holder.

The user verifies the one-time password via a notification message provided on the application and provides the sender with the one-time password. The third party uses the OTP for authentication while using the ATM, after performing the transaction any other transaction cannot be done, the ATM reject the card and end the transaction. The different users groups are referred to as actors in the common unified modeling language. This is the tool we used to model the web application

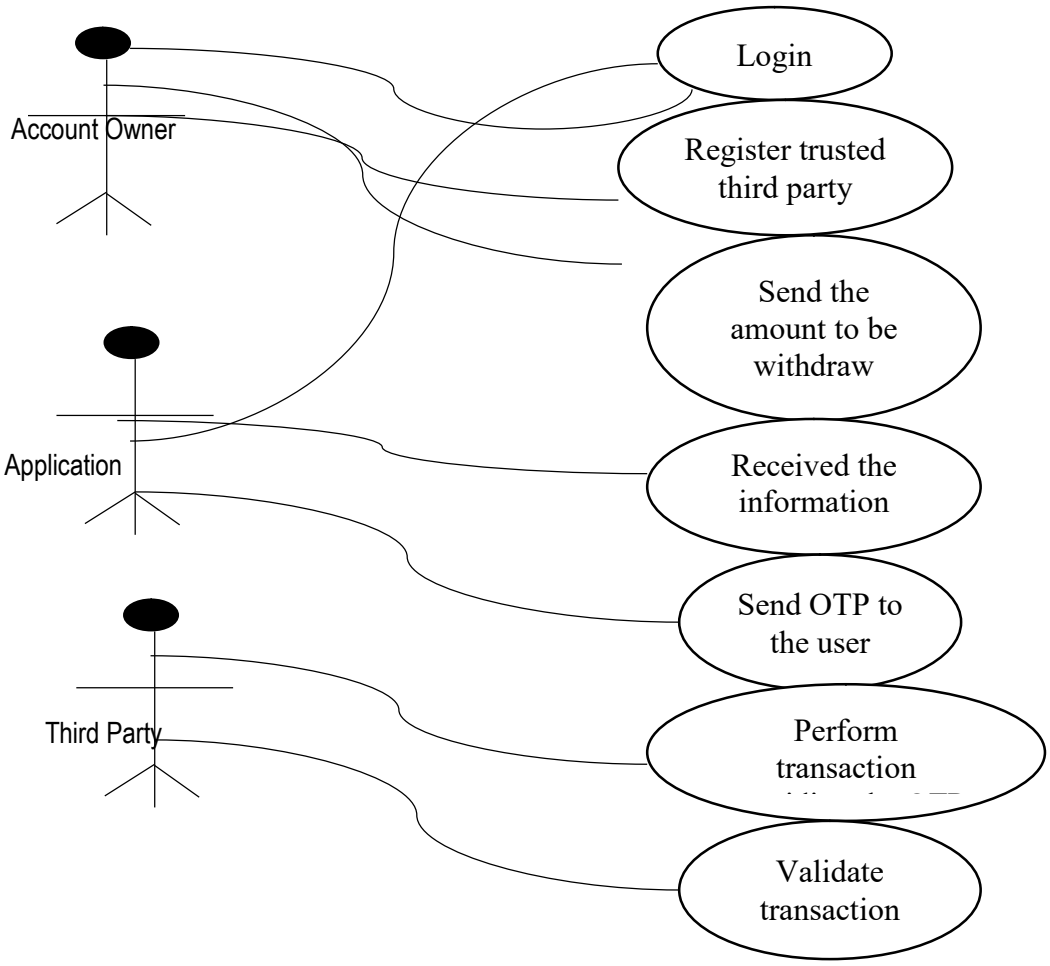

Figure 2: Use Case for the System

4. CONCLUSION

The current third party system available in banks is in form of issuing of cheques and ID is the means of authentication, for the bank to grant the request. With the finding of this study, third party is legalized in the use of ATM card on behalf of account owner. The OTP generated for third party, only allows specified amount embedded in OTP and no other transactions can be performed by the third party. The account owner is rest sure that nobody can check his or her account balance and perform any illegal transaction with his her ATM card.

REFERENCES

[1] Fasan B.G. (2018): ATM security using facial recognition. *International Journals of Engineering and computer scienece*, 33-32.
[2] Omankhanlen B.E. (2017): Inceased rate of using ATM machine in Nigeria. *International Journal of Research*, 101-102.
[3] Yasuharu F.A. (2018): ATM security using Biometric system. *International Journals for Engineering and Research*, 65-66.
[4] Guidance part 8. (2021): ATM security system. *International Journal for Engineering and Computer Science*, 54-55.
[5] Gupta Lee & Rae. (2019". ATM system using Fingerprint Athentication. *International Journal for Computer Science*, 76-78.
[6] Balunywa T.F. (2018): Advantages of using ATM. *International Journal of Engineering and Technology*, 16-17.
[7] Ashwini C (2020).:Card less multi banking ATM system services using biometrics and face recognition. *International Journal of computer science*, 200-223.
[8] Nawaya J.J (2019).:Designing a biometric using multispectral imaging biometric authentication measures for enhancing ATM security in Nigeria. 20-67.