AGBOR JOURNAL OF SCIENCE AND SCIENCE EDUCATION (AJOSSE) VOL.5 ISSUE 1

AN ENHANCED ALGORITHM FOR PREVENTING ATM FRAUD IN NIGERIA

S. Agholor
Department of Computer Science,
Federal College of Education, Abeokuta

AGBOR JOURNAL OF SCIENCE AND SCIENCE EDUCATION (AJOSSE) VOL.5 ISSUE 1

ABSTRACT

The problem of ATM frauds is universal in nature and its consequences on the society should be of great concern to all stakeholders. This study examined the existing algorithms that drive ATM transactions and found it to be somewhat faulty because of the problems associated with its implementation. Some of the problems are: allowing transactions to take place in the account before alerting the account's owner; inability to give notice to the ATM card owner that the card is about to expire so that the process of replacement can commence; inability to protect the ATM card owner from shoulder surfing and keyboard loggers; and not allowing the account owner to authorize payment before debit can take place in the account. It is against this background that a new algorithm was developed by the author to correct these observed lapses in the existing algorithm. The existing and the developed algorithms were subjected to laboratory experiment through simulation technique. The results obtained show that the developed algorithm performed better than the existing algorithm in terms of fraud prevention. Finally, the paper recommends the adoption of the developed algorithm by the banks among others.

Keywords: ATM, ATM Card, Fraud, Transaction

 ISSN : 1597-8774

INTRODUCTION

An Automated Teller Machine (also known as ATM or Cash Machine), is a computerized device that provides the customers of a financial institution with the ability to perform financial transactions without the need for a human clerk or bank teller (Devinaga, 2010).

The ATM is a terminal provided by bank or other financial institutions which enables the customer to withdraw cash, make a balance enquiry, order a statement, make money transfer or deposit cash. The ATMs are basically self-service banking terminals and are aimed at providing fast and convenient service to customers. Some of the new generations of ATMs are able to cash a cheque, dispense traveller's cheques and postage stamps, perform stock transfers, print discount coupons, issue phone cards, and even sell concert tickets.

In the early days of Automated Teller Machine (ATM), the machine operated in a local mode without any connection to the banking systems, and transaction authorization took place based on the information recorded in the magnetic bands of the cards. The next step in the evolution of this industry was the connection of these devices to the bank's centralized systems. In the early 90's, taking advantage of the technological boom in microcomputers and communications, ATMs started to work exclusively online. This led to unprecedented expansion in the deployment and usage of ATM worldwide. According to the estimates developed by ATM Industry Association (ATMIA), the number of ATMs worldwide in 2007 was over 1.6 million (Essien, 2011).

An ATM hardware is classified into two major categories: the first one corresponds to its PC architecture (a microprocessor, memory, drives, monitor, keyboard, etc.), the second one relates to ATM specific functions such as card reading, cash dispensing, cash storage, user and operator's video and keyboard interaction, etc. Based on the PC architecture, the software included in an ATM is not very different to that which is found in a personal computer. It has an OS/2, or Windows based operating system. The application software is mostly provided by the manufacturer of the ATM machine and it normally offers an interface allowing for each financial institution to adapt its own applications (Suresh, 2008).

The General ATM

Figure 1, according to Mosabber (2006) shows the interactive components of ATM. The functions of each component are described below.

Card Reader: Customer inserts the card in where it is written on the screen "Please Insert your card".

Keypad: Use for PIN code input, choices, amount of money etc as the input to the ATM machine.

ISSN : 1597-8774

Display Screen: This screen shows all the instructions or options for the customers' convenience.

Screen Buttons: When options are given on the screen the user can choose any of the options accordingly by the use of button on left or right side of the screen. These buttons select the option from the screen.

Cash Dispenser: Withdrawal money is given by this slot.

Deposit Slot: To deposit money, this slot is used.

Speaker: Speaker provides the facilities to the customer by giving auditory feedback.

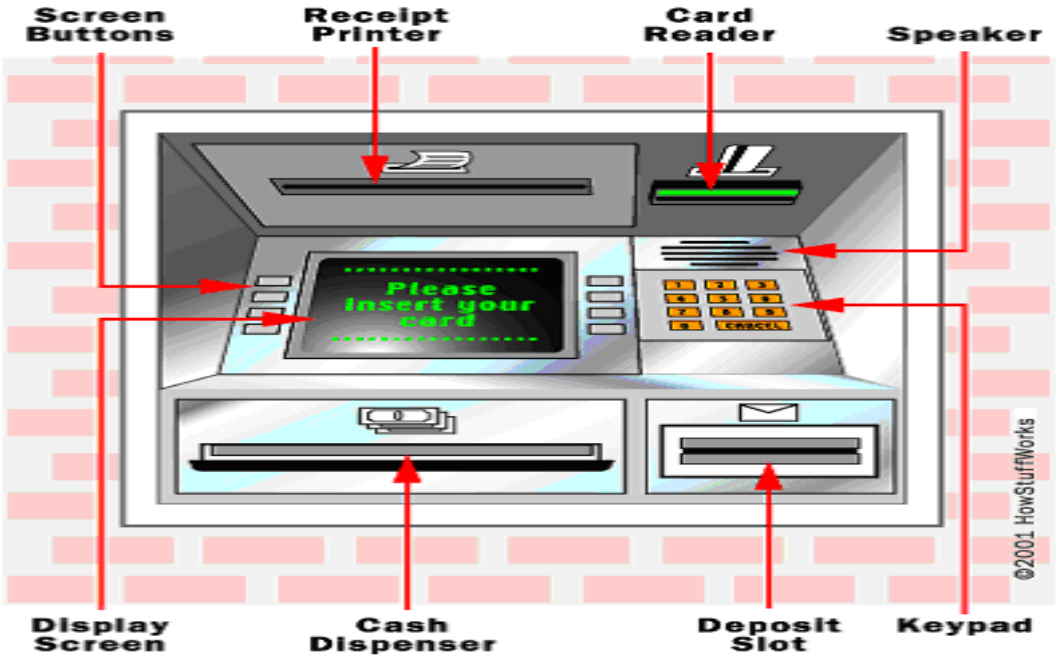

Figure 1: Interactive Components ATM (Source: Mosabber, 2006)

The rest of this paper is structured as follows: Section 2 deals with the Literature Review where existing algorithms were critically reviewed. Section 3 describes the Design Methodology. In section 4, Implementation and Evaluation were carried out. Finally, Recommendation, Limitation and Conclusion were discussed in section 5.

LITERATURE REVIEW

ATM fraud is universal and old as the arrival of ATM. According to Devinaga (2010), in 1989, 570 pounds was wrongly deducted from John Allan's account with Bank of Scotland. A total of 8 cash withdrawals were carried out, three of them when he was away with his card in Andorra.

ISSN : 1597-8774

In the words of Ayo (2010), a large sum of money was withdrawn in 2009 from my account with GTB of Nigeria and I received alerts on the transactions shortly after my account was completely looted.

According to Adeoti (2011), the first bank to introduce ATM in Nigeria was the Moribund Societe Generale Bank of Nigeria (SGBN) in 1990. The trade name for SGBN's ATM was "Cash Point 24". One of the first generation banks then, First Bank Plc came on stream with their own ATM in December 1991, a year behind SGBN. They also gave a trade name "FIRST CASH" to their ATM. While that of SGBN was the drive-in-system, that of the First Bank ATM was through-the-wall.

The growth of ATMs in Nigerian banks rose from 83% in 2006 to 289% in 2007 as can be seen in table 1. Almost all banks introduced the ATM in their banks' premises in 2007. The increase in number of customers using ATM has also increased the propensity to fraudulent practices by the ATMs fraud perpetrators.

Table 1: ATM Growth in Nigeria

Year	No. of ATMs	Growth Rates
2005	425	6.3%
2006	776	83.0%
2007	3,017	289.0%
2008	5,894	95.0%

Source: Inter-switch Reports 2008

Access to ATM is through the use of Personal Identification Number (PIN) and a plastic card that contains magnetic strips with which the customer is identified. Banks usually hand over the PIN to the customer personally and the customer is usually instructed not to disclose the number to a third party. ATM card is about the size of a normal credit card and apart from the need to ensure its safety, its surface strips could be mutilated which may make the machine to reject it even though the PIN number is entered correctly.

Obiano (2009) blamed the menace of ATM frauds on indiscriminate issue of ATM card without regard to the customer's literacy level. According to him 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. Omankhanleu (2009) opined that the current upsurge in nefarious activities of Automated Teller Machine (ATM) fraudsters are threatening electronic payment system in the nation's banking sector with users threatening massive dumping of their cards if the unwholesome act is not checked.

ISSN : 1597-8774

Adeloye (2008) identified security as well as power outage as major challenges facing the ATM users in Nigeria.

A Report on Global ATM Frauds according to Adeoti (2011) identified the following types of ATM Frauds:

(a) Shoulder Surfing: This is a fraud method in which the ATM fraudster uses a giraffe method to monitor the information the customer keys in into the ATM machine without the knowledge of the customers.

(b) Lebanese Loop: This is a device used to commit and identify theft by exploiting Automated Teller Machine (ATM). Its name comes from its regular use among Lebanese financial crime perpetrators, although it has now spread to various other international crime groups.

(c) Using Stolen Cards: This is a situation in which the ATM card of a customer is stolen and presented by a fake presenter.

(d) Card Jamming: Once the ATM card is jammed, fraudster pretending as a genuine sympathizer will suggest that the victim re-enter his or her security code. When the card holder ultimately leaves in despair the fraudster retrieves the card and enters the code that he has doctored clandestinely.

(e) Use of Fake Cards: Fraudsters use data collected from tiny cameras and devices called 'skimmers' that capture and record bank account information.

(f) Duplicate ATMs: The fraudsters use software which records the passwords typed on those machines. Thereafter duplicate cards are manufactured and money is withdrawn with the use of stolen Passwords. Sometimes such frauds are insiders' job with the collusion of the employees of the company issuing the ATM Cards.

(g) Card Swapping: This is a card theft trick whereby a fraudster poses as a "Good Samaritan" after forcing the ATM to malfunction and then uses a sleight of hand to substitute the customer's card with an old bank card. As the customer is endlessly trying to push the card through, the fraudster offer assistance by pretending to help the customer push through the card.

(h) Diversion

(i) ATM Burglary

According to Maenpaa et. al. (2008), security can stand for the reliability of an innovation and an overall belief on the part of the user that banking transactions can be completed confidentially and safely. Study by Rogers et. al.(1997) asked the eight non-users if they had any concerns about using ATMs. The result of the study indicated that most of them have mentioned safety as the main concern. This result is almost similar to that of Mirza et .al. (2009) study in respect to internet banking. However, Mcandrews (2003) interviewees also focused on many issues related to safety and security. These include their inability to use ATMs in a remote location especially in the evening.

 ISSN : 1597-8774

In this context, the majority of ATMs today are located at sites other than banks such as malls and grocery stores (Gowrisankaran and Krainer, 2011). Study of Maenpaa et al. (2008) focused on many aspects for security of internet banking users, most of which are also related to ATMs. These include privacy of their bank transactions and safety of their bank transactions. Study by Adepoju and Alhassan (2010) revealed that the security level is poor in Nigerian banks as some banks do not offer any tools where customers can easily report cases of ATM fraud.

ATM, which has been widely applied, has played a significant positive roles in people's lives, but fraudsters began to endlessly take advantage of the ATM fraud-related issues such as huge security holes, peeping at passwords, exchanging fake cards, installing miniature camera head and fake keyboard (Mengxing et. al., 2013). ATM has security keys programmed. Between the ATM, the bank and the network processor, the code changing can guarantee the credit of access and the safety of ATM card numbers by scrambler.

Review of Transaction Functionality/Existing Algorithms

ATM transaction elements are the card and the ATM components. Figure 2, according to Suresh (2008) shows the sequence of events involved in the authorization process together with the functionality of the central authorization system to which the ATM is connected.

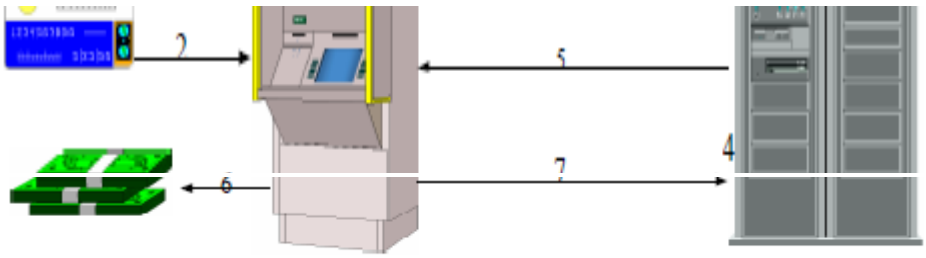

Figure 2: ATM Transaction Sequence (Source: Suresh, 2008)

According to Suresh (2008), in India, the algorithm used to drive ATM is:

Step1. Insert Card and enter PIN code
Step2. Select Transaction type and amount
Step3. Information sent to Authorizing (central) system
Step4. Central system validates information

 ISSN : 1597-8774

Step5. Authorization sent to ATM
Step6. Cash/receipt provided to user if it is cash request. Otherwise deposit is accepted
Step7. Transaction confirmed
The algorithm is explained in detail as follows:

The user accesses the ATM through the magnetic band card issued by the financial institutions. Once the card is validated by the ATM, the application requests the user's PIN and the type of transaction to be conducted. This information is combined with control data to create a requirements message to the authorizing system; this message, a Transaction Request (TREQ), is sent over a public or private data communications network.

The authorizing system receives the TREQ and proceeds to decode and process the information as follows: card identification, PIN validation, financial transaction execution, application file updates, and reply preparation. The Transaction Reply (TREPLY) is then sent via the communications network to the ATM originating the transaction.

Upon TREPLY reception, the ATM decodes and processes the information and presents the transaction results to the user. If it is a cash request, the cash is presented; if it is an information request, it is shown on the screen or printed on a receipt. Finally, the ATM's application puts together and transmits a Transaction Confirmation (TCONFIRM) to the authorizing system including feedback on the success or failure of the transaction. In general, a centralized system has the ability to connect with each and every ATM, and at the same time communicate with each and every centralized system that is required to complete a transaction.

According to Mosabber (2006), in Bangladesh, the algorithm used to drive ATM is:

Step1: First customer insert ATM card (E-cash card) into the machine and wait to insert PIN (personal identification number). When both processes are done ATM Machine check account number and PIN for further processing like requesting money to the bank server.
Step2: Bank Server debited the amount of money from the customer account. And update database for that customer account and send all transaction information to ETN server.
Step3: ETN server then update database so that they can send report to the banks. And then ETN send clearance signal to the ATM machine to dispenser.
Step4: After the clearance signal ATM machine dispense money to the customer; where ETN stands for Electrical Transaction Network.

According to Triton (2004), an ATM manufacturer company in USA, the ATM Algorithm provided is:
Step1: Insert the ATM card into the card reader of the terminal. The card must be inserted so that the magnetic strip can be scanned by the card reader's sensor.

ISSN : 1597-8774

If the customer inserts the card incorrectly, a warning message will be displayed, accompanied by several beeps to get their attention. If there is a problem reading a card, make sure the customer is inserting the card correctly. Most problems are the result of inserting the card incorrectly. Once the card has been read in successfully, a surcharge message, if applicable, may be displayed (the surcharge message may be displayed at the end of the customer's transaction selection).
Step2: The customer must then enter his secret Personal Identification Number, or PIN code.
Step3: Select transaction type and account and the desired amount of the transaction, if needed.
Step 4: If the transaction was processed successfully, the customer is prompted to retrieve the requested cash (for withdrawal transactions) and/or the applicable transaction receipt, as needed. If the transaction was declined, a short receipt indicating the problem is printed.

In Nigeria, Zenith Bank (2012) while educating their customers on how to use ATM gave a vivid algorithm on how its ATM works using "Making Withdrawal" as a case study as follows:
Step1: Insert your card when prompted to do so, with the red surface facing up and ensuring that the edge with the white arrow indication goes in first.
Step2: Enter your PIN number and press "PROCEED".
Step3: From the list of transaction types, select "WITHDRAWAL"
Step4: Select "CHECKING" if you are withdrawing from your current account, "SAVINGS" to withdraw from your savings account, or "CREDIT" to withdraw from your mastercard account.
Step5: Select from the list any amount you intend to withdraw. Otherwise select "OTHERS" if the amount you want to withdraw is not in the listing. Enter the amount you want to withdraw eg N15,500.00 and press the "PROCEED" button to process your transaction.
Step6: Choose "YES" if you want to do another transaction. Otherwise "NO" to end transaction.
It should be noted that Zenith Bank gave step by step description on how to perform other transactions such as Checking your Balance, Fund Transfer etc. The procedure is same except that in step3, you select the actual transaction you needed.

Flaws of the Existing ATM Banking Algorithms

1) It sends SMS alert only after deduction has been carried out on the end-user's account.
2) It allows illegal withdrawals/transfers when end-user's password is compromised. In other words, illegal withdrawals/transfers are allowed without the consent of the legitimate owner for at least once.

ISSN : 1597-8774

3) It does not give notice/reminder on the expiration of the card.

Preventive Measures put in place by the Banks in Nigeria to reduce ATM Fraud

Various banks in Nigeria have taken preventive measures to correct some of the flaws enumerated above. The measures are:

1) Maximum ATM withdrawal per transaction put at N20,000.00.
2) Maximum ATM daily cumulative withdrawal put at between N60,000.00 and N100,000.00 depending on the bank.
3) If you suspect a fraudulent withdrawal on your account, text XXXNNN to the bank's dedicated phone number to block your account from further withdrawals where:
XXX= Stop, Block, Deactivate with little variation such as STOPATM or STOP ATM etc depending on the bank;
NNN= full account number or last three digits of your account number etc depending on the bank.

There are flaws in this arrangement put in place by the banks even though it helps to reduce ATM fraud. They are:

1) As good as the measures are, it still allow the end-user to part with their hard earned money to the fraudsters at least for the first transaction before the measure put in place can allow the end-user stop further cash withdrawal from the account.
2) It did not accommodate fund transfer which can sweep a huge sum of money before the end-user could stop further transaction on the account.

DESIGN METHODOLOGY

In this study, we developed an algorithm to correct the flaws found in the literature. We called this algorithm the Confirmation Algorithm for ATM Banking. The algorithm is presented in section 3.1. The algorithm was tested alongside the existing algorithm.

The Proposed Algorithm for ATM Banking

The architecture for the proposed algorithm is shown in figure 3.

ISSN : 1597-8774

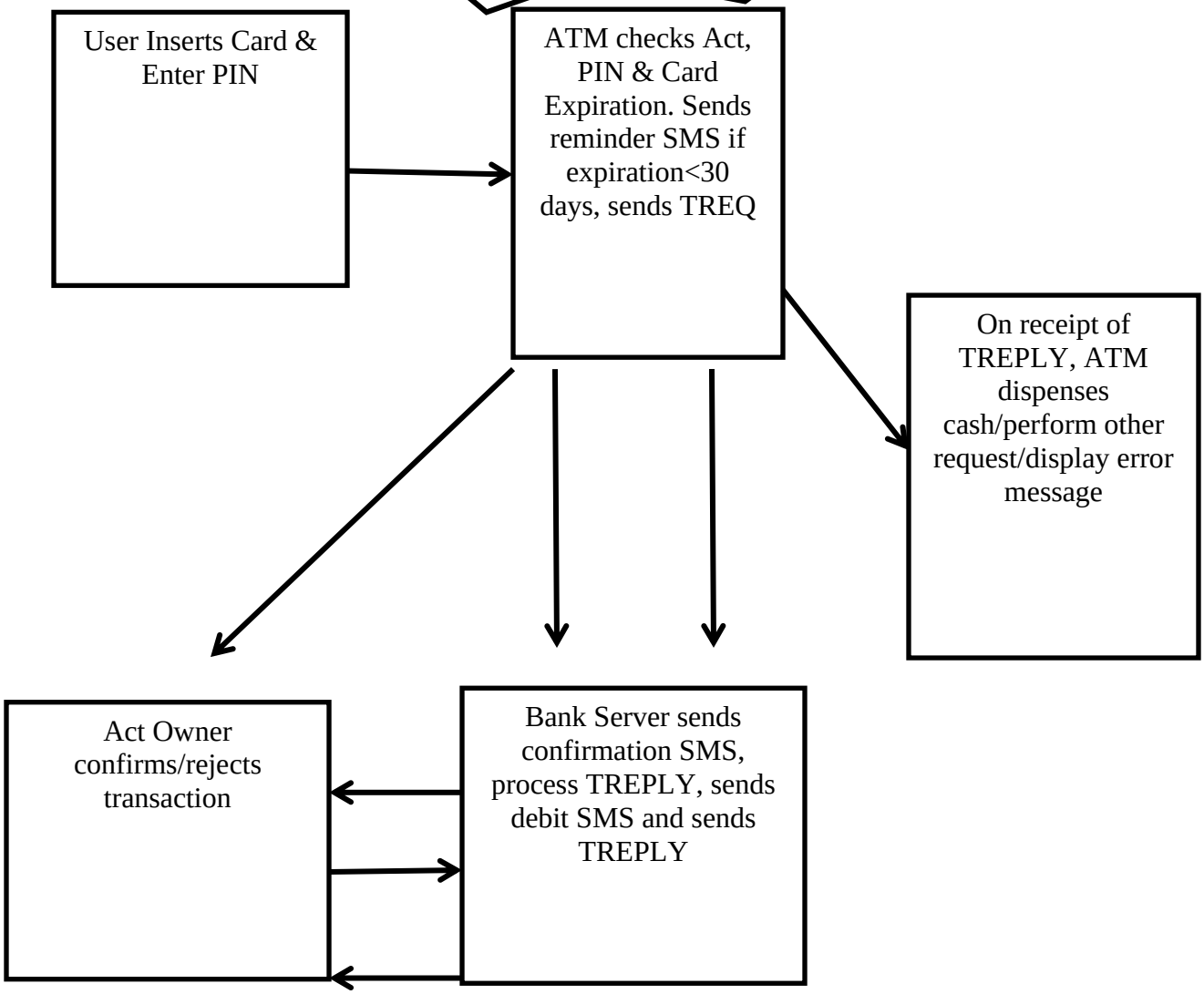

Figure 3: The Architecture of the Proposed Algorithm

The architecture is further explained by the following algorithm.

Step 1: Insert ATM Card (e-Cash card)

If card is ok then

If expdate<30 days then

Send SMS reminder to account holder to renew card

Request for PIN

ISSN : 1597-8774

Else output "Invalid card and stop transaction"
If PIN ok then
20: create transaction request (TREQ)
Send TREQ to authorization (central) system in step 2
Else display "Invalid PIN, please enter your PIN again"
PIN re-entered
If PIN ok then proceed to 20
Else display "Invalid PIN, please enter your PIN again"
PIN re-entered
If PIN ok then proceed to 20
Else block account and seize card
Step 2: Authorizing system decodes and processes information
If card and PIN validation ok then
Send SMS to account holder to confirm or reject transaction using Y or N
If Y then process transaction
Send SMS to the account holder on transaction performed
Prepare transaction reply (TREPLY)
Send TREPLY to ATM
Otherwise stop transaction and block account
Send message "transaction not permitted" to the ATM
Else send error message to ATM
Step 3: ATM decodes TREPLY
If TREPLY is successful then perform 30 else display error message; goto 40
30: if cash request then cash is presented to the user. Otherwise perform other request
elseif information request, then display on the screen or print on a receipt or both
40: Transaction confirmation (TCONFIRM) is sent to the authorizing system, which include success or failure of the transaction.
END OF ATM TRANSACTION

IMPLEMENTATION AND EVALUATION

Conduct of Experiment

An experiment was conducted using 500 participants via simulation since no bank was ready to allow us use their database. In this experiment, we call the bank XYZ Bank PLC and divided the participants into two equal groups of 250 each in both the Control group and the Experimental Group.

 ISSN : 1597-8774

It should be noted that the Control group simulation was done using the current ATM Banking Algorithm as well as the preventive measures put in place by the banks to prevent fraud in these accounts while the experimental group was simulated using the confirmation algorithm.

The Personal Identification Numbers (PINs) of the participants for this experiment were given to us. We then perform various ATM transactions on the accounts of the 500 participants ranging from cash withdrawal to fund transfer between accounts since we were in possession of the PINS

DATA ANALYSIS

Statistical Package for Social Sciences (SPSS) version 17 was employed in the analysis of the data.

RESULTS AND DISCUSSION

Gender Distribution of Participants

Table 2 shows the gender distribution of participants. In the Control Group, 52% of the participants were males while 48% were females. Similarly, in the Experimental Group, 54% of the participants were males while 44% were females.

Table 2: Gender Distribution of Participants

Sex of Participants	**Control Group**		**Experimental Group**	
	No. of Participants	% of Participants	No. of Participants	% of Participants
Male	130	52%	140	56%
Female	120	48%	110	44%
Total	250	100%	250	100%

ATM Transactions on the Control Group using the Existing Algorithm

We performed two transactions, that is, cash withdrawal and fund transfer on the participants' accounts using the existing ATM algorithms. The results are presented in table 3.

ISSN : 1597-8774

Table 3: ATM Transactions on the Control Group

Transactions	Success	% Success
Cash Withdrawal	250	100%
Fund Transfer to another account	250	100%

From table 3, it shows that fraudulent activities can go on unhindered once the PIN and the ATM card are compromised. In this study, we succeeded in making transactions in all the 250 accounts unhindered. This finding confirmed the flaws inherent in the current ATM algorithm.

These flaws were purportedly corrected by the preventive algorithm developed by the banks. Cash withdrawal and fund transfer were performed on the participants' accounts using this algorithm. The results are as shown in table 4.

Table 4: Using Bank's Preventive Measure

Transactions	Success	% Success
Cash Withdrawal	190	76%
Fund Transfer to another account	237	95%

From table 4, it shows that the bank's current preventive measure is somewhat faulty. For instance, in cash withdrawal, we made the maximum allowable withdrawal of N20,000.00 per transaction for 190 accounts out of the 250 accounts. This represents 76% success. The case of fund transfer is 95%, which unfortunately, have no transaction limit. Since the preventive measure allows for at least one transaction, which may wipe out the money if it is fund transfer, then the preventive measure is not reliable. A clever criminal may avert cash withdrawal since the maximum he can get for one transaction is N20,000.00 and go for fund transfer which has no set limit.

ATM Transactions on the Experimental Group using the proposed Algorithm

Just as done in the Control Group, we performed two transactions, that is, cash withdrawal and fund transfer on the participants' accounts. The results are presented in table 5.

Table 5: ATM Transactions on the Experimental Group

Transactions	Success	% Success
Cash Withdrawal	0	0%
Fund Transfer to another account	0	0%

From table 5,

ISSN : 1597-8774

the success rate is 0% which means that our developed algorithm has helped correct the lapses found in the current Algorithm. It has the following advantages over the existing algorithm.

1) Before transaction can occur in your account, you must confirm. In other words, you are to authorize transaction in your account via SMS.

2) With this algorithm, you can give your ATM and PIN to someone to make transaction on your behalf bearing in mind that the transaction cannot be complete without your authorizing it through SMS.

3) If your ATM card is stolen or missing, the person in possession cannot do any transaction with it without your knowledge.

4) The problems of Shoulder Surfing and Keyboard loggers attacks have been eliminated because every transaction on the account has to be confirmed by the owner.

5) ATM card owners are continuously reminded in every transaction of the possible expiration of their cards once it is less than 30 days to enable them place order for replacement.

RECOMMENDATION, LIMITATION AND CONCLUSION

Recommendation

1) We recommend that the banks should as a matter of urgency, adopt this algorithm for the safety of their customers' transactions.

2) We recommend that the network providers should be alive to their responsibilities by ensuring uninterrupted GSM services to their customers.

Limitations

The following limitations are common to both the Control Group and the Experimental Group.

1) The failure of Mobile Wireless Network providers to allow account holders to send/receive SMS. This failure may be due to congestion in the Mobile Wireless Network which could involve loss of SMS or delay in the receipt of SMS by the user. This accounts for why we made repeated withdrawals on the Control Group despite the account holders being aware that they could block their account when they noticed unauthorized transaction in their accounts. It is either they did not receive alert, or the alert came late or the SMS meant to stop the further transaction came late or was lost in transit due to network congestion. On the Experimental Group, it accounts for few cases where we were unable to make transactions, which is an advantage to the account holder though it could lead to frustration when the owner actually needed to make transaction.

 ISSN : 1597-8774

In this case, we strongly recommend that Mobile Wireless Network providers expand their network base and be alive to their responsibilities to their customers.

2) The user Mobile Phone was not charged or was switched off and in either case the user was unable to send/receive SMS. This is also one of the reasons why we were able to make repeated withdrawals on the Control Group without hindrance. For the Experimental Group, it is a blessing in disguise as no transaction can occur in that account. As earlier pointed out, it could be frustrating for a legitimate account holder to be denied of service. Here, the account holder should ensure that his or her Mobile Phone is always switched on.

CONCLUSION

ATM has great possibilities in terms of bank-customer transactions but that will depend on the extent to which the ATM frauds are controlled. For effective control of ATM frauds, the recommendations should be put to use.

ISSN : 1597-8774

REFERENCES

Adeloye, A. L (2008). *E-banking as new frontiers for banks*. *In Sunday Punch*, September 14, p. 25

Adeeoti, J. O (2011). Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out. In *Journal of Social Science*, 27(1),53-58

Adepoju, A and Alhassan, M (2010). Challenges of Automated Teller Machine (ATM) Usage and Fraud Occurences in Nigeria- A Case Study of Selected Banks in Minna Metropolis. *In Journal of Internet Banking and Commerce*, 15(2),1-10

Ayo, N (2010). *Illegal ATM Withdrawals: How To Seek Justice*? From www.nairaland.com/446737. Date visited 07/08/12

Devinaga, R (2010). ATM Risk Management and Controls. *In Europena Journal of Economics, Finance and Administrative Sciences*, 21, 161-171.

Essien, E. E (2011). *Proposed Algorithm for Automated Teller Machine*. *In Proceedings of the 10th International Conference of the Nigeria Computer Society*, Abuja, Nigeria, 22, 180-186.

Gowrisankaran, G and Krainer, J (2011). Entry and Pricing in a differentiated Products Industry: Evidence from the ATM Market. *In RAND Journal of Economics*, 42,(1), 1-22.

Maenpaa, K., Kale, S., Kuusela, H., and Mesiranta, N (2008). *Consumer perceptions of Internet Banking in Finland: The Moderating Role of Familiarity*. From www.epulications.bond.edu.au/business-pubs. Date visited 12/01/14.

Mcandrews, J (2003). *Automated Teller Machine Network Pricing-A Review of the Literature*. *In Review of Network Economics*, 2, (2), 146-158.

Mengxing, Z., Feng, W., Deng, H., and Yin, J (2013). *A Survey on Human Computer Interaction Technology for ATM. In International Journal of Intelligent Engineering and Systems*, 6, (1), 20-29.

Mirza, A., Beheshti, H., Wallstrom, A., and Mirza, O (2009) Adoption of Internet Banking by Iranian Consumers: An Empirical Investigation. *In Journal of Applied Sciences*, Vol. 9, pp. 67-75.

Mosabber, H (2006) Understanding of ATM (Automated Teller Machine) in Bangladesh. An Unpublished Thesis submitted to the Department of Computer Science and Engineering, BRAC University, Bangladesh.

Obiano, W (2009) How to fight ATM fraud Online Nigeria. *In Daily News*, June 21, p. 18.

Omankhanlen, O (2009) ATM fraud rises: Nigerians groan. *In Daily News*, June 20, pp. 8-10

 ISSN : 1597-8774

Rogers, W., Gilbert, D., and Cabrera, K (1997) An analysis of automatic teller machine usage by older adults: A structured interview approach. *In Applied Ergonomics*, 28(3), 173-180.

Suresh, S. R (2008) A Social-Technical Business Model Using Automatic Teller Machines and Biometrics. *In Journal of Research in Engineering, IT and Social Sciences*, 2(1),132-141.

Triton (20040 Automated Teller Machine Model FT5000 User Manual Version 3.0.

Zenith Bank (2012) How To Use An ATM. From www.zenithbank.com/howtouse_atm.cfm. Date visited 07/08/12.

ISSN : 1597-8774