International Journal of Research

Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 18
December 2016

Real Time SMS-Based Hashing Scheme for Securing Financial Transactions on ATM Systems

[1]PERURU ANOOSHA,[2] S.HABEEMUNNEESHA

[1]M.Tech., Dept. Digital Electronics & Communication Systems (DECS), Email id. anoosha0406@gmail.com, Sir C.V.Raman Institute of Technology & Sciences, , Tadipatri - Anantapur - Andhra Pradesh

2Asst. Professor, Dept:Digital Electronics & Communication Systems (DECS), Email id: cvrtecetdp@gmail.com, , Sir C.V.Raman Institute of Technology & Sciences, Tadipatri - Anantapur - Andhra Pradesh

Abstract- One detectable profit of the reception and utilization of Automated Teller Machine (ATM) by Nigerian banks going back to the mid 1990s is the simple entry to money by bank clients. Nonetheless, rates of ATM fakes has risen as a restricting variable bringing about a decay reception for executing managing an account organizations. Fraudsters now utilize diverse intends to chase for client's Personal Identification Numbers (PIN) keeping in mind the end goal to dupe clueless clients. Existing measures embraced by monetary establishments require ATM card holders to alternatively subscribe to money related exchanges message alarms through Short Message Services (SMS) (charge and credit exchanges) and the utilization of publications glued in managing an account corridors to caution clients on the need to shield PIN numbers from unapproved clients. These measures are simply instructive and don't sufficiently manage the issues continuously. In this paper, we present a Real Time Instructive SMS-Based plan called MophTem conspire which urges all clients to subscribe to SMS alarms as a reason for starting exchanges for them. The bank produces a hash code utilizing the client PIN number and telephone number. The produced hash key is then used to decode messages asking for exchanges from the client. The expectation is to give extra security layer and sustain existing PIN get to along these lines defending client records and record data

Keywords: ATM fraud, Security, cyber crime, yahoo boys, SMS.

INTRODUCTION

The appearance of the portable transformation has brought forth another e-culture portrayed by e-Banking, e-Payment, e-Learning, e-Passport, e-Immigration, e-Governemnt and so on and has conveyed innovation to the doorsteps of many more than ever. Digitalization is quick turning into a lifestyle with the Nigerian individuals [1]. The insurance of information and

frameworks in systems that are associated with the Internet has kept on posturing genuine difficulties to people, firms and governments as of late as tricksters have culminated their amusement in the fight to wool individuals off their well deserved cash. Despite the fact that innovation brings growthand improvement, it additionally empowers false practices. Data Technology (IT) advances accommodation and it is this exceptionally trademark is being utilized to help and a wager wrongdoing. Since the presentation and selection of Automated Teller Machine (ATM) by Nigerian banks going back to the mid 1990s, clients have delighted in simple access to money even outside traditional keeping money hours. In any case, rates of ATM misrepresentation have risen as a constraining component bringing about a decrease in client certainty and the utilization of ATM cards as a method for executing managing an account organizations. Fraudsters now utilize distinctive intends to chase for the client's close to home distinguishing proof numbers (PIN) with a specific end goal to swindle clueless clients. Existing measures embraced by money related organizations require ATM card holders to alternatively subscribe to monetary exchanges message alarms through Short Message Services (SMS).

A few clients have relinquished the utilization of ATM card having fallen casualty of fraudsters. In addition, the machines have the disturbing inclination to charge records of card proprietor without really apportioning money. In about all causes, endeavors at recouping such monies have been vain. Interswitch, the card innovation organization that handles the ATM innovation for banks, and the banks themselves have conceded that the card is inclined to control for misrepresentation purposes. The card weakness is from an attractive stripe card innovation that does not ensure security. Helpful as the ATM offices seems to be, Internet fraudsters have found in it a road to make fiscal advantage. Over the recent years, the rate at which bank clients lose their stores to these hoodlums through the ATM has turned out to be disturbing. The fraudsters utilize different intends to execute their demonstrations. For example, a typical fake misrepresentation alarm includes the trickster claiming to be from a client's bank advising the client that his ATM card or record has been scratched off in light of suspicious criminal action. They will then trap the client to give account points of interest to "affirm" his personality. Likewise, it is normal for them to clone sites of banks through which they send messages/trick letters to clueless clients to unveil their ATM points of interest. Some are adjust at spying and rapidly retaining the PINs of ATM cards at area focuses and swapping such points of interest on another card using a card peruser. To make matters, these con artists are praised by performers who should be certain chang.e agents[2]

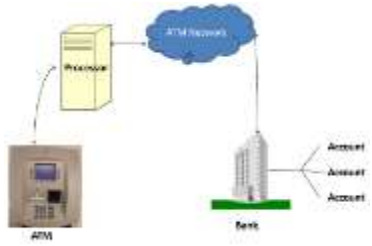
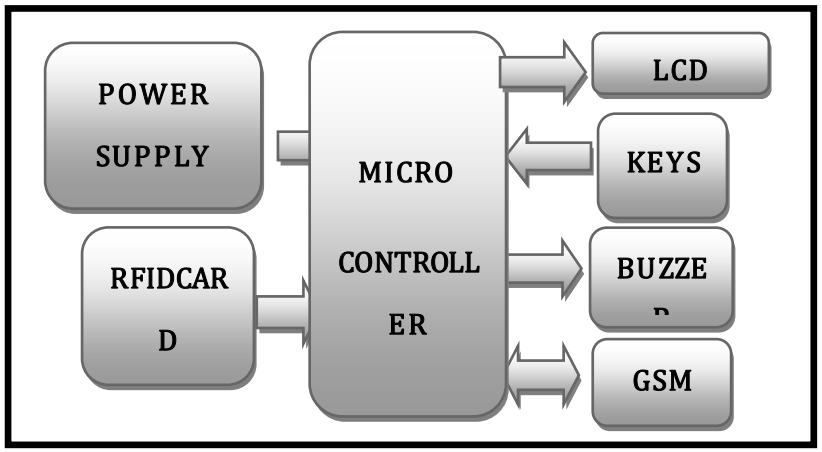


Fig 1 ATM Transaction process

In the existing design it is designed by using ATM card only ATM machine is activated by placing the card and then entering the pin number of the particular card but this system is not safe to use because anybody can access the system if they have the card and pin number like we share our card and pin number to our friends who may miss use it this is the main disadvantage of the system.

Existing Method:

BLOCK DIAGRAM:



Customer Transactions

ATM is a pay-now payment system and its capacity is to bolster a mechanized managing an account organize. All ATM framework must manage the passage of a client's stick, which is known just by the national bank and the client. A run of the mill client's exchange can be outlined by the accompanying activities. A client starts an exchange by selecting an administration from the Customer screen alternatives. He embeds his ATM card nto the card peruser of the terminal. The client's ATM card is encoded with an individual record number. The card must be embedded so that the attractive stripe can be filtered by the card peruser's sensor. On the off chance that the customr embeds the card inaccurately, a notice message will be shown, joined by a few beeps to stand out enough to be noticed. Once the card has been embedded and perused in succesfully, an additional charge message, if relevant, might be shown. The client must enter his mystery

PIN code. Once the PIN is entered, the exchange sort and record are chosen, and the desried measure of the tansaction if necessary. The exchange will be handled, ordinarily in amatter of seconds. On the off chance that the exchange was prepared effectively his is promopted to retriev the asked for money or potentially the relevant exchange receipt, as required. On the off chance that the exchange was declined, a short receipt showing the issue is printed. Generally a screen prompts the client that the ATM card won't be returned , and no entrance to ATM functio is given after three unscussful opportunities to enter the right PIN.

The Proposed System: MophTem Schme

An ATM is a piece of a more unpredictable dispersed sytem composd by different on-screen characters that convey trading messages. A few ATMs are associated with a middle person framework that stores exchange in an incorporated Database. Fraudsters require some delicate information as said before to get to these data. The proposed plan is to anticipate such access to existing exchanges. This is accomplished by invigorating the current s ystem with a layer of security utilizing mobiles telephones. Bank clients would lean toward an ATM framework that gives them what they need than the standard trent of ATMs that have tormented clients with various messages, for example, "out of request, please attempt later", "briefly inaccessible to apportion money", out of utilization or request" and so forth.

.Operation of the proposed Framework

At the point when a client embeds an ATM Card and enters a PIn both the card number and the PIN will be sent to the bank for approval as a component of every exchange notwithstanding this is the telephone number with the tex t messge sent to bank before the real withdrawal. The approved cusotmer will then have the capacity to perform at least one exchanges. The MOphTem plot tries to abuse the messages particularly SMS. The proposed framework is intended to improve the security of the exchange. Clients will have the capacity to caution their manages an account with their cell phone by means of SMS of the withfrawals they aim to do indicating the sum if need be. In the MophTem schme, the message exchange and development will be between the bank and client, subsequently there will be no space for outsider or fraudsters.

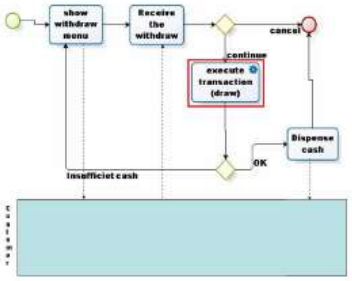


Fig 2 Wiithdrawal Cash Process sub-process

Fig 3 Pin more prone to Miscellaneous Attackers than Phone Number(SMS)

The bank creates a hash code utilizing the Customer PIN number and the telephone number and keeps it in Bank's database and utilizations the genrated hash key to endeavor decoding the getting messages from the client. The bank utilizes the pre-put away PIN number and client's telephone number to offer access to the client's record. Just afte that, is the ATM approved to apportion money to the client. Recognizable proof, monetary and approval information are put away in database in the encoded frame.

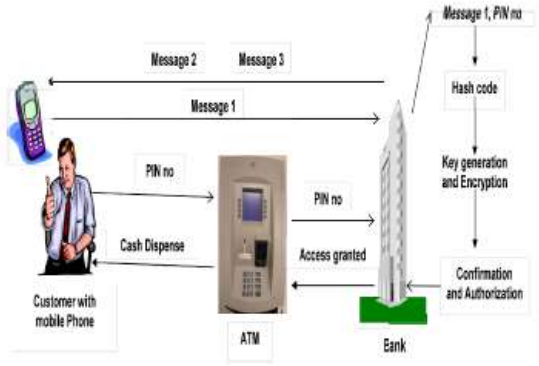


Fig 4 High level architecture of MophTem system

DISCUSSION

Losing cash is said for card holdrs, is more excruciating and baffling that when they answer to their financiers, all they get for their torments are these words. Shockingly, this has been the destiny of casualties of ATM extortion in Nigeria. To exacerbate matters now and again, there is no pictorial proof of the individual who did the withdrawal as a consequence of absence of CCTV camera at some ATM terminal where the withdrawal were made. Customres have been told severally by the banks that the most conspicuous of this ATM misrepresentation happens when their card PIN has been traded off, is this right. The bansk in an offer to escape from liabilites tell the clients that they have intentionally or unknowingly bargained their PIN numbers. With MophTem schme, such deceitful occurrences can be minimized, as an additional layer of verification is presently presented that guarantees that even with the right stick data and possessing someone else's ATM card, a fraudster won't have the capacity to pull back any cash since the cell phone number is extraordinary to each person. In other to keep the culprits from doing such loathsome plans, we have proposed the utilization of the clients telephone preceding withdrawal as proof that the correct proprietor is in charge of the withdrawal without which the client will never be allowed the privilege to get to his record by means of ATM

CONCLUSION

The prosperity of our financial industry is essential to the economy of Nigeria. The

economy of any country turns around its cash related organization and welfare. The Nigerian Government, fiscal establishments and CBN ought to be more proactive about the cash related organization of Nigeria by placing assets into forefront development and HR to complete 21st century budgetary mechanical assemblies in Nigeria and not when the advancement has ended up being obsolete in Europe, America and parts of Asia. This will help in minimizing ATM blackmail in Nigeria. Utilizing MophTem plot an additional layer suggests that the cheat needs sent a fundamental substance using phone which is remarkable to customer. This arrangement will end up being more secure as the administration is moving toward selecting each SIM card with the biometric components of the customer. Additionally, as an industry, Nigeria is moving towards a more secure 'Chip and PIN'. The 'Chip and PIN' stores data on the chip of the card rather than the appealing segment of the card. This chip resembles the Chip used for convenient SIM card and is all the more difficult to 'clone'. This is the standard that the entire cash related industry is moving towards. We assume that by giving a broad assortment of organizations at the ATM which has MophTem plan, donors and customers can favorably do dealing with a record trades round the clock sureness. Completely, a triumphant business case in perspective of rate of return (ROI) can be made by placing assets into using MophTem plan to secure ATM trades. We think with customers' trust in ATM trade ROI will totally take off upwards.

REFERENCES

[1] E. Nkanga, "Combating Cyber Crime Menace in Nigeria", 16 April 2008, THIS DAY Newspaper in Nigeria.

[2] I. Oguntoye, "Bolstering Scammers", The News magazine, October 20, 2008, pp. 62-63.

[3] M. S. Odapu, "Cyber Crime - Time to Stop County's Dominance", 6 September 2008, Daily Trust newspaper in Nigeria.

[4] E. Aginam, "Cybercrime Can Wipe Out Development Gains of a Nation – Experts", 4 March 2009, Vanguard newspaper in Nigeria.

[5] Y. Ishola, "ATM fraud: What safeguard for bank customers?" http://sunday.dailytrust.com/

[6] T. Ogunseye , N10m ATM fraud lands female banks in court. Sunday Punch 10/01/2010, p. 2.

[7] B. Olaleye, . "HEARTACHES OF ATM" Daily Sun, Tuesday 2/3/2010, pp. 45.

[8] G. Oni-Orisan, "Nigerian ATM Card Holders And Their Bankers" http://www.nigeriavillagesquare.com, Thursday 24 June 2010.

[9] F. Ayodele, "Automated Theft Machine: Crook intensity their fleece of bank account holders through the Automated Teller Machine" the News magazine. Vol. 34, no. 3, 2010, pp. 39-40.

[10] F. Balogun, "Automated Problems", The News February 18, 2008, vol. 30 no. 06, pp. 46-48.

[11] http://www.matasano.com/ ATM Backdoor why is no one talking about this.

[12] http://www.mydigitallife.info (2006). ATM Hacking and Cracking to Steal Money with ATM Backdoor Default Master Password

[13] N. A. Azeez, A.R. Ajetola, B.A. Sulaimon, and F.A. Atanda, "Framework from Computer Aided Investigation of ATM Fraud in Nigeria". Pacific Journal of Science and Technology. Vol. 11 no: 1, 2010, pp.356-361.

[14] R. Simutis, D. Dilionas and L. Bastina, "Enhanced Supervision of Automatic Teller Machines via Auto associative Neural Networks", The 8TH International Conference on "Applied Stochastic Models and Data Analysis"(ASMDA-2009), pp. 450-454.

[15] M. Launce, "All you need to know to ensure Safe and Secure ATM Transactions" Africa's Global Bank, *www.ubagroup.com,* pp. 1-3.

[16] Little Linda, "Attitudes Towards Technology Use in Public Zones: The Influence of External Factors on ATM use" CHI of ACM, 2003, pp. 990 -991.

[17] J. J. McAndrews, "Automated Teller Machine Network Pricing – A Review of the Literature" Review of Network Economics Vol.2, Issue 2,2003.

[18] A. Karunanayake, K. De Zoysa, S. Muftic, (2008). "Mobile ATM for Developing

Countries", MobiArch'08, ACM: pp. 25-30.

[19] Triton, "Model 8100: Automated Teller Machine, User / Installation Manual, version 1.0" Delaware Capital Formation, Inc., Triton, 2005.

[20] F. Ricca and A. Marchetto, "A 'Quick and Dirty' Meet-in-the-middle Approach for Migrating to SOA" IWPSE-Evol'09, 2009, pp. 7 3-75.