Multiple Electronic Identity Test: A Modern Approach to Prevent Financial Crimes On Automatic Teller Machines (ATM)

[*]Aigbokhan E.E., [2]Babalola I.T, [3]Oloyede O. & [4]Yekini, N.A.
[1]Computer Technology Department
[2]Electrical Electronic Department
[3.4]Computer Engineering Department
Yaba College of Technology, Yaba, Lagos, Nigeria.

Corresponding Author: nureni.yekini@yabatech.edu.ng

ABSTRACT

In recent time Automatic Teller Machine (ATM) has replaced the face-to-face method of withdrawing money and managing one's bank account. Identity test must be passed before user of ATM could be granted access to the available transaction. There are several advantages of this modern banking system where one accesses his/her fund through ATM with use of card and text password popularly known as PIN (personal identification number). We conducted a survey using questionnaire to assess the use of PIN as it affects ATM user's satisfaction, efficiency, error vulnerability, memorability, and need for robust security platform to deter third part from accessing one's account via ATM machine. It was observed that overall advantages obtained from the use of ATM can be undermining with the use of only PIN. This paper presents a framework for deterring third party access to individual account via ATM. In this paper, PIN and biometric identity test were used for access control. When PIN identity is passed (PIP), X transactions (balance enquiry and deposit) can be made; while PIN plus biometric identity pass (BIp) will allow X transactions plus further transactions (i.e. X + pay bill, fund transfer, cash withdrawal, change pin).

Keywords: Multiple Electronic Identity Test, Financial Crimes, Automatic Teller Machines (ATM), Security

iSTEAMS Proceedings Reference Format
Aigbokhan E.E., Babalola, I.T., Oloyede O. & Yekini, N.A. (2019): Multiple Electronic Identity Test: A Modern Approach to Prevent Financial Crimes On Automatic Teller Machines (ATM). Proceedings of the 19th iSTEAMS Multidisciplinary Conference, The Federal Polytechnic, Offa, Kwara State, Nigeria. 7th – 9th August, 2019. Pp 83-92. www.isteams.net/offa2019 - DOI Affix - https://doi.org/ 10.22624/AIMS/iSTEAMS-2019/V19N1P12

1. INTRODUCTION

Some of the reasons for the invention of Automatic Teller Machine (ATM) are: to minimize queue and congestion in the banking hall; to increase speed of access to fund and at any time; and to improve service to customers. ATM dispenses cash and performs other human teller functions; and transactions are carried out through the use of card that enables the card holder(s) to perform banking transactions on their own **(First Bank of Nigeria, 2014)**. ATM users can access their bank accounts to make some transactions without third party. "If the currency being withdrawn from the ATM is different from that in which the bank account is denominated, the money will be converted at an official exchange rate. Thus, ATMs often provide the best possible exchange rates for foreign travelers" **(Ugwuishiwu, Ezema, & Ugwuegbu, 2013).** "Security of bank customer fund has always been a concern since ATM was introduced. Consequently, access control for ATM represents an important tool for protecting customers' funds and guaranteeing that the authentic owner of the ATM card is the one using it for transaction".

The use of PIN alone cannot guarantee safety of funds due to the following problems: card and PIN can be stolen, hence, third party can access and process transactions with accuracy **(Sultan, 2009).** To curtail the major problem of PIN identity test when using ATM smartcard, we propose the use of multifactor identity test, which is the combination of PIN and Biometric identity tests. The PIN identity test will limit the transactions to view account balance, but no modification actions will be permitted; while PIN plus biometric test will allow the user to perform all form of transactions associated with a bank account. As at time of writing this paper we have the following major transactions from ATM: balance check, pay bill, fund transfer, cash withdrawal, PIN change, and cash deposit).

The pseudocode for our multifactor identity test is outlined below:

Let
PIN identity is pass = PI_P
Biometric identity pass = BI_p
If
PI_P then X = balance enquiry, cash deposit
BI_p then Y= X + pay bill, fund transfer, cash withdrawal, change PIN
Stop

Statement of Problem

The problems encountered in the previous system where the use of PIN is paramount are: impersonation and insecure authentication of ATM user. With the increasing rate of theft from ATM through impersonation, banking sector and government are required to inculcate a tight security measure to ensure that these activities of ATM cash theft/crime stop.

Objectives of the Study

The objectives of this study include:

- To create a system that is capable of deterring impersonators in the use of ATM cards via the methodology of finger print biometric.
- To reduce rate of financial crime via ATM in the banking sector and increase the rate of confidence on fund security.

Justification

The justification for the system include:

- To add more security measures to the banking processes using MULTIFACTOR ACCESS CONTROL SYSTEM, which comprises finger print biometrics and text based password methods.
- To eliminate the possibility of an imposter appearing in the use of ATM.

2. SURVEY OF RELATED LITERATURE

Access Control in ATM via Voice Recognition

In the work titled Automated Biometric Voice Based Access Control in Automatic Teller Machine (ATM), the authors conducted an interview with questionnaires targeting ATM users in Lagos, Nigeria. The result of the research revealed problems like: theft and impersonation with accuracy, loss and duplication of smart card. They addressed the problems with the use of biometric based access control method in which access is only authorized by enrolling user speaking into a microphone attached to the automatic teller machine **(Yekini, Itegboje, Oyeyinka, & Akinwole, 2012).**

ATM Model

In ATM Transaction is to be authorized by the customer's bank on demands via ATM, which is online with the ATM user's bank using ROP (Real-time Online Processing) technique **(Fabumni, 2011)**. Model of ATM network is given in Figure 1, which depicts the flow of operation of automatic teller machine: request for personal identification number (PIN); if PIN is valid, then access is authorized; online banking transaction then follows upon fulfilling other conditions for such transaction.

Figure 1: ATM Model
(Source: Snellman 2006)

Cardless Electronic Automated Teller Machine (CEATM) With Biometric Authentication

Alebiosu et al. (2015) present prototype of alphanumeric PIN and biometric finger print. The proposed CEATM is a virtual banking system that allows bank customers to complete one or more banking transactions without ATM card or banking official. It is a self-service technology in financial service delivery usually adopted by financial institutions to reach their customers outside the banking hall. The user of existing ATM uses card to access their account to perform one or more financial transactions. However, Card cloning, card damaging, card expiring, cast skimming, cost of issuance and maintenance, accessing customer account by third parties, waiting time before issuance expiring or new card, will be a forgone issue through the use of CEATM.

Knowledge-Based Authentication System

The User authentication systems with text-based and graphical password schemes are difficult to memorize but easy to hack, which is responsible for the trade-off between usability and security. A PhD thesis titled: "A Usable Knowledge-Based Authentication System (UKBAS)", was designed to balance the trade-off between the two composite factors of security and usability. The architecture of UKBAS consists of Message-Digest 5 (MD-5) algorithm, which was used to encrypt the text password before being stored in the database. Digital Watermarking Algorithm (DWA) was used to watermark each of the selected images (**Ayannuga, 2012).**

3. RESEARCH METHODOLOGY AND FRAMEWORK

A. Methodology and Result Presentation

We prepared and administered questionnaire to assess the usability of the common PIN authentication method in ATM, based on the following criteria: efficiency, error vulnerability, satisfaction, and memorability. The questionnaire contained 20 questions, five questions for each criterion. The sample population was 785, which was 98.12% of the distributed questionnaire. Investigation was conducted in Lagos, the economic nerve center of Federal Republic of Nigeria.

The efficiency, error vulnerability, satisfaction, and memorability of the ATM bank transactions using PIN as regards security was tested and data below was extracted from the questionnaire. The following questions were used to assess the criteria mentioned.

Q1. The use of PIN for authentication of ATM user is enough for efficient banking transactions outside banking hall and customer's identification.
Q2. Four-digits password popularly called PIN is vulnerable to error due to fat finger syndrome, and it can subsequently deny a user access to bank transaction using ATM.
Q3. The four-digit PIN currently in used for access authentication in ATM is easily remembered and memorable.
Q4. The use of PIN as authentication check on ATM is satisfactory in regards to fund security, and prevention of third party from accessing bank account.
Q5. Combination of PIN and biometric access control will enhance customer satisfaction, and fund security when using ATM.

Table 1 shows the frequency of the respondents' responses, while Table 2 shows the same data in percentage.

Table 1: Data Obtained from Questionnaire

Questions	Strongly Agreed	Agreed	Strongly Disagreed	Disagreed	Undecided	Total
Q1	13	77	573	109	13	785
Q2	579	109	77	11	9	785
Q3	601	111	73	0	0	785
Q4	53	13	603	113	3	785
Q5	613	93	73	2	4	785

Table 2: Data Obtained from Questionnaire in Percentage

Questions	Strongly Agreed	Agreed	Strongly Disagreed	Disagreed	Undecided	Total
Q1	2%	10%	73%	14%	2%	100%
Q2	74%	14%	10%	1%	1%	100%
Q3	77%	14%	9%	0%	0%	100%
Q4	7%	2%	77%	14%	0%	100%
Q5	78%	12%	9%	0%	1%	100%

4. RESULT OF DATA ANALYSIS

The result obtained from data analysis using bar chart is as follows:

Q1: Testing Efficiency of Using Pin in Accessing ATM

73% of the respondents strongly disagreed, 14% disagreed to the authors posed questions, 10% agreed, while 2% were undecided, see Figure 2 below. By extrapolation, a total of 87% of our respondents disagreed with the notion that the use of PIN for authentication of ATM transaction is enough for efficient banking transactions outside banking hall and customer's identification. In other words, they affirmed that the use of PIN for authentication of ATM transaction cannot guarantee efficiency.

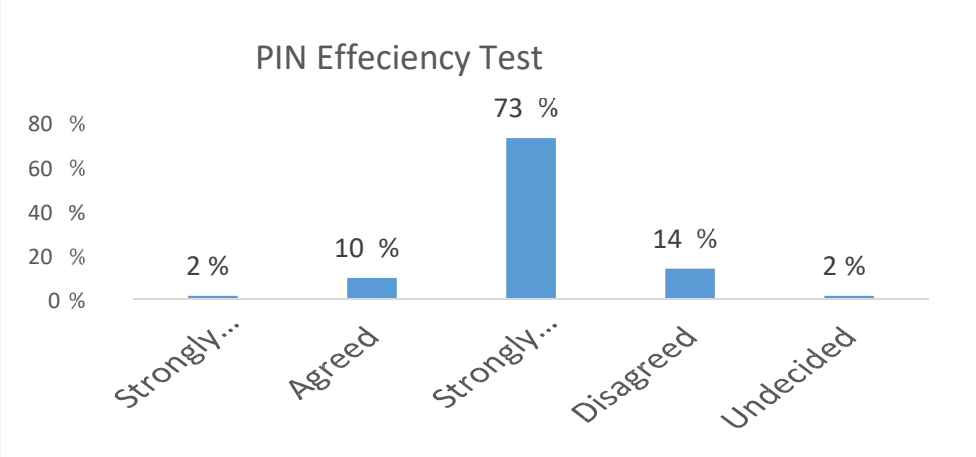

Figure 2: Testing Efficiency of Using PIN in Accessing ATM

Q2: Testing Vulnerability of Error When Using PIN

74% of the respondents strongly agreed to the authors posed questions, 14% agreed, 10% strongly disagreed, 1% disagreed, while 1% were undecided, see Figure 3 below. This implied that four-digit password, popularly called PIN is vulnerable to error.

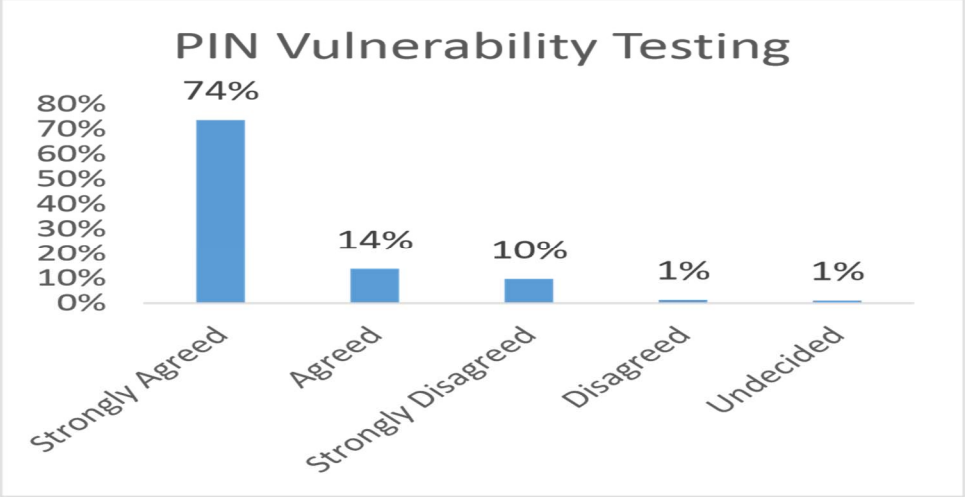

Figure 3: Testing Vulnerability of Error When Using PIN

Q3: Testing Users Experiences as Regards to Four Digit PIN Memorability

The authors are of the opinion that four-digit PIN currently being used for access authentication in ATM is easily remembered and memorable. 77% of respondents strongly agreed, 14% agreed, 9% strongly disagreed, none of the respondents disagreed, and none was undecided, see Figure 4 below. The implication of this is that four-digit PIN is easily remembered and memorable.

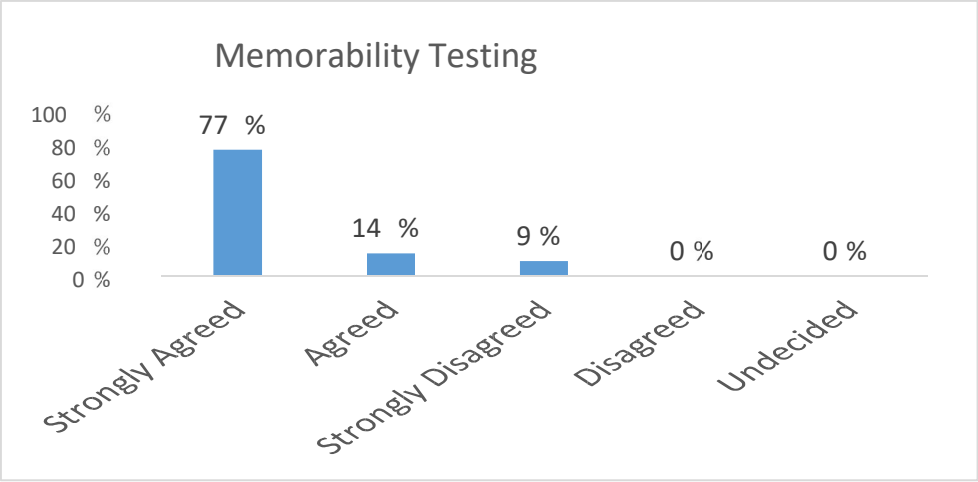

Figure 4: Testing Users Experiences as Regards Four Digit PIN Memorability

Q4: Testing Users Satisfaction with Use of PIN as ATM Access Control

The use of PIN as authentication check on ATM is satisfactory in regards to fund security, and prevention of third party access to one's bank account. 77% of respondents strongly disagreed, 14% disagreed, 7% strongly agreed, 2% agreed, while 0% was undecided, see Figure 5 below. This implies users are not satisfied with the use of PIN as ATM access control.

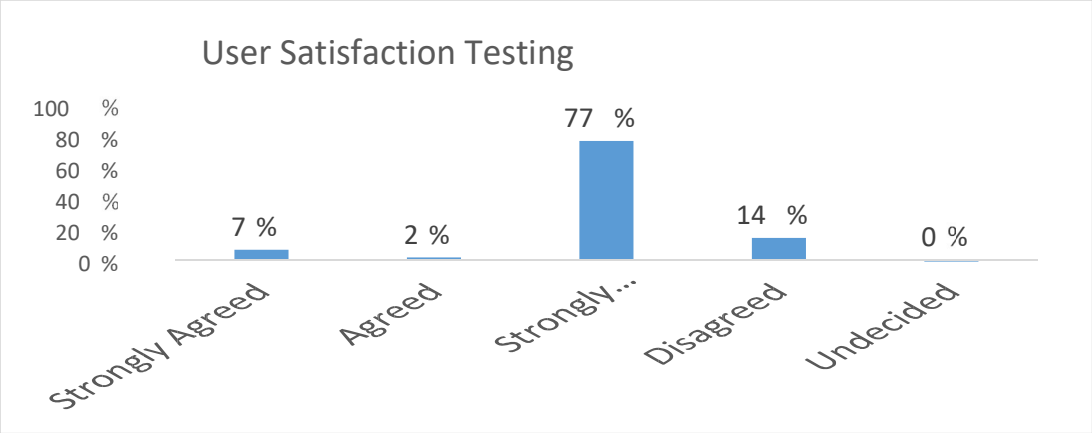

Figure 5: Testing Users Satisfaction with Use of PIN **as ATM Access Control**

Q5. Testing ATM Users Response to Multifactor Authentication Process When Using ATM Combination of PIN and biometric access control will enhance customer satisfaction, and fund security when using ATM. 78% of the respondents strongly agreed, 12% agreed, 9% strongly disagreed, 0% disagreed, while 1% undecided, see Figure 6 below. This means that multiple authentication will enhance customer's satisfaction and fund security.

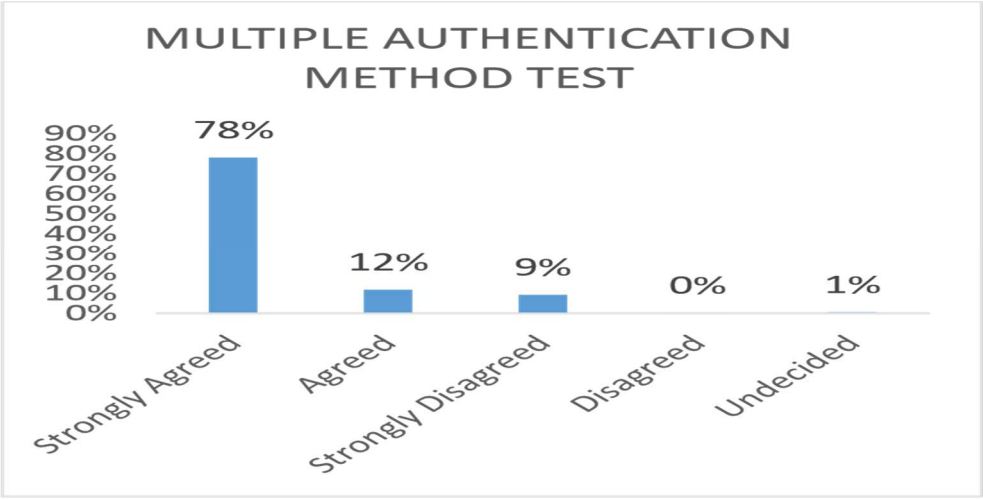

Figure 6: Testing ATM Users Response to Multifactor Authentication Process When Using ATM

4. DESCRIPTION OF PROPOSED SYSTEM

The proposed system is an updating of technology, concepts and tools, giving new content, concepts and methods for better security of funds through ATM, so the existing method is not totally jettisoned. The proposed access control system work as follows:

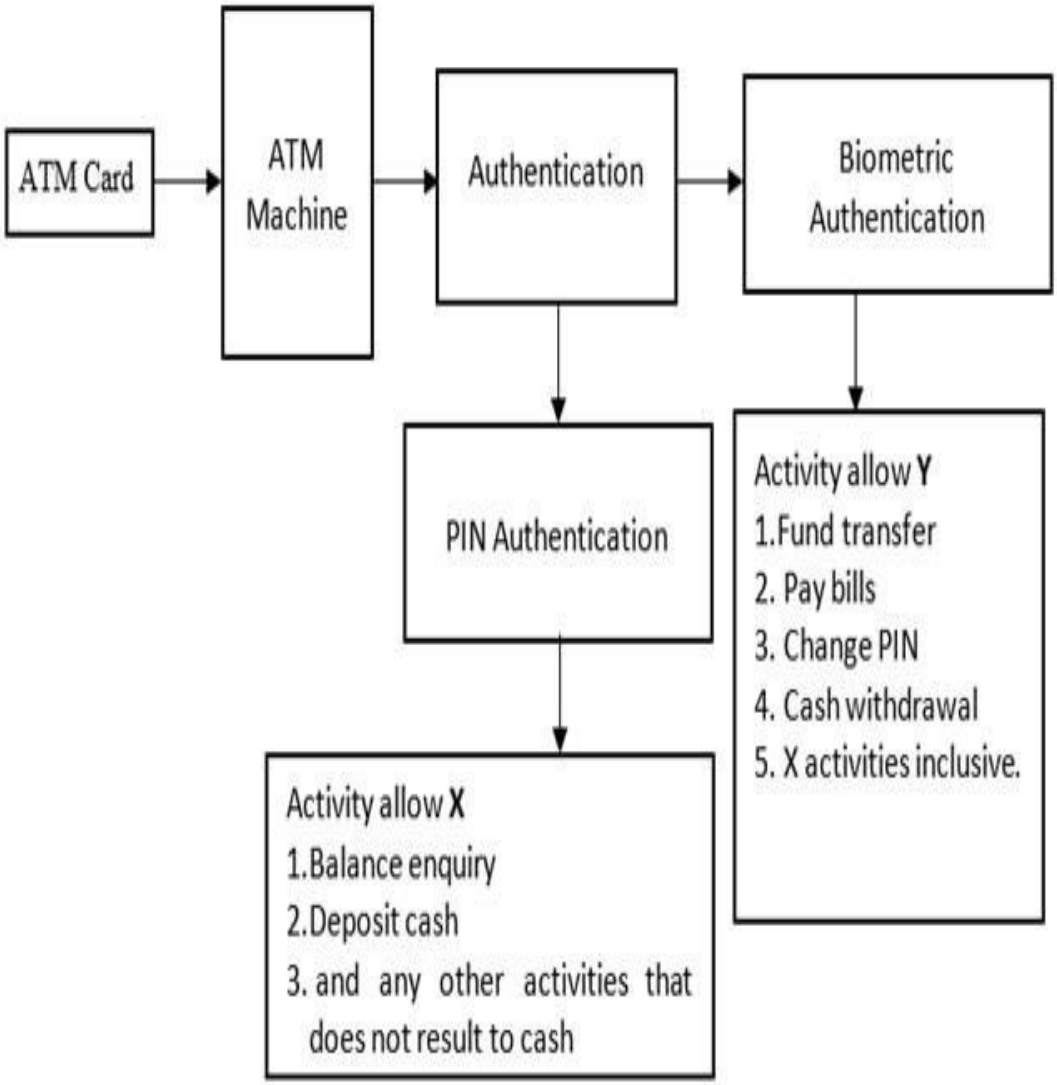

Figure 7: Model of proposed system

5. CONCLUSION

This paper presents a framework for deterring third party from accessing individual account via ATM. The use of personal identification number (PIN), and biometric identity test is used for access control. The proposed system is an updating of technology, concepts and tools, giving new content, concepts and methods for better security of funds through ATM. When PIN identity is passed (PI_P), X transactions (balance enquiry, deposit) can be made, while PIN plus biometric identity pass (BI_p) will allow further transactions plus X transactions (X + pay bill, fund transfer, cash withdrawal, change **pin).** The access to the bank account and operations like balance enquiry, deposit can be done through PIN test, further transaction such as pay bill fund transfer, cash withdrawer, change PIN will only be authorized through BI_P test. If the proposed system could be deployed and implemented, it will go a long way to eradicate or reduce to miniature the fraudulent activities via ATM in banking sector.

REFERENCES

1. Ayannuga, O.O. (2012). Usable Knowledge-Based Authentication System. A PhD Thesis submitted to the Department of Computer Science, College of Natural Sciences, Federal University of Agriculture, Abeokuta, Nigeria.
2. Alebiosu, M.I., Yekini, N.A., Adebari, F.A., & Oloyede, A.O. (2015). Card-Less Electronic Automated Teller Machine (EATM). With Biometric Authentication. International Journal of Engineering Trends and Technology (IJETT), 30 (2), December 2015.
3. Ugwuishiwu, C.H., Ezema, M.E., & Ugwuegbu, N.G. (2013). Design and Implementation of ATM Emulator. Afr J. of Comp & ICTs, 6 (4), pp. 165- 172. Education ISSN: 2201-2958 Volume 5, Number 2, 2014, 137-157.
4. Fabumni, O.A. (2011). Appraisal of the Use of Automated Teller Machine in the banking industry in Nigeria. https://www.unilorin.edu.ng/studproj/cis/0730g c071.pdf. Retrieved January 20, 2019.
5. First Bank of Nigeria (2014). Automated Teller Machine (ATM). Retrieved on November 30, 2018, from http://www.firstbanknigeria.com/products/eban king/automated-teller-machine-atm/
6. Snellman, H. (2006). Automated Teller Machine network market structure and cash usage Scientific monographs. ISBN: 952-462-318-8 ISSN 1238-1691(print) ISBN 952-462-319-6 ISSN 1456-5951 (online).
7. Schlichter, S. (2007-02-05). Using ATMs Abroad - Travel - Travel Tips - msnbc.com. MSNBC. Retrieved 25/07/2018.
8. Sultan, S.M. (2009). Impact of ATM on Customer satisfaction: a comparative Study of SBI, ICICI and HDFC bank, Business Intelligence Journal, 2 (2).
9. Yazeed, A., Yazidu, U., & Ibrahim, Y. (2013). Automated Teller Machine (ATM) Operation Features and Usage in Ghana: Implications for Managerial Decisions. Journal of Business Administration and Management.
10. Yekini, N.A., Oyeyinka, I.K., Itegboje, A.O., & Akinwole, A.K. (2012). Automated Biometric Voice-Based Access Control in Automatic Teller Machine (ATM). International Journal of Advanced Computer Science and Applications (IJACSA), 3 (6). www.ijacsa.thesai.org
11. Yingxu, W. (2010). The Formal Design Model of an Automatic Teller Machine. International Journal of Software Science and Computational Intelligence, 2(1), 102-131.