Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2017, 4(5):241-249**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Biometric Authentication Model for Card-Based Transactions in Nigerian Banking Industry

O. O. Adeuyi*, M. A. Waheed

Department of Mechanical Engineering, College of Engineering, Federal University of Agriculture, Abeokuta, Ogun State, Nigeria.

Abstract With the advent of internet technology banks adopted experts system, this allows banks to provide real-time services to their customers. Electronic banking is the most widely used form of expert system in the banking industry; this has being abused by cybercriminals. This work identified the authentication challenges associated with the use of expert system in the bank; developed rule-based expert system software for card-based transaction using biometric authentication system; and validated the software. A three- factor-authentication method was used, a password, token (smart card) and biometric trait (fingerprint), which is an improvement on the existing two-factor-authentication method. The work showed that a properly designed and implemented multifactor authentication method is more reliable and serves as stronger fraud deterrents for card based transactions. It was observed that the users reluctantly accepted biometric authentication, due to religious, social or cultural beliefs. The result also showed a basis on which cardless Automated Teller Machine should be designed and constructed. It can then be concluded that a three- factor- authentication method reduces fraudulent transactions to the minimum.

Keywords Development, Enhanced, Expert System, Automated Teller Machine, Biometrics, Banking industry

Introduction

Expert systems are computer programs designed to model the knowledge and experience of human experts. This expertise is often the key ingredient used in solving difficult problems.

Generally, financial institutions employs expert system to get advice on question of regulatory compliance, providing cross-selling support, commercial and consumer lending systems, expert auditing, portfolio risk management systems and provide electronic banking services. The widely used form of expert system by financial institution in Nigeria is electronic banking which resulted from the blossoming of internet technology and has several benefits for the financial system [1].

Mish and Mello (1999) [2] described the main advantage of expert systems as the ability to permit an incredible leveraging of human expertise. They are readily cloned (copied) and they do not forget or misrepresent what they have been taught. Their primary function is to deliver knowledge that is relevant to the user's problem, in the context of the user's problem.

According to Krishnamoorthy and Rajeev (1996) [3] the most widely used form of expert system in the banking industry is electronic banking which has been abused by cybercriminals, who use fake websites to scoop money from their unsuspecting victims. Previously the threats were all passive such as password guessing, dumpster-diving and shoulder surfing. Now attackers use techniques such as phishing, trojan attack and man-in-the middle attack to steal victim's information which is used to carry out their nefarious activities [4].

Problems of Electronic Banking in Nigeria

Continuing technological innovation and competition among existing banking organisations and new entrants have allowed for a much wider array of banking products and services to become accessible and delivered to retail and wholesale customers through an electronic distribution channel collectively referred to as e-banking. However, the rapid development of e-banking capabilities carries risks as well as benefits [5].

At present, about 90 percent of the banks in the country offer different forms of electronic banking services like telephone banking, ATM and electronic fund transfer, but Internet banking is yet to take centre stage. This aspect of banking is still at the basic informative stage [6].

Part of the reasons identified for the inability of banks in Nigeria to take full advantage of this mode of banking includes lack of adequate operational infrastructure like telecommunication and power, upon which electronic banking generally relies, due to the inability of the banks to integrate their operations into the internet development process, Internet banking has not being fully incorporated in the existing banking structure in the country. The poor telecommunication infrastructure in the country poses a major challenge in the adoption of internet banking in Nigeria.

In addition, the fact that internet usage in the country has been abused by cybercriminals makes its window unattractive for domestic banking operations and legitimate international operations. The inherent fear associated with patronizing internet banking services in Nigeria is evidenced by the growing claim that fraudsters use fake websites to scoop funds from unsuspecting victims [6].

Security Incidents

The years 2003 and 2004 saw the emergence of fraudulent activities pertaining to internet banking or better known in the industry as "phishing". The modus operandi of this activity is to use spoofing techniques to gain names and passwords of account holders. The victims reported being deceived into going to a fake website where perpetrators stole their usernames and passwords and later use the information for the "perpetrators" own advantage. Phishing is an attempt to commit fraud via social engineering. The impact is the breach of information security through the compromise of confidence data. Banks have urged their customers to be extra vigilant following reports of fraudulent email purportedly sent by banks with internet banking service to their online customers [7-8].

The fraudulent activities mentioned above are not limited to the Nigerian banking industry. It is a worldwide problem particularly in the United States. There are 2560 new unique phishing sites reported to the anti phishing working group (APNG) [9].

Attack Techniques

Nowadays, the nature of attacks is more active rather than passive. Previously the threats were all passive such as password guessing, dumpster-diving and shoulder surfing. The techniques used by the attackers today include but may not be limited to:

- Trojan Attack -The attacker installed a Trojan such as key logger program, on a user's computer. This happens when users visited different certain websites and downloaded programs. As they are doing this, key logger program is also installed on their computer without their knowledge. When users log into their bank's website, the information keyed in during that session will be captured and sent to the attacker. Here the attacker uses the Trojan as an agent to piggy back information from the user's computer to his backyard and make any fraudulent transactions whenever he wants [7].
- Man-in-the-middle Attack - Here the attacker creates a fake website and catches the attention of users to that website. Normally, the attacker was able to trick the users by disguising their identity to make it appear that the message was coming from a trusted source. Once successful, instead of going to the designated website users do not actually realise that they actually go to the fraudster's website as displayed in Figure 1. The information keyed in during that session will be captured and the fraudsters can make their own transactions at the same time [9].

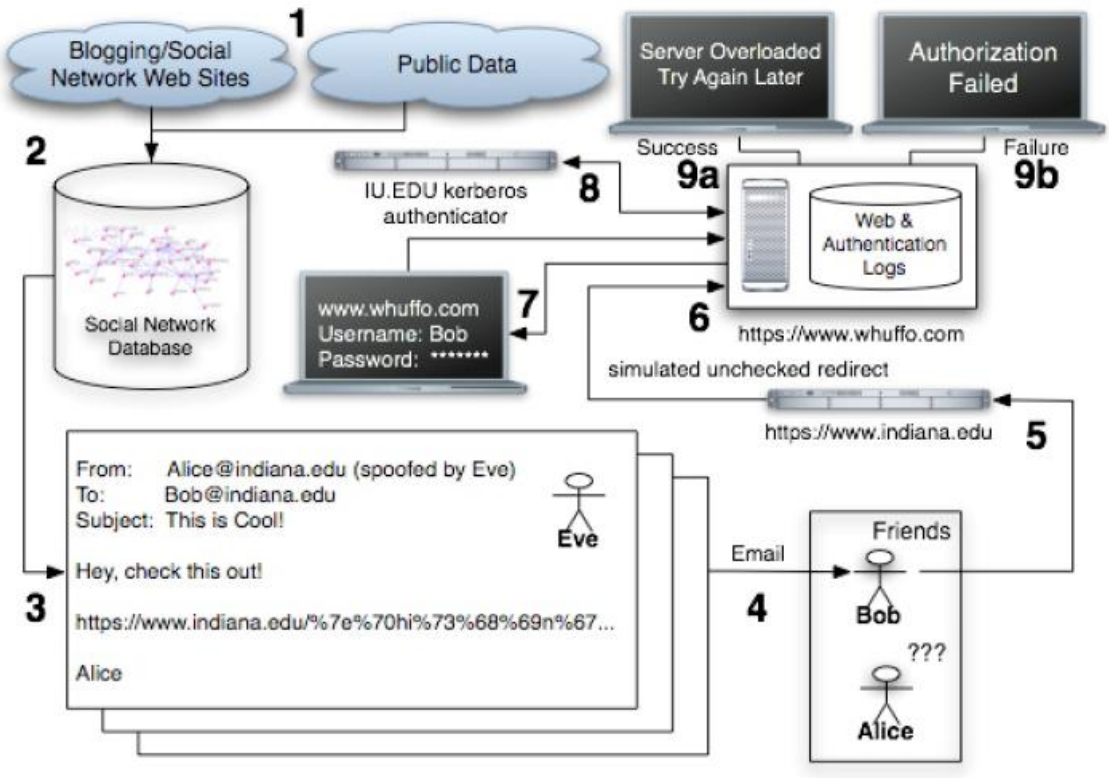


Figure 1: Phishing System [10]

Illustration of Phishing Experiment

1. Blogging, social network, and other public data is harvested.
2. Data is correlated and stored in a relational database.
3. Heuristics are used to craft "spoofed" email message by Eve "as Alice" to Bob (a friend).
4. Message is sent to Bob.
5. Bob follows the link contained within the email and is sent to an unchecked redirect.
6. Bob is sent to attacker whuffo.com site.
7. Bob is prompted for his University credentials.
8. Bob's credentials are verified with the University authenticator.
9. Bob is successfully phished or
10. Bob is not phished in this session; he could try again [10].

Methodology

Presently electronic Banking users only need a computer with access to the internet to use the services. Users can access their banking accounts from anywhere in the world with a login ID and a password to access the service.

However, the use of password does not provide adequate protection against internet fraud such as phishing. The problem with password is that when it is compromised, the fraudster can easily take full control of all transactions. In this case the password no longer works as an authentication because we can't be sure who is behind the keyboard typing that password in, hence the need to get stronger deterrent to this menace [7].

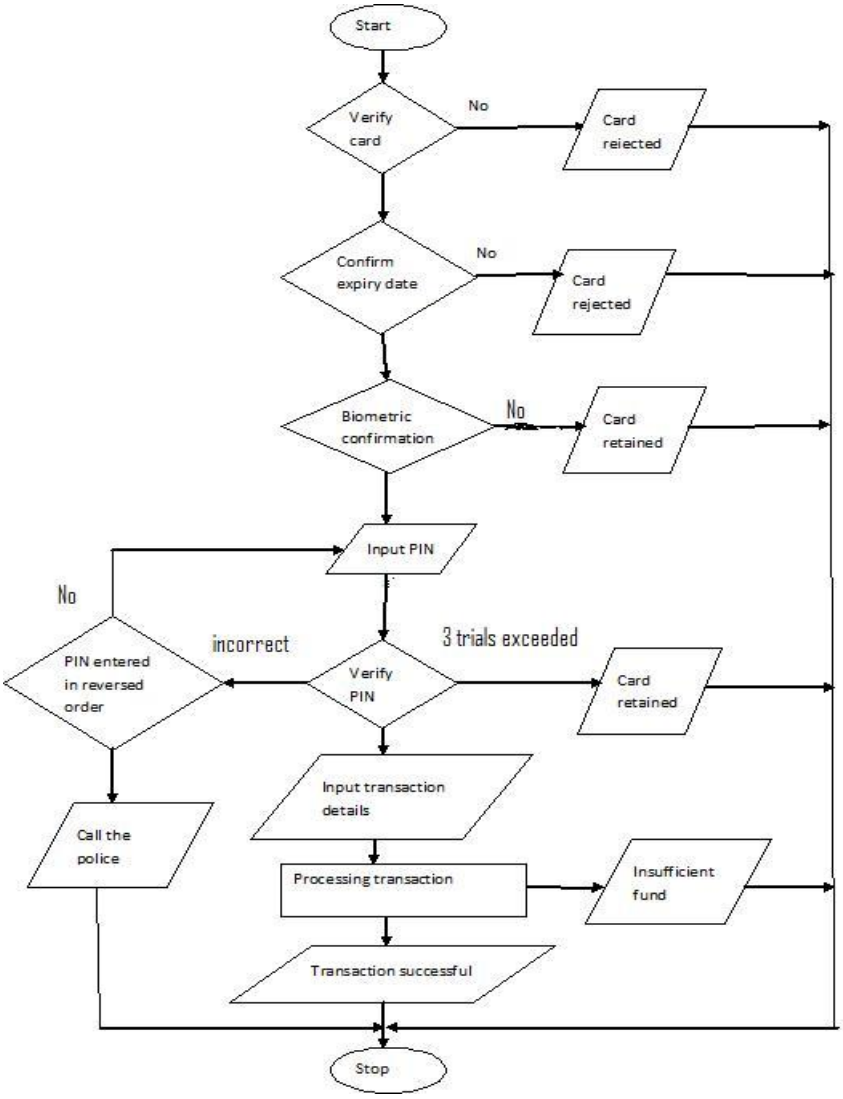


Figure 2: Flowchart for Card-based Transaction with Three Factor Authentication

Authentication Method

One Factor Authentication: This involves the use of only password as the authentication factor. This is not adequate to prevent fraud, as it has its own weakness. The essence of authentication is to restrict unauthorised access to a system [11]. The use of password method is the cheapest and simplest authentication method. But this makes the system more susceptible to attack, it is quite simple to obtain the data from the authorised user by extracting the information from the person itself using deceits, such as password guessing, dumpster-diving and shoulder surfing. Ones the password is compromised an unauthorised user can gain an unrestricted access to the platform.

Two-factor authentication: This involves the use of passwords and a second authentication factor such as the use of tokens (such as smart cards). The token smart card provides a second layer of authentication. The Smart Cards are very useful since they are combined with the use of password, and these cards also serve as storage system. Self-containment of smart card makes it resistant to attack as it does not need to depend upon external resources that are susceptible to attack. We believe that this is not excessively trustworthy, since it can be easily stolen, lost or simply forgotten at home [12].

Three - factor Authentication - for a better security, a three factor authentication process should be considered. The third authentication factor is the use of biometric such as iris, or thumb print recognition [13]. Biometrics traits are unique for each individual and it can identify the individual in spite of variations in the time. It is an

effective and safe method of authentication (is very difficult to falsify). The authentication method is the basis of the expert system software we built; this is implemented using .Net C# software tool.

The research was carried out for the sole purpose of designing a three factor authentication metrics, that is, a password to ascertain what one knows, a token (smart card) to ascertain what one has, and biometric recognition (fingerprint) to ascertain who one biologically is.

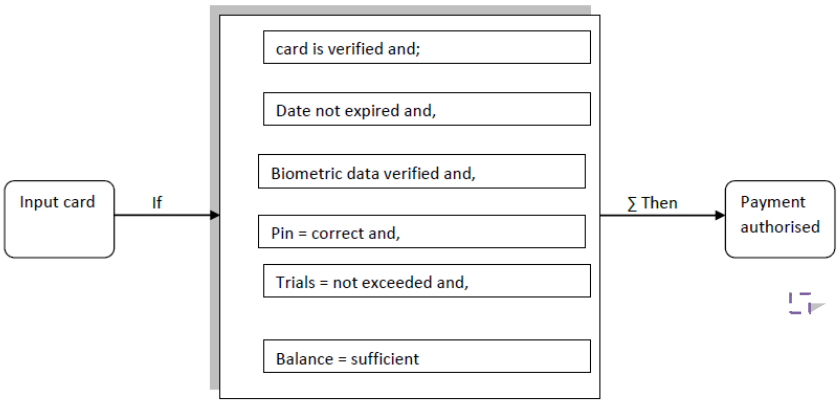
Figure 2 shows the flowchart of the model on which our expert system software was built, which was an improved card based transaction process flow. An additional authentication requirement (biometric identification) was employed here. Also it made provision for the system to automatically call the police when the PIN is entered in reverse order, which was for usage when card owner is under duress.

Results and Development

We developed a set of rules for card based transactions; this forms the knowledge base for the experts system.

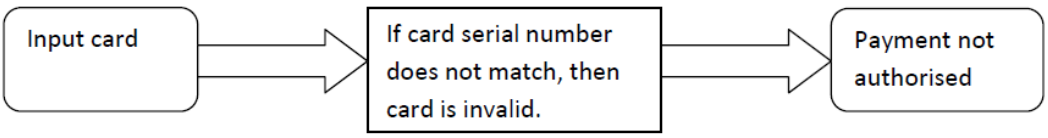
RULE I

IF Card = verified
and Date = not expired
and Fingerprint = matches
and PIN = correct
and Trials = not exceeded
and Balance = sufficient
and Limit = not exceeded
THEN Payment = authorized



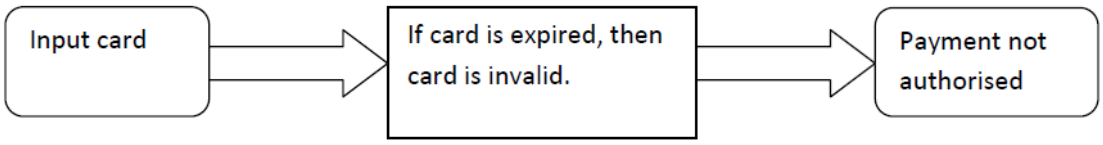
RULE 2

IF Card = not verified
THEN Payment = not authorised

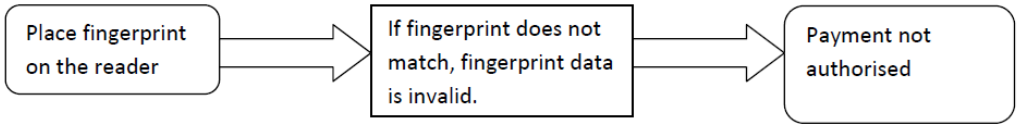


RULE 3

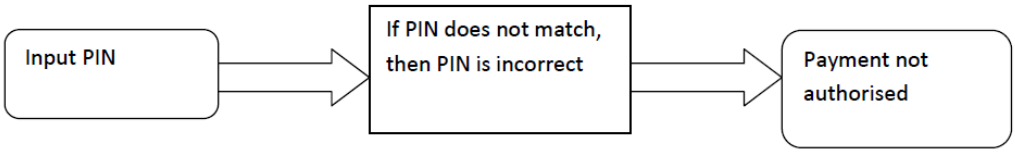
IF Date = expired
THEN Payment = not authorized



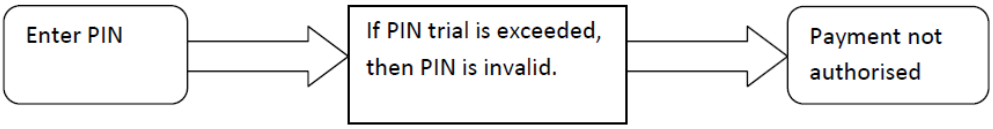
RULE 4
IF Fingerprint = does not match
THEN Payment = not authorised



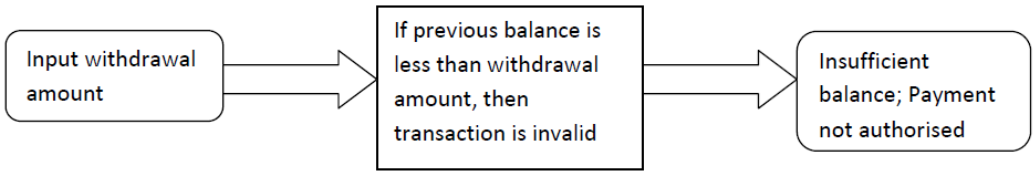
RULE 5
IF PIN = incorrect
THEN Payment = not authorised



RULE 6
IF Trials = exceeded
THEN Payment = not authorised



RULE 7
IF Balance = insufficient
THEN Payment = not authorised



The customer/cardholder is expected to know and remember his/her PIN number and to have previously enrolled his/her fingerprint into the fingerprint device/reader adapter into the system. After which the fingerprint database compares the live sample provided by the customer with the template in the database.

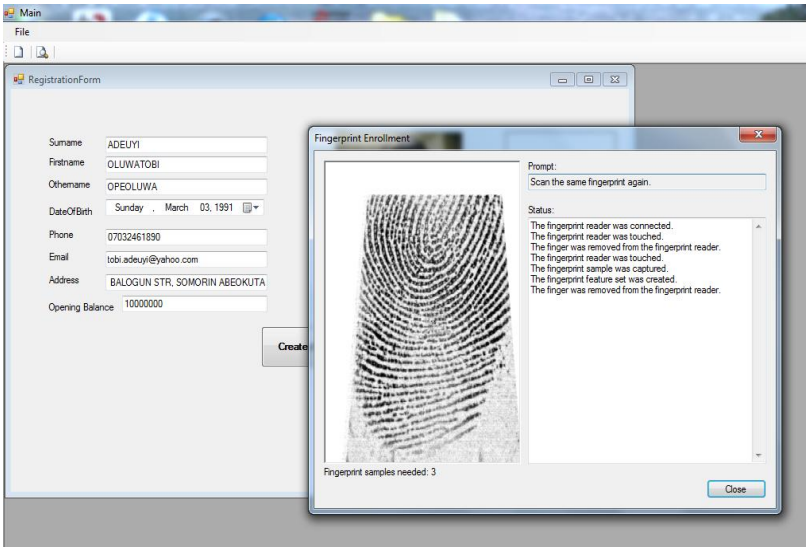


Figure 3: Fingerprint Enrollment

Fingerprint Enrollment/Verification Process

At earlier stage users are required to enrol their fingerprint on a scanner as shown in Figure 3, this fingerprint image is converted to binary codes and transmitted to the bank server via secured channel. In the Figure 3, the system prompts the user to enrol his/her fingerprint, which is converted to binary codes and serves as part of the knowledge base of our experts system.

Also after the finger print enrolment, the photograph of the user is also taken and stored as shown in Figure 4, in addition with other details of the user, in the bank's database.

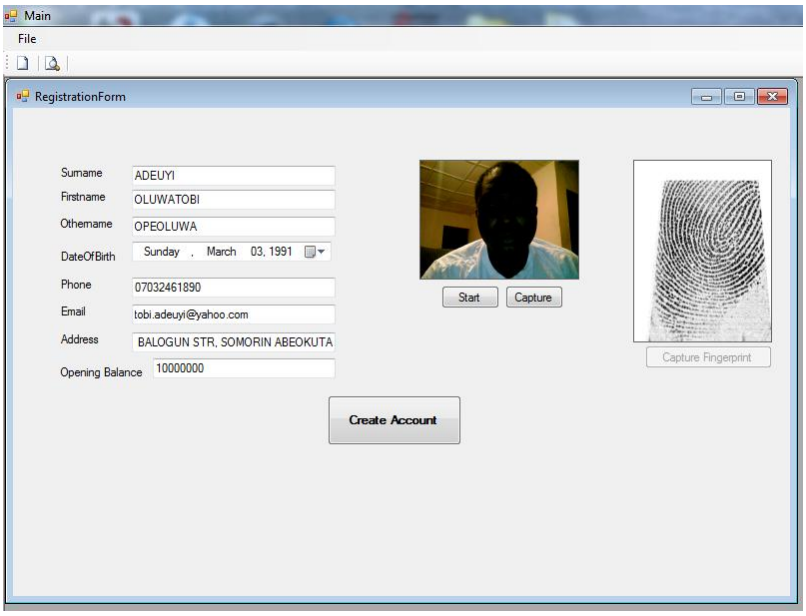


Figure 4: Data capturing screen

Graphic User Interface Design

The interface allows the user to interact with the expert system. The user input their enquiries into the system through the interface, the system processes the enquiries based on the information stored in the knowledge base and the rules in the inference engine to draw conclusion and give advice. The system advises users and gives explanation for any action taken, through this interface

This interface can be broken down into two stages: authentication/verification interface and Banking transaction interface.

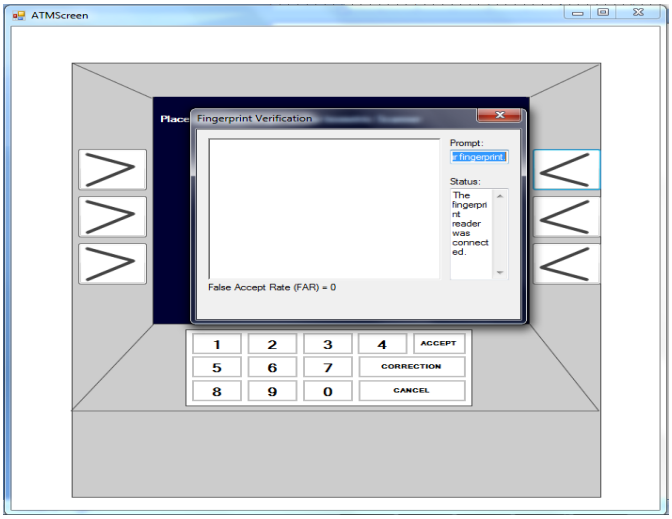


Figure 5: Fingerprint verification

Authentication/Verification Interface

This interface prompts the customer to insert ATM card (by inputting the card serial number) the machine verifies the validity of the card. If the card is valid the system prompts the user to verify his/her fingerprint else it will reject the card giving the user an 'invalid card' error message as shown in Figure 5.

It proceeds further with the entire authentication processes, by verifying that the fingerprint matches with the one earlier enrolled for the card in the banks database. If it matches the system continues with the verification process by asking the user to enter his/her PIN, else it terminates the transaction process.

After validating the user's fingerprint, the system prompts the user to enter his/her PIN. If the user enters an invalid PIN, the system gives a prompt for an invalid PIN and asks the user to enter a valid PIN, stating the number of chances/trials the user has left. The system is configured such that it retained the card after three trials of inputting an invalid PIN number.

However, if the user enters the PIN number in the reverse order as shown in Figure 6, the system will automatically make an emergency call to the nearest police station. This feature is included in the process flow so that users can make use of it when under duress at the ATM point.

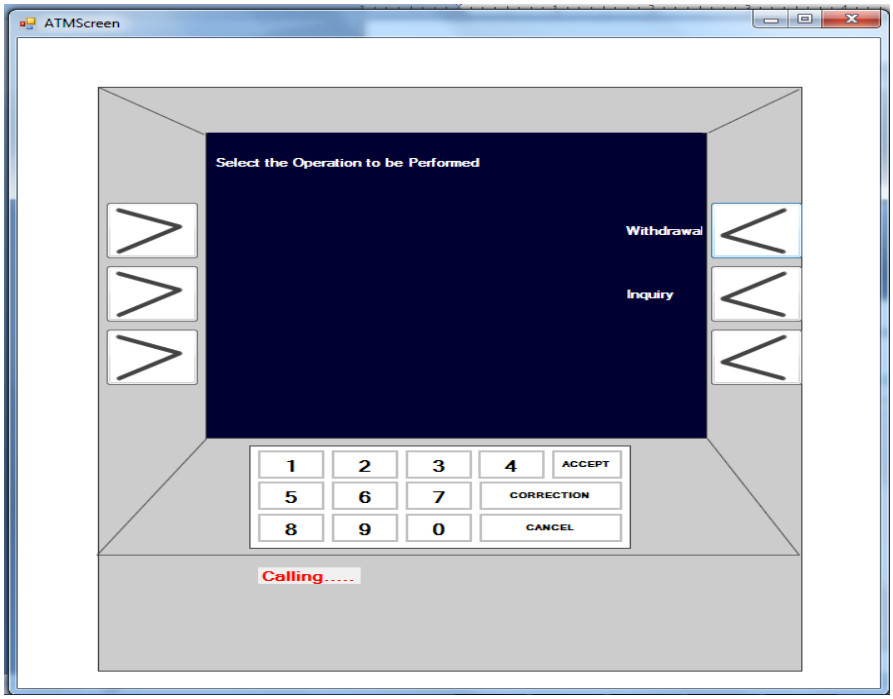


Figure 6: PIN Entered in Reverse Order

The next stage is the transaction phase.

The customer is taken to the transaction phase where he/she will select which transaction he wants to carry out. After inserting a valid card, enrolling a valid fingerprint and PIN number, the user can access transactions. We focused on withdrawal and inquiry Interface, This interface allows the user to check his/her previous balance and also withdraw money from his/her account.

For withdrawals the system compares the withdrawal amount inputted by the user with his/her previous balance. If previous balance is greater than withdrawal amount then, the transaction goes on successfully, else the system notifies the user that he/she has insufficient fund.

Conclusion

This work identified the authentication challenges associated with the adoption of electronic banking and proffered solution by developing a rule-based expert system software that employs biometric authentication method. This is aimed at making the electronic banking platform more secured.

This work developed an improved model for the existing ATM transactions process flow and also tested the validity the model developed.

Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents.

To make the electronic banking platform more secured, we came up with expert system software that makes use of a three factor authentication process. The third authentication factor is the use of biometrics; this ascertains who one is biologically. With this a more secure method was implemented- a password to ascertain what one knows, a token (smart card) to ascertain what one has, and biometric recognition (for example fingerprint or thumbprint) to ascertain who one biologically is. With this, if passwords have been compromised, fraudsters need to get through another two levels of authentication to access a customer's account. This would be difficult if not totally impossible.

In the course of this work we discovered that expert system is to a large extent still underutilised in Nigerian financial industries. To this end we want to recommend that a prototype machine that works on this three-factor authentication expert system model that we came up with in this work should be deployed. This model has been found promising on account of its multifactor authentication methods and if deployed, it will be a deterrent to fraudulent activities. It can then be concluded that a three- factor- authentication method reduces fraudulent to the barest.

References

[1]. Enrique, C., José, M.G. and Ali, S.H. 1997. Expert Systems and Probabilistic Network Models, pp 1-15.

[2]. Mish, K.D. and Mello, J. 1999. Computer-Aided Engineering. Mechanical Engineering Handbook, pp 1-80.

[3]. Krishnamoorthy, C.S. and Rajeev, S. 1996. Artificial Intelligence and Expert Systems for Engineers. CRC press.

[4]. Adejuyigbe, S.B. 2010. Manufacturing and Computer Aided Engineering: A Panacea for Wealth Creation, 2010. 27th Inaugural Lecture of Federal University of Agriculture, Abeokuta

[5]. Hedberg, A. and Taylor, N. 2001. Net Banking Must Do Better. Marketing Week (23:50):36–37.

[6]. Ovia, J. 2001. Internet Banking: Practices and Potentials in Nigeria.

[7]. Ekundayo, E. 2009. Capacity Constraints in Developing Countries: a need for more E-Learning Space? The case of Nigeria, Proceedings Ascilite Auckland, pp243.

[8]. Daniel, E. 1999. Provision of Electronic Banking in the UK and the Republic of Ireland. International journal of Bank Marketing, 17(2):72-82.

[9]. Oriola, M. 2004. Advance Fee Fraud on the Internet: Nigeria's Regulatory Response, Computer Law and Security Report, 21(3): 237.

[10]. Jagatic, T., Johnson, N., Jakobsson, M. and Menczer, F. 2005. Social Phishing

[11]. Raja, J. 2008. E-payments: Problems and Prospects Journal of Internet Banking and Commerce, 13(1):10-12.

[12]. Stafford, B. 2001. Risk Management and Internet Banking: What Every Banker Needs to Know. Community Banker (10:2):48–49.

[13]. Nath, R., Schrick, P. and Parzinger, M. 2001. Bankers' Perspectives on Internet Banking. E-Service Journal, 1(1):21-36