International Journal of Emerging Technology and Advanced Engineering

A Hybrid Authentication Mechanism for Preventing Phishing Attacks on E-banking Systems: The Nigeria Case Study

G. B Oggunniye¹, O. M Afolabi²

¹Department of Computer Science, Adekunle Ajasin University, PMB 001, Akungba Akoko, Ondo State, Nigeria
²IT Department, Resourcery Plc, 18, Adeola Hopewell Street, Victoria Island, Lagos, Nigeria

Abstract—This paper presents multifactor authentication method for securing access to e-banking systems in Nigeria using fingerprint recognition and SiteKey authentication. Fingerprint authentication is based on the notion of fingerprint individuality; the idea that fingerprint image of an individual is unique and can be used to uniquely identify him/her. SiteKey authentication on the other hand, uses a unique image chosen by customers to help banks recognise their genuine customers and to help customers recognise the genuine website of their bank through its authentication process. Verifying e-banking systems users’ identity claims by combining these two authentication methods will be a promising solution to the problems of phishing attacks and identity theft facing e-banking systems implementation in Nigeria. Phishing attack and identity theft are the major threats to the success of the newly introduced cashless economy policy in Nigeria. Traditional password-based authentication used in the past seems insufficient hence the need for improved authentication methods. This paper contributes to the state-of-art knowledge of fingerprint recognition and SiteKey authentication by improving the understanding of the technologies and by demonstrating how the technologies can be used in e-banking environment.

Keywords—e-banking systems, phishing attacks, authentication systems, sitekey authentication, biometrics.

I. INTRODUCTION

The continuous advances in the information technology have significantly impacted banking operations and services across the globe. Today, financial institutions rely greatly on information technology infrastructure for financial services such as e-money, e-brokering, e-insurance, e-finance, e-exchange and e-banking among others. In particular, E-banking is known as the automated delivery of new and traditional banking product and services directly to customer through electronic interactive communication channels also referred to as online or internet banking [6].

Today in Nigeria, banks are investing greatly in information technology to provide various e-banking solutions with a view of satisfying the growing needs and demands of their customers as well as competing effectively in the competitive and dynamic international e-commerce market [7]. However, one of the key hurdles of e-banking systems in Nigeria is identity theft through spam/phishing attacks and hacking among others. This has adversely affected the growth of e-banking services in the country.

The Nigerian Advance Fee Scam (popularly known as 419), e-banking phishing attacks, and other financial crimes among others are the major limiting factors to the adoption and wider patronage of the newly-introduced e-banking solutions by Nigerian banks. These e-banking solutions are introduced in compliance to new Central Bank of Nigeria banking reforms and regulations towards cashless economy. Survey reveals that reasonable number of e-banking subscribers in Nigeria are susceptible to phishing attacks and identity theft among others and hence the need for reliable and secured authentication mechanism. Traditional authentication techniques involving the use of PIN and Username/Password that are used for authenticating users into these systems have its shortcomings. Several studies have revealed that it is not sufficient for securing e-banking systems [28].

The idea of using fingerprint authentication is based on the notion of fingerprint individuality and the fact that fingerprint authentication has the lowest False Acceptance Rate (FAR) and False Rejection Rate (FRR) among other biometric authentication techniques [19]. SiteKey authenticating on the other hand, has been used by in the USA by the Bank of America [30]. Verifying e-banking systems users’ identity claims by combining these two authentication methods will be a promising solution to the problems of phishing attacks and identity theft facing e-banking systems implementation in Nigeria.
II. LITERATURE REVIEW

A. Brief Overview of E-banking Systems

According to Oxford dictionaries (2012), “e-banking is a method of banking in which the customers conducts transactions electronically via the internet”. E-banking system architectures vary in various banking institutions where it is used depending on a number of factors including the e-banking objectives of the bank; scope, activities, equipments and the security requirements of the e-banking systems. E-banking systems are implemented and managed either internally by the concerned banking institution or outsourced to a verified third party.

The use of information and communication technology (ICT) in the financial institution has made available various types of e-banking technology including Automated Teller Machine, personal internet banking, debit or credit card system, direct payment (also known as electronic bill payment), electronic check conversion, electronic fund transfer, mobile banking, preauthorised debit (or automatic bill payment), prepaid card, smart card, stored value-card, payroll cards and direct deposit among others [24].

E-banking systems allow bank customers to access various banking services such as balance reporting, inter-account transfers, bill-payment etc., via a telecommunication network and without leaving the comfort of their homes or organisation [4]; [3]. Its importance is growing because of its wider reach and lower cost per transaction [4].

Kurnia et al (2010) argued that there is a vast disparity in the adoption and diffusion of e-banking among different countries of the world, especially between the developed countries and developing countries of the world. Their study revealed that while developing countries are just starting to adopt the concept of e-banking, developed countries have benefitted immensely from the use of e-banking solutions and applications.

A number of factors affecting the implementation and management of e-banking systems from the customers and banking service providers includes: employee resistance, security issues, regulatory issues, project management issues, IT and telecommunication issues, availability and system integration issues, trust issues, organisational structure and resistance, acceptance issues, service delivery channels issues, ethical issues, change management issues among others [11].

Attacks on e-banking services threaten bank customers, their personal data and finances and as well as customers, these attacks also threaten banks reputation and trustworthiness [18].

In Nigeria, in spite of the numerous advantages e-banking systems offer, this study reveals that its patronage by Nigerian bank customers is still limited. This is due to the poor level of access to internet infrastructure and more importantly security challenges of these systems. As an exploratory qualitative research, this paper aims at increasing the users’ awareness of the risks of phishing attacks on e-banking systems in Nigeria and to propose the combination of SiteKey authentication and fingerprint recognition as multifactor authentication mechanism for preventing phishing attacks. Fingerprint authentication has been used in Nigeria for commercial applications such as Automated Teller Machine (ATM), E-voter registration among others. Its general acceptability in Nigeria makes it a favourable biometric technology that will attract widest patronage among other biometric technologies [25].

B. Concept of Trust in E-Banking Systems

Trust and security are the key hurdles to the growth of e-banking systems. Trust in particular, is enablers that will make any e-banking consumers undertake any risky operation such as the use of personal internet banking details on a particular e-banking website. In view of this, e-banking service providers focus on the provision of security and building of trust towards making their respective e-banking solutions reliable and acceptable. Trust and commercial activities dates back to the ancient times where commercial activities and exchanges between two parties is based on trust.

French et al (2007) referred to the concept of trust in e-banking as the technologies employed such as trusted protocols, public key cryptography and information architectures to engender trust on the e-banking website. Their study revealed that tangible trust factors include such factors as security policy and trust seals while intangible trust factors entails psychological studies, formal mathematical and cognitive models of trust as well as emotional response to computer based stimuli. These trust factors are grouped into different categories of criteria as shown in the table below:
TABLE I
CATEGORIES OF CRITERIA FOR E-BANKING TRUST FACTORS

<table>
<thead>
<tr>
<th>Categories of criteria</th>
<th>Referenced phenomena</th>
</tr>
</thead>
<tbody>
<tr>
<td>External trust seals/third</td>
<td>Verisign, Padlocks, ‘best Internet bank’ award</td>
</tr>
<tr>
<td>Party accreditation</td>
<td></td>
</tr>
<tr>
<td>Internal regulatory seals</td>
<td>Security information, privacy policy, legal policy, branding, banking codes, guarantees, policy on liability</td>
</tr>
<tr>
<td>Task-related content</td>
<td>Interest rates, offers, products and promotions, adverts, support features for tasks</td>
</tr>
<tr>
<td>Design Aspects</td>
<td>Graphic style, use of colour, navigation support, page layout, text style, overall impression of appearance</td>
</tr>
<tr>
<td>Other</td>
<td>Online only or high street presence, contact information, trustworthiness, customer service facilities, planned maintenance information</td>
</tr>
</tbody>
</table>


Several studies (as cited in [17]) have shown that online trusts are also influenced by factors such as the site’s navigational model, style, aesthetics and branding.

Furthermore, to enhance trust in the use of e-banking, e-commerce and e-banking systems among others, Trusted Third Party is of relevance. Trusted Third Party is an independent body that engenders trust through attestation and certification.

C. Variants of Phishing Attacks

Phishing attack involves the process of sending fraudulent emails or fraudulently enticing people to visit a phishing website by fraudsters or hackers with the sole aim of acquiring their identity information illegally.

Phishing attacks may also take the form of user receiving a fraudulent link (url) that directs him/her to a fraudulent websites where he/she will be provided with a customer service number to call. Upon calling the number, the user is requested to enter his/her username or password. The information are then used to impersonate victims in any e-banking or e-banking system in order to withdraw money from their account illegally, obtain loans with their identity or commit any form of financial crime [1].

Gartner Group (as cited in [8] ) revealed that 57 million US consumers have received a phishing email in 2006. 2 million users accessing their accounts online have been attacked with an estimated $2.4 billion in fraud. Similarly, between April 2006 to 2007, Anti Phishing Working Group (APWG) in 2007 (as cited in [8] ) revealed that over 316,736 various phishing attacks are reported. Phishing attacks and identity theft are sometimes used interchangeably but in reality there are some distinctions between the two. Identity theft is a form of fraud where criminals use another person’s personal details to open bank accounts and get credit cards, loans, state benefits and documents such as passports and driving license etc.

Dhamija et al (2006 ) carried out a research on why phishing attacks works and reported that:

- Good phishing websites fooled 90% of participants in their study
- 23% of participants in their study did not look at the security indicators of websites
- Popup warnings and fraudulent certificates are ineffective
- Participants are vulnerable across board to Phishing attacks

Basically, predicting or detecting phishing websites has to do with the authentication mechanism and anti-phishing techniques put place between the users and servers. Therefore, anti-phishing measures employed by any service provider must be strong enough to sufficiently guarantee their customers of the security and safety of their personal details.
Phishing attacks come from numerous vectors some of which are:

- Deceptive attacks (spear phishing), in which internet users are tricked into giving out their personal information through deceptive messages [8].
- Domain-based attacks (pharming style), in which the lookup of host names is altered to direct users to a malicious server [8].
- Malicious code-based or Trojan-based attacks, in which malicious codes or softwares are used for data compromises [8].

Some of the popular phishing attacks used nowadays are as discussed below:

- **Spear Phishing**
  This type of phishing is usually directed towards a single user or department within an organisation. It usually appears to come from a trusted party, requesting the user or the department to update their username and passwords. This information is then later used by hackers to gain access into a secured network [8].

- **Search Engine Phishing**
  In this type of phishing attack, phishers get their phishing websites indexed by search engines and trick users into entering their personal information as part of sign up, order and fund transfer process. The phishing websites are usually designed for fake products and services.

- **Key loggers**
  Key loggers are spyware programs that install themselves into a web browser or as a device driver. They are developed to extract user input events and activities and transfer them to phishing server [8].

- **Content Embedded Phishing**
  This phishing attack involves inserting malicious links or contents into a genuine website. The malicious link are used to redirect users to malicious websites, install malware on the user computer or insert another frame of content that will redirect the user to a phishing server. [8].

- **Session Hijackers**
  Session hijacking is used to monitor internet user activities usually by a malicious browser component. Malicious software is used to hijack user transaction session to perform malicious actions after the user has entered his personal information [8].

**D. E-banking Phishing Attacks in Nigeria**

As part of the Central Bank of Nigeria regulations on e-banking products and services in Nigeria, only the banks which are fully licensed, supervised and physically present in Nigeria are permitted to offer electronic banking products and services to Nigerians [10]. However, hackers are still using fake websites representing those banks to carry out fraudulent activities.

Crime and corruption with 75% and 71% respectively are the major key hurdles to the economic and business activities in Nigeria. Identity theft and fraud are the most popular crimes in the country after burglary [29]; [15]; [16]. Basically, identity theft is carried out through phishing attacks. Wada and Odulaja (2012) carried out a study on the types of cyber crimes that have economic impact either directly or indirectly on the financial system of a nation. Some of the cyber crimes identified include: phishing attacks, cyber terrorism, electronic spam mails, cyber-stalking and fake copy-cat websites [29]; [22]. Their study revealed that the most recent phishing attacks in Nigeria were on the customers of Inter-switch. Inter-switch is an electronic switching and payment company in the Nigeria Studies revealed that the company has 9 million ATM cards of about 23 banks in Nigeria connected to its network [2].

Nigeria Deposit and Insurance Corporation (NDIC, 2007) reported that attempted fraud cases from the underhand deals of bank staff among others totalled ₦10.1 billion (Over 65 million USD) and actual losses of ₦2.76 billion (13 million USD). In the same vein, banks like the United Bank of Africa Nigeria Plc and Guaranty Trust bank Plc customers witnessed phishing attacks in 2009 [14].
Like every other countries of the world, phishing attacks remain one of the popular cyber crimes that pose serious security threats to e-banking/e-banking systems in Nigeria. In this regard, Onwubiko (2010) suggested that adequate protection should be made available to the ICT systems and network in Nigerian banks and government system.

The implication of the cash-less economy policy recently introduced by the Central bank of Nigeria is that most financial transactions in the country will be carried out online. Consequently, this is likely going to attract more phishing attacks on the e-banking solutions in the country.

First Bank of Nigeria plc, one of the commercial banks in Nigeria, has introduced biometric based ATM machines with a view of engendering trust and confidence in the use of their e-banking services. However, it can be pointed out that the use of biometric measures in e-banking systems in Nigeria has been restricted to ATM machines. Much work has not been done in the area of using biometric authentication for the other forms of e-banking systems in the country like direct debit, personal internet banking and point of sale (POS) services among others.

With the rapid increase in the introduction and use of various forms of e-banking solutions in the country as a result of the recent banking reforms and regulations, more work is expected to be done on securing e-banking systems in Nigeria. Biometric authentication as pointed out in this work will be of maximum relevance in that regard. This study is an effort towards suggesting multifactor authentication system for fighting phishing attacks and other related cyber crimes in Nigeria.

E. Overview of Fingerprint Recognition Systems

Fingerprint authentication technique uses the ridge and furrow patterns of the finger tip to carry out authentication of people into any application that involve personal authentication [20]. Fingerprint is a physiological characteristic of humans that can be used to uniquely identify them. The use of fingerprint authentication technology is based on the notion of fingerprint individuality. Fingerprint individuality refers to the extent of the uniqueness of fingerprint image in a target population [12].

Fingerprint authentication has the widest acceptability and popularity among the various forms of biometric authentication technologies because of its ease of use, ease of acquisition and its longest history among other forms of biometric authentication. Moreover, Itakura and Tsujii (2005) in their work, presented fingerprint authentication to have the lowest False Acceptance Rate and False Rejection Rate among different types of biometric authentication technologies.

In the early years of fingerprint technology, fingerprint images are imprinted on a paper and then converted to machine-readable image for authentication. With the improvement in sensing technology, various live scanners are used to extract fingerprint image and used for authentication.

F. Overview of SiteKey Authentication Techniques

SiteKey authentication technique was introduced in 2006 by Bank of America as part of their anti-spoofing and anti-phishing program [9]. It was introduced to tackle phishing attacks by establishing the authenticity of protected web sites and the web sites users. It was designed to prevent unauthorised access to a web site even in the case of identity theft by asking the web site user questions with difficult-to-guess answers [30].

Site Key provides secured authentication in two ways:
- It helps the bank to identify genuine owner of an account; the bank display the customer’s SiteKey after recognising the device the customer is logging in from [9].
- It helps customers to identify the genuine web site of their bank; when the customer sees his/her SiteKey, he/she can be sure he/she is on the valid online banking website of their bank [9].

The SiteKey consists of three main components:
- A unique image chosen by the customer
- The image title accompanying the SiteKey image
- Three challenging questions only the customer can answer in case the customer is signing in from another computer different from the one pre-registered with the bank [9].

III. Method and Materials

This research work proposed multifactor authentication including fingerprint authentication and SiteKey authentication system for tackling the problem of phishing attacks on E-banking systems in Nigeria. In view of this, the following methodology was adopted:

A. Research Methodology

This research work involves the literature review of related works on phishing attacks, fingerprint recognition and Sitekey authentication. A prototype authentication system was also developed to secure access into e-banking system (see sample in figure IIa and IIb) and the activity diagram of the proposed hybrid authentication system for e-banking systems was also presented (see sample in figure III)
Therefore, a mixed-method approach was used to carry out the research work as outlined below:

- Literature review – qualitative
- Data collection and analysis through market research and consultation – quantitative
- Development of a prototype authentication system – Waterfall Software Life Cycle Model

B. System Components

Fingerprint authentication system is developed in this work to secure the authentication of users into their personal internet banking environment. The system is required to have the fingerprint enrollment and fingerprint verification phase. At the enrollment phase, the fingerprint image of the user is captured using fingerprint scanner and it is stored in the application database as the fingerprint template. At the verification phase, fingerprint image in enrolled for verification and it is compared with the preregistered fingerprint template using fingerprint verification algorithm. In case of fingerprint matching, access is granted into the user personal internet banking page otherwise access is denied.

The artefact is developed to accept both the user fingerprint image and personal internet banking PIN for authentication. The proposed system if implemented will help tackle the problem of identity theft from phishing attack by allowing only the legitimate users of an e-banking system to gain access to his/her e-banking account using a trait unique to him/her. Fingerprint authentication was chosen because of its effectiveness in all other applications that involve personal authentication and because of its strength and advantage over other traditional method of authentication. On the other hand, SiteKey authentication works by allowing users to choose their own custom image during the registration process for internet banking. This personalised image comes up each time a user log in with his/her username and password on e-banking website.
IV. CONCLUSION

This paper has discussed the problems of phishing attacks and identity theft affecting e-banking systems in Nigeria. In addition, the paper has proposed the combination fingerprint recognition and SiteKey authentication for securing e-banking system in Nigeria. This paper is novel in that it proposes the combination of fingerprint recognition and SiteKey authentication for preventing e-banking systems in Nigeria against phishing attacks. Nigeria is chosen as the case study because of the new policy of her government to move the country from cash-based economy to cash-less economy and the consequent need of securing e-payment solutions to support the policy.

REFERENCES


