Mitigating Cyber Identity Fraud using Advanced Multi Anti-Phishing Technique

Yusuf Simon Enoch
Department of Mathematics and Computer Science
Federal University, Kashere
Gombe, Nigeria

Adebayo Kolawole John
Department of Computer Science
Oduduwa University, Ipetumodu
Ile-Ife, Nigeria

Adetula Emmanuel Olumuyiwa
Department of Computer Science
University of Ibadan, Ibadan
Nigeria

***Abstract*—Developing Countries are gradually transiting from cash to an electronic based economy by virtue of cashless policy implementation. With this development, cyber criminals and hackers who hitherto attacked businesses and individuals across the Atlantic now see this development as a new venture for their criminal acts and are thus re-directing their energies towards exploiting possible loopholes in the electronic payment system in order to perpetuate fraud. In this paper, we proposed an enhanced approach to detecting phishing attempts and preventing unauthorized online banking withdrawal and transfer. We employed the use of Semantics Content Analysis, Earth Mover Distance and Biometric Authentication with finger print to construct a model. We demonstrated the efficacy of the implemented model with the experiments conducted, a good and considerable result was achieved.**

***Keywords*—Security; authentication; attack; Cybercrime; Identify theft**

I. INTRODUCTION

The ubiquitous nature and fast pace of the internet growth has aided the number of criminal exploits on the cyberspace. Criminals targeting user information are able to profit from the increased adoption of online services for many day-to-day activities, including banking, shopping, and leisure activities. Today, the Internet is used for espionage and as a medium to commit terrorism and global crimes.

Cybercrime refer to misconducts in the cyber space as well as wrongful use of the internet for criminal purposes. Various categories of these crimes include cyber stalking, phishing (identity theft), virus attacks, malware attack, the use of anonymous proxies to masquerade and sniff information and the popular electronic spam mail problem [16].

The days of dramatic bank heists have been over for years, ambitious criminals are globally embracing cybercrime and other fraudulent cyber activities; this is partly due to the wide availability of automated software tools, mostly intelligently driven being employed by these cyber-criminals. This makes them almost deceptive to detection and poses a hard problem combating crime on the cyber space. As a matter of fact, the newest cyber grenades have fully automated capabilities that eliminate the need for hackers to manually transfer funds from one account to another.

This allows the criminals to stay much more hidden than in the past. Hackers also now use entire servers that are customized to target individual banks and other victims; unfortunately, most users being attacked don't even suspect that their account has been compromised until long after their money has disappeared [13].

Several approaches exist to deceiving unsuspecting users. These include the offer to fill out a survey for an online banking site with a monetary reward if the user includes account information, and email messages claiming to be from a reward clubs, asking users to verify credit card information that a customer may store on the legitimate site for reservation purposes.

Often included in the message is a URL for the victim to use, which then directs the user to a site to enter their personal information. This site is crafted to closely mimic the look and feel of the legitimate site. The information is then collected and used by the criminals. Over time, these fake emails and web sites have evolved to become more technically deceiving to casual investigation.

II. CONSEQUENCES AND TREND OF CYBERCRIME

According to Internet Crime Complaint Centre Report, cybercrime cost a total loss of $485,253,871 in the year 2011. On the other hand, the Economic and Financial Crimes Commission Report [7][8] ranks Nigeria as third among the top ten sources of cyber-crime in the world. It is estimated that after the United States with 65 per cent of cyber-criminal activities and the United Kingdom with 9.9 per cent, Nigeria is the next hub of cyber criminals in the world with 8 percent.

The growth of online banking further presents enhanced opportunities for perpetrators of cyber-crime. Funds can be embezzled using wire transfer or account takeover. Criminals may submit fraudulent online applications for bank loans; disrupt e-commerce by engaging in denial of service attacks, and by compromising online banking payment systems [2][27].

Identity takeover can also affect online banking, as new accounts can be taken over by identity thieves, thus raising concerns regarding the safety and soundness of financial institutions [27].

TABLE I. TOP 10 COUNTRIES - PERPETRATOR OF CYBERCRIME

Year 2008		Year 2009		Year 2010		Year 2011	
United States	66.1 %	United States	65.4 %	United States	65.9 %	United States	90.99 %
United Kingdom	10.5 %	United Kingdom	9.9%	United Kingdom	10.4 %	Canada	1.44 %
Nigeria	7.5%	Nigeria	8.0%	Nigeria	5.8%	United Kingdom	0.97 %
Canada	3.1%	Canada	2.6%	China	3.1%	Australia	0.66 %
China	1.6%	Malaysia	0.7%	Canada	2.4%	India	0.50 %
South Africa	0.7%	Ghana	0.7%	Malaysia	0.8%	Puerto Rico	0.22 %
Ghana	0.6%	South Africa	0.7%	Spain	0.8%	South Africa	0.22 %
Spain	0.6%	Spain	0.7%	Ghana	0.7%	France	0.19 %
Italy	0.5%	Cameroon	0.6%	Cameroon	0.6%	Germany	0.19 %
Romania	0.5%	Australia	0.5%	Australia	0.5%	Russian Federation	0.17 %

Source: Internet Crime Complaint Centre Report [29].

In the USA, online fraud has overtaken viruses as the greatest source of financial loss [26]. Among on-line fraud threats, phishing represents a major threat for financial institutions and according to the Anti-Phishing group organization, 93.8% of all phishing attacks in 2007 are targeted at financial institutions. Also a recent study indicates that phishing attacks in the USA alone soared in 2007 to 3.6 Million victims for a total reported customer loss of USD 3.2 Billion. During 2011, FBI-related scams were the most reported offense with 35, 764 complain with claim of dollars losses, followed by identity theft with 28, 915 then advance fee fraud with 27, 892 [29].

III. RELATED WORK

A wide range of phishing detection techniques have been proposed and deployed. One of the most used techniques seems to be blacklisting. Most of the anti-phishing applications available, including those built into mainstream web browsers, use blacklists for detecting phishing sites.

Some other widely available phishing detection techniques include whitelisting [4] and heuristics [6][12]. The disadvantage of the blacklisting approach is that non blacklisted phishing sites are not recognized. The approaches are only effective as the quality of the lists.

In contrast, whitelists manage a list of known-good websites. Whitelists are generally divided into global lists updated by central servers and personalized lists managed by the end users as needed. Due to its inherent usability issues, whitelists are currently used only in the preprocessing step, i.e. before the heuristics are checked, to reduce false positives. Kirda and Krugel [14] have developed a browser extension called AntiPhish to maintain trusted websites' domain names and credentials.

Some of the well-known Anti-phishing tools are PWDHASH [3] and SpoofGuard [20]. PWDHASH create domain specific passwords that are been rendered useless if submitted to another domain [5] .SpoofGuard in contrast looks for phishing obfuscated URLs symptoms in web pages and raise alerts**.**

A. Social Engineering

Social engineering is the act of tricking computer users into performing actions or revealing private and confidential information e.g. passwords, email addresses etc, by exploiting the natural tendency of a person to trust and/or by exploiting a person's emotional response. Phishing, Scamming, Spamming are some techniques used for social Engineering.

Social engineering schemes use spoofed e-mails purporting to be from legitimate businesses and agencies, designed to lead consumers to counterfeit websites that trick recipients into divulging financial data such as usernames and passwords. Technical subterfuge schemes plant crime-ware in form of robots or malware agents onto PCs to steal credentials directly, often using systems to intercept consumers online account user names and passwords and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher controlled proxies used to monitor and intercept consumers' keystrokes) [22] .

B. Phishing

The word "phishing" is used to describe hackers and cyber-criminals "fishing" the Internet for personal information such as credit card numbers, bank account information and passwords.

Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials [22]. The idea behind the term is that if they send out enough fake emails, some receivers will surely "take the bait."

The Anti-Phishing Working Group estimates that the volume of phishing e-mail is growing at a rate of over 30%, month after month [30]. Furthermore, the attacks are becoming more sophisticated as attackers leverage vulnerabilities in client software (mail user agents and web browsers) as well as design vulnerabilities in targeted website applications [30].

In February 2010, some attackers craftily cloned the (Central Bank of Nigeria) CBN site, they periodically send email to bank customers requesting them to update their records with the CBN for a new exercise being carried out to create a database of all the commercial banks' customers in Nigeria, the victims allegedly, were to submit their various account numbers and ATM pins before a deadline date. Victims who clicked on the link in the email were taken to a clone of the CBN's site, thereby posing as the legal CBN site [21].

Most phishing occurs on hacked or compromised Web servers. The United States continued to be the top country hosting phishing sites during the first quarter of 2012.

TABLE II. TOP 10 COUNTRIES – HOSTING PHISHING SITE.

January		February		March	
USA	68.92%	USA	70.86%	USA	66.20%
Canada	11.20%	Romania	3.25%	Germany	3.04%
Egypt	4.32%	Germany	2.66%	B. Virgin II	2.63%
Germany	1.85%	UK	2.62%	Brazil	2.54%
France	1.35%	Russia	1.78%	Egypt	1.98%
Israel	1.29%	France	1.73%	UK	1.91%
Netherlands	1.19%	Canada	1.66%	Netherlands	1.84%
Russia	0.68%	Netherlands	1.51%	Canada	1.83%
UK	0.68%	Brazil	1.35%	Turkey	1.54%
Turkey	0.63%	Australia	1.01%	France	1.51%

Source: Phishing Activity Trend Report [22].

The number of unique phishing sites detected in February, 2012 was 56, 859 by Anti-Phishing Work Group, which was an all-time high. The February figure eclipsed the previous highest record which was in August, 2009 by 1 percent [22].

Source: Phishing Activity Trend Report [22].

C. Spoofing Attacks

Spoofing is a broad term used to describe website, email or even caller ID entry made to trick a victim into thinking it is something other than what it really is. It is a method of attacking a network in order to gain unauthorized access. In a spoofing attack, the intruder sends a message to a computer indicating the message has come from a trusted system. To be successful, the intruder first determine the IP address of a trusted system and then modify the packet headers so that it appears that the packets are coming from the trusted system.

In essence, the attacker is fooling (spoofing) the distant computer into believing that they are legitimate members of the network. The goal of the attack is to establish a connection that will allow the attacker to gain root access to the host, allowing the creation of a backdoor entry path into the target system [10]. There are mainly four types of spoofing attacks. They are: IP Address spoofing, ARP poisoning, WEB spoofing, DNS spoofing.

D. Spoofing in Phishing

Hackers using phishing tactics to acquire victims' personal information often use spoofing in an effort to convince such victims to give up their sensitive information. For instance, to get peoples' bank account information, they send you email seemingly originating from their bank, include the banks logos and a spoofed "From" line to reflect a false sender. The email often contains a link to a spoof of such banks' website. The phishers aim is to use it to give the victims a false sense of security and not to give viruses or other harmful files. By tricking their victims into thinking they are on their bank's website, they can easily give up more information. The mail below shows a crafted mail of a particular bank, requesting customers to click on the link and providing vital information pertaining to their account information.

All customers who entered their details on the fraudulent pop-up were compromised. One must note that the targeted unsolicited email was directed to random email users who may not be Internet registered users. Hence there is a potential risk to non-Internet Banking users, who inevitably entered their ATM card (Master card / Verve card) and pin number, as instructed by the attacker.

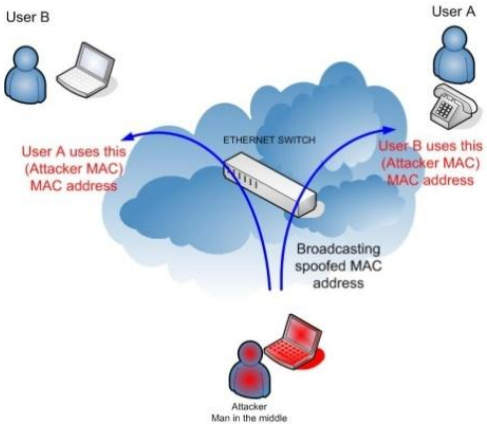

Fig.1. Spoofing Attack

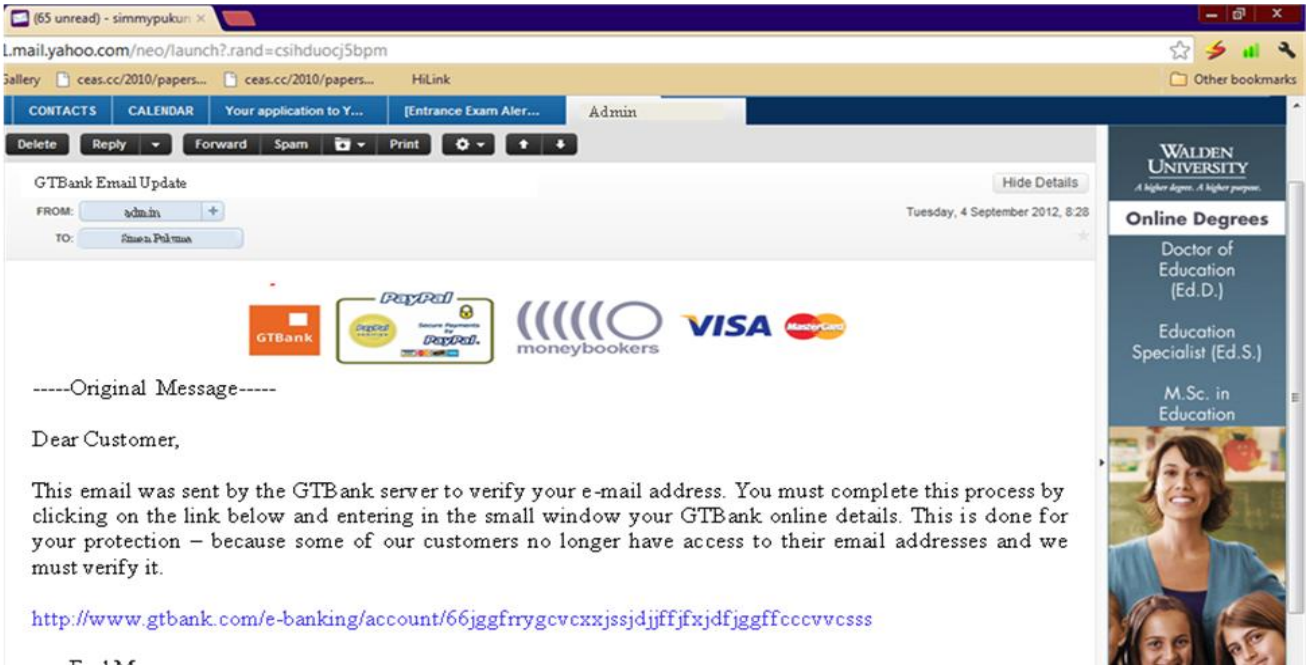

Fig.2. Screenshot of e-mail allegedly to be from GTBank adminstrator

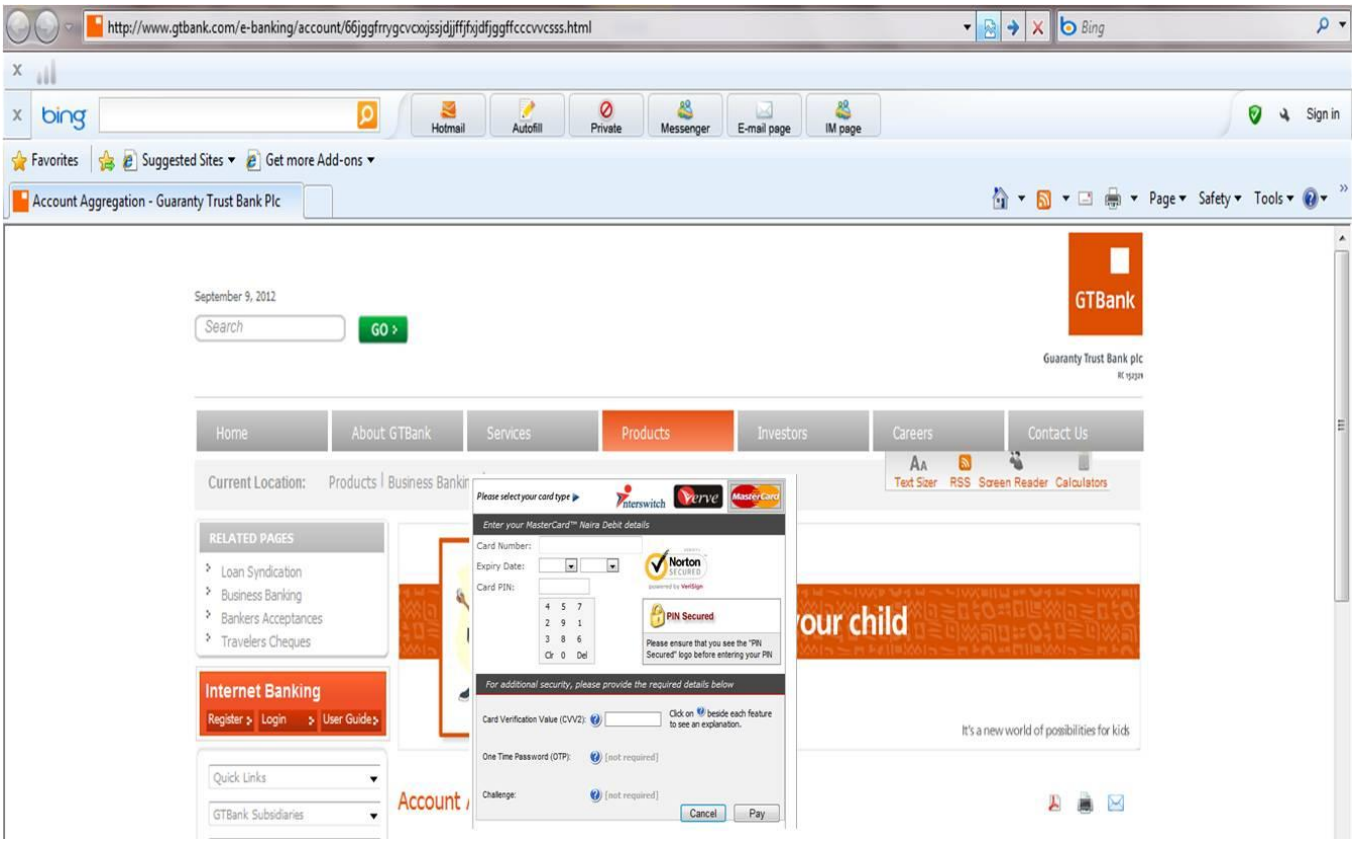

Fig.3. Screenshot of Scam pop up purportedly to be from GTBank website

E. Strategies employed by Phishers

Web Page Obfuscation: To prevent detection from HTML based phishing detector, Phishers employ the use of visual – based content such as images and flash in web site. They also use downloaded web page from real web site to make the phishing web page appear and react exactly the same as the real one.

Web link Obfuscation: This can be carried out in three ways. The first is by using an actual link different from the visible link. Secondly, by using cousin domain names (e.g. replacing certain characters in the target URL with similar characters) [9], thirdly, by adding a suffix to a domain name and redirecting the link to the phishing web pages[1].

F. Challenges with exisitng System

1) Phishers duplicate the content of the target site by using automated tools to download web pages and then use the downloaded web page to achieve main attack on their victim.

2) System that use password authentication fail the requirement for strong authentication, as password can be captured and replayed. Yingjie [28] demonstrated how PWDHASH can be faked.

3) Blacklisting approaches [25], only provide a partial solution with partial list of global phishing websites, and are not completely effective against new phishing websites.

To make the matters worse, the majority of the phishing websites are short-lived (e.g. lasting hours) and hundreds of new ones appear every day[19], making it difficult to update and check against the central databases [12].

IV. METHODOLOGY

This paper employs both primary and secondary research technique of data collection and analysis. This involves the distribution of questionnaire, interview, collection and review of relevant documentation on the evolution of Cybercrime. Data exploited includes; published reports; conference papers; newspaper articles and other media coverage; information accessed through the internet and official records from government agencies.

We proposed a model where by online financial transaction can be secured using a multi-agent system involving biometrics application and an anti-phishing model. We then proceed to present our findings, impediments, and discuss the measures that can be employed by banks to combat Phishing.

In essence, this paper proposes an enhanced approach to detecting phishing web pages and preventing unauthorized online banking withdrawal and transfer. We employed the use of semantics content analysis, earth Mover distance [11] and Biometric authentication[32].

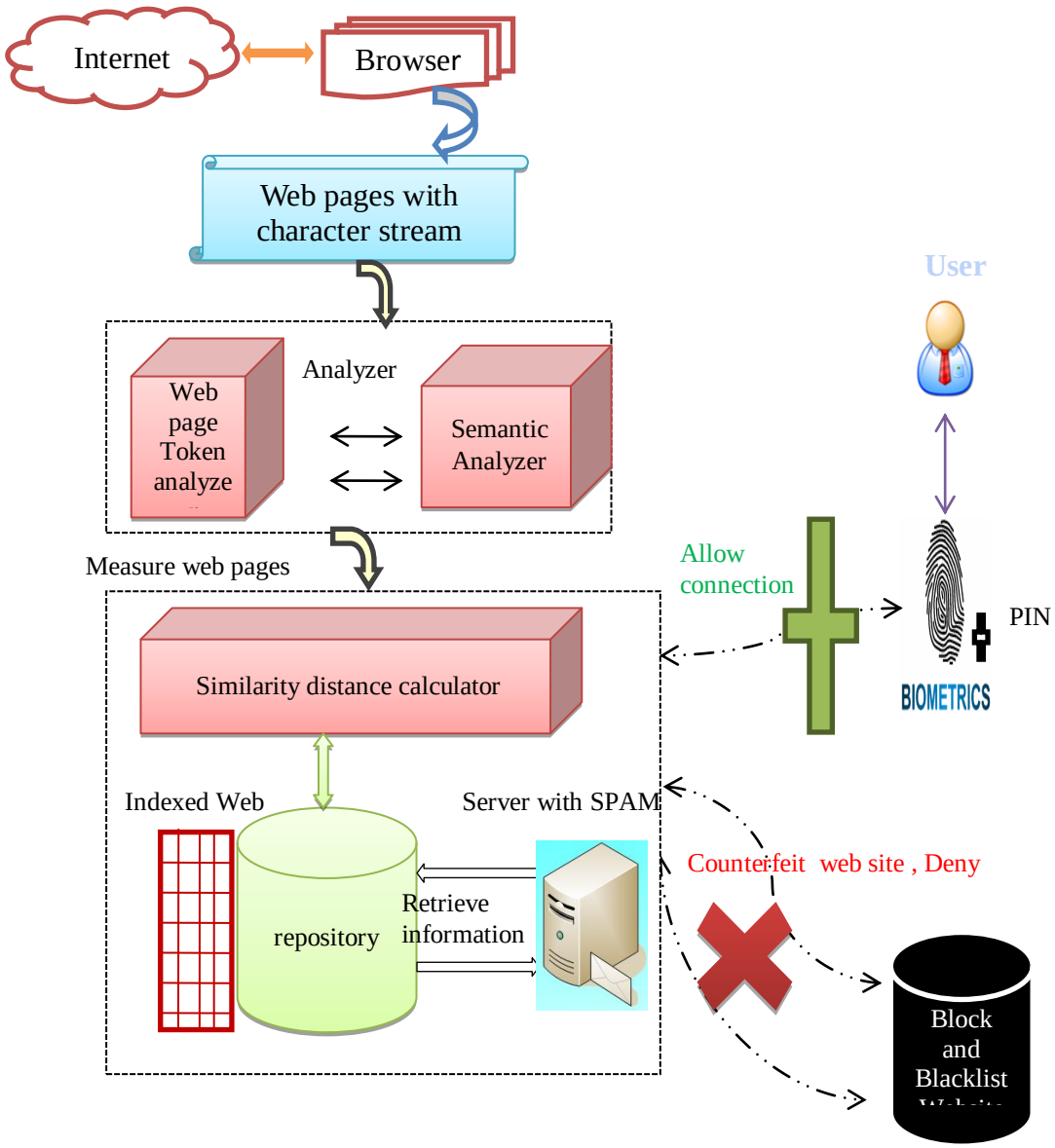

Fig.4. Design Architecture

1) Semantic Content Analysis: Here, sentences from web pages are broken down into small pieces called Token, a finite state automata was used to recognize each regular expression. The semantic analyzer converts all token to upper case letter, which are indexed according to web page and stored in a word repository. The token storage and retrieval scheme can be represented with a 4-tuple as follows:

$<W_p , C_r , q_e , q_f>$

Where,

W_p = set of all words in web pages

C_r = a classifier that Index words in repository

q_e = query matching evaluation function

q_f = feedback function

2) Biometric Authentication: Most popular anti-phishing methods include authentication, which includes email authentication, web page authentication, email filtering and web page filtering, all this listed authentication methods can be intruded by illegitimate professional programmers. We propose the use of finger print authentication [33][34][35][36] mechanism on web pages carrying sensitive information such as credit card information and Personal Information Number-PIN, etc; this is to replace single password verification and impersonation on internet transaction. Online transaction entries are accepted if both the PIN and the fingerprint of the user match with the Account holder. These basic information's are encrypted as they are captured. We adopted the use of biometrics characteristics because they contains physiological characteristics of individuals, are distinctive, cannot be forgotten or lost, and the person to be authenticated needs to be physically present at the point of the identification.

*3) Earth Mover Distance (EMD):*Internet user fall victim of phishing because phishing site has high similarities with original web pages. We adopted [1], EMD Visual Similarity Assessment. The Earth Mover distance was used to assess and calculate the distance between set of features and their respective weight with a bare minimum total price tag. The assessment was carried out on the graphic point of a computer screen. Web pages were converted to images and the coordinate feature and color of the image was used to represent the signature distances. The suspected web page and original web page retrieved from its respective URL will be converted to image and compared.

The EMD is represented as:

$$EMD(P,C,D) = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(f_{ij}.d_{ij})}{\sum_{i=1}^{m}\sum_{j=1}^{n}f_{ij}}$$

Where:

P = Producer

C = Customer

w = respective weight

F = flow matrix, indicating the amount of product to be moved from one producer to consumer. F = $[f_{ij}]$ where $1 \leq i \leq m$ and $I \leq j \leq n$.

n and m= number of customers and producers respectively

D= distance of each pair in distance matrix (Producer and Consumer). D = $[d_{ij}]$ where $1 \leq i \leq m$ and $I \leq j \leq n$.

V. EXPERIMENTAL SETUP AND RESULT

The study sample consisted of some commercial banks in Nigeria. Data was collected to know the level of phishing and other online financial fraud each of the bank experience. Statistical Package for Social Sciences (SPSS) was used as the statistical analysis tool while descriptive statistics were computed and used in the interpretation of findings. A total of fifty (50) questionnaires were randomly administered to IT personnel from different bank. Thirty-nine (39) were returned, which represents 78.00% of the total respondents or participants.

We randomized and attached some set of scores to each of the question raised in the questionnaire distributed in order to rank and determine the susceptibility of each bank, their level of awareness and steps already being put in place to stop the problems encountered. We observed that based on the returned questionnaire, attacks based on internet/online banking (42%)fraud takes the lead, followed by email scam (34%) and finally identity fraud (13%) also leading to online banking fraud while the other salient questions such as illegal ATM withdraw etc. takes the remaining space. We were actually concerned about the three most ranked attacks which are ostentatiously being perpetrated online.

The proposed model works like this, when the browser which have the system installed as a plugin was used to open the web pages, it triggers off the semantic analyzer which parsed the contents of the pages, if the semantic analyzer detects any broken link as a form of spoofed link based on some coded rules, it notifies the similarity distance calculator. The similarity distance calculator have access to the web pages that were used to train the system, it measures, ranks and index each pages based on rules allotted to it. The similarity calculator then index and rank the webpage supplied by the semantic analyzer earlier and compares it to the ranks of web pages in the database and which were used to train the similarity calculator. If a match exists in a region based on a particular threshold which is a set of allowable distance between the web pages being compared, the system index the page as genuine and triggers the authentication module which accepts the biometrics feature of the user and allows any financial transaction else if the distance exceeds the region of the thresholds, the similarity calculator indexed this page as a fake webpage and the authentication module remains calm.

We implemented our model as a system to monitor and safeguard online financial transaction. To test the efficacy of the system, we collected twenty-three sensitive web pages over the course of 8 months, these web pages were used in testing the efficacy of the model presented. The system developed was integrated into the browser as a plugin. Demo web pages mimicking each of the collected web pages and containing a spoofed link to a compromised site were also developed. We also had a demo database which contains some stored customers' details such as their fingerprint, personal ID and some other data. We made an attempt of redirecting the user from the mimic or the fake website to a site totally in our control and where acting as attackers, we could actually siphon information from unsuspecting users.

For the experiment as explained earlier, 23 sample web pages majorly dealing with online financial transactions were collected over the course of 8 months, our system was trained by these sample web pages. We designed some 17 web pages that are identical to the collected web pages albeit with spoofed links to another compromised site. The goal is to re-direct the user to a compromised website which should be in control of the attacker. It should be noted that also acting as the user, we used a browser which contains the system we developed as plugin. For the experiment conducted,20 web pages containing 17 fake pages and 3 original web pages included in the training pages were used to test the system while the whole of the initially collected 23 sample pages were used to train the system. Of the 20 test pages, 16 of the test web pages were suspected to have contained spoofed links when analyzed by the semantic analyzer and the similarity distance calculator. This represents a total of 80.00% accuracy. These pages were totally blacklisted by the system and when re-enrolled the user was automatically denied access through the page. We conducted another experiment in order to discover why one of the fake web pages was left undetected, for this experiment, we included another 7 sample web pages from the similarity calculator's database i.e. pages among those earlier used to

train the system and included the one that our system was not able to identify earlier, the total test pages thus used was 8 web pages. We used the earlier sample web pages used to train the system again. The result returned was however surprising, 1 of the web pages was returned by the system to contain a spoofed link, even though the webpage is genuine and actually part of the pages used in the system training. This shows a roughly 12.5% false positive rate. If we deduct this false positive from the initial true positive accuracy obtained earlier, we get 67.5% which we can use as a baseline accuracy rate for now. This anomalous behavior though unacceptable is still unclear to us i.e. we don't know why the system was not able to detect one fake page and why it detected one genuine page as compromised. We believe this should prompt another research in constructing a more robust system and will form the baseline of our future works where the rules employed by the semantic analyzer and the similarity calculator will be significantly altered.

The biometric authentication aspects come in when pages are certified to be okay by the system, we believe it will ensure trustworthiness and security since users will be authenticated by features unique to them and not what they possess like passwords which are still the de-facto approach. This we believe will definitely strengthen financial transactions on the internet.

The table below shows the results obtained.

TABLE III.

Web pages	True Positive %	True Negative %
With our model	80	20
Without our model	8	92

CONCLUSION

Unfortunately, all the existing solutions proposed to mitigate phishing attacks have their weakness. The increasing rate of novel security challenges in an online banking transaction calls for an unvarying fresh technique that mitigates such challenges. In this paper, we presented a novel technique that replaces the single password verification, web page obfuscation, web link obfuscation using biometric authentication, semantic content analysis and Earth mover distance which was incorporated into browsers as plug-in. The performance of our model shows a considerable improvement to existing systems and clearly opens up a new frontier of research space to be explored in the future. Presently, the proposed system achieved 80% accuracy which is commendable. The experimental result shows that the system effectively strengthens the numerous phishing (identity theft) security challenges on the World Wide Web.

REFERENCES

[1] Anthony Y. F., Wenyin L., and Xiaotie D.(2006). Detecting Phishing Web Pages with Visual Similarity Assessment Based on Earth Mover's Distance (EMD) IEEE Transactions on Dependable and Secure Computing, vol. 3, no. 4, October-December 2006.

[2] Atherton, M. (2010) Criminals switch attention from cheques and plastic to internet transactions. The Sunday Times of March 10, 2010.

[3] Blake R., Collin J., Nicholas M., Dan B., and John C. M. (2005). Stronger Password Authentication Using Browser Extensions. In 14th Usenix Security Symposium, 2005.

[4] Cao, Y., Han, W., Le, Y. (2008). Anti-phishing based on automated individual whitelist. In: DIM 2008: Proceedings of the 4th ACM Workshop on Digital Identity Management, pp. 51–60. ACM, New York (2008).

[5] Christian L., Sean M., Engin K., Christopher K. (2008). On the Effectiveness of Techniques to Detect Phishing Sites. Secure Systems Lab, Technical University Vienna.2008

[6] Chou, N., Ledesma, R., Teraguchi, Y., Mitchell, J.C.(2004). Client-Side Defense Against Web-Based Identity Theft. In: NDSS 2004: Proceedings of the Network and Distributed System Security Symposium (2004).

[7] EFCC/ NBS/ (2009) Business Survey on Crime & Corruption and Awareness of EFCC in Nigeria, Summary Report.

[8] EFCC/ NBS/ (2010) Business Survey on Crime & Corruption and Awareness of EFCC in Nigeria, Summary Report.

[9] Fu, A. Y. , Deng X. , and Liu, W., (2005). "A Potential IRI Based Phishing Strategy," Proc. Sixth Int'l Conf. Web Information Systems Eng. (WISE '05), pp. 618-619, Nov. 2005.

[10] Hamanta, R. B. (2010). A Protol for Network Security Assessment and Methodology. Unpublished Master's thesis, Anglia Ruskin University Chelmsford united kingdom.

[11] Hitchcock F.L. (1941). "The Distribution of a Product from Several Sources to Numerous Localities," J. Math. Physics, vol. 20, pp. 224-230, 1941.

[12] Huh, J. H. and Kim, H. (2010). Phishing Detection with Popular Search Engines: Simple and Effective. www.cl.cam.ac.uk/~hk331/Publications/PhishingDetectionSearchEngine.pdf

[13] Kellerman, T. (2012) Systems Technology Consultants Ltd. Available at http://www.sytech-consultants.com/blog/tag/tom-kellermann accessed date 24th July, 2012.

[14] Kirda, E., Kruegel, C.: Protecting Users Against Phishing Attacks with AntiPhish.(2005). In: COMPSAC 2005: Proceedings of the 29th Annual International Computer Software and Applications Conference, pp. 517–524. IEEE Computer Society, Washington, DC, USA (2005)

[15] Liu W., Guanglin H., Liu X., Zhang M., and Xiaotie D.(2005). Detection of phishing webpages based on visual similarity. In 14th International Conference on World Wide Web (WWW): Special Interest Tracks and Posters, 2005.

[16] Longe, O. B., Mbarika, V., Kourouma, M., Wada, F. &Isabalija, R, (2009).Seeing Beyond the Surface: Understanding and Tracking Fraudulent Cyber Activities.International Journal of Computer Science and Information Security, Vol. 6, No. 3, 2009

[17] Mello, J. P. (2011) "SpyEye Trojan Targets Online Banking Security Systems" Avaialable at http://www.pcworld.com/article/241263/spyeye_trojan_targets_online_banking_security_systems.html#tk.mod_stln

[18] MilletaryJ.(2006).www.cert.org/archive/pdf/Phishing_trends.pdf

[19] Moore, T., Clayton, R.(2007). Examining the impact of website take-down on phishing. In: eCrime 2007: Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit, pp. 1–13. ACM, New York (2007)

[20] Neil C., Robert L., Yuka T., Dan B., and John M. (2005). Client-side defense against web-based identity theft. In 11th Annual Network and Distributed System Security Symposium (NDSS '04), San Diego, 2005.

[21] Onifade, O.F.W. and Adebayo, K. J.(2011).Phishing and Identity Thefts on the Internet.Journal of Information Technology Impact Vol. 11, No. 2, pp. 133-144, 2011

[22] Phishing Activity Trend Report, Quarter 2012 January – March 2012 Published July 2012. http://www.antiphishing.org/reports/apwg_trends_report_q1_2012.pdf

[23] Sarah Jacobsson. Purewals Sunday Times Hackers Steal $6.7 Million in Cyber Bank Robbery Available at

http://www.pcworld.com/article/248340/hackers_steal_67_million_in_cyber_bank_robbery.html#tk.mod_stln

[24] Schneider F., Provos, N., Moll, R., Chew, M., and Rakowski, B.(2007). Phishing Protection Design Documentation. http://wiki.mozilla.org/Phishing_Protection:_Design_Documentation , 2007.

[25] Sheng, S., Wardman, B., Warner, G., Cranor, L.F., Hong, J., Zhang, C.: An empirical analysis of phishing blacklists. In: CEAS 2009: Proceedings of the 6th Conference on Email and Anti-Spam (2009).

[26] Symantec threat report http://www.symantec.com/business/theme.jsp?themeid=threatreport Gartner study: http://www.gartner.com/it/page.jsp?id=565125

[27] Wada, F. & Odulaja, G.O. (2012). Assessing Cyber Crime and its Impact on E-Banking in Nigeria Using Social Theories.Afr J. of Comp & ICTs.Vol 5.No. 1. pp 69-82.

[28] Yingjie , A. F. (2006) Web Identity Security: Advanced Phishing Attacks and Counter Measures. Doctor of Philosophy Thesis. City Univerdity of Hong Kong September 2006

[29] USIC3 (2012)- Internet Crime Complaint Centre Report (2007-2010). www.ic3.gov/media/annualreports.aspx

[30] www.antiphishing.org/Evolution%20of%20Phishing%20Attacks.pdf

[31] Adebayo Kolawole John, Onifade Olufade and Dada Adeniyi: "Vdetector- A model for combating phishing and identity theft on the internet". In Proc of Intl conference on ICT for Africa, Vol. 2, pg. 72-83, March 2011. *Available online at www.ictforafrica.org*

[32] Onifade, F.W. Olufade and Adebayo, J. Kolawole: "Biometric authentication with face recognition using principal component analysis and a feature-based technique", In International Journal of Computer Applications USA. (0975 – 8887) pg 13 – 20, Volume 41– No.1, March 2012. *Available online at www.ijca.org*

[33] Wahab A, S.H. Chin and Tan E.C: "Novel approach to automated fingerprint recognition" In IEEE proceedining of visual image signal process vol145, No 3, June 1998

[34] Nanili Ratha, Kale Karu, Shaoyun Chen and Anil Chain: "A realtime matching system for large fingerprint database" in IEEE transaction on pattern analysis and machine intelligence. Vol 18, no8, junme 1996

[35] Anil K. Jain, Salil Prabhakar, Lin Hong, and Sharath Pankanti: "Filterbank-Based Fingerprint Matching" In Ieee Transactions On Image Processing, Vol. 9, No. 5, May 2000

[36] Anil Jain, Lin Hong, and Ruud Bolle: "On-Line Fingerprint Verification" In Ieee Transactions On Pattern Analysis And Machine Intelligence, Vol. 19, No. 4, April 1997