

DETECTION AND PREVENTION OF PHISHING ATTACK USING LINKGUARD ALGORITHM

 Raphael Olufemi Akinyede¹⁺

 Joseph Adebowale Adelakun²

 Kemi Victoria Olatunde³

^{1,2,3}Department of Computer Science, The Federal University of Technology, Akure, Ondo State, Nigeria

¹Email: roakinyede@futa.edu.ng

³Email: victory4kemi@gmail.com



(+ Corresponding author)

ABSTRACT

Article History

Received: 21 May 2018

Revised: 22 June 2018

Accepted: 10 July 2018

Published: 17 July 2018

Keywords

Link Guard algorithm

Network security

Phishing

Anti-phishing

Algorithm

Attacks.

Phishing is another sort of network attack where the attacker creates an imitation of a current site page to trick users into submitting individual, financial related, or password information to what they believe is their service provider's site. The idea is an end-host based anti-phishing algorithm, called the Link Guard, by using the generic attributes of the hyperlinks in phishing attacks. The link Guard algorithm is the idea for finding the phishing electronic messages sent by the phisher to get hold on the data of the end user. Link Guard depends on investigation of the attributes of phishing hyperlinks. Each end user is implemented with Link Guard algorithm. Subsequent to doing as such, the end user perceives the phishing emails and can abstain from responding to such mails. Since Link Guard is qualities based, it can identify and prevent not only known phishing but also obscure ones.

Contribution/Originality: This study contributes in the existing literature by introducing an idea in an end-host based anti-phishing algorithm, called the Link Guard and it uses generic attributes of the hyperlinks in phishing attacks. This study uses new estimation methodology for finding the phishing electronic messages sent by the phisher to get hold on the data of the end user.

1. INTRODUCTION

According to [Anti-Phishing Working Group \(APWG\) \[1\]](#) phishing is a criminal instrument utilizing both social engineering and specialized subterfuge to steal consumers' personal identity data/information and financial record credentials. This has become a serious network security problem, causing financial loss to both consumers and electronic commerce (e-commerce) companies. This has made e-commerce to be less attractive to ordinary consumers. Social engineering plans utilize spoofed electronic messages implying to be from authentic business organizations and agencies, intended to lead consumers to fake sites that trap beneficiaries into divulging financial related information, for example, usernames and passwords. Specialized subterfuge plans plant crimeware onto PCs to steal credentials directly, frequently using systems to capture consumers' online record -user names and passwords - and to corrupt local navigational infrastructures to mislead consumers to fake sites (or authentic sites through phisher-controlled proxies used to screen and block consumers' keystrokes).

Research has demonstrated that the phishing hyperlinks do not have an indistinguishable attributes from the original one and such differences in the phishing hyperlinks are expressed beneath [\[2\]](#):

- i. The visual link and the actual link are not the same.
- ii. The attackers frequently utilize dotted decimal IP Address rather than DNS name.

- iii. Special tricks are utilized to encode the hyperlinks malignantly.
- iv. The attacker frequently utilize counterfeit DNS names that are comparative (however not indistinguishable) with the target site.

In general, phishing attacks are performed with the following steps:

- i. A phony site which looks precisely like the genuine site is setup by the phisher and which serves as an enticement.
- ii. Phisher at that point sends a link of the phony site in spoofed forms to target users for the sake of real organizations and/or organisations, attempt to persuade the victims to visit their sites.
- iii. The user gets the lure by clicking the link and input valuable and important data required by the phisher.
- iv. Phishers at that point steal the individual information provided and performs criminal acts without the users assent, for example, transferring money from the victims account into an unknown account and so numerous different types of fraud.

This research has developed a link guard algorithm for detecting phishing attacks via links sent to a user's email.

2. PHISHING ACTIVITIES AS AT 2017

The following shows the phishing activities in 2017

- i. In 2017 76% of organizations experienced phishing attacks. Nearly half of information security professionals surveyed said that the rate of attacks increased from 2016. 45% experienced phishing via phone calls (vishing) and SMS/text messaging (smishing) – a 2% increase from 2016 and 3% experienced a USB-based social engineering attack - A 25% decrease from 2016, Wombat Security [3].
- ii. In the first half of 2017 businesses and residents of Qatar were hit with more than 93,570 phishing events in a three-month span [4].
- iii. A phishing email to Google and Facebook users successfully induced employees into wiring money – to the extent of US\$200 million – to overseas bank accounts under the control of a hacker. He has since been arrested by the US Department of Justice [5].
- iv. In May 2017, the WannaCry ransomware attack is suspected of having impacted more than 230,000 people in 150 countries [6].
- v. In the beginning of June 2017, a Ukrainian FinTech company, MeDoc, was breached, and its systems were injected with malware called Petya. Through a Microsoft vulnerability, the malware spread across the globe – impacting hundreds of organisations in Russia, Europe, India and the United States [7].
- vi. By the end of June, a new series of attacks called Not-Petya has wrought havoc globally, shutting down hundreds of businesses, including Maersk, WPP, TNT, Mondelez, Cadburys, Russian steel and oil firms Evraz and Rosneft, Kiev airport and Chernobyls monitoring systems [8].
- vii. In August 2017, customers of Amazon faced the Amazon Prime Day phishing attack, when hackers are sending out seemingly legitimate deals to customers of Amazon. When Amazon's customers attempted to purchase the 'deals', the transaction would not be completed, prompting the retailer's customers to input data that could be compromised and stolen [9].

The Anti-Phishing Working Group (APWG) is an international consortium that brings together businesses affected by phishing attacks, security products and services companies, law enforcement agencies, government agencies, trade association, regional international treaty organizations and communications companies. Table 1 and figures 1-4 show the trend

Table-1. Phishing Activity Trends Report for 1st half of 2017

	January	February	March	April	May	June
Number of unique phishing websites detected	42,889	50,567	51,265	50,328	45,327	50,720
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	96,148	100,932	121,860	87,453	93,285	92,657
Number of brands targeted by phishing campaigns	424	423	444	460	457	452
Number of domain names used in attacks	13,977	15,877	17,397	21,652	21,373	18,404

Source: Anti-Phishing Working Group (APWG) [1]

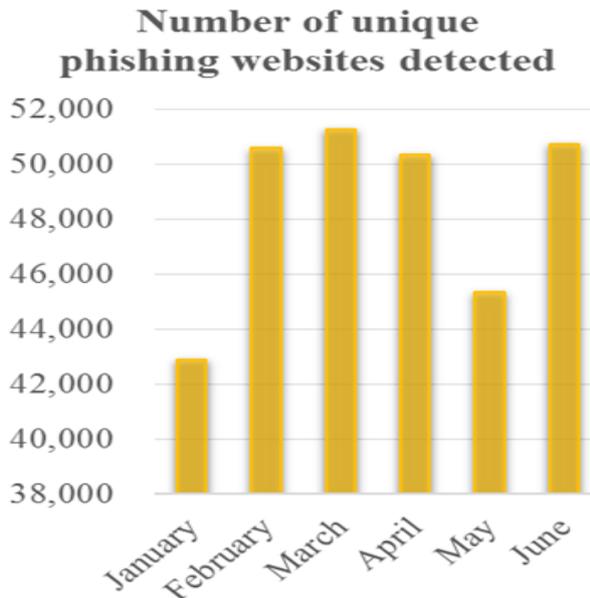


Figure-1. Number of unique phishing websites detected
Source: Anti-Phishing Working Group (APWG) [1]

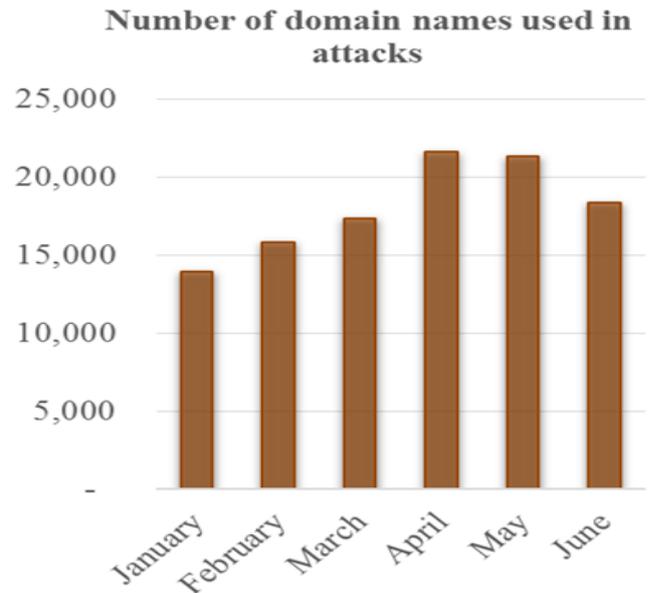


Figure-2. Number of domain names used in attacks
Source: Anti-Phishing Working Group (APWG) [1]

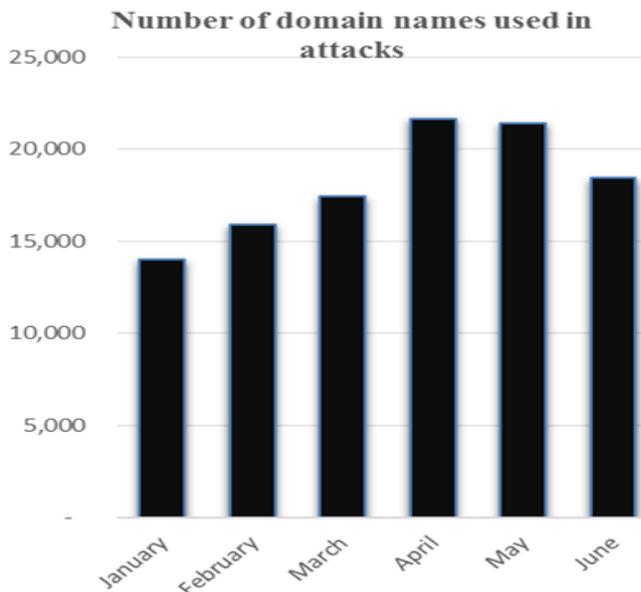


Figure-3. Number of brands targeted by phishing campaigns
Source: Anti-Phishing Working Group (APWG) [1]

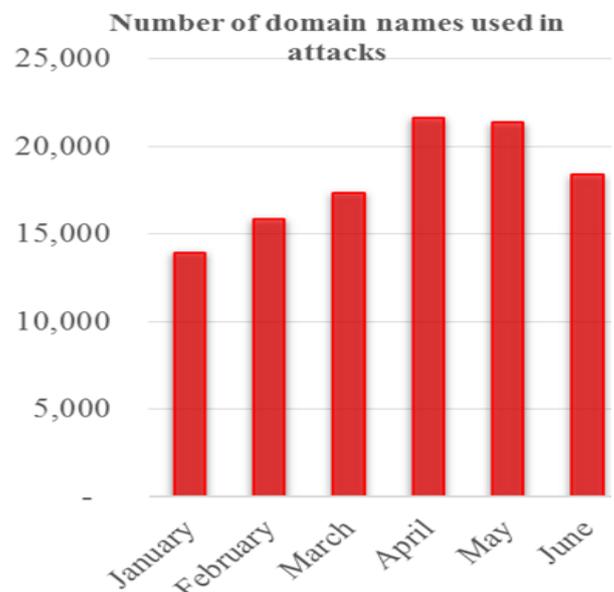


Figure-4. Number of domain names used in attacks
Source: Anti-Phishing Working Group (APWG) [1]

The statistic shows (in figure 5) the online industries most targeted by phishing attacks. During the third quarter of 2017, 15.48% of phishing attacks worldwide were directed towards financial institutions. Payment services accounted for 41.99% of phishing attacks.

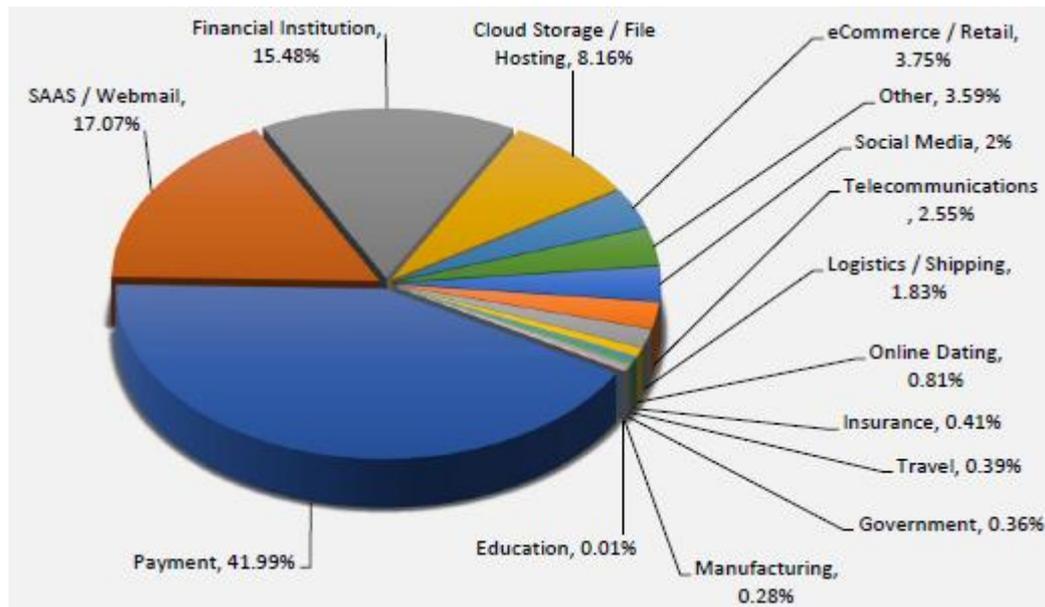


Figure-5. Most Targeted Industry Sectors 3rd Quarter 2017.

(Source: Anti-Phishing Working Group (APWG) [1])

3. PHISHING ACTIVITIES IN NIGERIA

US-based FBI (Federal Bureau of Investigation) is clamming that Nigerian hackers and cyber criminals masterminding a fabulous burglary of data and cash running into billions of dollars, around the world. As reported by the specialists, Nigerians can do the heist by sending phishing messages to business associations and industrial enterprises, which they later steal dry [10].

As indicated in [Kaspersky Lab ICS CERT \[11\]](#) 'Nigerian letters' (a.k.a. 419 scams) have moved toward becoming online fraud. The makers of intriguing stories about heiresses/widows/secretaries/lawyers of deceased millionaires/disgraced dictators/other fat cats did not win the Ig Nobel Prize for literature in 2005 in vain. They may not be exceptionally qualified, but rather they positively have an ability for blackmail, and may well have been benefitting from the ravenousness and artlessness of their victims for quite a long time. Several years ago, Nigerian phishers showed up on the radar of researchers. They were the same scammer who spent significant time in purported Nigerian letters, yet in the meantime they were acing new strategies for stealing money – this time, from companies. They are typically the ones behind business email trade off attacks. There have been a good numerous publications on phishing attacks by Nigerian fraudsters in the previous three years. This is no fortuitous event: this generally new kind of criminal business is gaining momentum. As indicated by FBI estimates, the harm from Nigerian phisher action from October 2013 to May 2016 surpassed US\$3 billion and the number of affected companies was as high as 22,143. Those companies are scattered crosswise over 79 nations of the world. In 2013-2015, for the most part of small and medium-size companies were attacked. The phishers gathered the email addresses of potential victims on the Internet

4. RELATED WORKS

Many researches are working on this field and published their works based on detecting and obstructing the phishing Websites, enhance the security of the sites, block the phishing e-mails by numerous spam channels, Install online anti-phishing software in user's computers. In [Gaurav, et al. \[12\]](#) proposed an Anti-Phishing Technique Using Pattern Matrix which fends off users from phished websites. They proposed a prevention based technique by which each site require user credentials for accessing it instead of using the hyperlinks. The users can access the website from anywhere by setting authentication using code generation and hashing.

In Juan and Chuanxiong [13] presented Link Guard based online detection and prevention of phishing attacks on Windows Xp was presented. They designed Link Guard algorithm not only for detecting phishing as well as it resists users to click on malicious and un-requested links. The system detects the phishing up to 96%.

In Kirda and Kruegel [14] an anti-phishing techniques using Anti-Phish algorithm was proposed. This technique tracks the sensitive information of a user and generates warnings whenever the user attempts to give away details to a web site that is considered untrusted. It is used to check the trustworthiness of a web site. The system mainly focused on web based attacks.

In Smadi, et al. [15] a phishing detection model based on data mining algorithms, and using features extracted from different parts of emails with the aim of enhancing the general measurements benefits of grouping emails was proposed. The authors tried to discover the best algorithm to be used by laying accentuation on the pre-processing part of extracting features. The designed model arranged emails into two sorts: genuine and phishing messages. This classification is made by the features hauled out from the header and content of the messages tried. To produce this detection mechanism, and data mining algorithms were used. The experiment model achieved 98.87% exactness for arbitrary forest algorithm, delineating the benefit of utilizing the pre-handling stage to extricate the arrangement features from emails. The authors have brilliantly used the pre-processing stage and expanded the total metrics of the model. Considering countless that represent a wide range of phishing attacks brought about low false positive rates and high precision of the detection mechanism. Comparing the results of the model with the past researches it can be genuinely presumed that the model ends up being the best as far as exactness and false positive rate for affirmed dataset.

In Aburrous, et al. [16] a distinctive approach to deal with phishing website by using Data mining and Fuzzy logic combination to save Internet users while doing on the web transaction was proposed. The approach used logic evaluated e-banking phishing website hazard on twenty-seven (27) features to construct a model to foresee sites based on fuzzy data mining. This model took a shot at multilayered approach where each layer has its own particular control to characterize the sites in five distinctive ways i.e. very legitimate, legitimate, suspicious, phishy or very phishy. In spite of the fact that the methods obtained 83.7% in any case, this research proposed a powerful strategy utilizing fuzzy data mining algorithms and tools to detect ebanking phishing websites in a computerized way.

In Islam and Abawajy [17] many different types of content-based filters approaches were observed. The examination found that numerous researchers' content based email groupings have been focused on more complex machine learning algorithms. The author proposes an elite approach of Multi-Tier Classification Model alongside the method of extracting the features of phishing email in view of a weighting of message substance and message header and choosing the feature according to the priority ranking. The experiment results with a high precisions rate of 97% in detecting phishing email and became one of the highest accuracy results achiever.

5. THE PROPOSED SYSTEM

The new system will be designed with C# programming language written in Visual Studio Platform because of its flexibility and its ability to invoke other languages into it and a database MySQL which will act as a store for the links. The system will be a software application that will properties of a web browser embedded in it.

It will also involve implementing regular expressions in the programming language. Regular Expressions (R.E) is a set of pattern matching rules encoded in a string according to certain syntax rules. Although the syntax might be complex but it is very powerful and allows useful pattern matching than simple wildcards like ? and *. Wildcards are symbols that can be used to represent any character that may appear in the same position in a computer search argument. A single character is usually represented by ? and multiple characters by *.

The system will categorize the links based on the result generated. The result generated will be in form of counts. The counts machine will assign values to the links in respect to its phishing properties. It classifies the link

based on phishing properties or features and non-phishing properties. The system scans the link using the five categories defined in the previous chapter.

The categorized links will be classified based on the below categories.

Category 1: If the phishing properties found is more than the non-phishing properties then it classifies it under blacklist.

Category 2: If the non-phishing properties found is more than the phishing properties then it classifies it under whitelist.

Category 3: If the non-phishing and phishing properties are equal, the user will then have to use his discretion.

5.1. Strength of the Proposed System

- i. The major advantage of this proposed system is that it is an application that can be installed on any system.
- ii. It also allows subsequent viewing of the database both online and offline.
- iii. It is very interactive

5.2. The Design of the Proposed System

The systems design will be based on the link guard algorithm and also C# programming language.

5.2.1. Interface Design

A user interface is the system by which people (users) interact with a machine. The user interface includes hardware (physical) and software (logical) components see figures 6 and 7.

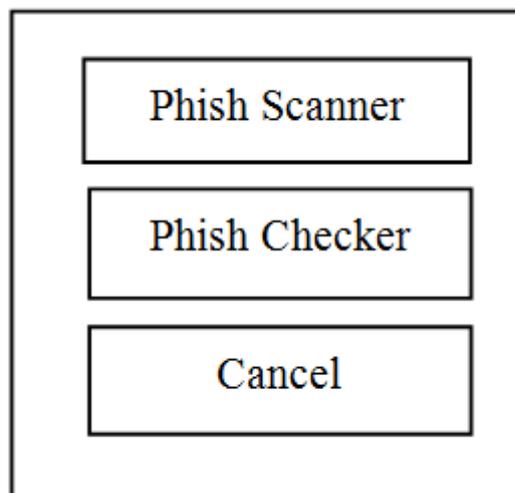


Figure-6. Interface design

Source: Self drawn

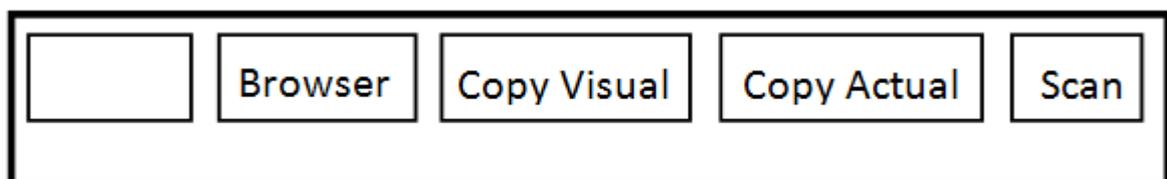


Figure-7. The Browser Interface

Source: Self drawn

5.2.2. Algorithm Design

Below is the systematic way the algorithm processes links.

- i. The visual link in the email is copied.
- ii. The actual link in the email is copied.
- iii. The visual and actual links are both scanned.
- iv. Result is displayed
- v. Result is stored in database.
- vi. End.

As shown in figure 8, a flowchart is a type of diagram that represents an algorithm or process. It shows the steps as boxes of various kinds and their order by connecting them with arrows. The diagrammatic representation can give a detailed step-by-step solution to a problem. Operations processes are represented in these boxes with arrows representing flow of control.

Below is the diagram showing the flowchart of the proposed system as it will be accessed on the desktop and on the web browser.

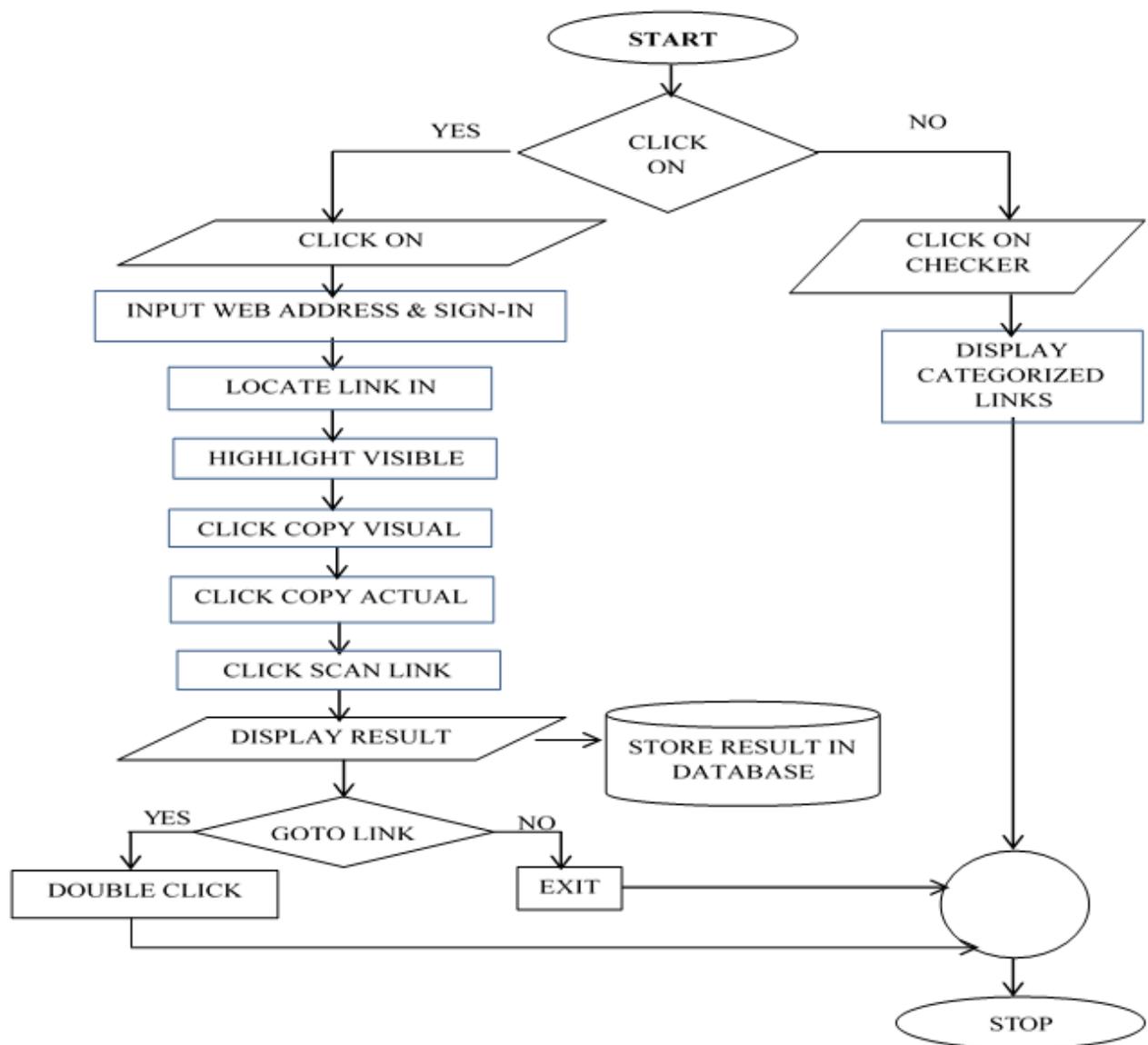


Figure-8. Flowchart of the proposed system

Source: Self drawn

5.2.3. The Proposed Algorithm

This Link Guard work is to examine the differences between the actual link and visual link (Figure 9).

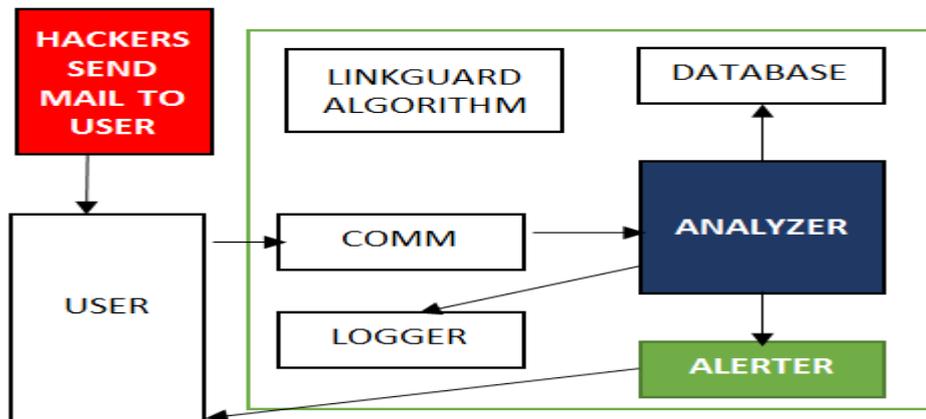


Figure-9. Link guard algorithm Architecture.

Source: Self drawn

5.2.4. Operations of Link Guard Algorithm

- i. Comm: collects information of the users and sends it to the analyser.
- ii. Database: It stores the user input URL'S, Blacklist and White list.
- iii. Analyser: It is the most important part of Link Guard is the main component which is applied on link guard algorithm. It uses data provided by communication and database, and sends all results to Alert and then to logger modules.
- iv. Alerter: It alerts the user immediately there is a warning message from Analyser. It then sends back reactions of the user to the Analyser.
- v. Logger: It archives all related information for future use.

The following terms are used in the algorithm.

v_link: visual link;

a_link: actual_link;

v_dns: visual DNS name;

a_dns: actual DNS name;

sender_dns: sender's DNS name.

5.2.5. Algorithm

Link guard algorithm used in Sarannia and Padma [18] was adopted for the work.

```

int LinkGuard(v_link, a_link) {
1 v_dns = GetDNSName(v_link);
2 a_dns = GetDNSName(a_link);
3 if ((v_dns and a_dns are not
4 empty) and (v_dns != a_dns))
5 return PHISHING;
6 if (a_dns is dotted decimal)
7 return POSSIBLE_PHISHING;
8 if (a_link or v_link is encoded)
9 {
10 v_link2 = decode (v_link);
11 a_link2 = decode (a_link);

```

```

12 return LinkGuard(v_link2, a_link2);
13 }
14 /* analyze the domain name for
15 possible phishing */
16 if(v_dns is NULL)
17 return AnalyzeDNS(a_link);
18 }
19 if (actual_dns in blacklist)
20 return PHISHING;
21 if (actual_dns in whitelist)
22 return NOTPHISHING;
23 return PatternMatching(actual_link);
24 }
25 int PatternMatching(actual_link){
26 if (sender_dns and actual_dns are different)
27 return POSSIBLE_PHISHING;
28 for (each item prev_dns in seed_set)
29 {
30 bv = Similarity(prev_dns, actual_link);
31 if (bv == true)
32 return POSSIBLE_PHISHING;
33 }
34 return NO_PHISHING;
35 }
36 float Similarity (str, actual_link) {
37 if (str is part of actual_link)
38 return true;
39 int maxlen = the maximum string
40 lengths of str and actual_dns;
41 int minchange = the minimum number of
42 changes needed to transform str
43 to actual_dns (or vice verse);
44 if (thresh<(maxlen-minchange)/maxlen<1)
45 return true
46 return false;
47 }

```

This shows the skeletal structure of the implemented algorithm

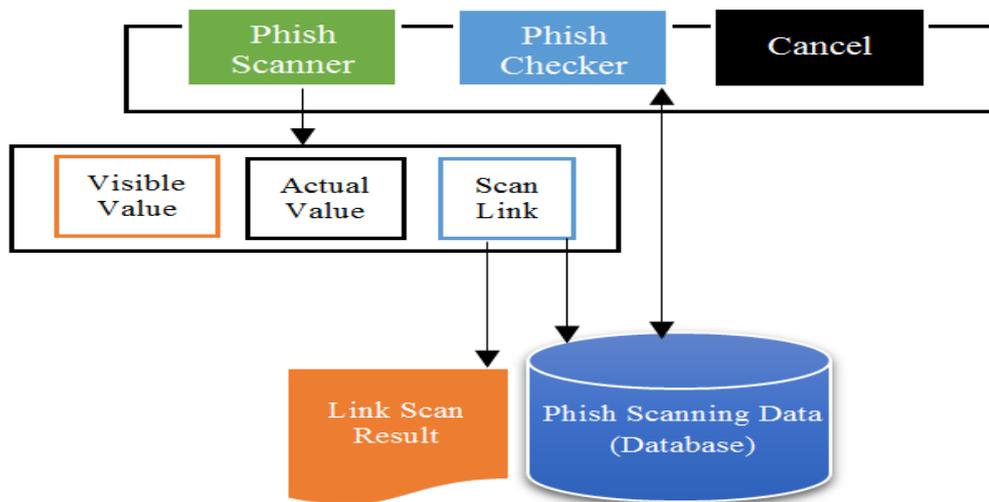


Figure-10. Architecture of the designed software

Source: Self drawn

6. SYSTEM IMPLEMENTATION AND TESTING

6.1. Software Used in the Design

As discussed in the previous chapter, the following components were used in the build-up of this plugin: Visual Studio.Net, C# programming language, MySQL database and SQL Management Studio.

6.1.1. Visual Studio.Net

Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft. It is used to develop console and graphical user interface applications along with Windows Forms or WPF applications, web sites, web applications, and web services in both native code together with managed code for all platforms supported by Microsoft Windows, Windows Mobile, Windows CE, .NET Framework, .NET Compact Framework and Microsoft Silverlight.

Visual Studio .NET is Microsoft's visual programming environment for creating Web services based on use of the Extensible Markup Language (XML). The product suite provides a visual interface for identifying a program as a Web service, forms for building a user interface (including support for mobile device interfaces), features for integrating existing application data, and for debugging. Visual Studio .NET comes with the .NET Framework, including the Common Language Runtime, and includes several programming languages including Visual Basic, Visual C++, and Visual C#.

6.1.2. C# Programming Language

C# (pronounced see sharp) is a multi-paradigm programming language encompassing strong typing, imperative, declarative, functional, procedural, generic, object-oriented (class-based), and component-oriented programming disciplines. It was developed by Microsoft within its .NET initiative and later approved as a standard by Ecma [19] (ECMA-334) and ISO (ISO/IEC 23270:2006). C# is one of the programming languages designed for the Common Language Infrastructure. It is also a general-purpose, object-oriented programming language C# is intended to be a simple, modern, general-purpose, object-oriented programming language. The most recent version is C# 5.0, which was released on August 15, 2012.

6.1.3. MySQL

MySQL is a database management system. It gives a structured collection of data, for the general management, addition, accessibility, processing and storage of data. It handles large amount of data conveniently with the use of PHPMYADMIN on servers.

6.1.4. SQL Management Studio

SQL Server Management Studio is an integrated environment for accessing, configuring, managing, administering, and developing all components of SQL Server. SQL Server Management Studio combines a broad group of graphical tools with a number of rich script editors to provide access to SQL Server to developers and administrators of all skill levels.

SQL Server Management Studio combines the features of Enterprise Manager, Query Analyzer, and Analysis Manager, included in previous releases of SQL Server, into a single environment. In addition, SQL Server Management Studio works with all components of SQL Server such as Reporting Services and Integration Services. Developers get a familiar experience, and database administrators get a single comprehensive utility that combines easy-to-use graphical tools with rich scripting capabilities.

6.2. System Implementation/Testing

PhishScan: This is the main application that contains the embedded browser as well as the database file used for viewing the categorized links.

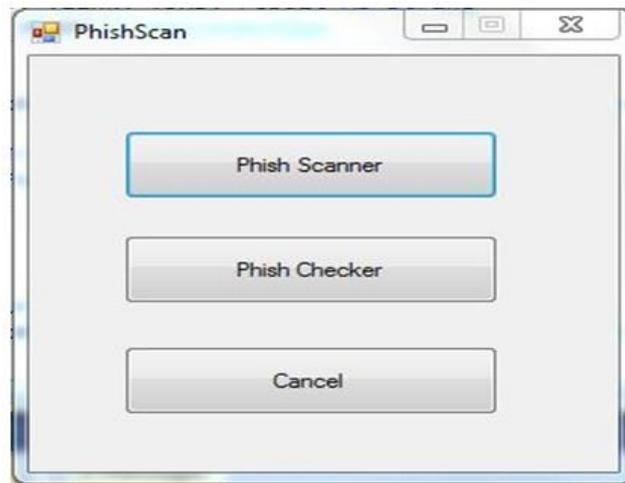


Figure-11. The Anti-Phishing Software Application

Source: Self drawn

Web Browser: As the name implies, it is used to surf the internet and consist of buttons that aid in the testing of the links in the email or any link.

For the bad link

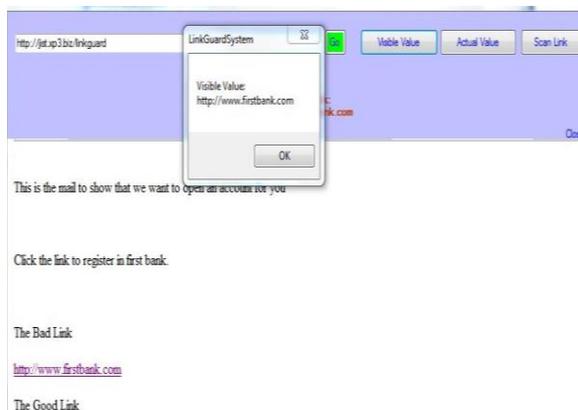


Figure-12. A link highlighted for testing (Visible Link)

Source: Self drawn

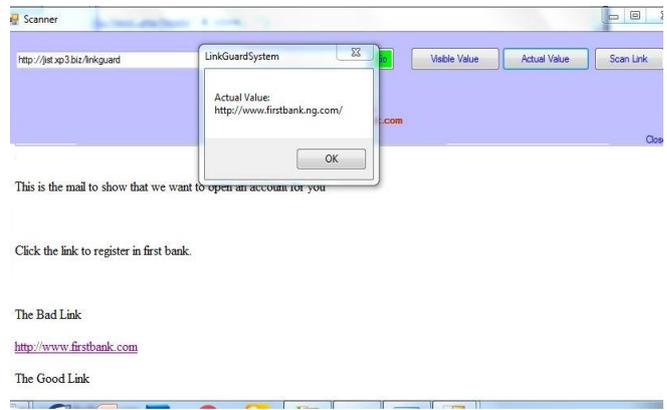


Figure-13. Getting the Actual link

Source: Self drawn

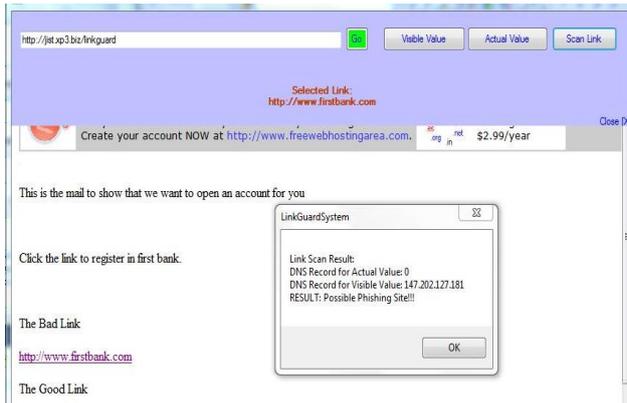


Figure-14. Scanned Result (Possible phishing site)

Source: Self drawn



Figure-15. Link highlighted for testing (Visible Link)

Source: Self drawn



Figure-16. Getting the Actual link

Source: Self drawn

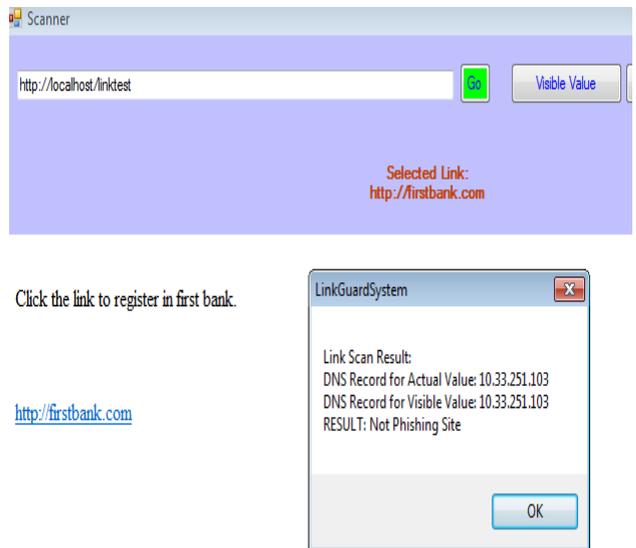


Figure-17. The good link's result

Source: Self drawn

7. CONCLUSION

Phishing has become a serious network security problem, causing financial loss to both consumers and e-commerce companies. This in has made e-commerce to be less attractive to ordinary consumers. In this research, we have studied the characteristics of the hyperlinks that were embedded in phishing e-mails and used the Link-Guard algorithm to develop an Anti-Phishing tool using Visual Studio.Net & C# programming language to develop a system with browser properties. However recommendations have been put forward to improve upon the Anti-Phishing tool such as making it work on multiple platforms and on mobile devices.

9. CONTRIBUTIONS

1. This study contributes in the existing literature by introducing an idea in an end-host based anti-phishing algorithm, called the Link Guard and it uses generic attributes of the hyperlinks in phishing attacks.
2. This study uses new estimation methodology for finding the phishing electronic messages sent by the phisher to get hold on the data of the end user.
3. This study proposes new algorithm, called Link Guard to develop an Anti-Phishing tool using Visual Studio.Net & C# programming language with browser properties

4. This study is one of very few studies which have investigated phishing attack using linkguard algorithm. The paper contributes the first logical analysis, which is to examine the differences between the actual link and visual link by using the generic attributes of the hyperlinks in phishing attacks
5. The paper's primary contribution is finding that not only known phishing but also obscure ones can be identified and prevented.
6. This study documents detection and prevention of phishing attack using linkguard algorithm.

Funding: This study received no financial support from anywhere

Competing Interests: The authors declare that they have no competing interests

Contributors/Acknowledgement: Our thanks goes to the head of the Department of Computer Sciences and the School of Computing, The Federal University of Technology, Akure, Nigeria for providing a space and facilities during the process of the research. We also appreciate our Postgraduate Student, Mr. Owolawi, L. O. who did most of the experiment as part of his postgraduate diploma work.

REFERENCES

- [1] Anti-Phishing Working Group (APWG), The APWG Phishing Activity Trends Report is published by the APWG, 2018.
- [2] U. Naresh, V. Sagar, and R. C. V. Madhusudan, "Intelligent phishing website detection and prevention system by using link guard algorithm," *IOSR Journal of Computer Engineering*, vol. 14, pp. 28-36, 2013. *View at Google Scholar* | *View at Publisher*
- [3] Wombat Security, *State of the phish*: Wombat Security Technologies, Inc. Retrieved: <https://www.wombatsecurity.com/state-of-the-phish>. [Accessed 2018-05-13], 2018.
- [4] V. Joseph, *Qatar faced 93,570 phishing attacks in first quarter of 2017*: Gulf Times, 2017. Retrieved: <http://www.gulf-times.com/story/547784/Qatar-faced-93-570-phishing-attacks-in-first-quart>. [Accessed 2018-05-10], 2018.
- [5] Fortune, "Facebook and google were victims of \$100M payment scam," *Fortune*, pp. 1. Retrieved from www.theverge.com/2017/4/28/.../facebook-google-phishing-scam-rimasauskas. [Accessed 2018-05-10], 2018.
- [6] J. Fruhlinger, "What is WannaCry ransomware, how does it infect, and who was responsible?," *CSO Online*, 2017, pp. 1. Retrieved: www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html. [Accessed 2018-08-13], 2018.
- [7] O. Solon and A. Hern, "Petya' ransomware attack: what is it and how can it be stopped?," *Guardian*, 2017, pp. 1. Retrieved: <https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how>. [Accessed 2018-04-22], 2017.
- [8] M. Mark, "NotPetya - another entirely predictable major incident?" Retrieved from www.htbridge.com. [Accessed 2018-01-28], 2018.
- [9] M. Jones, "Amazon prime day phishing scam spreading now! Kim Komando Show." Retrieved: www.komando.com/happening-now/415020/amazon-prime-day-phishing-scam-spreading-now. [Accessed 2018-04-24], 2018.
- [10] Tekedia, "FBI elevates Nigeria (Unfortunately), claims Nigerian Hackers Stole \$3 Billion Worldwide, 2017," pp. 1. Received: <https://www.tekedia.com/fbi-elevates-nigeria-unfortunately-claims-its-hackers-stole-3-billion-worldwide/>. [Accessed 2018-01-28], 2018.
- [11] Kaspersky Lab ICS CERT, "Nigerian phishing: Industrial companies under attack. Kaspersky Lab." Retrieved from <https://securelist.com/nigerian-phishing-industrial-companies-under-attack/78565/>, 2017.
- [12] M. Gaurav, M. Madhuresh, and J. Anurag, "A preventive anti-phishing technique using pattern matrix," *International Journal of Engineering Research and Applications*, vol. 2, pp. 1825-1828, 2012.
- [13] C. Juan and G. Chuanxiong, "Online detection and prevention of phishing attacks," presented at the First International Conference on Communications and Networking in Beijing, China. 25-27 Oct. 2006. IEEE Xplore. 10.1109/CHINACOM.2006.344718, 2006.

- [14] E. Kirda and C. Kruegel, "Protecting users against phishing attacks," *Computer Journal*, vol. 49, pp. 554–561, 2006. [View at Google Scholar](#) | [View at Publisher](#)
- [15] S. Smadi, N. Aslam, L. Zhang, R. Alasem, and M. A. Hossain, "Detection of phishing emails using data mining algorithms," presented at the 9th International Conference on Software, Knowledge, Information Management and Applications (SKIMA), 2015, 2015.
- [16] M. Aburrous, M. A. Hossain, K. Dahal, and F. Thabtah, "Intelligent phishing detection system for e-banking using fuzzy data mining," *Journal of Expert Systems with Applications*, vol. 37, pp. 7913–7921, 2010. [View at Google Scholar](#) | [View at Publisher](#)
- [17] R. Islam and J. Abawajy, "A multi-tier phishing detection and filtering approach," *Journal of Network and Computer Applications*, vol. 36, pp. 324–335, 2013. [View at Google Scholar](#) | [View at Publisher](#)
- [18] A. Sarannia and U. R. Padma, "Prevention model for phishing attacks in web applications using linkguard algorithm," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, p. 8, 2014. [View at Google Scholar](#)
- [19] Ecma, *C# language specification*, 4th ed.: Ecma International. Retrieved: www.ecma-international.org. [Accessed 2018-01-28], 2018.

Views and opinions expressed in this article are the views and opinions of the author(s), Journal of Information shall not be responsible or answerable for any loss, damage or liability etc. caused in relation to/arising out of the use of the content.