Advance Mailing System for the Detection of Malicious Network Activities

Harsh Gupta
Hapur Adda, Meerut
Department of Computer Science and Engineering
Meerut Institute of Engineering & Technology, Meerut

Sarthak Yadav
Pallav Puram, Meerut
Department of Computer Science and Engineering
Meerut Institute of Engineering & Technology, Meerut

Shalendra Dhariwal
Shatabdi Nagar, Meerut
Department of Computer Science and Engineering
Meerut Institute of Engineering & Technology, Meerut

Vinod Kumar
Miet, Meerut
Department of Computer Science and Engineering
Meerut Institute of Engineering & Technology, Meerut

ABSTRACT
From the word fishing, the term malicious is derived. The idea concentrated upon the anti-malicious algorithm of the final host, The Link Guard, which uses basic elements of the links in the malicious attacks, involves the act of attracting users to visit a fake website by sending false emails to obtain the private information of the victim (for example, personal and financial information). To locate the malicious messages sent by the fraudster to get the target person's details, the link guard algorithm is used. The properties of malicious hyperlinks are the basis of this algorithm. The algorithm is adopted by all users, allowing users to identify such malicious emails and prevent any malicious attacks. Both visible and invisible attacks can be identified and avoided because the Connection Guard Algorithm is a property-based algorithm. The project utilizes PHP and MYSQL technologies.

Keywords
Phishing, Malicious Email Attack Prevention

1. INTRODUCTION
From the terminology phishing, the term malicious is derived. It involves the act of attracting users to visit a fake website to obtain sensitive user-related information such as personal information, financial information, ID for personal privacy, etc[6].. This substantial victim data can be rendered to damage the user and take undue benefits from the user (for example, transfer of the asset of the victim in the name of the perpetrator and/or even other egregious crimes such as identity theft) or for actions such as targeted ads, etc. The most employed phishing strategy is to send e-mails to possible targets that appear to be e-mails forwarded by organizations[5]. Relevant reasons, for example, the plastic card password is inserted incorrect on several occurrences, offering improvements to current facilities, or attracting users to offer some money in return for a substantial quantity of money.

If the clients tend to enter their correct data by some chance, then the attackers analyze the data on the server side successfully and are now able to misuse this information. Phishers are now stealing information and committing business crimes, and over the past one or two years, the numbers for such attacks have risen significantly.

In malicious emails, the common hyperlink characteristics are that the following properties are shared among the harmful urls. These are as follows, the visible link and real links may not be the same, but with the DNS name, assailants often use dotted decimal IPs, the use of special tricks to maliciously encrypt the hyperlinks[1], the use of fake DNS names close to the target website (but not identical).

In order to extract substantial personal data from the victim, this device prevents malicious phishing attacks carried out by attackers. This system would protect users from various email attacks ranging from financial fraud to targeting personal information and hacking the computer of the user by clicking on compromised links. This framework helps users not only to avoid and track known attacks[1], but also unknown attacks, and can prove to be a good service to add to existing email services.

2. METHODOLOGY
In this project, a mailing system based on a client server that is capable of preventing and detecting both known and unknown malicious phishing attacks has been built. The user must first sign up, log into the mailing system after signing up[9], and can now send emails to other registered users. In this project, the Link Guard Algorithm is taken into use, which works by analyzing hyperlink characteristics and thus protects the user from potential phishing attacks. Technologies like PHP[2], and MYSQL[3] have been used by us.

2.1 Module Explanation
Financial services websites or e-shopping platforms may usually be used for illegal purposes. The application of the Link Guard algorithm using a mail-box method is discussed in this project. Let's talk about what we're going to do in this project.

Involved in this project are three modules:

2.1.1 Module-1: Mail framework development [7] and database operations[8].

2.1.2 Module-2: Writing, sending and receiving mail.

2.1.3 Module-3: Link Guard algorithm implementation.

2.2 Link Guard Algorithm
The structured way the algorithm processes connections is below.

1) The email's visual connection is analysed.

2) The real connection of the mail is analysed.

3) Both the visual and real connection are isnpected.

4) Show the result

5) The result is stored in the database.

6) End

By observing the variations among the foreseeable link and the real connection, Link Guard works. It also decides the resemblance of an Address to a known trusted location.

3. DESIGN AND IMPLEMENTATION

The design and implementation of the project is given as follows:

3.1 Inter Relation between Design Systems

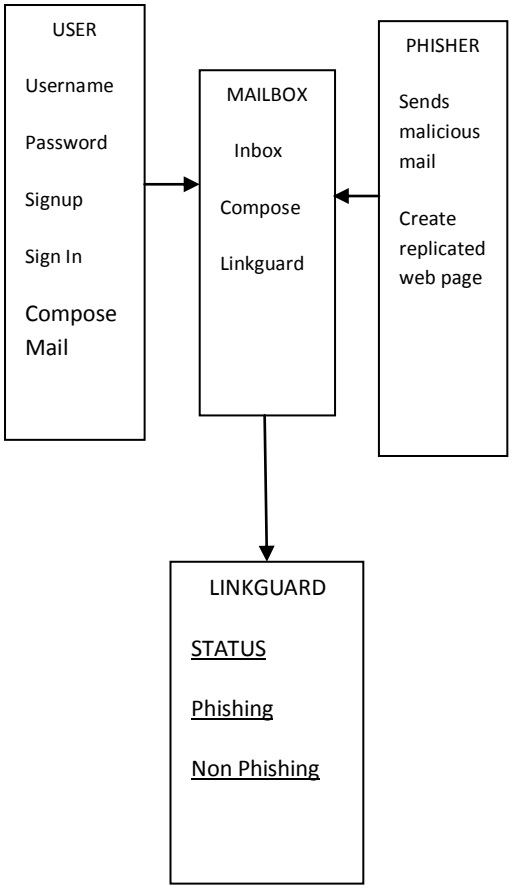

Fig 1: Inter-relation Between Design Systems

The various design elements in the project include designing of the signup and login page and also designing the inbox and spam page.

The design of components like compose mail is also an important consideration in the designing of the project.

3.2 Implementation of Link Guard Algorithm

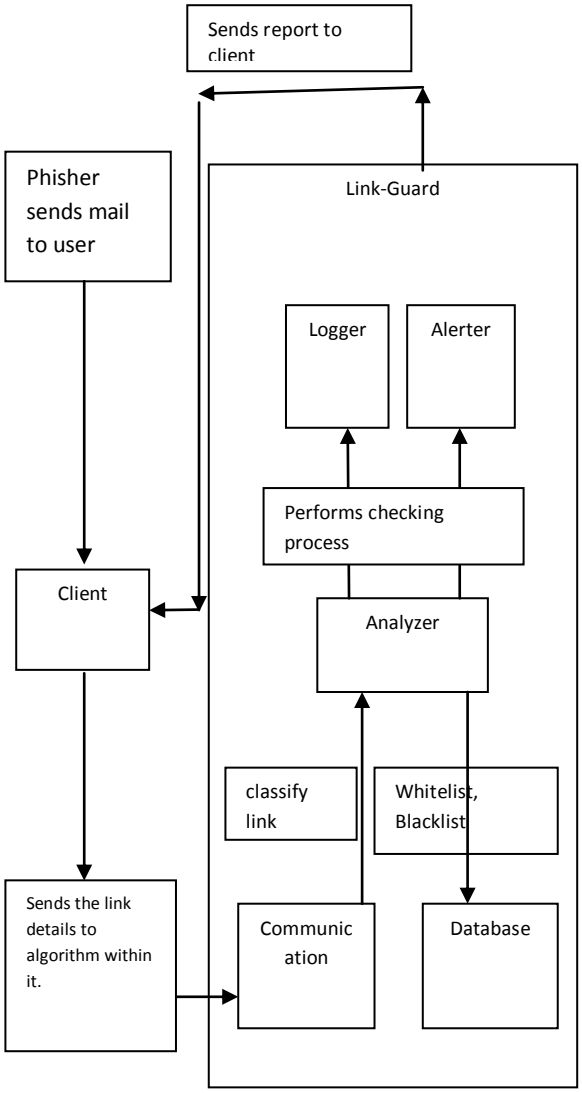

Fig2: Implementation of Link Guard Algorithm

The main component of the implementation is Link Guard[1]. This is a GUI autonomous Windows software. It comprises five elements, as shown in the figure: Analyzer, Alerter, Logger, Database, and Comm. Here are the functionalities of the following 5 sections:

Communication: Interact to all controlled processes, collect user feed information from different operations, and submit this information to the Analyzer. You may also submit orders from the LinkGuard executive. The parallel data environment that the software provides understands the communication between the LinkGuard process and other processes.

Database: Input URLs for permissible, banned, and users are stored.

Analyzer: It applies the LinkGuard algorithm as the main component of LinkGuard. It uses information supplied by Communication and Database and return the information to the Alert and Logger modules.

Alerter: Displays similar information while receiving a warning message from the Analyzer to alert users and send user reactions Return to the Analyzer.

Logger: Log history data for future use, such as user activities, warning records.

4. EXPERIMENTAL ANALYSIS

The proposed project offers a reliable, easy to use and a user-friendly user interface that helps the user to send mails. The system is able to identify an email as a spam mail based on the content of the email i.e. whether it contains any fraudulent or malicious content which can harm a user.

Table 1: Experimental Results

S/N	Total mails received	Marked as spam	True Spam	False Spam	Accuracy
1	10	4	4	0	100%
2	10	3	3	0	100%
3	20	5	4	1	80%
4	10	4	3	1	75%
5	10	2	2	0	100%
6	10	3	3	0	100%
7	10	5	4	1	80%

The details of the experimental analysis are shown in the table above.

As it is clearly visible from Table 1, the experiment was conducted in the following manner.

The authors conducted the experiment a total of seven times. In the experiment, the authors sent some mails to each other with real and fraudulent data in the e-mail body. The authors noted down the observations based on whether the system was able to detect the spam emails or not. It was observed that the system performed with 100% accuracy in four instances, 80% in two instances and 75% in an instance out of the seven instances recorded by the authors. Hence, the mean accuracy of the system can be calculated as a ratio of the sums of the accuracy to the total number of instances which equals to 90.71% accuracy. Hence, we can say the proposed project is fairly reliable in the detection of malicious emails sent by an attacker.

The graphical representation of the experimental results is given below.

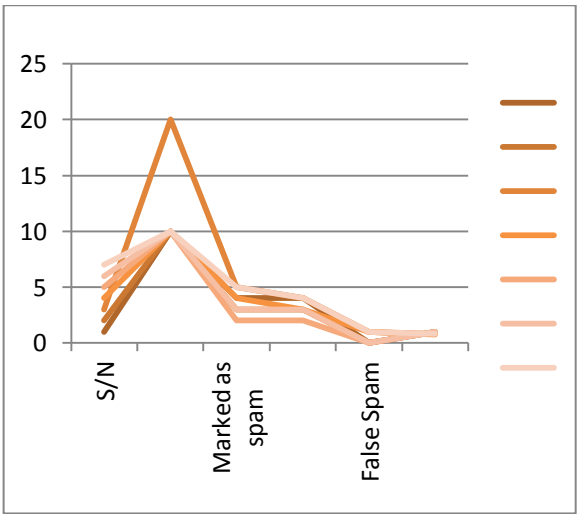

Fig3: Graph on marked as spam and false spam

The above graph indicates that although there are some emails characterised as false spam but they are very less in number than true spam emails which are indeed characterized as spam. Hence, the proposed system is fairly reliable.

5. CONCLUSION AND FUTURE WORK

Malicious practices such as phishing are actually causing serious issues, ranging from network security issues to financial losses. The characteristics of hyperlinks that were applied to the malicious emails in this paper have been analyzed. An anti-malicious algorithm, Link Guard, built upon the acquired properties, to address these problems is used, since the guard of malicious activity is characteristic-based, it is now able to detect both the known and the unknown attacks. In addition to being useful for detecting malicious attacks, it is assumed that the Link Guard

The algorithm can also secure users on internet sites and communications from fraudulent or inappropriate links. The future work will include gradually extending the Link Guard Algorithm such that it is possible to handle Cross Site Scripting attacks.

Future work involves expanding the algorithm of the Link Guard and allowing it to tackle attacks from Cross Site Scripting (CSS). In web applications, CSS is a type of vulnerability that enables malicious web users to add special code to web pages accessed by other users. To get past access control like the same origin policy, a CSS vulnerability can be used by malicious web users. There have been some instances where attackers have taken advantage of this kind of loophole to execute malicious attacks and even use browsers to their good advantages. Because of the misunderstanding between Cross Site Scripting and Cascading Style Sheets[4], the reference to Cross Scripting Sites as CSS was then discontinued.

6. REFERENCES

[1] Online detection and prevention of phishing , University/Mathematical and Computer Sciences/Information Technology/Information Systems, 2011-01-03

[2] PHP documentation.

[3] MYSQL documentation available at https://www.dev.mysql.com/docs

[4] CSS ducmentation at https://developer.mozilla.org/docs

[5] 6 common phishing attacks and how to protect against them.

[6] What is phishing available at https://www.phishing.org/what-is-phishing

[7] E-mail Architectutre https://bachelorstudy.in/e-mail-architecture/

[8] How to manage MYSQL databases,users and Tables from the Command Line.

[9] Login and Signup using PHP and MYSQl with validation. https://www.studentstutorial.com/php/signup-login-form-in-php-mysql.php.

7. AUTHOR'S PROFILE

Harsh Gupta, currently pursuing my Bachelors degree in Computer Science Engineering from Meerut Institute Of Engineering and Technology.

Sarthak Yadav, currently pursuing my Bachelors degree in Computer Science and Engineering from Meerut Institute Of Engineering and Technology.

Shalendra Dhariwal, currently pursuing my Bachelors degree in Computer Science and Engineering from Meerut Institute Of Engineering and Technology.

Vinod Kumar, B.Tech, M.Tech, PhD pursuing from Shobhit University, Meerut. Presently working at M.I.E.T,Meerut,as an Associate Professor. Algorithms, database systems, data structure and operating systems are the areas of concern. NPTEL's Python certification completed. R-language, certified gold.