ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

Intelligent Phishing Detection Scheme with Enhanced Fuzzy Norms over Fog Networks

B.Seetha

M.E. Computer Science and Engineering, Department of Computer Science and Engineering, Shanmuganathan Engineering College, Thirumayam Rd, Arasampatti, Pudukkottai, Tamilnadu, India.

ABSTRACT: The main objective of this system is to enhance the security mechanisms and avoiding the Phishing attacks over web medium.Anti-phishing detection solutions employed in industry use blacklist-based approaches to achieve low false-positive rates, but blacklist approaches utilizes website URLs only. This study analyses and combines phishing emails and phishing web-forms in a single framework, which allows feature extraction and feature model construction. The outcome should classify between phishing, suspicious, legitimate and detect emerging phishing attacks accurately. The intelligent phishing security for online approach is based on machine learning techniques, using Adaptive Neuro-Fuzzy Inference System and a combination sources from which features are extracted. An experiment was performed using two-fold cross validation method to measure the system's accuracy. The intelligent phishing security approach achieved a higher accuracy. The finding indicates that the feature model from combined sources can detect phishing websites with a higher accuracy. This project contributes to phishing field a combined feature which sources in a single framework. The implication is that phishing attacks evolve rapidly. Therefore, regular updates and being ahead of phishing strategy is the way forward.

KEYWORDS: Phishing websites, Neuro-fuzzy network, Neural network, Fuzzy, Fog computing, Cloud computing.

I. INTRODUCTION

Phishing attacks are increasing rapidly costing the global economy billions of dollars per year . Although various Pstudies have concentrated on phishing attacks and used a variety of solutions in the recent years to combat phishing. There is still a lack of accuracy in real-time causing vast amount of losses annually. In general, detection techniques are classified in 2 main categories namely, URL blacklist-based and web-page feature-based. URL blacklist use human-verified URL based on server-side that performs URL matching with real-time website URLs to detect phishing websites. This category works on the principle of detecting phishing attacks and provides warning to users to prevent them from taking risky actions that could otherwise result in compromising their sensitive information. Although existing approaches are effective to some extent, effective generalization to new threats is still a challenge.

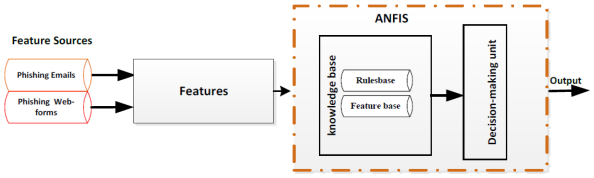

Fig.1 Proposed System Architecture

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

Phishing is a criminal activity that steals victims' personal information using misleading emails or fake websites [1]. The word "phishing" is originated from the word "fishing" [2]. Online users can be easily deceived into entering their personal information because phishing websites are highly similar to real ones. Maliciously, by creating phishing sites, "phishers" use a number of techniques to fool their victims, including email messages, instant messages, forum posts, phone calls, and social networking information [3]. Phishing results in severe economic loss all over the world, and phishing sites are also growing rapidly in quantity and complexity. According to reports from the Anti-Phishing Working Group [3], the number of phishing attacks is increasing by 5% monthly. Fig. 1 illustrates the urgency and importance of phishing identification in modern society, which is based on a phishing website report received in the first quarter of 2016 [3]. However, at the edge of networks, the anti-phishing problem has not been well-addressed due to the following reasons. First, mobile users check their emails and use web browsers more frequently than desktop users [4]. Thus, they are much more likely to access on phishing sites that have not yet been detected or taken down by anti-phishing applications and firewalls at their local networks or on their devices.

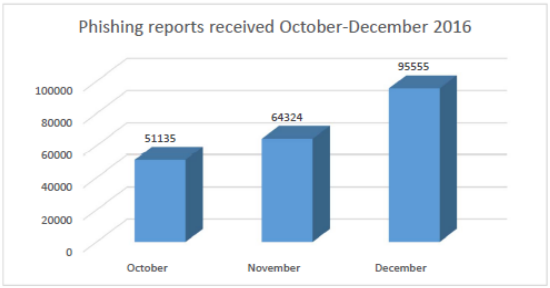

Fig.2 Phishing reports received in the period of October-December 2016 [3].

Second, mobile devices are always "hungry" for energy and computing resources (e.g., limitations of CPU, memory, and user interfaces), so anti-phishing tools are usually ignored or removed on these devices. Hence, it is hard for users to discern if an incoming link is legitimate or not. Third, existing anti-phishing tools (e.g., default plug-ins on web browsers or local anti-phishing applications) are inefficient in terms of detection (this will be analyzed concretely later in Section III), and mobile users may be exposed to phishing attacks when engaging in usual behaviors. According to the report [5], mobile users are three times more likely to submit their login information than desktop users do. Therefore, preventing phishing attacks against terminal users is a critical issue in the edge of networks.

II. SYSTEM IMPLEMENTATION

A. SOURCES AND FEATURE IDENTIFICATION

To reduce phishing attacks, it is important to utilize effective techniques and identify important sources to extract comprehensive features that can detect phishing websites accurately. One hundred phishing emails that contain links to phishing websites and two hundred web-forms used to collect sensitive information from users are gathered to be the representative of sources to extract features. From these sources, 56 features were extracted in which 22 features are novel, while 34 features have been used in the previous work as stated in the above section. These features are presented. Emails and web-forms are selected from Millersmiles‟ website archive. Millersmiles is one of the leading anti-phishing web services dedicated to maintain a large archive of phishing websites and emails. Other anti-phishing services that maintains huge archives for phishing websites is PhishTank. The sources are chosen because new phishing attacks are added to them regularly and they supplement each other well.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

B. FEATURE NORMALIZATION

To comply with fuzzy inference system principles, variable ranges are determined. Intelligent phishing security has four main linguistic variables as detailed in Section D: Legitimate (low), suspicious (medium) and phishing (high). The degree of risk is the most important criteria to determine the accuracy of models. The average percentage accuracy should not exceed the limit acceptable in phishing detection. To determine the degrees of risk, feature‟s linguistic values (legitimate, suspicious and phishing) ranges are specified, the degree which are normalized to values within the range of (0, 1) by assigning the numerical value. Website are classified between legitimate, suspicious or phishing. Other values like „very low‟ are not practical to use. Features are normalized since they are textual and the assigned values are used to define the level of risk of a website. Also, features are of different types. However, some tools for intelligent systems like MATLAB toolbox requires a specific type of data.

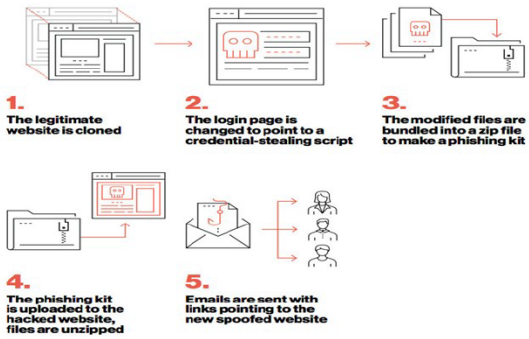

Fig.3Anatomy of a Phishing Kit

C. FEATURE SIZE

Features size can vary depending on the type of measuring tool. However, features should have sufficient size that can be analyzed when using standard measurement method. If for instances, two-fold cross validation method is used, the features size should be split into two pairs with a reasonable amount in each pair. Therefore, assume 56 feature size are used for experiment in the intelligent phishing security is within the minimal sufficient amount. They are split into 28 training set and 28 testing set. These features are the most frequent phishing features found across all the two hundred phishing web-forms and a hundred phishing emails.

D. ADAPTIVE NEURO FUZZY INFERENCE SYSTEM

Adaptive Neuro-Fuzzy Inference System (ANFIS) is a type of adaptive network that is functionally equivalent to Fuzzy inference systems. It combines both fuzzy logic principles and a neural network. It represents Sugeno Tsukamoto fuzzy models that utilize a hybrid learning algorithm. Its outputs depend on input data and the parameters relating to the neurons. ANFIS is used in this study not only because of its advantage of imprecise reasoning, but also for its suitable functionalities when modeling the intelligent phishing security fuzzy models.

E. INTELLIGENT PHISHING SECURITY FUZZY RULES

In phishing detection structure, there are inputs which are represented in the form of inputs as , and one output z. A single input is represented by two-fuzzy sets and the output by a first order polynomial then the rules are presented in

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

the form x y. Where x , y and z (feature and website) are linguistic variables, A1 , A2 , A3 (details confirmation, credit_card_startdate and card number) are linguistic values decided by fuzzyset on the universe of discourse x ; B1, B2 and B3 are fuzzy sets on the universe of discourse z (website).

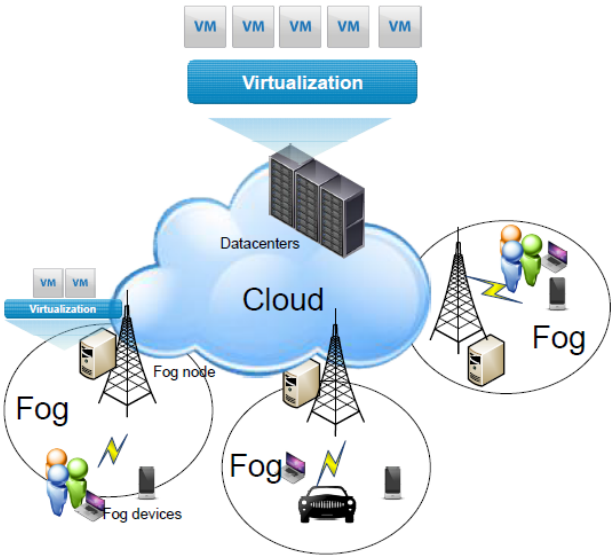

Fig.4 Fog computing architecture: using virtualization techniques, fog nodes can provide services at the edge of a network.

F. PHISHING KIT

The availability of phishing kits makes it easy for cyber criminals, even those with minimal technical skills, to launch phishing campaigns. A phishing kit bundles phishing website resources and tools that need only be installed on a server. Once installed, all the attacker needs to do is send out emails to potential victims. Phishing kits as well as mailing lists are available on the dark web. A couple of sites, Phishtank and OpenPhish, keep crowd-sourced lists of known phishing kits. Analyzing phishing kits allows security teams to track who is using them. “One of the most useful things we can learn from analyzing phishing kits is where credentials are being sent. By tracking email addresses found in phishing kits, we can correlate actors to specific campaigns and even specific kits,” said Wright in the report. “It gets even better. Not only can we see where credentials are sent, but we also see where credentials claim to be sent from. Creators of phishing kits commonly use the ‘From’ header like a signing card, letting us find multiple kits created by the same author.”

G. TYPES OF PHISHING

If there's a common denominator among phishing attacks, it's the disguise. The attackers spoof their email address so it looks like it's coming from someone else, set up fake websites that look like ones the victim trusts, and use foreign character sets to disguise URLs. Generally, a phishing campaign tries to get the victim to do one of two things:

(i) Hand over Sensitive Information.
These messages aim to trick the user into revealing important data — often a username and password that the attacker can use to breach a system or account. The classic version of this scam involves sending out an email tailored to look like a message from a major bank; by spamming out the message to millions of people, the attackers ensure that at least some of the recipients will be customers of that bank. The victim clicks on a link in the message and is taken to a

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

malicious site designed to resemble the bank's webpage, and then hopefully enters their username and password. The attacker can now access the victim's account.

(ii) Download Malware.
Like a lot of spam, these types of phishing emails aim to get the victim to infect their own computer with malware. Often the messages are "soft targeted" — they might be sent to an HR staffer with an attachment that purports to be a job seeker's resume, for instance. These attachments are often .zip files, or Microsoft Office documents with malicious embedded code. The most common form of malicious code is ransomware — last year it was estimated that 93 percent of phishing emails contained ransomware attachments.

(iii) Link Manipulation
The most common of all phishing techniques in existence is link manipulation which, as the name states, directs your browser to a website different from the original website you are to visit through fiddled links. Link manipulation usually comes in the form of an e-mail message from what you think is your trustworthy website. Let's look at a scenario that shows how link manipulation works. You are checking your e-mail account when suddenly you receive a notice telling you to protect your PayPal account. As you click on the e-mail message link, you read through a seemingly original PayPal message, telling you that PayPal administrators have "noticed" that you attempted to log in using a foreign IP address (a clever alibi, I must say). In the middle of the baffling message appears a highlighted sentence telling you to verify your account, followed by the manipulated link. And after that, a frightening message appears: "If you choose to ignore our request, you leave us no choice but to temporarily suspend your account." That really leaves you no choice but to follow their manipulated link. Since you cannot afford to temporarily lose access to your virtual bank account, you clicked on the link, which opened the website created by the phisher. On the webpage, you are asked to enter your username and password to "log in" to your account. Thinking that you are furthering the security of your PayPal account, you provided the username and password, et voila! The phisher now knows your username and password and can eventually use them for his gain.

(iv) Website Forgery
Phishers can also use fake web pages to phish out information. This method is known as website forgery, which comes in two devilishly wise packages. The first method of website forgery uses scripting methods to conceal the manipulated link in the web page's address bar. Commonly, phishers imitate the address bar logos of trustworthy websites and put them beside URLs of their deceiving website. Further, the phisher's scripts can even close the address bar containing the phisher's link, replacing it with an address bar containing the genuine URL to obscure the website's identity. The second method of website forgery is done through exploitation of a website's flaws. Cross-site scripting or XSS uses a website's programming defects to trick an unsuspecting visitor. XSS is a very convincing phishing technique, because what it does is open the authentic website wherein the victim fills up forms for usernames, passwords, and other confidential information. But upon submitting the page, XSS scripts start working, linking you, the persuaded victim, away from the authentic website and into the phisher's own.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

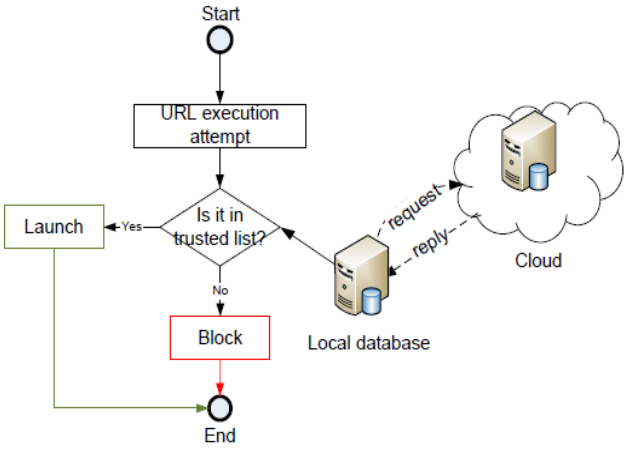

Fig.5 The blacklist/whitelist mechanism in phishing detection.

H. OTHER TECHNIQUES

Internet frauds don't only involve websites. When you receive an e-mail message telling you to dial a certain number, doubt it immediately (unless you are expecting some transactions from the website, of course). This might be a voice phishing attack. If you dial the number provided by the phisher in the email message, voice prompts will be asking you to press numeric information about your bank account like your account and PIN number. Phishers have arrays of faking techniques to employ to fool users. They can use fake caller ids to give the call a legitimate, trustworthy feel, an IP service that provides voice-overs to communicate with you in real-time setting, and even access on information keyed through a landline phone. Although there are anti-phishing toolbars that check websites if they are one of the identified spoof websites in an Internet-wide database, phishers have found a way to further conceal their identity from anti-phishing programs which evolved from mere filter evasion. Introducing: the phlashing technique. Confident that the anti-phishing programs are the ultimate salvation from phishers, users get that false security feeling that they are protected from any kind of phishing attack. Sadly, phishers were able to think outside the box (or the four corners of the webpage window) and learned to use Macromedia Flash animations as means to create their spoof websites. Such knowledge, in essence, defeats the purpose of anti-phishing services "with the phisher's hands tied behind his back." Since anti-phishing programs scan only the text contents of a suspicious website, phlashes can just pass the anti-phishers with flying colors.

I. SOCIAL NETWORK PHISHING

Although this only comprises a small percentage of phishing activities, social network phishing is just as grave as its ancestors in the sense that it attacks major groups of web users at once through online community websites. In here, a phisher targets a certain social network like MySpace or Live Journal, planting in those websites some botnets, automatic and autonomous programs run remotely by a hacker. Although there isn't much money involved in social networks, phishers still consider them their pot of gold as it is very easy for them to spread key loggers, programs that can capture every keystroke of the user. Phishers use such networks in order to hopefully capture a home computer that is often used to shop online or store money via online banks. Further, most of the people in social networks use the same password for any and almost every account they have in the Internet universe, including their e-mail addresses where most confirmation messages for online transactions are stored. That and the fact that key loggers can acquire passwords are enough warnings for amateur people who use the web for transactions. Other typical social networks that phishers target are bulletins, forums, commentary, and profile websites. Spear phishers actually need three things in

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

order to execute an attack to an organization: (1) an identity of somebody within the organization, preferably a person with high authority to make the attack convincing, (2) wide knowledge about the company's transactions and daily activities to back up the validity of the phish, and (3) a seemingly valid and well-researched reason for requesting confidential data like the PayPal account of one of the company's departments. If these three are already available to the phisher, then the spear phishing comes to actuality, as described below.

J. STEPS TO PREVENT PHISHING

The best way to learn to spot phishing emails is to study examples captured in the wild! This webinar from Cyren starts with a look at a real live phishing website, masquerading as a PayPal login, and tempting victims hand over their credentials. Check out the first minute or so of the video to see the telltale signs of a phishing website.More examples can be found on a website maintained by Lehigh University's technology services department where they keep a gallery of recent phishing emails received by students and staff. There also are a number of steps you can take and mindsets you should get into that will keep you from becoming a phishing statistic, including:
(a) Always check the spelling of the URLs in email links before you click or enter sensitive information.
(b) Watch out for URL redirects, where you're subtly sent to a different website with identical design.
(c) If you receive an email from a source you know but it seems suspicious, contact that source with a new email, rather than just hitting reply.
(d) Don't post personal data, like your birthday, vacation plans, or your address or phone number, publicly on social media.
(e) If you work in your company's IT security department, you can implement proactive measures to protect the organization, including:
(f) "Sandboxing" inbound email, checking the safety of each link a user clicks.
(g) Inspecting and analyzing web traffic.
(h) Pen-testing your organization to find weak spots and use the results to educate employees.
(i) Rewarding good behavior, perhaps by showcasing a "catch of the day" if someone spots a phishing email.

III. LITERATURE SURVEY

L. Wenyin et al(2005) [1] proposed Phishing detection systems are principally based on the analysis of data moving from phishers to victims. In this paper we describe a novel approach to detect phishing websites based on analysis of userspsila online behaviours - i.e., the websites users have visited, and the data users have submitted to those websites. Such user behaviourscan not be manipulated freely by attackers; detection based on those data can not only achieve high accuracy, but also is fundamentally resilient against changing deception method.

P. Stavroulakis et al(2010)[2] demonstrated that Phishing is a new type of network attack where the attacker creates a replica of an existing Web page to fool users (e.g., by using specially designed e-mails or instant messages) into submitting personal, financial, or password data to what they think is their service providers' Web site. In this paper, we propose a new end-host based antiphishing algorithm, which we call LinkGuard, by utilizing the generic characteristics of the hyperlinks in phishing attacks. These characteristics are derived by analyzing the phishing data archive provided by the anti-phishing working group (APWG). Because it is based on the generic characteristics of phishing attacks, LinkGuard can detect not only known but also unknown phishing attacks. We have implemented LinkGuard in Windows XP. Our experiments verified that LinkGuard is effective to detect and prevent both known and unknown phishing attacks with minimal false negatives. LinkGuard successfully detects 195 out of the 203 phishing attacks. Our experiments also showed that LinkGuard is lightweighted and can detect and prevent phishing attacks in real-time.

B. B. Gupta et al(2016)[3] proposed detection of phishing attacks. Phishing attacks target vulnerabilities that exist in systems due to the human factor. Many cyber attacks are spread via mechanisms that exploit weaknesses found in endusers, which makes users the weakest element in the security chain. The phishing problem is broad and no single silver-bullet solution exists to mitigate all the vulnerabilities effectively, thus multiple techniques are often

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

implemented to mitigate specific attacks. This paper aims at surveying many of the recently proposed phishing mitigation techniques. A high-level overview of various categories of phishing mitigation techniques is also presented, such as: detection, offensive defense, correction, and prevention, which we belief is critical to present where the phishing detection techniques fit in the overall mitigation process.

V. M. Gandhimathi et al(2013)[4] proposed that the development of internet comes with the other domain that is cyber-crime. The record and intelligently can be exposed to a user of illegal activity so that it has become important to make the technology reliable. Phishing techniques include domain of email messages. Phishing emails have hosted such a phishing website, where a click on the URL or the malware code as executing some actions to perform is socially engineered messages. Lexically analyzing the URLs can enhance the performance and help to differentiate between the original email and the phishing URL. As assessed in this study, in addition to textual analysis of phishing URL, email classification is successful and results in a highly precise anti phishing.

Y. Zhang et al(2007) [5] proposed that describes a set of innovative attribute based checks for defending against phishing attacks. We explain a number of anti-phishing algorithms implemented as plugins and highlight which attributes of phishing sites they consider.To assess the effectiveness and applicability of this prototype,we performed extensive experimental testing. We present a fully automated crawling framework that we developed for testing,along with the main experimental results.

Y. Li et al(2015) [6] proposed that it is a security attack that involves the creation of websites that mimic legitimate websites, and these fraud websites bring Internet users a lot of loss. Traditional anti-phishing methods usually worked in a passive way by receiving report data of user. Due to the growing shorter survival time of phishing, this kind of methods is not efficient enough to find and take down new phishing attacks. In this paper, we propose an Intelligent Phishing Detection (IPD) system to address phishing detection problem actively. Specially, IPD first generates the detection dataset from the global massive domain name registration data automatically; then it applies the Naïve Bayes algorithm which is optimized by position-based features to achieve the high precision detection; finally, in order to find more phishing websites, IPD expands detection dataset by generating Uniform Resource Locator (URL) templates based on the detection results. The experimental results of IPD demonstrate the effectiveness and timeliness in detection phishing websites.

S. Sheng et al(2009)[6] proposed that an anti-phishing technique based on email extraction and analysis is proposed. The technique approached with phishing email, the channel phishing attack transmits, distinguish phishing emails and extract the suspicious URL from the e-mail for further analysis. Upon arrival, a protected list is built according to those third parties which are the most vulnerable to phishers in order to filter those confusing advertising spams in China and a neural network based model is proposed in order to detecting phishing messages from an e-mail stream. In this anti-phishing technique, email stream captured by our honey pot subsystem from the Internet is parsed into a MIME email firstly, various feathers are extracted from the email and outputted into feather vectors. The feature vectors will be self-organized by ART2 neural network one by one and classified into corresponding categories. Link URLs in the suspected emails' messages will be extracted for further detection in phishing site subsystem. Experiment using collected emails shows a good performance aiming at detecting phishing emails in China while foreign method performs badly in distinguishing phishing emails from spam.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

IV. SYSTEM ANALYSIS

A. *Existing System*

In the existing system, there are three classes of technical methods to identify phishing websites.

(a) Including The Blacklist/ Whitelist Methods
These methods has to maintain a list of phishing websites using a manual/automatical update process managing the blacklist/whitelist database is inefficient for both the local database and the cloud database due to the rapidly increasing number of phishing sites.

(b) The Web Structure-Based Methods
This approach is based on 15 features web pages, including URL features and content features, which are expensive during the analysis. When a user requests a web page, the classifier determines whether that page is a phishing site. This approach can detect new phishing sites and temporary phishing sites because it extracts features from the requested web page.

(c) The Web Content-Based Methods
Certain page-ranking features to identify phishing web pages by using the Google Page Rank value. However, using only the PageRank value is insufficient to identify phishing URLs due to many phishing websites are created on popular websites such as blogs or Google sites, where the ranking features (e.g., domain age) are not useful for phishing identification. New URLs have low ranking values that are similar to phishing URLs.

DISADVANTAGES OF EXISTING SYSTEM

(a) Difficult to apply in real-time Detection
(b) Preventing phishing attacks against terminal users is a critical issue in the edge of networks

B. *Proposed System*

Phishing detection is recognized as a criminal issue of Internet security. By deploying a gateway anti-phishing in the networks, these current hardwarebased approaches provide an additional layer of defense against phishing attacks. However, such hardware devices are expensive and inefficient in operation due to the diversity of phishing attacks. With promising technologies of virtualization in fog networks, an anti-phishing gateway can be implemented as software at the edge of the network and embedded robust machine learning techniques for phishing detection. In this paper, we use uniform resource locator (URL) features and web traffic features to detect phishing websites based on a designed Adaptive Neuro-Fuzzy InferrenceSystem(ANFIS). Based on the new approach, fog computing as encouraged by Cisco, we design an anti-phishing model to transparently monitor and protect fog users from phishing attacks. Here, author use famous ranking systems to identify phishing sites. They look similar; however, combining them can improve the accuracy of detection due to the following reason. First, with new URLs that have just been created, Google Index system returns empty values, while others can compensate with positive values. Second, Google Index is not a ranking system, but it owns huge dataset and trusted results. This combination reflects exactly the lifetime of URLs. Other features, such as special characters in URLs or the number of dots, the length of URL, can be used to detect phishing websites, but they are really specific, and attackers can replace or fake them easily. In this work, we focus on detecting phishing attacks in real time. Hence, the system has less time to analysis and makes a decision. Therefore, we do not select identification features that cannot analyze in real time. The identification component is integrated on a fog node and interacts with fog users. It contains a ANFIS network that is already trained to classify URLs into two classes: the phishing URL class and the legitimate URL class. There is a connection between these components to update trained parameters of the ANFIS network. This step does not spend large network traffic or time consumption to update the phishing database compared to the blacklist method (the network traffic measurement is discussed later. Further, the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

training procedure can be invoked and adjusted easily by administrators in the back-end component. Finally, the training phase and updating phase do not impact the identification phase in a fog node.

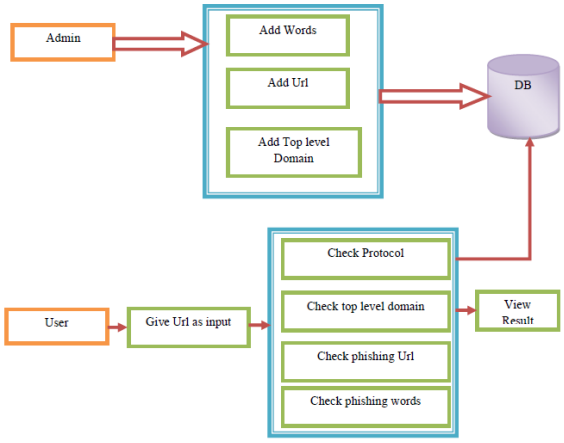

Fig.6System Architecture Design

This weight can be based on a Gaussian distribution. Crucially, the weights depend not only on Euclidean distance of pixels, but also on the radiometric differences (e.g., range differences, such as color intensity, depth distance, etc.). This preserves sharp edges.The bilateral filter is defined as the filtered image. As the range parameter or increases, the bilateral filter gradually approaches Gaussian convolution more closely because the range Gaussian widens and flattens, which means that it becomes nearly constant over the intensity interval of the image.

ADVANTAGES OF PROPOSEDSYSTEM

It is based on a large scale dataset collected from real phishing cases, have shown that our system can effectively prevent phishing attacks and improve the security of the network. The fuzzy network is also used in the field of Artificial Intelligence.

V. RESULTS AND DISCUSSION

In this section, we provided the simulated results of entire project with its practical proofs. The following figure shows the Homepage perspective of the Proposed System.

Fig.7Home Page

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

The following figure illustrates the User Login Pageof the proposed system.

Fig.8User Login Page

The following figure illustrates the Registration Pageof the proposed system.

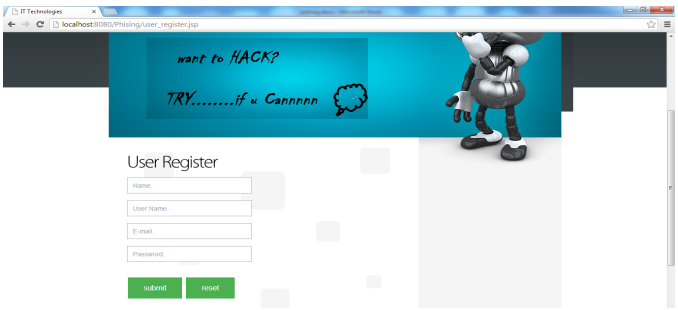

Fig.9Registration Page

The following figure illustrates the URL Authentication View of the proposed system.

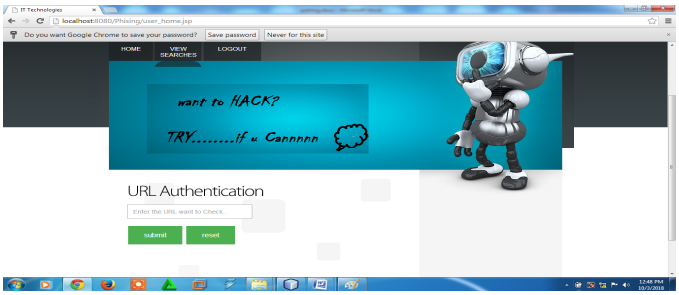

Fig.10URL Authentication

The following figure illustrates the View of blacklisted URLs of the proposed system.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

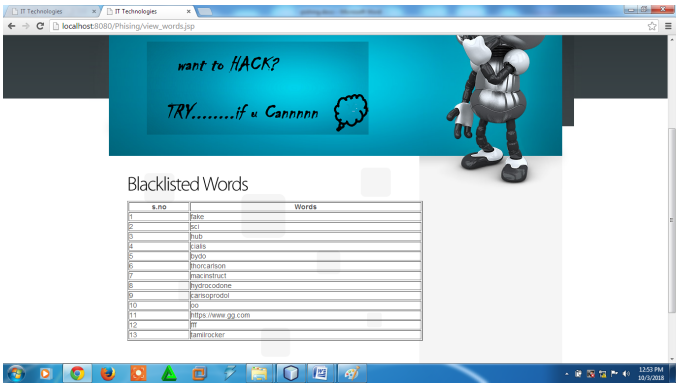

Fig.11 Blacklisted URLs

The following figure illustrates the View of Phishing Identification of the proposed system.

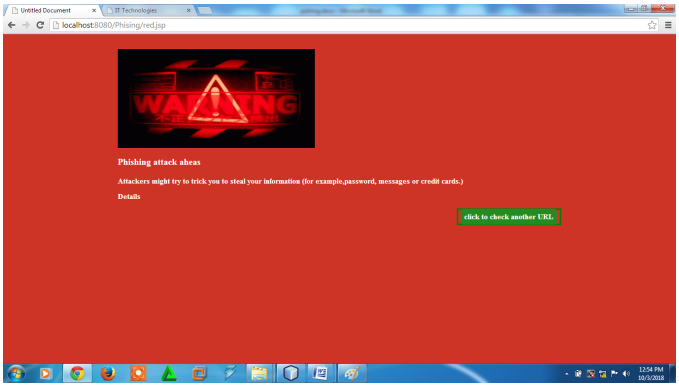

Fig.12 Phishing Identification

VI. CONCLUSION AND FUTURE SCOPE

This paper analyzed phishing e-web-form sources to identify and extract effective features to classify and detect emerging phishing websites. These features were used based on ANFIS algorithms. These features are specific to the main sensitive information that attackers acquire from users. The intelligent phishing security approach obtained promising results which demonstrates effectiveness of phishing e-web-form and feature model to classify and detect phishing websites with a higher accuracy. This is the first study to use phishing e-web-form framework, which is a source for effective features that has demonstrated effectiveness to detecting emerging phishing attacks accurately. Our simulation results indicate that the efficiency of phishing identification after training with the training dataset by improving the average accuracy to 98.36% and reducing the missed detection and false alarm rates to 0.9% and 0.74 %, respectively. We also compare our approach with current methods [17], [20] and [24] to evaluate our model. Simulation results show that our method is more efficient, stable and accurate. Especially, various testing results indicate that our model in a fog computing environment is not only possible, but also can be applied practically.

In future, the proposed work is further extended by means of some intensive algorithms such as Artificial Neural Classification (ANC) Algorithms with powerful authentication strategies and has a plan to improve the accuracy range higher than the proposed system.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

REFERENCES

[1] L. Wenyin, G. Huang, L. Xiaoyue, X. Deng, and Z. Min, "Phishing web page detection," in Document Analysis and Recognition, 2005. Proceedings.Eighth International Conference on. IEEE, pp. 560–564.
[2] P. Stavroulakis and M. Stamp, Handbook of Information and Communication Security, 1st ed. Springer Publishing Company, Incorporated, 2010.
[3] Anti-phishing working group. Accessed Sept 2016.[Online]. Available: http://www.antiphishing.org.
[4] Mobile marketing statistics. Accessed Mar, 2017.[Online]. Available: http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/
[5] Phishing attacks. Accessed Sept 2015.[Online]. Available: https://securityintelligence.com/
[6] Y. Zhang, J. I. Hong, and L. F. Cranor, "Cantina: a content-based approach to detecting phishing web sites," in Proceedings of the 16th international conference on World Wide Web. ACM, 2007, pp. 639–648.
[7] PhishTank. Accessed Nov 2015.[Online]. Available: http://www.phishtank.com/stats/2014/01/
[8] S. Sheng, B. Wardman, G. Warner, L. F. Cranor, J. Hong, and C. Zhang, "An empirical analysis of phishing blacklists," in Proceedings of Sixth Conference on Email and Anti-Spam (CEAS), 2009.
[9] V. M. Gandhimathi K1, "Identifying similar web pages using scoring methods for web community mining," in Proc. of Int. Conf. on Advances in Computer Science, AETACS, 2013.
[10] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: state of the art and future challenges," in Neural Computing and Applications, 2016.
[11] Apwg reports. [Online]. Available: http://docs.apwg.org/reports/
[12] Fog computing and the internet of things: Extend the cloud to where the things are. [Online]. Available: http://www.cisco.com/c/dam/en us/solutions/trends/iot/docs/computing-overview.pdf
[13] Y. Li and M. Chen, "Software-Defined Network Function Virtualization: A Survey," IEEE Access, vol. 3, pp. 2542–2553, 2015.
[14] Real time anti-phishing. Accessed on Sept 2016.[Online]. Available: http://www.brightcloud.com/services/real-time-anti-phishing.php
[15] Anti Spam Hardware. Accessed Sept 2016.[Online]. Available: http://www.windowsnetworking.com/hardware/Anti-Spam-Hardware/modusGate-Anti-Spam-Appliance.html
[16] Security Intelligence Blacklisting. Accessed Sept 2016.[Online]. Available: https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Security Intelligence Blacklisting.pdf
[17] N. Zhang and Y. Yuan, "Phishing detection using neural network, cs229 lecture notes." [Online]. Available: http://cs229.stanford.edu/proj2012/ZhangYuan-PhishingDetectionUsingNeuralNetwork.pdf,2012
[18] G. Xiang, J. Hong, C. P. Rose, and L. Cranor, "Cantina+: a feature-rich machine learning framework for detecting phishing web sites," ACM Transactions on Information and System Security (TISSEC), vol. 14, no. 2, pp. 1–28, 2011.
[19] Vulnerability in spotify android-app. Accessed on Sept 2015. [Online]. Available: http://blog.trendmicro.com/trendlabs-security-intelligence/vulnerability-in-spotify-android-app-may-lead-to-phishing/
[20] Google safe browsing. Accessed Sept 2016.[Online]. Available: https://safebrowsing.google.com/
[21] N. Abdelhamid, "Multi-label rules for phishing classification," Applied Computing and Informatics, vol. 11, no. 1, pp. 29 – 46, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2210832714000210
[22] W. Hadi, F. Aburub, and S. Alhawari, "A new fast associative classification algorithm for detecting phishing websites," Applied Soft Computing, vol. 48, pp. 729 – 734, 2016.[Online]. Available: http://www.sciencedirect.com/science/article/pii/S1568494616303970 [23] L. . T. C. James, J. ; Sandhya, "Detection of phishing urls using machine learning techniques," in Control Communication and Computing (ICCC), 2013 International Conference on, 2013, pp. 304–309.
[24] M. Aburrous, M. A. Hossain, K. Dahal, and F. Thabtah, "Intelligent phishing detection system for e-banking using fuzzy data mining," Expert systems with applications, vol. 37, no. 12, pp. 7913–7921, 2010.
[25] A. N. V. Sunil and A. Sardana, "A pagerank based detection technique for phishing web sites," in Computers & Informatics (ISCI), 2012 IEEE Symposium on. IEEE, 2012, pp. 58–63.
[26] R. Verma and K. Dyer, "On the character of phishing urls: Accurate and robust statistical learning classifiers," in Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, ser. CODASPY '15. New York, NY, USA: ACM, 2015, pp. 111–122.
[27] L. Wenyin, G. Liu, B. Qiu, and X. Quan, "Antiphishing through phishing target discovery," IEEE Internet Computing, vol. 16, no. 2, pp. 52–61, March 2012.
[28] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, Fog Computing: A Platform for Internet of Things and Analytics. Springer International Publishing, 2014, pp. 169–186.
[29] IoT, from cloud to fog computing. Accessed Sept 2015.[Online]. Available: http://blogs.cisco.com/perspectives/iot-from-cloud-to-fog-computing
[30] J. Shropshire, "Extending the cloud with fog: Security challenges & opportunities," in Information Systems Security, Assurance, and Privacy Track Conference, 2014.