An Anti-phishing Method Base on 2-Steps Fuzzy System

Ali Sadeghi Mobarakeh[1], Seyed Javad Mirabedini[2], Ali Haroonabadi[3]
[1]M.S.C student, Department of Computer Science, Islamic Azad University, Bushehr, Iran
[2,3]Department of Computer Science, Tehran Central Unit, Islamic Azad University, Tehran, Iran

Abstract: Phishing is a type of social engineering activity which is used to deceive user, to acquire their personal information like credit card numbers, social security numbers, passwords etc., by illegal ways. A lot of cyber attacks are done through weaknesses in the system and their end-users as the weakest element in the chain is the safety of the operation. In this paper we use a hybrid model by combination of content based and non content based features. The selected features classified in three classes and use the fuzzy system to determine the risk of each class. Then use the output for final fuzzy inference system. the fuzzy system to provide best result of positive alarm and reduce false negative alarm of phishing detection. We used phishtank dataset with 2100 record of phishing urls to test our system. Also used the dataset for genuine web pages collected from google search engine Our experiments show that our method is good at detecting phishing sites, correctly labeling approximately 98% of phishing sites and only 2% of false negative alarm of phishing detection.

Keywords: anti phishing, phishing, fuzzy, social engineering.

Introduction

Phishing is a type of social engineering activity which is used to deceive user, to acquire their personal information like credit card numbers, social security numbers, passwords etc., by illegal ways. A lot of cyber attacks are done through weaknesses in the system and their end-users as the weakest element in the chain is the safety of the operation. The word phishing came from the word "fishing", by replacing the letter "f" with "ph" to make it a new word, which represents the act of deceiving users by faked e-mails or websites in order to steal their personal information[1,2]. A phishing technique was described in detail in 1987, and the first use was made in 1996.

According to the reports of AntiPhishing Working Group[3], the number of phishing attacks is increasing by monthly(Figure 1) and they can usually convince of the phishing email recipients to respond to them. By providing Internet transaction operations, it is the obligation of the companies to keep it safe. The companies may be expected to shoulder the responsibility, take the initiatives to go out to actively detect those phishing emails land phishing websites, and then prevent potential phishing attacks.

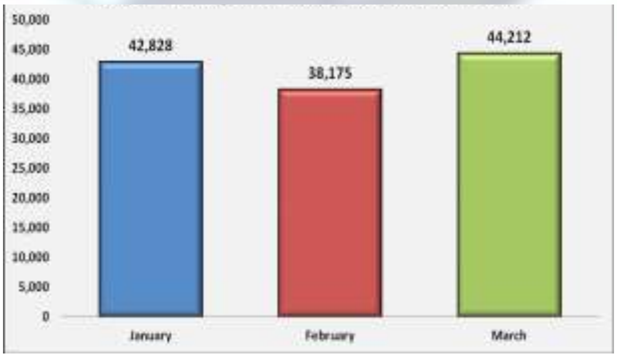


Figure 1: Unique phishing site detected January-March 2014[3]

According to the literature, in phishing attacks, a site is crafted to closely mimic the look and feel of the legitimate site in a way that the users can't distinguish the forged faked website from the original legitimate one and are lured into divulging their personal information. Despite the effort of phishers to build a completely similar website, there are some features and clues which can differentiate the phishing site from the original site.

Designing any system which would be capable of detecting phishing websites requires list of all phishing characteristics. Identifying the critical phishing indicators is really vital due to the importance of considering all effective features in a phishing detector. This list of critical indicators not only should include all important characteristics of phishing sites but also should be concise and precise. Using redundant characteristics in designing phishing detectors results in wasting time and resources and decreases efficiency. In contrast, applying accurate list of phishing indicators will increase efficiency and produce better results in shorter time.

Literature review and related works

Phishing solutions can be broadly classified into four categories [2]. They are:

a) Content based:

Content-based features are mostly derived from the technical (HTML) contents of web pages e.g., counting external and internal links, counting IFRAME tags, and checking whether IFRAME tag‘s source URLs are present in blacklists and search engines, checking for password field and testing how the form data is transmitted to the servers (whether Transport Layer Security is used and whether —GET‖ or —POST‖ method is used to transmit form data with password field), etc.

URLs and domain part of the URLs are checked against top 3 search engines (Google, Yahoo, and Bing) indexes to see if the URLs are indexed. Features also include checking IPs and domain name of the URLs against the top list of IPs and domains historically popular for hosting phishing and other malicious websites. Features also include a list of eye-catching keywords (e.g., log, click, pay, free, bonus, bank, user, etc.) that are more commonly used in phishing URLs to deceive the end users.

b) URL base:

URL-based features include lexical properties of URLs such as counting number of —.‖, —-—, —_‖, etc. in various parts of URLs, checking whether IP address is used and what type of notation is used to represent the IP address in place of a domain name.

c) Visual Similarity:

It impersonates a well-known website by replicating the whole or part of the target site, showing high visual similarity to its target. Most advanced techniques try to distinguish a phishing page from a legitimate page by comparing their visual similarities. The visual similarity between two web pages is then measured. A web page is considered a phishing page if the similarity to the legitimate web page is higher than a threshold.

d) Hybrid:

In this technique multiple features are combined to detect phishing.

In this section we review some previous work done in the field of anti-phishing pay:

CANTINA is a content-based phishing detection algorithm proposed by Zhang et al [4]. This method calculates term frequency-inverse document frequency (TF-IDF) of the content of a website and generates a lexical signature. The generated lexical signature will be used as the keyword to perform web search using Google search engine. The returned result will be used to classify the legitimacy of a website. However, CANTINA performance will be influenced by the language used in the website.

In [5] Phish Zoo technique is implemented , it is a blend of 5 features that is profile making, Profile matching, Image matching using SIFT Running , Phish Zoo in Bulk and Online and offline profile matching. This approach provides similar accuracy to blacklisting approaches (96%), with the advantage that it can categorize zero-day phishing attacks and targeted attacks against smaller sites (such as corporate intranets). A key contribution of this paper is that it includes a recital analysis and a structure for making use of computer vision techniques in a practical way.

In [6] the proposed model is based on FL operators which is used to illustrate the website phishing factors and indicators as fuzzy variables and produces six measures and criteria's of website phishing attack dimensions with a layer structure. fuzzy logic techniques is the use of linguistic variables to represent Key Phishing Characteristic Indicators and relating website phishing possibility .This experimental results showed the significance and importance of the phishing website criteria (URL & Domain Identity) represented by layer one, and the variety influence of the phishing characteristic layers on the final phishing website rate.

Our Method

Evolving with the anti phishing techniques, various phishing techniques and more complicated and hard-to-detect methods are used by phishers. The most straightforward way for a phisher to defraud people is to make the phishing Web pages similar to their targets.

Actually, there are many characteristics and factors that can distinguish the original legitimate website from the forged faked phishing website like using iframe, Long URL address and Abnormal DNS record. The full list is shown in table1 which will be used later on our analysis and methodology study.

Our proposed method consists of three steps to detect phishing attacks. The general structure of the proposed method is shown in Figure 2:

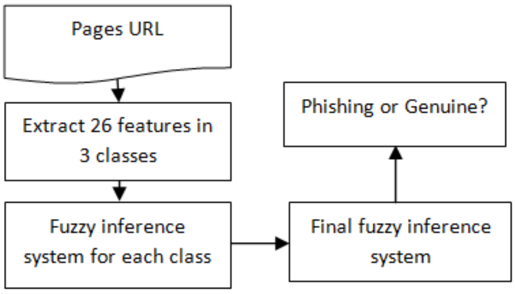

Pages URL
Extract 26 features in 3 classes
Fuzzy inference system for each class
Final fuzzy inference system
Phishing or Genuine?

Figure 2: General structure of the proposed method

1. Feature Extraction

Total of 26 features from Web pages used (include content based and url based features) are shown in the table below (table 1).

Features are extracted in three categories:

- The first category includes Google page ranking and the URL position in Bing search results based on keywords extracted from the webpage.
- The second category includes URL based and content-based features.
- The third set of features are extracted by WHOIS command includes the domain name, and the age of domain.

Table 1: selected features in proposed method

Class	Category	Features
1	Search engine features	Position of URL in Bing search result by keywords of page
		Google page rank
		Alexa rank for page
2	Content based features from source code	Use Copy page
		Number of sensitive words in page like payment, login,…
		Use iframe
		Using External image in page
		Using External JavaScript
		Using pop-up windows
		External link count in CSS
		Redirect count
		Internal URL count in page
		Input box count in page
		Password box count in page
		Submit count in page
		Hidden items count in page
		Spelling error
	URL based features	Using @,- symbol in URL
		URL length
		Replace similar character in URL
		Using IP address in URL
		Using Hex code in URL
		Number of dots in URL
3	Domain Based features	Domain age
		URL exist in same domain
		Certificate exist in same domain

2. Fuzzy Inference System

For each class we calculate the risk of phishing separately. For all fuzzy input, linguistic descriptors such as low, medium, high.

We use three fuzzy inference system to calculate the risk of each class:

- Class 1 fuzzy system is designed which has 3 inputs and one 1 for search engine features.
- Class 2 fuzzy system is designed which has 20 inputs and 1 output for content based and url based features.

- Class 3 fuzzy system is designed which has 3 inputs and 1 output for domain based features.

Our final fuzzy system is designed which has 3 inputs and 1 output. Clipping method is used in aggregation the consequences, and the aggregated surface of the rule evaluation is defuzzified using Mamdani method. The structure of the fuzzy system is described below: (Figure 3):

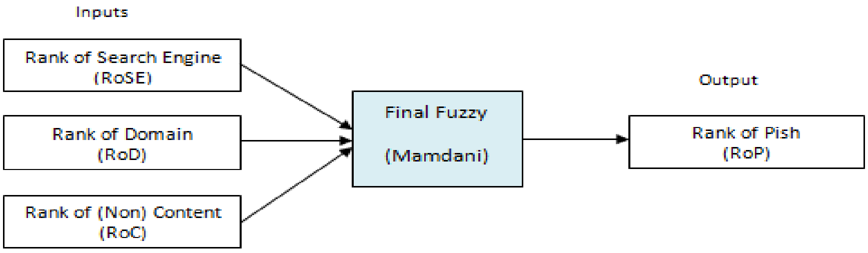


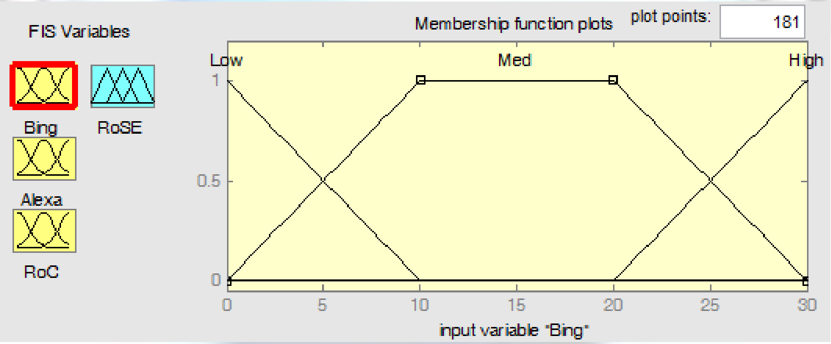
Figure 3: Our fuzzy system

2.1 Fuzzification

In this step, linguistic descriptors such as high, low, medium, for example, are assigned to a range of values for each class characteristic indicator. Valid ranges of the inputs are considered and divided into classes, or fuzzy sets. For example, Rank of domain can range from "low" to "high" with other values in between.

The degree of belongingness of the values of the variables to any selected class is called the degree of membership; membership function is designed for each input from step 2, which is a curve that defines how each point in the input space is mapped to a membership value between [0,1]. Linguistic values are assigned for each input class as low, medium, and high while for phishing website risk rate as genuine, trust, Suspect, Phishing, and Very phishy (triangular and trapezoidal membership function).

For each input, their values range from 0 to 1 while for output, range from 0 to 1. An example of the linguistic descriptors used to represent one of the key phishing characteristic indicators (bing and Rank of Domain) and a plot of the fuzzy membership functions are shown in Figure 4.



plot points: 181

Figure 4(a): Input variable for Bing component in class 1

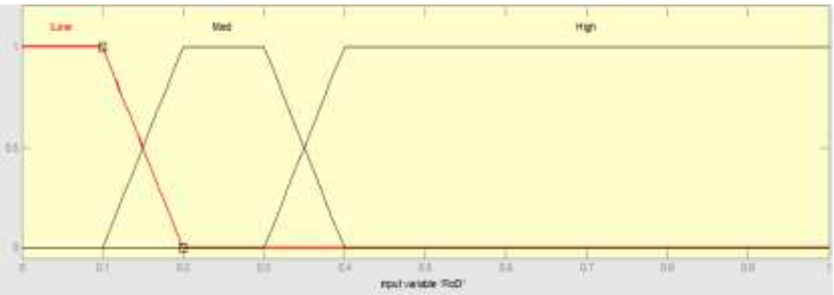


Figure 4(b): Input variable for Rank of Domain (RoD) component.

2.2 Aggregation of the rule outputs:

This is the process of unifying the outputs of all discovered rules.Combining the membership functions of all the rules consequents previously scaled into single fuzzy sets (output).

2.3 Defuzzification

This is the process of transforming a fuzzy output of a fuzzy inference system into a crisp output. Fuzziness helps to evaluate the rules, but the final output has to be a crisp number. The input for the defuzzification process is the aggregate output fuzzy set and the output is a number. This step was done using centroid technique since it is a commonly used method. The output is phishing website risk rate and is defined in fuzzy sets like "very phishy" to "Genuine". The fuzzy output set is then defuzzified to arrive at a scalar value. Plot of the fuzzy output membership functions are shown in below (Figure 5).

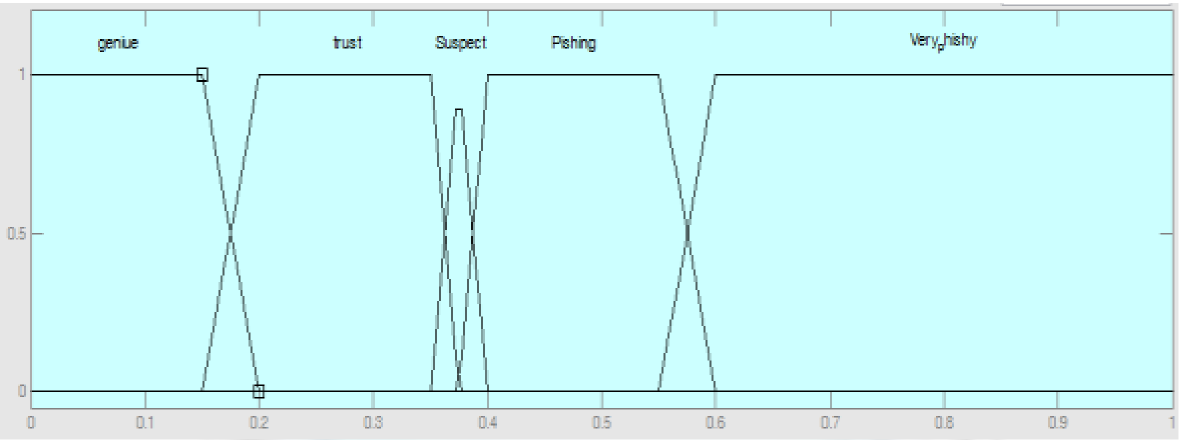


Figure 5: Output variable for Risk of Phishing (RoP) component

2.4 The rule base

2.4.1 The rule base for class1

The rule base has three input parameters and one output and contains all the “IF-THEN” rules of the system. The output of rule base 1 is one of the phishing risk fuzzy sets (Low, High) representing search engine criteria phishing risk rate. A sample of the structure and the entries of the rule base 1 for class 1 are shown in below. The system structure for search engine criteria is the joining of its three components (Google page rank, url position in bing search, alexa rank), which produces the rank of search engine (RoSE).

If (Bing is Low) and (Google is Low) and (Alexa is Low) then (RoSE is Low) (1)
If (Bing is Low) and (Google is Low) and (Alexa is High) then (RoSE is Med) (1)
If (Bing is Low) and (Google is High) and (Alexa is Low) then (RoSE is Med) (1)
If (Bing is Low) and (Google is High) and (Alexa is High) then (RoSE is High) (1)
If (Bing is High) and (Google is Low) and (Alexa is Low) then (RoSE is Med) (1)
If (Bing is High) and (Google is Low) and (Alexa is High) then (RoSE is High) (1)
If (Bing is High) and (Google is High) and (Alexa is Low) then (RoSE is High) (1)
If (Bing is High) and (Google is High) and (Alexa is High) then (RoSE is High) (1)

2.4.2 The rule base for class2

The rule base has 20 input parameters and one output and contains all the “IF-THEN” rules of the system. The output of rule base 2 is one of the phishing risk fuzzy sets (Low, Med, High) representing content based & URL based phishing risk rate. A sample of the structure and some entries of the rule base 2 for class 2 are shown in below. The system structure for content based & URL based criteria is the joining of its 20 components (Using Iframe, URL lenght, Use ip address ,Using text input , etc), which produces the rank of Content (RoC).

If (Url_lengh is low) and (Dots_in_url is low) and (use@symbol is No) then (RoC is Low) (1)
If (Url_lengh is med) and (Dots_in_url is med) and (use@symbol is Yes) then (RoC is High) (1)
If (Url_lengh is high) and (Dots_in_url is high) and (use@symbol is No) then (RoC is High) (1)
If (Url_lengh is med) and (Dots_in_url is high) and (use@symbol is No) then (RoC is Med) (1)

2.4.3 The rule base for class3

The rule base has three input parameters and one output and contains all the “IF-THEN” rules of the system. The output of rule base 3 is one of the phishing risk fuzzy sets (Low, Med, High) representing Domain criteria phishing risk rate. A sample of the structure and the entries of the rule base 3 for class are shown in below. The system structure for Domain criteria is the joining of its 3components (Age of domain, URL in same Domain, Certificate in Domain), which produces the rank of Domain (RoD).

If (Age is low) and (Url_in_Domain is Yes) and (Cer_in_domain is Yes) then (RoC is Low) (1)
If (Age is med) and (Url_in_Domain is Yes) and (Cer_in_domain is Yes) then (RoC is Low) (1)
If (Age is high) and (Url_in_Domain is Yes) and (Cer_in_domain is Yes) then (RoC is Med) (1)
If (Url_in_Domain is No) then (RoC is High) (1)
If (Cer_in_domain is No) then (RoC is High) (1)

2.4.4 The rule base for final phishing risk

The rule base has 27 input parameters and one output and contains all the "IF-THEN" rules of the system. The structure and the entries of the Rule base are shown in Table 2.

Table2: The Rule base structure and entries for final fuzzy

	RoSE	RoD	RoC	RoP
1	Low	Low	Low	Genuine
2	Low	Low	Med	Genuine
3	Low	Low	High	Trust
4	Low	Med	Low	Trust
5	Low	Med	Med	Suspect
6	Low	Med	High	Phishing
7	Low	High	Low	Suspect
8	Low	High	Med	Suspect
9	Low	High	High	Phishing
10	Med	Low	Low	Trust
11	Med	Low	Med	Suspect
12	Med	Low	High	Suspect
13	Med	Med	Low	Suspect
14	Med	Med	Med	Suspect
15	Med	Med	High	Phishing
16	Med	High	Low	Phishing
17	Med	High	Med	Phishing
18	Med	High	High	Very Phishy
19	High	Low	Low	Suspect
20	High	Low	Med	Suspect
21	High	Low	High	Phishing
22	High	Med	Low	Suspect
23	High	Med	Med	Phishing
24	High	Med	High	Phishing
25	High	High	Low	Phishing
26	High	High	Med	Very Phishy
27	High	High	High	Very Phishy

Experimental Results

For experiment our method we used standard dataset from phishtank [7] that contain 2100 records of phishing urls. Also prepared one dataset of genuine urls form google search involved 100 urls of online ebanking, login pages, payment services, etc.

We defined RPD as Rate of phishing detection and RFD as Rate of false detection to evaluating the purpose method. Also we calculated the True Positive (TP) and False Negative (FN) alarms for each result from datasets.

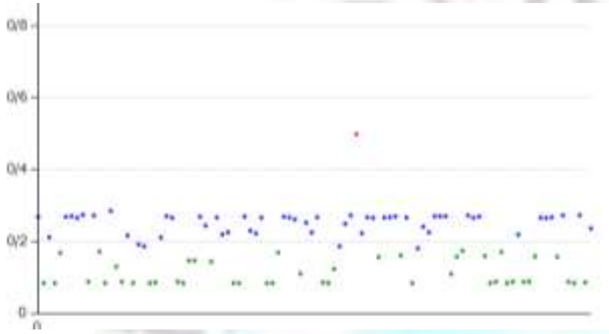
$$RPD = \frac{TP}{Total\ Records} \qquad (1)$$

$$RFD = \frac{FP}{Total\ Records} \qquad (2)$$

a) Running test on the genuine dataset:

After running the system on the genuine pages dataset, results shown that our method detect 99% of genuine urls and 1% of false alarm (Figure 6).

TP = Genuine + Trust = 44+55=99
FN = Suspect + Phishing + Very phishy = 1+0+0=1
RPD = 99%
RFD = 1%



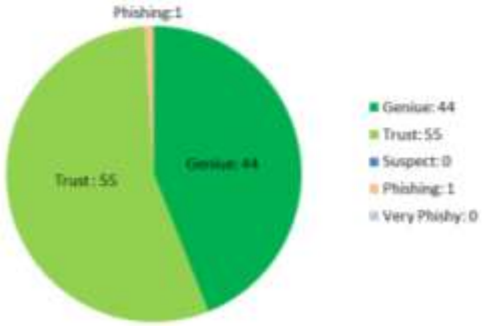


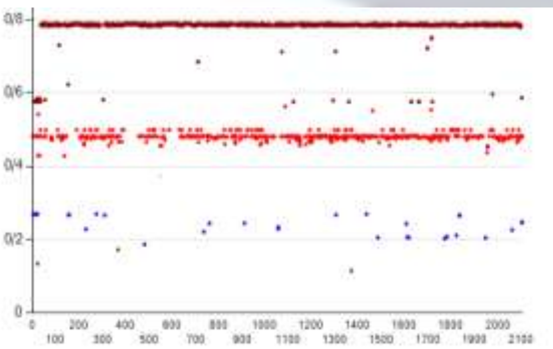
Figure 6(a) : Result for Genuine dataset

Figure 6(b): Clustering result in Geniune dataset

b) Running test on the phishing dataset:

After running the system on the phishing dataset , results shown that our method detect 98% of phishing urls and 2% false alarm(Figure 7).

TP= Suspect + Phishing+Very phishy = 1410+657=2067
FN= Genuine + Trust+Suspect = 3+34+1=38
RPD = 98%
RFD = 2%



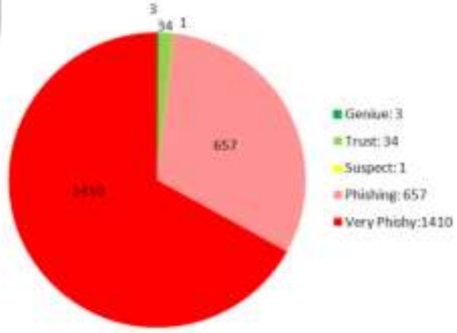


Figure 7(a): result for Phishtank dataset

Figure 7(b): clustering result in phishtank dataset

c) Evaluation of purpose method

Our proposed method is compared with other tools[8] and existing methods[4,5,6,9,10,11] that show it below (Figures 8,9).

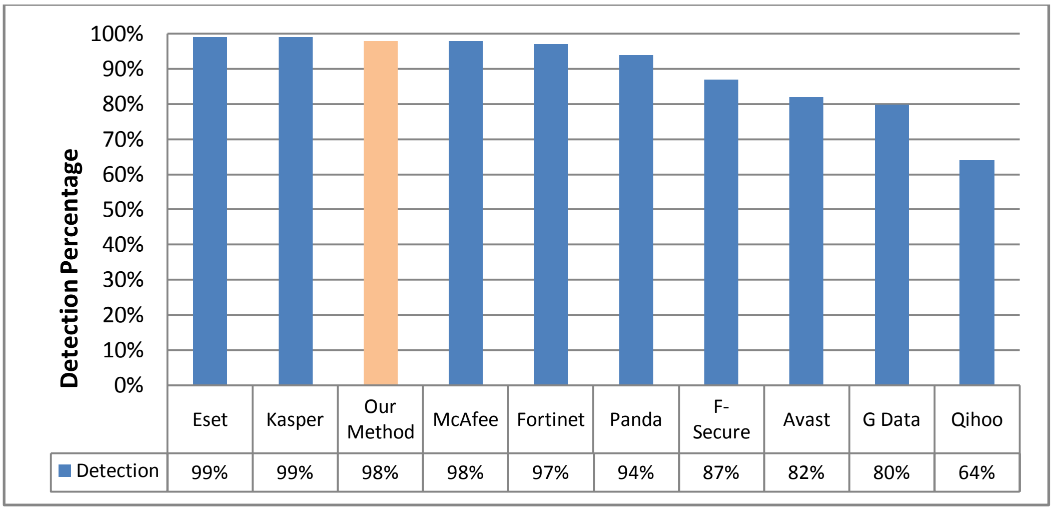


Figure 8: Compare our method with the other antiphishing tools[8]

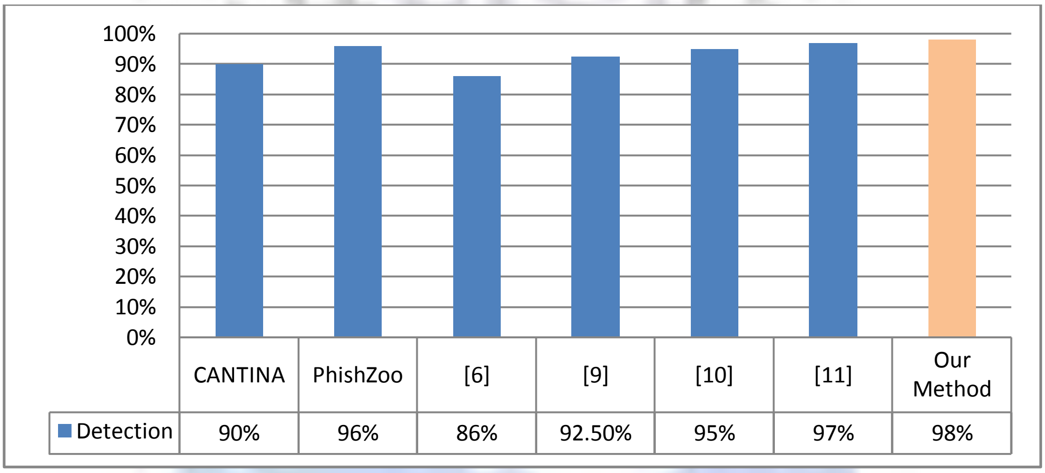


Figure 9: Compare with the Performance of other methods

Conclusion

We use a hybrid model by combination of content-based and non content based features. The selected 26 features classified in three classes and use the fuzzy system to determine the risk of each class. Then use the output for final fuzzy inference system. the fuzzy system to provide best result of positive alarm and reduce false negative alarm of phishing detection. We used phishtank dataset with 2100 record of phishing urls to test our system. Also used the dataset for genuine web pages collected from google search engine Our experiments show that our method is good at detecting phishing sites, correctly labeling approximately 98% of phishing sites and only 2% of false negative alarm of phishing detection.

We are not convinced that we have used the best feature sets and we think that there is more work to be done in this area. Moreover, there are number of emerging technologies that could greatly assist phishing classification that we have not considered. However, we believe that using features such as those presented here can significantly help with detecting this class of phishing websites.

References

[1]. Khonji M, Iraqi Y, Jones (2013). A Phishing Detection: A Literature Survey. IEEE communications surveys & tutorials. Vol 15, No 4 , 1-31.

[2]. Minal Chawla,Siddarth Singh Chouhan. (May 2014). A Survey of Phishing Attack Techniques. International Journal of Computer Applications. Vol 93 , No 3, 32-35.

[3]. Phishing Activity Trends Report, 1st Quarter 2013. Available:http://apwg.org/resources/apwg-reports/ Phishing Attack Trends Report - 1Q2014.pdf.

[4]. Zhang Y, Hong J, Cranor L F (2007). CANTINA: a Content-based Approach to Detecting Phishing Web Sites. In Proceedings of the 16th international conference on World Wide Web. ACM , 639-648.

[5]. Sadia AFROZ, GREENSTADT, Rachel (2011) . Phishzoo: Detecting Phishing Websites by Looking at Them. Semantic Computing (ICSC), 2011 Fifth IEEE International Conference on. IEEE. 368-375.

[6]. Aburrous Maher, Adel Khelifi (2013). Phishing Detection Plug-In Toolbar Using Intelligent Fuzzy Classification Mining Techniques .The International Journal of Soft Computing and Software Engineering. Vol 3, No 3, 54-61.

[7]. Phishtank dataset. Available: http://data.phishtank.com/data/online-valid.csv.

[8]. AV-comparatives anti-Phishing test july 2013, Available: http:// www.av-comparatives.org/wpcontent/uploads/2013/08/avc_aph_201308_en.pdf.

[9]. Chang E H , Chiew K L , Sze S N , Tiong W K. (2013). Phishing Detection via Identification of Website Identity. In IT Convergence and Security (ICITCS), 2013 International Conference on ,1-4.

[10]. Jun Ho Huh, Hyoungshick Kim (2011). Phishing Detection with Popular Search Engines: Simple and Effective, FPS 2011, LNCS 6888, pp. 194–207, 2011.

[11]. Nguyen, L. A. T., To, B. L., Nguyen, H. K., & Nguyen, M. H. (October 2013). Detecting Phishing Web Sites: A Heuristic URL-based Approach. In Advanced Technologies for Communications (ATC), IEEE, International Conference on, pp. 597-602.