An Efficient Detection and Isolation of Phishing Attacks using Customized Hidden Markov Model based False Prediction

S. Edwin Raja[1], Dr. R. Ravi[2]

[1] Assistant Professor, P.S.R Engineering College, Tamilnadu, India

edwinrajas@gmail.com

[2] Professor, Francis Xavier Engineering College, Tamilnadu, India

fxhodcse@gmail.com

Abstract: Providing security for web pages against various web-based attacks is a challenging task. The web–based attacks are motivated to harm web activities or to steal web contents. The attacks like phishing, SQL injection, password cracking, and cookies tracking are considered as web-based attacks. In these attacks, phishing is noted as a very serious threat to web pages. Phishing is the unauthorized attempt to observe crucial information like login identifiers, usernames and passwords. This attack's serious impact goes into the web pages which deal with debit card details, credit card details and internet banking. Due to this kind of attack, the entire trust on web pages goes down. This work proposes a novel trust based phishing attack identification and isolation on web pages. These page data trustworthy and false levels are predicted using Hidden Markov Model (HMM).

1. Introduction

The phishers are the people doing malicious activities on web pages by creating phishing web pages. They create fakes of genuine web pages, to snip parties' sensitive private information relevant data such as bank details, account passwords, cash card numbers, and other business data. Careless web users are effortlessly misled by these phishing web pages since of their extraordinary resemblances to the real web pages. The Anti-Phishing Working Group (APWG) testified that there are at minimum 55,700 phishing attacks between January and June 2009. The modern statistics show that phishing ruins a major unlawful activity comprising great losses of money and private data.

Efficient detection of phishing web pages has concerned ample attention from security providers, financial sectors and also researchers. The phishing attack detection techniques are differentiated as web content-based anti-phishing technique, user interface oriented anti-phishing technique and customized toolbar oriented anti-phishing technique. Nowadays, the phishing attack detection strategy has steps of authentication, attack root trace, analysis, report generation and event filtering technique. These anti-phishing internet facilities are built into respective servers and toolbars of web browsers. In web content-based anti-phishing technique, the features of web pages like surface plane properties, textual and

visual contents are evaluated to avoid harmful web pages [1]. Figure 1.1 shows the nature of phishing information flow.

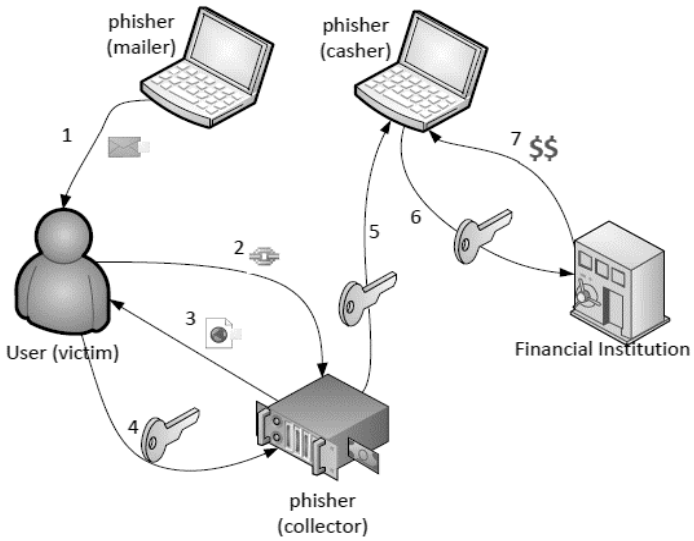

Figure 1.1 Phishing attack scenario

Many research works focus on the development of three basic components (toolbars and warning modules) and the deployment of a well-defined anti-phishing environment. To deploy an efficient anti-phishing environment, this work creates different lists for the identification of authorized and unauthorized textual/visual contents. The HMM is used to identify observed and unobserved false details of the page to remove phishing sites.

2. Related Works

To develop this proposed work many existing anti-phishing techniques are surveyed. The industrial amenities lag to know all phishing attacks. Wu et al. have led the detailed analysis of the effectiveness of anti-phishing toolbars. They have three security concern toolbars and other browser security pointers. The study designates that all inspected toolbars are unsuccessful to prevent web pages from effective phishing attacks [2].

In this connection, Cranor et al. [3] have done an alternative study on an assessment of 10 anti-phishing apparatuses. They have specified that solitary tool reliably detects more than 60% of phishing websites deprived of a high rate of false positives. Separately from these studies on the efficiency of anti-phishing toolbars, Li et al. [4] have explored the suitability of five emblematic anti-phishing toolbars. They have found that the main interface of the

toolbar, warning system, and help system should be well calculated for the identification of phishing attack. In this manner, this work has concluded that the need for the separate list to classify the web activities.

Lately, Aburrous et al. [5] have established a robust model by using a fuzzy logic approach. This is used to enumerate and qualify the website features with a layered structure. Finally, this model sets a kind of web rate for phishing nature. The idea of visual content validation for phishing detection is presented by Liu et al. [6]. This method has Documentary Object Model (DOM)-based visual resemblance of web pages.

Fu et al. [7] have followed another method to compute the visual resemblance of web pages. They have transformed web pages into small images. Then they have engaged the earth mover's distance technique to calculate the resemblance of images. This method examines phishing detection at the pixel level deprived of the text level. Apart from these methods, content-based approaches for detecting phishing emails have also been extensively studied for designing and developing the proposed work. Most of the existing systems are equipped with conventional data fusion technique, Bayesian approach and simple image classifiers which are insufficient to maintain the web pages free from phishing attackers. Thus the need for proposed work is inevitable to identify and predict the different types of data patterns of phishing attacks.

3. Proposed System

The proposed system is designed to achieve certain vital goals against phishing attacks.

- Extract the characteristics that are used by the users to access a web page or to connect to other web pages.
- Extract textual content defined as the terms or words that appear in a given web page, except for the stop words.
- Visual content refers to the characteristics with respect to the overall style, the layout, and the block regions including the logos, images, and forms.
- Then combine the results from the text classifier and the image classifier and check with a threshold.
- Use HMM for detecting clear and unclear variations between legitimate websites and phishing sites.

There are several feature extractors are involved in this figure. They are text and image feature extractors. According to the evaluation of web pages, they are maintained either at white or blacklists. Additionally, anti-phishing proxy server and secure data server are maintained at a top level. The HMM is used in the position of the server for high-level computation.HMM evidently separates genuine and false data items of web pages [8] [9].

The following figure 3.2 shows HMM for false data computation (observable and unobservable data).In this figure 3.2, V1 to VN are false rate variances denotes phishing data patterns. According to that, the trust probabilities are provided for effective detection of phishing attacks.

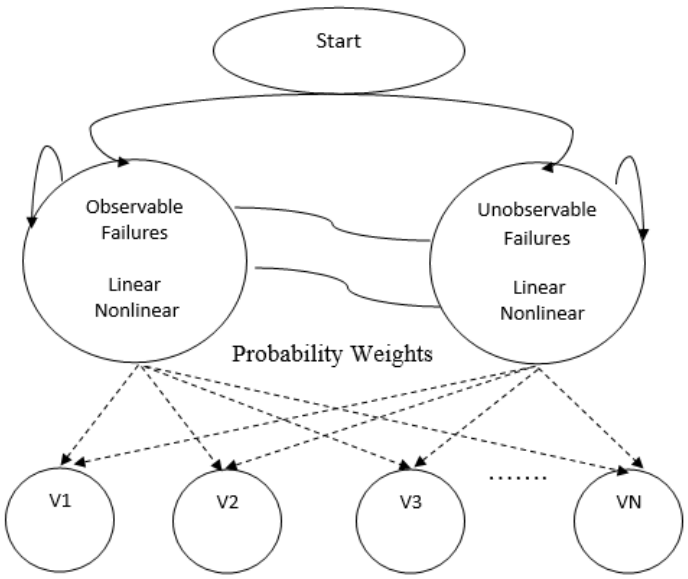

Figure 3.2 HMM for false variances identification

3.1 Algorithm: HMM based Anti-Phishing

Input: 'n' web pages; **Output:** True page lists and False page lists

---

Step 1: Initiate HMM, H(M)=W(P)+T(P)+U(P);

Where, W(P)-Web page contents; T(P)-Observed trained page contents (Available patterns);

U(P)- Unobserved trained page contents (Runtime identification)

Step 2: Execute Support Vector Machine (SVM) routine to classify TX(P) & VI(P);

Where, TX(P)-Textual page contents; VI(P)-Visual page contents

Step 3: Further classify OTX(P), UTX(P), OVI(P) & UVI(P); Observed and Unobserved text and visual data respectively.

Step 4: Form classes C1- OTX(P), C2-UTX(P), C3-OVI(P) & UVI(P) for linear and nonlinear contents

Step 5: Execute HMM weight assignment function, HW(S) on each class sample

Step 6: Initiate binomial probability distribution function, assign probability values for unobserved items.

Step 7: Calculate output values w.r.t legitimate content production rate of web pages.

Step 8: Detect phishing attacks and form white and black lists for web pages (Algorithm 3.2)

3.2 Phishing Attack Detection

Input: Classes C_1, C_2, C_3 and C_4 items

Output: Detection of duplicate items in web page

Step 1: Identify the items of content classes C_1, C_2, C_3 and C_4

Step 2: Extract features of class items.

Step 3: Identify URL items (https://, www, website name, domain name, sub domain name)

Step 4: Check if (DNS resolved IP == Visited DNS IP database)

Step 5: Execute the trace path for 'n' hops between source IP to web server IP.

Step 6: Check if ((Items (C_1 or C_2 or C_3 or C_4)!= Legitimate patterns), declare the item as phishing item.

Check if ((trace path to server IP && DNS lookup!= Null Conflict) declare the item as phishing item.

Step 7: Block the contents and traced path and DNS resolved IP. Create blacklists

---

4. Results

The proposed system has been implemented and the performance is evaluated with 50 web page details (legitimate and phishing attacked). Both textual and visual contents are examined in order to identify false web pages. The evaluated results are given below. Sample web pages details are illustrated table 4.1.

Table 4.1 has the details of legitimate and phishing attack contents for various sites. At maximum PayPal like sites are having maximum phishing contents in all pages. In addition to that figures 4.1 and 4.2 illustrate the details of suspected contents from various websites.

Table 4.1 Detection of phishing attack contents at different websites

Web pages	URLs	Total Contents	Phishing suspected Contents	Legitimate Web Contents
Wiki	https://en.wikipedia.org/wiki/Wiki	9845	1258	8587
Twitter	https://twitter.com/login?lang=en	10452	1248	9204
Paypal	https://www.paypal.com/in/signin	11436	2587	8849
ICICI	https://www.icicibank.com/	8965	998	7967
Psrec	https://www.psr.edu.in	4596	958	3638
Yahoo mail	https://login.yahoo.com/	10456	2120	8336

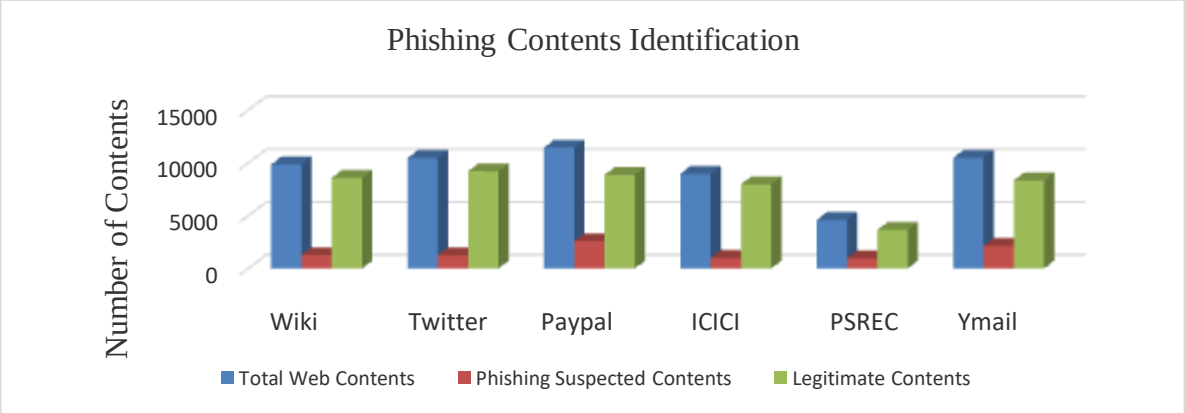

Figure 4.1 Detection of phishing attack contents at different websites

This HMM-based phishing content detection process also finds unobserved contents (text or images). This means that the similarity level cannot be determined always in the detection of phishing attack. The HMM observes both recognized and hidden or likely suspected contents as malfunctioned contents. The HMM can be applied over various similarity measurement parameters like (Web contents, events, attributes of network parameters etc). In this work, the HMM is applied over the contents of several websites.

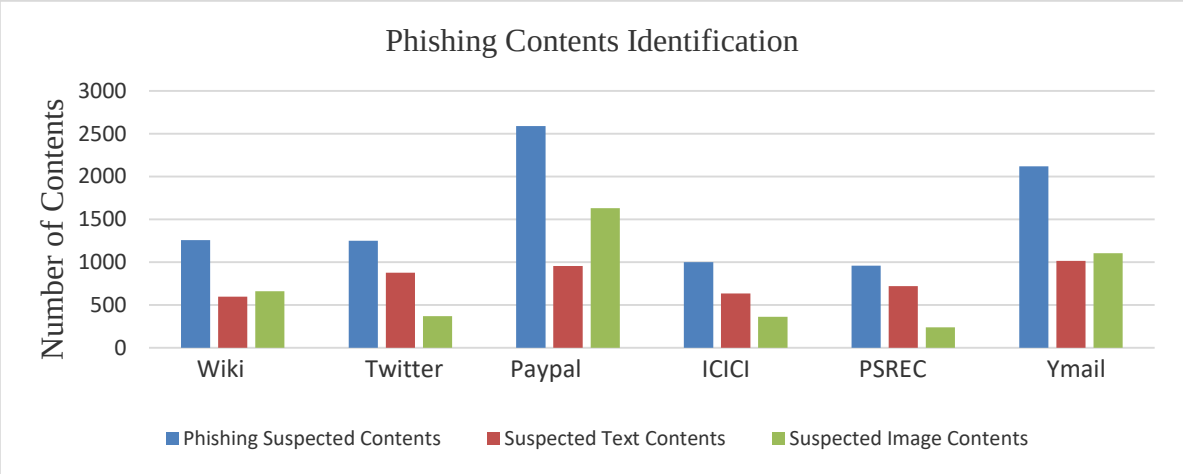

Figure 4.2 Detection of attacked content types at different websites

Web pages	URLs	Phishing Attack Detection Rate
Wiki	https://en.wikipedia.org/wiki/Wiki	12.8
Twitter	https://twitter.com/login?lang=en	11.9
Paypal	https://www.paypal.com/in/signin	22.6
ICICI	https://www.icicibank.com/	9.9
Psrec	https://www.psr.edu.in	20.1
Yahoo mail	https://login.yahoo.com/	20.2

Table 4.2 Detection Rate of phishing attack contents at different websites

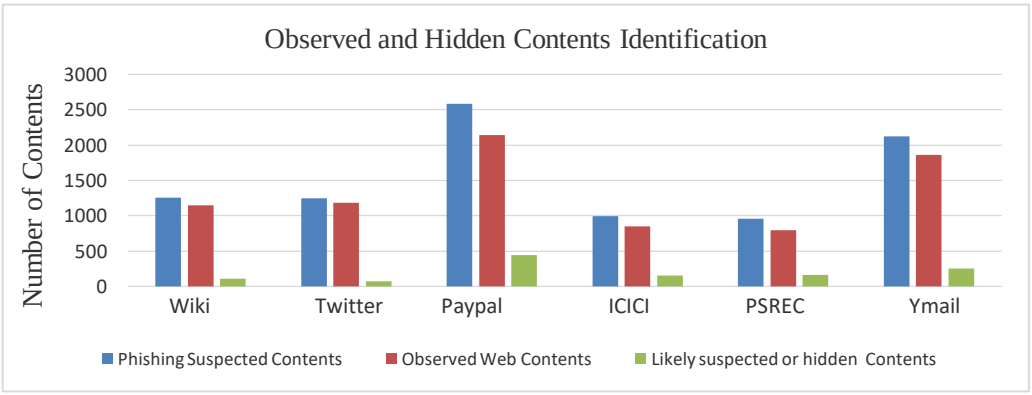

Figure 4.3 Hidden and Observed Contents Detection

Figure 4.3 shows the observed false contents and likely suspected contents of various websites. In this regard, table 4.2 shows attack detection rate of proposed work. This shows that the proposed work finds all possible similarities of false web contents and websites.

5. Conclusion

The proposed work has been designed and developed with the help of high level HMM based false page prediction approach. Using this HMM, both clearly defined false data and unobservable details are identified for the effective validation of phishing attacks. This gives better performance on both textual and visual content based phishing attack detection.

References

[1] HAIJUN ZHANG, GANG LIU, TOMMY W. S. CHOW, and WENYIN LIU, *"Textual and Visual Content-Based Anti-Phishing:A Bayesian Approach"* IEEE Transactions on Neural Networks, October 2011, vol. 22, no. 10, pp.1532-1546.

[2] Wu. M, R. C. Miller, and G. Little. (2006) *"Web wallet: Preventing phishing attacks by revealing user intentions,"* in Proc. 2nd Symp. Usable Privacy Secur., Pittsburgh, PA, pp. 102–113.

[3] ZHANG. Y, J. HONG, and L. CRANOR. *"CANTINA: A content-basedapproach to detecting phishing websites,"* in Proc. 16th Int. Conf. World Wide Web, Banff, AB, Canada, 2007, pp. 639–648.

[4] Li. L, and M. HELENIUS. *"Usability evaluation of anti-phishing toolbars," Journal in Computer Virology,* Springer, June 2007, vol. 3, no. 2, pp. 163–184.

[5] ABURROUS. M, M. HOSSAIN, F. THABATAH, and K. DAHAL. *"Intelligentphishing website detection system using fuzzy techniques,"* in Proc. 3rd Int.Conf. Inf. Commun. Technol., Damascus, 2008, pp. 1–6.

[6] Liu. W, X. DENG, G. HUANG, and A. Y. FU. *"An antiphishing strategy based on visual similarity assessment,"* IEEE Internet Computing., April 2006, vol. 10, no. 2, pp. 58–65.

[7] FU. A. Y, W. LIU, and X. DENG. *"Detecting phishing web pages with visual similarity assessment based on earth mover's distance (EMD),"* 2006 IEEE Trans. Dependable Secure Computing., vol. 3, no. 4, pp. 301–311.

[8] V. BHUSARI, S. PATIL *"Application of Hidden Markov Model in Credit Card Fraud Detection"* International Journal of Distributed and Parallel Systems (IJDPS) , November 2011 Vol.2, No.6, pp.203-211.

[9] RUCHI JAIN, NASSER S. ABOUZAKHAR *"A Comparative Study of Hidden Markov Model and Support Vector Machine in Anomaly Intrusion Detection"*, Journal of Internet Technology and Secured Transactions (JITST), Volume 2, Issues 3/4, September/December 2013, pp. 176-184.