PhishFighter: A Hybrid Anti-Phishing Plug-in

[1]Beena Kurian, [2]Jasmine Jolly, [3]Beena M V
[1]M-Tech Student, [2]M-Tech Student, [3]Professor
[1]Department of Computer Science & Engineering,
[1]Vidya Academy of Science & Technology, University of Calicut - Thrissur, India
[1]beenakurian123@gmail.com, [2]jasminejparakkal@gmail.com, [3]beena.m.v@vidyaacademy.ac.in

***Abstract*— Phishing is a type of internet crime in which phishers create copy-cat web pages which is almost visually and textually similar to target organizations like PayPal, eBay, etc. Even though browsers have built-in anti-phishing functionality, a major problem is that most web browsers rely on a blacklist of known phishing sites. Almost all phishing sites have a short lifespan as a few hours. In order to identify non-blacklisted phishing sites in this hour, a faster anti-phishing system is needed. The proposed system is a hybrid anti-phishing framework for phishing webpage detection. The system will take URL as input and detect whether it is phishing web page or not. The first phase of detection process is initiated by blacklist checking and lexical feature collection of URL. In the second phase, the detection process starts with a form tag checking. Third phase is started, if there is a form tag and user click on the safety checking icon. In this phase the system will go for visual content analysis, textual content analysis and URL scheme checking to measure the similarity between protected web page and suspicious web page.**

***Index Terms*—Anti-Phishing, PhishFighter, Visual Similarity, Textual Similarity, Blacklist and Whitelist**

I. INTRODUCTION

Phishing has been a growing phenomenon, comprises 50 % of all reported Internet Security reports. As new communications technologies drive new opportunities for commerce, they inevitably create new opportunities for criminal actors as well [1]. Phishing is threatening people's confidence to use the Web to conduct online finance & other related activities. It is public interest for ISPs to implement anti-phishing measures to protect their users. Automatic detection has attracted much attention from security and software providers, financial institutions, to academic researchers [2].Phishers naturally want to target a site that has a high reward with little risk. Obviously these high value targets have the biggest reward because money can be transferred from an account or a fraudulent credit card purchase or transfer can be made. Most phishing attacks target financial institutions. These high value targets include eBay and PayPal. Other less damaging targets include online email accounts and social networking sites. This work focuses mainly on PayPal, since it is highly targeted company.

PhishFighter uses blacklist, lexical features of input URL, white list, screenshot of webpage, textual content of webpage and URL scheme to evaluate a page as either phishing or legitimate. The combination of these techniques allows PhishFighter to fill some of the gaps left by previous anti-phishing solutions. The main objectives of this work are detecting zero day phishing websites, balancing security of user with the availability of web pages, low false positive rate, high true positive rate, and high true negative rates.

II. RELATED WORKS

There are many anti-phishing tools available today. Among them, some of the browser based tools are reviewed. Netcraft anti-phishing toolbar [3], displays a risk rating between one and ten as well as the hosting location of the site. It also traps suspicious URLs containing characters which have no common purpose other than to deceive CallingID Link Advisor [4] is an add-on that identifies the true address of a website, and displays information about the location, at which the site is maintained, by performing a quick who-is lookup. It relies on passive visual indicators, warns if passwords/info not protected, analyzes all links of a search, and analyzes links in email/instant messenger. BogusBiter [5] system not attempt to prevent vulnerable users from "biting the bait", it transparently feed a relatively large number of bogus credentials into a suspected phishing site. Web Of Trust (WOT) [6] add-on, which relies on visual indicators. Website reputations as traffic lights are shown next to search results. By clicking on the traffic light icon will give information about a website's reputation and other user's opinions. PhishZoo [7] Makes profiles of sites, profile consist of website contents and images. These profiles are stored in a local database and matched against the newly loaded sites at the time of loading. PhishTank Site checker [8] blocks visits to known phishing sites in its open phishing database. SpoofGuard [9] compares outgoing passwords with its database of <username, password, domain>, and it computes a score for each web page. Score in the form of a weighted sum of the results of each set of heuristics. Based on the score, indicator will be triggered. VeriSign EV Green Bar Extension [10] identifies VeriSign's own EV SSL certificates and makes the address bar to indicate the result. Thawte and GeoTrust are VeriSign companies. PhishNet [11] grows blacklist by generating URL variations from known phished links.

III. PHISHFIGHTER ARCHITECTURE

The proposed system is a hybrid framework for anti-phishing. It mainly uses three main characteristics of web pages. First is the URL of the webpage, which we used to access the webpage. Second, it makes use of screen shot of the webpage. Third, the textual content of the webpage is used. Thus the framework is named as a hybrid framework. Each phase is only initiated if a web page survives the previous level without being flagged. In the first phase of the proposed method, the lexical feature collection of URL is carried out and risk rating is computed. If the risk rating is greater than a threshold, then the system will classify the webpage as phishing. In the second phase, system will check whether there exists a form tag. If there is a form in the webpage and the user clicked on the safety checking icon, the third phase is started. During this phase, the system will check the similarity of screenshots of loaded web page and that of protected site. If they are similar, the system will block the loaded site. If they are different, then the system will also check the textual content similarity of loaded page with stored keywords like credit card number, card type, ATM Pin, etc. If the textual similarity is greater than or equal to 2, then PhishFighter will check for URL scheme. If URL scheme is not "https", then the system will block the loaded web page. Even though, phishing web pages are visually different, textual similarity combined with URL scheme checking can be used to capture the phishing page.

Phase I-Blacklist Checking and Lexical URL feature Collection

Figure 1 shows blacklist checking and lexical URL feature collection of PhishFighter plug-in. Blacklist contains URLs of known phishing sites. This helps in filtering out phishing websites very fast that have already been classified as phishing websites without performing additional checks. If the URL entered by the user is not found in PhishFighter Blacklist, the website is evaluated on the basis of its lexical features of URL. Normally phishing is done via sending mails to thousands of users urging them to visit the fake website through the link or URL present in it. The input for proposed system is URL. These URLs are mostly similar to authorized URLs, with very minor variation which couldn't observed by normal users.

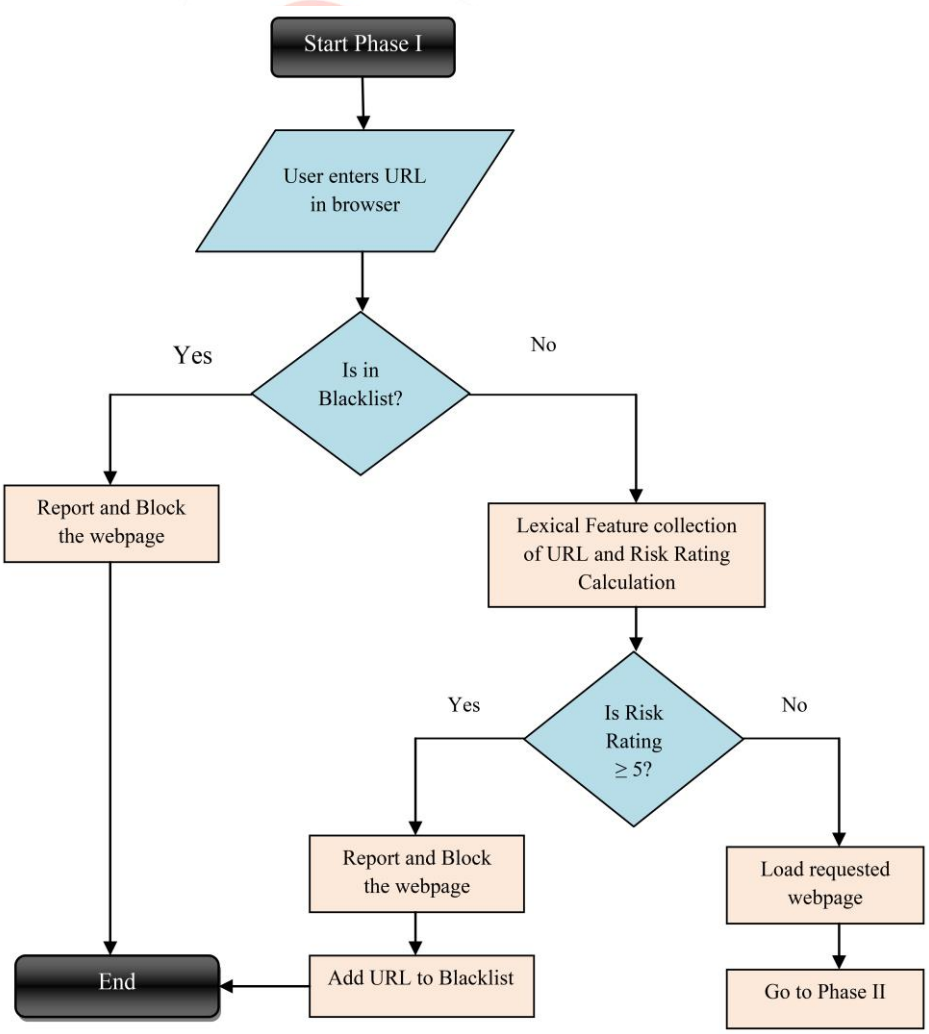

Figure 1: Architecture - Phase I

Lexical features are the textual properties of the URL itself, not the content of the page it references. Table 1 shows list of lexical URL features and their corresponding weights. From the input URL, these features are collected and total risk is computed. If total risk of accessing the webpage is greater than threshold 5, then the system will classify the webpage as phishing and block the webpage. If total risk is less than threshold, then page is loaded and Phase II is initiated.

Table 1: Lexical URL features and their weights

Lexical Features of URL	Features Extracted	Weight/ Risk
Number of dots (.) in Domain Name without TLD	3 >3	1 3
Standard TLD	No	1
'https' in Domain name	Yes	5
Standard TLDs in other parts of URL	Yes	1

Phase II- Form tag Checking

When a webpage loaded, HTML content is scanned in order to find a form tag in it. PhishFighter will check and set a flag if form tag is present in loaded web page as shown in fig.2. When user clicked on the safety checking icon and if the flag is also set, then visual similarity checking is carried out. This can reduce additional processing overhead.

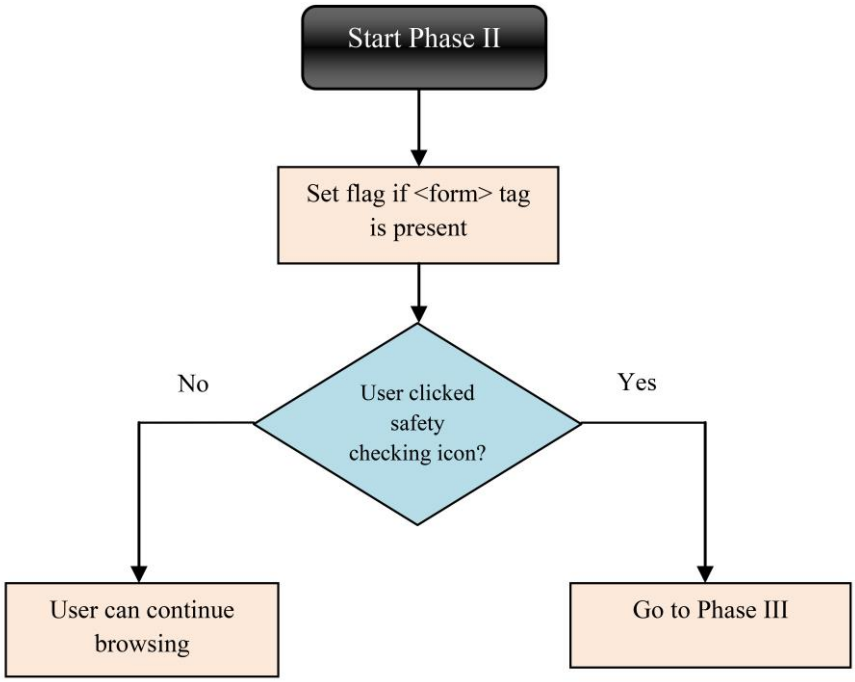

Figure 2: Architecture - Phase II

Phase III- Whitelist, Visual Similarity and Textual Similarity Checking

Figure 3 shows Phase III of PhishFighter architecture. PhishFighter store login page image of web site which need protection. When the phase III check is invoked, then the system will first check whether the input URL is in whitelist. If it is there, then the user can continue browsing. Otherwise the visual similarity is calculated. Since, the PhishFighter is Google Chrome plug-in, it can use browser API for capturing screenshot of currently active tab. The captured screenshot will be in base64 encoded string format. In that format, the string is send to the server for decoding and comparison purposes. At the server, image is decoded and writes into a file temporarily. Then the function for image comparison is invoked by passing stored image and captured image as arguments. First, the histogram for the input images is calculated. Then with those histograms as input, the distance between the images is measured using EMD (Earth Mover's Distance) algorithm [12] [13]. If the images have a difference equal to zero indicate copy-cat (phishing) website. PhishFighter then report and block the web page immediately. Then the URL is added to PhishFighter blacklist. In case of difference greater than zero, the next step textual similarity check is invoked.

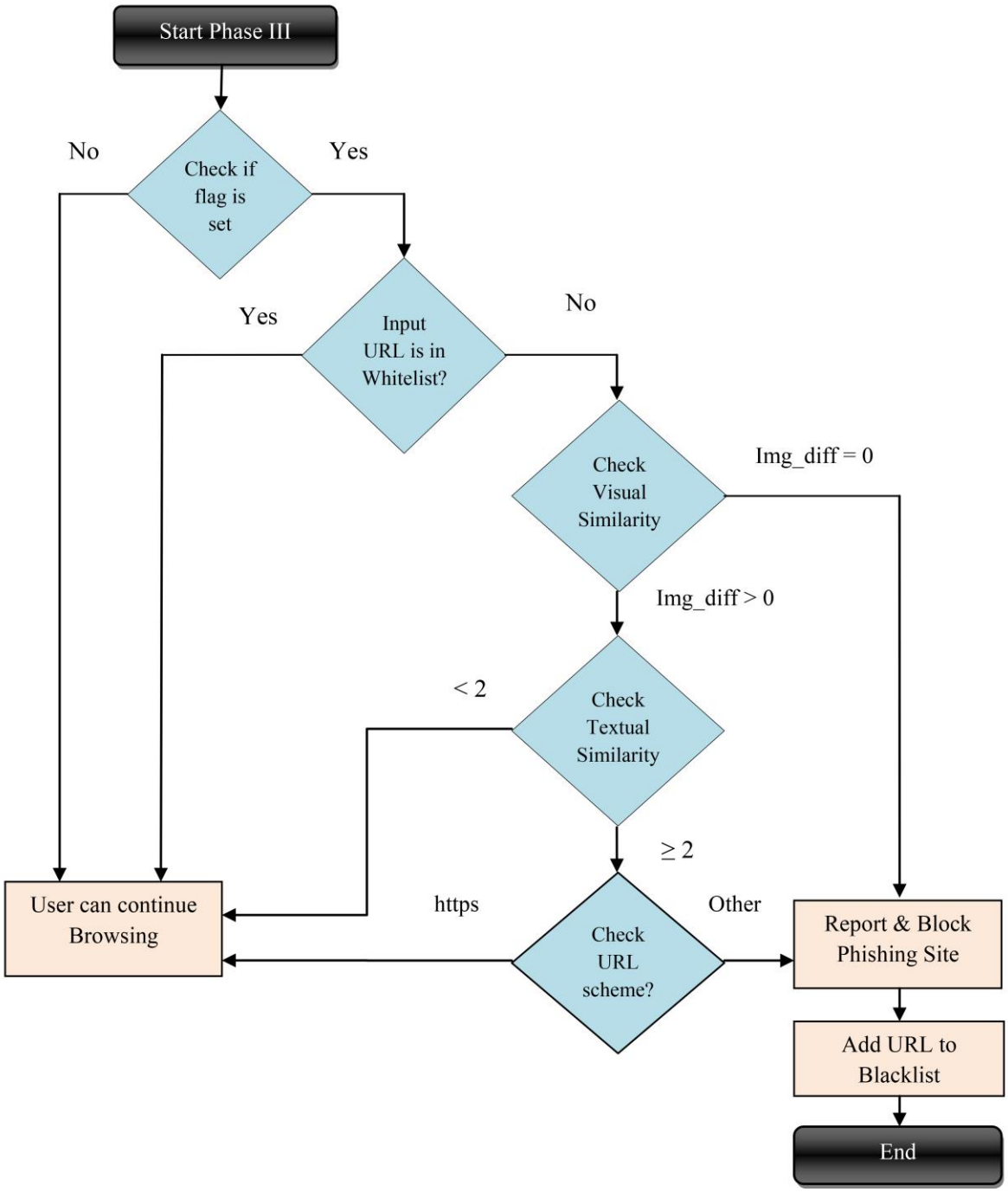

Figure 3: Architecture - Phase III

Textual Similarity Checking is initiated when the previous visual similarity checking step couldn't confirm a page as phishing. When textual similarity check is invoked, then PhishFighter will match keywords. Table 2 shows list of keywords stored in PhishFighter server that may appear in phishing pages related to financial organizations and their corresponding weights. PhishFighter will extract textual content from the loaded page by removing the html tags. Then the text content is send to the server address for comparison. These two lists are compared in the server and total weight for matched keywords is computed.

If the match is less than 2, then user can continue browsing. Otherwise URL scheme checking is carried out. If URL scheme is not https, but the page ask your credit card number, card type, etc then PhishFighter will immediately block the webpage. Then the blocked URL is added to PhishFighter Blacklist.

Thus in Phase III, if the visual similarity is equal PhishFighter immediately blocks the webpage. Otherwise textual and URL scheme is used to capture phishing web page.

Table 2: Keywords and their weights stored in PhishFighter server

Keywords	Weight/Risk
PayPal username	2
PayPal password	2
1999 - 2014 PayPal	2
1999 - 2013 PayPal	2
1999-2014	1
1999-2013	1
PayPal	1
ATM pin	2
Credit Card Number	2
3D Secure Password	2
Card Type	2
Card Number	2
Card Verification Number	2
Cardholder Name	2
Name on card	2

IV. Implementation Details

Google Chrome (version 33 and above) is chosen as the platform to host PhishFighter Plug-in because it is one of the most widely used internet browser available. To integrate PhishFighter anti-phishing functionality into Google chrome browser, a chrome extension is developed. The anti-phishing solution consists of 2 components; PhishFighter plug-in and PhishFighter website. To implement PhishFighter plug-in 5 languages; HTML, CSS, JavaScript, JSON, and Python are required. A chrome extension can only be developed using JSON, HTML & JavaScript. For creating warning page HTML, CSS, JavaScript is used. For the phase where visual similarity is calculated, the screenshot is captured and sent to server for comparing the images.
Images are compared using Earth Movers Distance Algorithm, which uses python- OpenCV. The Proposed System also uses python development framework Django. PhishFighter website is created using Google sites.

Graphical User Interface of PhishFighter Plug-in

When PhishFighter plug-in is installed and enabled, then current tab will show an icon in the chrome browser address bar. It is a green tick icon. When user put the mouse pointer above the icon, user can read the message “check your safety”, which is shown in fig. 4.

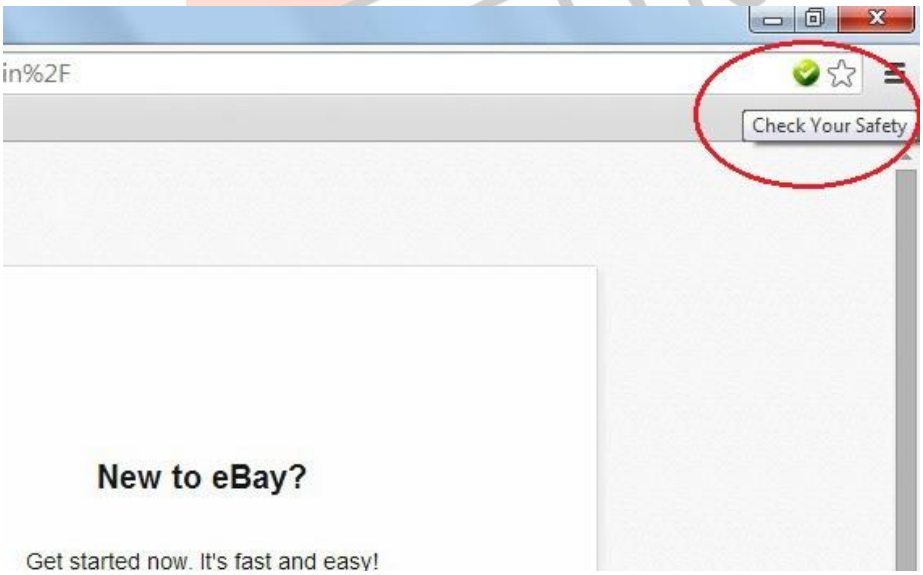

Figure 4: Safety checking green tick icon in the address bar of chrome

The icon is used for interacting user with anti-phishing functionality. Phase I checking is done automatically when user accesses a web page and block immediately if it is a phishing page. If the webpage is loaded without being blocked, then the user must click on the green tick icon if the page asks users personal account information like credit card number, card type, ATM pin number, etc . After clicking this icon and form tag also present in the page, then only Phase III check is carried out. Checking visual similarity for every loaded web page will increase the processing overhead. That is the reason for using an icon in the address bar.

Warning page of PhishFighter

When a web page is detected as phishing, then PhishFighter immediately blocks the page. Warning page of PhishFighter is shown in Fig.5.

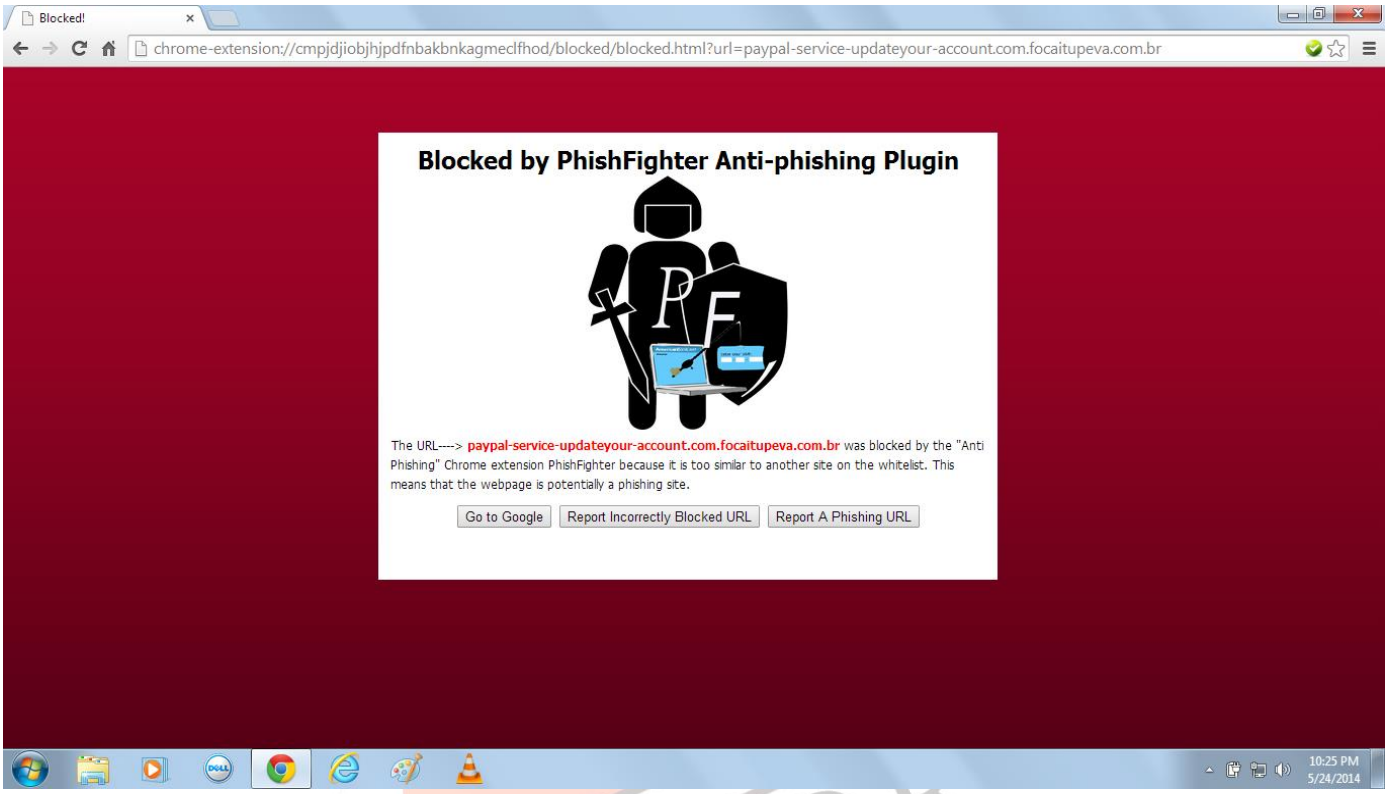

Figure 5: Warning page of PhishFighter

Warning page contains buttons to go to Google search engine and to PhishFighter Website's 'Report' tabs. By clicking through this links, users can report incorrectly blocked URL or a phishing page.

PhishFighter website

PhishFighter Website https://sites.google.com/site/antiphishingtool consists of 5 tabs; 'Home', 'About PhishFighter', 'Research Papers', 'Report', 'Feedback', and 'Contact Us'. Report link contain sub links to report a phishing site and report incorrectly blocked URL. 'Home' is the landing tab for PhishFighter website. Home tab also contains two report buttons which direct users to different reporting sections on website; a phishing site and incorrectly blocked URL. Clicking on any button will direct the user to other sections of the website where users can report accordingly. Also it gives note on what phishing is. 'About PhishFighter' tab give information about the working of plug-in. 'Research papers' tab contain some PDF files regarding phishing and anti-phishing. Its main purpose is to help future researchers to know about different anti-phishing measures. 'Report' tab is the most important part of this Component. This section allows users to report URLs they consider as potential phishing websites or URLs they think have been blocked incorrectly. Each sub tab of Report allows users to report about that particular issue by filling a form as shown in fig.6. These tabs have a similar form with following fields: Name, Email Address, URL to report, Comments, CAPTCHA Code. 'Feedback' tab contain a form, which is to analyze the plug-in. 'Contact us' allows users to contact PhishFighter team regarding any queries or help.

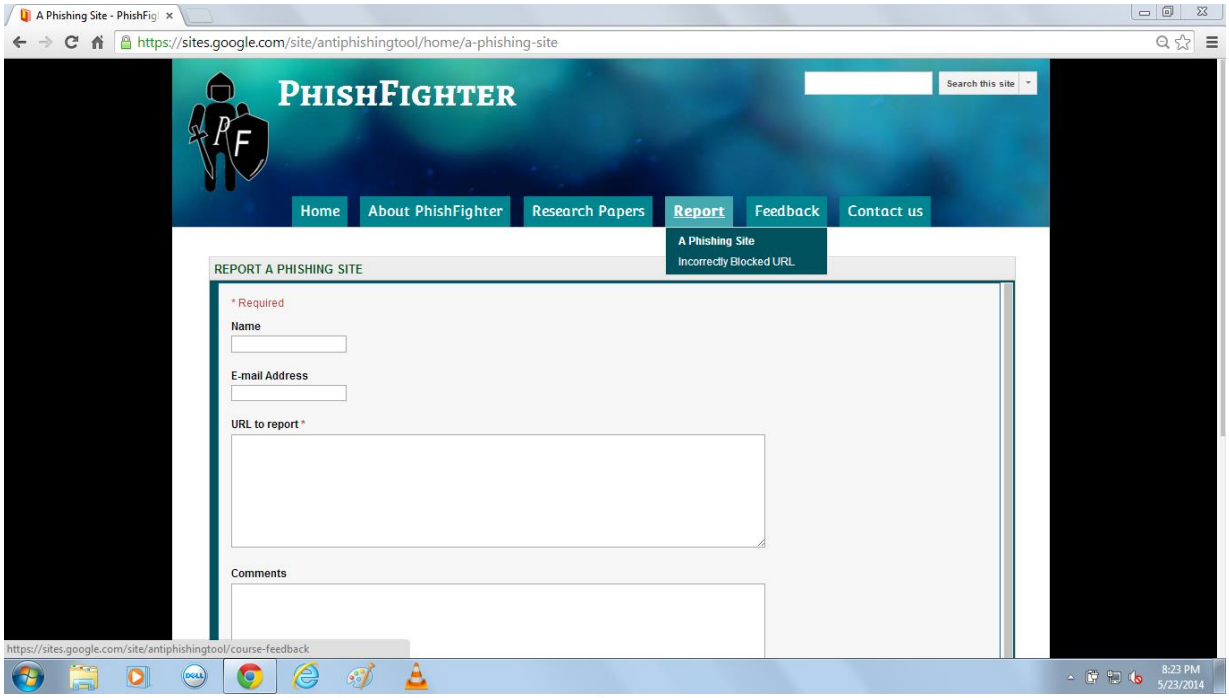

Figure 6: Report A Phishing site page of PhishFighter

V. EXPERIMENTAL RESULTS

PhishFighter plug-in and its phishing checks are tested and evaluated. Initially, PayPal login page is captured and stored in server. A dataset consisting of phishing and legitimate URLs is used to evaluate its performance, where PayPal's phishing URLs are obtained from PhishTank and legitimate URLs from Alexa.com, which lists top ranked websites globally. Also some legitimate payment gateway's login pages are also added for testing. To compute the accuracy, a dataset consisting of 200 phishing and 300 legitimate websites is used. Each URL is accessed using a Google Chrome version 33.0 with PhishFighter Plug-in enabled. The accuracy of PhishFighter is computed using True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN), as shown in Equation 1.

$$\text{Accuracy} = (TP + TN)/ (P + N) \quad (1)$$

Where:
TP = when a web page is a phishing page and PhishFighter classifies it as a phishing page
TN = when a web page is not a phishing page (legitimate) and PhishFighter classifies it as not a phishing page
FP = when a web page is not a phishing page (legitimate) and PhishFighter classifies it as a phishing page
FN = when a web page is a phishing page and PhishFighter classifies it as not a phishing page

$$P = TP + FP \quad (2)$$
$$N = TN + FN \quad (3)$$

The values of TP, TN, FP and FN for accuracy computation are shown in table 3. Substituting the values in Eq.1, the accuracy of PhishFighter is computed as 97.8%. PhishFighter correctly classified 489 web pages among 500 URLs and failed to classify 11 web pages, where these 11 are phishing as shown in fig .7. PhishFighter achieved high TP and TN rates, and zero FP rate.

Table 3: Values for calculating accuracy

Label	Value	Rate
TP	189	94.50%
TN	300	100%
FP	0	0%
FN	11	5.50%

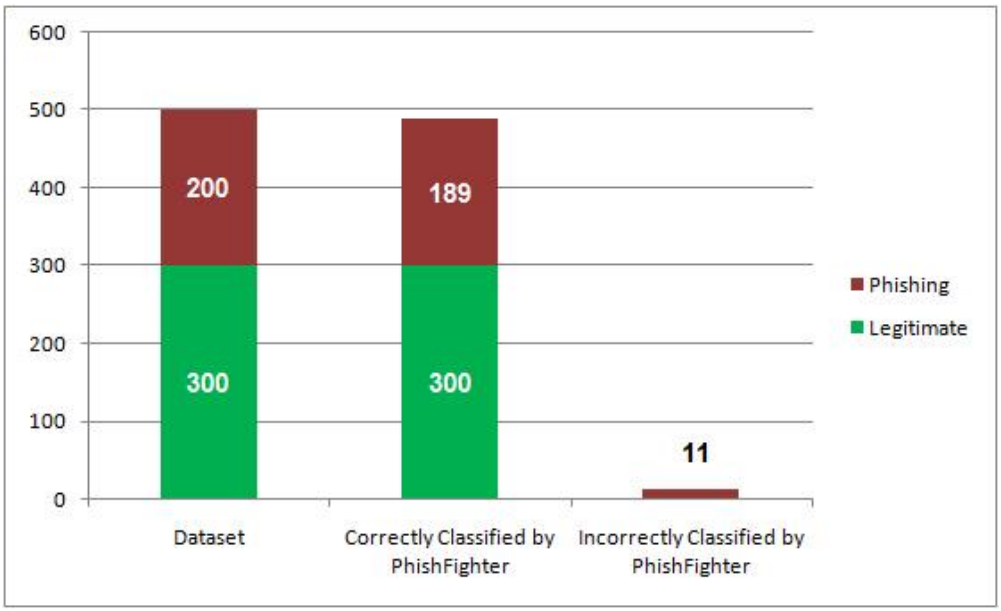

Figure 7: PhishFighter experimental results

Limitations of PhishFighter

- It is only developed for Google chrome browser and will not work for other browsers.
- It cannot protect users against JavaScript based attacks.
- It cannot protect users against malware based phishing attacks.
- Phishing pages may use images of text instead of actual text like credit card number, ATM pin, etc. In these cases, PhishFighter couldn't detect phishing based on textual similarity.

VI. CONCLUSION

Phishing has become a severe problem of Internet security. The work used new hybrid anti-phishing framework. PhishFighter works at URL, textual and visual contents of Web pages. The proposed Lexical feature collection of URL collects the features in real time. Also the framework used a Visual Similarity & Textual Similarity Checking. Using visual similarity checking, PhishFighter captures visually similar webpage. Using textual similarity checking along with URL scheme checking, PhishFighter captures visually dissimilar phishing pages which escaped from previous phases without being blocked. Including the form tag checking reduced the extra processing overhead. In case of browsers, blacklisting is widely used today. But it cannot detect phishing pages before it appears in a blacklist. But PhishFighter can detect the first time it occurs with an accuracy of 97.8%, because it uses screenshot similarity, textual content similarity, and URL scheme checking. Thus it can provide zero hour phishing detection. Including URL scheme checking in PhishFighter reduced FP rate. The future work for PhishFighter includes adding features to counter malware based attack, Unicode attacks, JavaScript based attacks, extending PhishFighter to other commonly used browsers. Only 4 lexical URL features are analyzed in phase I for risk rating. Although these features are important in determining the nature of a page, still a lot more needs to be done in order to provide users with a phishing free environment.

REFERENCES

[1] Justin Ma JTMA, Lawrence K. Saul, Stefan Savage, and Geoffrey M. Voelker, "Identifying Suspicious URLs: An Application of Large-Scale Online Learning", in Proceedings of the 26th International Conference on Machine Learning, Montreal, Canada, 2009.

[2] Haijun Zhang, Gang Liu, Tommy W. S. Chow, and Wenyin Liu, "Textual and Visual Content-Based Anti-Phishing: Bayesian Approach", IEEE transactions on Neural networks, Vol. 22, No. 10, October 2011.

[3] Netcraft Anti - phishing Toolbar. Accessed: February 14, 2014. http://toolbar.netcraft.com/.

[4] CallingID, Ltd. Accessed: February 2, 2014. http://www.callingid.com/linkadvisor-2.0

[5] Chuan Yue and Haining Wang, "BogusBiter: A Transparent Protection Against Phishing Attacks," ACM Transactions on Internet Technology, Vol. 10, No. 2, Article 6, Publication date: May 2010.

[6] WebOfTrust Add-on. Accessed: February 6, 2014. https://www.mywot.com/en/download

[7] Sadia Afroz and Rachel Greenstadt, "PhishZoo: Detecting Phishing Websites By Looking at Them," Department of Computer Science, Drexel University.

[8] Phishtank Sitechecker. Accessed: February 22, 2014. https://addons.mozilla.org/en-US/firefox/addon/phishtank-sitechecker/

[9] Chou, Neil, Robert Ledesma, Yuka Teraguchi, Dan Boneh and John C. Mitchell, "Client-Side Defense against Web-Based Identity Theft," in *Proceedings of the 11th Annual Network and Distributed System Security Symposium (NDSS '04)*, San Diego, CA , February, 2004.

[10] Verisign EV Green Bar Extension. Accessed: February 24, 2014. https://addons.mozilla.org/en-US/firefox/addon/verisign- ev-green-bar-extensio/
[11] Pawan Prakash, Manish Kumar, Ramana Rao Kompella, Minaxi Gupta, "PhishNet: Predictive Blacklisting to Detect Phishing Attacks", Purdue University, Indiana University.
[12] A. Y. Fu, L. Wenyin, and X. Deng, "Detecting phishing web pages with visual similarity assessment based on earth movers distance (emd)",in IEEE Trans. Dependable Secur. Comput., vol. 3, no. 4, pp. 301311, Oct. 2006.
[13] Y. Rubner, C. Tomasi, and L. J. Guibas. "The earth movers distance as a metric for image retrieval", IJCV, 2000.