Network Security :Technique To Save Information

Er.Akshay dixit[1] ,Dr Rahul Sharma[2]

Abstract –The Internet has brought enormous benefits to mankind, but it could be many potential risks. Internet crimes are growing rapidly, phishing is one of the new type of online crime. Phishing site is a fake-site aimed to steal personal information such as password, banking account and credit card information, etc. Most of these phishing pages look similar to the real pages in terms of interface and uniform resource locator (URL) address. Many techniques have been proposed to identify phishing sites. However, the numbers of victims have been increasing due to inefficient protection technique. In this paper, we develop a neuro-fuzzy model for phishing identification efficiently. The model eliminates the subjective factors to improve efficiency such as if-then rule sets, the parameters of membership functions, etc. Moreover, the efficiency features to identify phishing were used for the neuro-fuzzy model. The effectiveness of the proposed technique is examined with large-scale datasets collected from phishing sites and legitimate sites. The results show that the proposed technique can identify over 99% phishing sites.

I. INTRODUCTION

Phishing is a form of fraud in which an attacker masquerades as a reputable entity or person in email or other communication channels. The attacker uses phishing emails to distribute malicious links or attachments that can perform a variety of functions, including the extraction of login credentials or account information from victims

In this paper, an efficient method is proposed to identify the phishing sites that focuses on the features of URL (Primary-Domain, SubDomain, PathDomain) and Google's parameters (PageRank, BackLink, GoogleIndex). Then, a proposed neuro-fuzzy model is a system which reduces the error and increases the performance. The neuro-fuzzy model uses computational models to perform without using if-then rule sets. The pro-posed technique achieved identification accuracy above 99% with low false signals
In this section author should give introduction about his/her research related contents and brief details of its integrated parts.

II. SYSTEM MODEL

Online trades are at present a days end up being to a great degree typical and there are distinctive ambushes show behind this. Thusly the security in these cases should be high and should not be easily tractable with execution adequacy. Picture dealing with and an improved visual cryptography is used. Visual Cryptography (VCS) is a methodology for encoding a riddle picture into shares, with the ultimate objective that stacking a satisfactory number of offers reveals the puzzle picture.

The primary goal of this venture is to conceal information in a picture and give security to the same. Our approach depends on Image CAPTCHA approval plot utilizing
visual cryptography. Visual Cryptography is use to safeguard the security of picture CAPTCHA. Visual cryptography is a cryptographic system which gifts visual data (pictures, substance, and so forth.) to be encoded to such a degree, to the point that translating changes into the control of the individual to disentangle. One of the best-known systems has been credited to Moni Naor and Adi Shamir, who made it in 1994. They demonstrated a visual perplex sharing course of action, where a photograph was separated into n imparts so some person to all n offers could translate the photograph, while any n 1 shared no data about the essential picture. Each other was engraved on a substitute straightforwardness, and deciphering was performed by overlaying the offers. Precisely when all n offers were overlaid, the primary picture would show up. There are a few hypotheses of the key game plan including k-out-of-n visual cryptography.
.In this section author should explain in little bit dept about his research or model he/she is working on. Author can be use suitable diagrams and images with the references mentioned [1] in square brackets from particular resource image or diagram author taken.

III. PREVIOUS WORK

Methods for identifying phishing can be divided into three groups: blacklist, heuristic and machine learning. The blacklist-based technique [1][2][3][4] maintains a list of phishing websites called blacklist. The technique is inefficient due to the rapid growth in the number of phishing sites. Therefore, the heuristic and machine learning approaches have received more attraction of researchers.

Cantina [5] presented the TF-IDF algorithm based on 27 features of webpage. This technique can identify 97% phishing sites with 6% false positives. Although this technique is efficient, the time extracting 27 features of webpage is too long to meet real time demand and some features are not necessary for improving the phishing identification accuracy. Similarly, Cantina+ [6] used machine learning techniques based on 15 features of webpage and only six of 15 features are efficient for phishing identification such as bad form, Bad action fields, Non-matching URLs, Page in top search results, Search copyright brand plus domain and Search copyright brand plus hostname. In [6], the author used the URL to identify phishing sites automatically by extracting and verifying different terms of a URL through search engine. Even though this paper proposed a new interesting technique, the identification rate is quite low (54.3%). The technique [5] developed a content-based approach to identify phishing called CANTINA, which considers the Google Page Rank

value of a page, the evaluation dataset is quite small. The characteristic of the source code is used to identify phishing sites in [6].

IV. PROPOSED METHODOLOGY

For phishing revelation and neutralizing activity, we are proposing another way to deal with recognize the phishing site. Our framework relies upon the Anti-Phishing Image Captcha endorsement plot using visual cryptography. It checks mystery word and other private information from the phishing destinations. We likewise propose inserting diverse parts of a solitary watermark into various scenes of a video. We at that point dissect the qualities of various watermarking plans, and apply a half breed way to deal with frame a super watermarking plan that can oppose the majority of the assaults. For actualizing Watermarking Technique we are utilizing SCD, LSB, Split,DES calculations. [2]

1.Registration Phase

In enrollment stage, a key string(password) is being asked from the client at the season of enlistment for the safe site. The key string acts as a blend of letters in order and numbers to give more secure condition. This string is connected with haphazardly produced string in the server and a picture captcha is created. The picture captcha is partitioned into two offers to such an extent that one of the offer is kept with the client and the other offer is kept in the server. The client's offer and the _rst picture captcha is sent to the client for later conformation amid login stage. The picture captcha is likewise put away in the genuine database of any secret site as classified information. After the enrollment, the client can themselves change the key as and when it is required. Enrollment handle is portrayed in figure Registration phase.[2]

- Login Phase

Right when the customer sign in by entering his private information for using his record, by then first the customer is made a demand to enter his username(customer id).Then the customer is made a demand to enter his offer which is kept with him. This offer is sent to the server where the customer's offer and offer

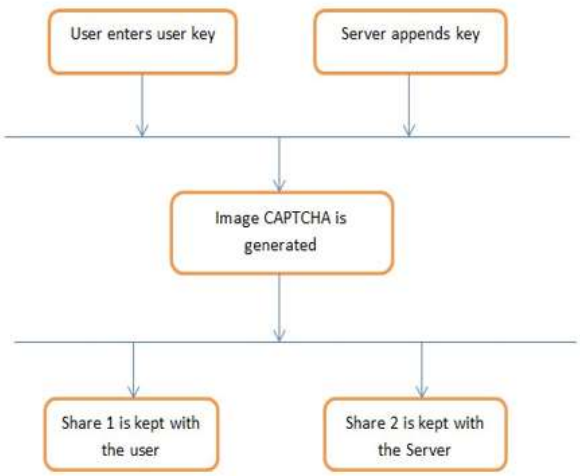

Figure :Registration Phase

which is secured in the database of the site for each customer, is stacked together to make the photo captcha. The photo captcha is appeared to the customer .Here the end customer can check whether the indicated picture captcha matches with the captcha made at the period of enlistment. The end customer is required to enter the substance appeared in the photo captcha and this can be the need of mystery key and using this, the customer can sign in into the site. Using the username and picture captcha created by stacking two offers one can say whether the site is guaranteed/secure site or a phishing site and can similarly check whether the customer is a human customer or not. This stage is portrayed in Figure login phase.[2]

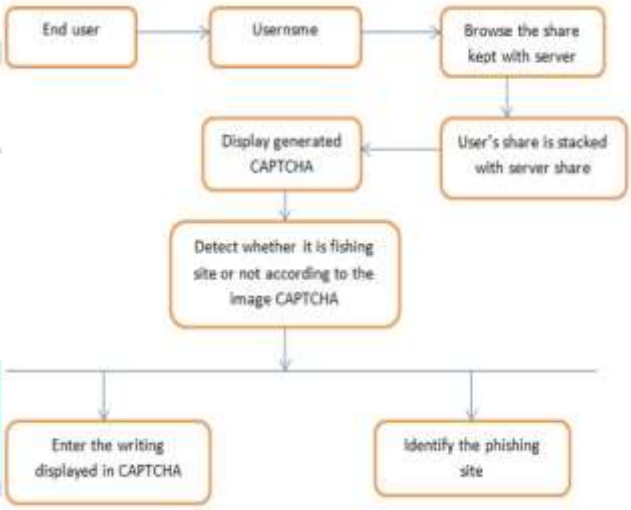

Figure :Login Phase

V. CONCLUSION

We have proposed a new technique to identify phishing sites efficiently. In the technique, the system model is built to identify phishing sites by using neuro-fuzzy network with five layers and six heuristics (Primary Domain, Sub Domain, Path-Domain, Page Rank, Back Link, Google Index). The technique is experimented with the training dataset containing 11,660 sites and 2 testing datasets that each dataset contains 5,000 phishing sites or 5,000 legitimate sites. The best accuracy results can obtain 99.31%. We also make a comparison about the accuracy identification with, our work shows that it is more efficient and accurate. In the future, the neuro-fuzzy model will be improved to enhance the identification ratio. Besides, the system could be furthermore enhanced by using larger datasets and more heuristic parameters.

VI . FUTURE SCOPES

Enhancement can be provided for the authentication by using alternate active functions like Hyperbolic Tangent, Linear, Soft Max, Tangential, Sin Wave, Bipolar and Gaussian etc. In the proposed work a password authentication scheme using

associative memories based on normalized combined text and graphical passwords can be used. A virtual keypad can be provided through which password can be entered and can define some special characters in the character set for text passwords. For graphical passwords we can draw images or symbols on the virtual screen and can use those images as passwords. Here author will explain the future of his/her research.

REFERENCES

[1] Liang-Jie Zhang; Qun Zhou, "CCOA: Cloud Computing Open Architecture," in proceeding of IEEE International Conference on Web Services (ICWS), 2016, pp. 607-616, 6-10 July 2009.
[2] Shyam Patidar; Dheeraj Rane; Pritesh Jain "A Survey Paper on Cloud Computing" in proceeding of Second International Conference on Advanced Computing & Communication Technologies, 2015.
[3] Yashpalsinh Jadeja; Kirit Modi, "Cloud Computing - Concepts, Architecture and Challenges" in Proceeding of International Conference on Computing, Electronics and Electrical Technologies [ICCEET], 2012.
[4] Qi Zhang, Lu Cheng and Raouf Boutaba, "Cloud computing: state-of-the-art and research challenges".
[5] Tharam Dillon, Chen Wu and Elizabeth Chang, "Cloud Computing: Issues and Challenges," in Proceeding of 2010 24th IEEE International Conference on Advanced Information Networking and Applications, pp. 27-33, 20-23 April 2010.
[6] Yashpalsinh Jadeja; Kirit Modi, "Cloud Computing - Concepts, Architecture and Challenges" in Proceeding of International Conference on Computing, Electronics and Electrical Technologies [ICCEET], 2012.

AUTHOR'S PROFILE

Akshay Dixit has received his Bachelor of Engineering degree in Computer Science Engineering from B.M college of Technology Engineering College in the year 2012. At present he is pursuing M.Tech. with the specialization of Computer Science in BTIRT College Sagar (M.P)

Dr.Rahul Sharma has received his Ph.d in Computer Science & Engineering. At present he is working as an dean at BTIRT Engineering College, Sagar.