REVIEW ON DETECTION OF PHISHING ATTACKS USING MACHINE LEARNING ALGORITHM

[1]Avinash P Bhat, [2]Bhargav A, [3]Jessica M, [4]Shri Prasada, [5]Deepthi V S

[1]UG student, [2] UG student, [3]UG student, [4]UG student, [5]Assistant Professor,
[1]Department of Information Science and Engineering,
[1]Global Academy of Technology, Bengaluru, India.

Abstract : Internet users can access the internet from any location around the globe. Internet provides access to communication services such as world wide web, email. Internet is more prone to attacks Due to increased internet usage the cyber-attacks are also increasing. Different types of attacks include Malware, Denial of Service, SQL injection, Man in the middle, Password attacks. This has been an enormous threat for an average internet user who is not well versed technically or is not aware of these attacks. The most common attack is the Phishing attack. Phishing is a variant of cyber-crime or cyber-attack, which exploits social engineering attack techniques to perform fraud and has an adverse effect on people where the user is directed to reveal their sensitive and private information which includes sensitive data of accounts, details about the bank account, and also card details such as pin number, CVV number, etc. Hence securing sensitive data from phishers or web phishing is a tedious task. Technology is essential to provide the organization the tools to provide security to shield from cyber-attacks. Machine learning has become an important part of information technology for cybersecurity. Machine learning pre-emptively stamps out cyber threats and bolsters security infrastructure through pattern detection, real-time cybercrime mapping, which has shown solutions in recent times in opposing phishing pages when distinguished with visualization, legal solutions, including awareness work-shops, and classic anti-phishing approaches. In this survey, various techniques are adopted which includes Machine learning and Deep learning techniques are used to derive different kinds of anti-phishing tools. This survey helps to know about different methods to detect and prevent phishing attacks.

***IndexTerms* -. Phishing attack, Machine learning, Deep Learning, Legitimate URL, Feature extraction, Prediction, Accuracy**

I. INTRODUCTION

Cybercrime is all about illegal activities and crimes which involves communication devices and network channels that are used as a medium for attacks. With the increasing popularity of online banking, online shopping which needs sensitive personal and financial data, it's a term that will be heard within the news with some frequency. Now, so as to guard ourselves against this crime, knowledge about these attacks is important.

From [11], it is clear that there are all types of attacks possible on different layers of OSI. Some of the attacks are listed in the below table:

Table 1.1: Different types of attacks

SL NO	LAYERS	ATTACKS
1	Application	Worms and Viruses, Buffer Overflow, Two-house, App/OS weakness
2	Presentation	Personal information retrieval, RPC, NetBIOS attacks
3	Session	
4	Transportation	Unauthorized access, End point identity theft, TCP SYN flooding attack, UPD flooding attack, Scanning
5	Network	Phishing, IP Modification, DHCP attack, ICMP attack, Wormhole, Blackhole attack, DOS, DDOS attack, Jellyfish, spoofing
6	Data-link	MAC modification, MAC flooding, ARP spoofing, Spanning tree attack
7	Physical	Cable disconnection, Inadequate power, open wall port, floods

In this paper, an attempt is formed to realize complete knowledge on phishing attack. Phishing may be a quiet attack during which phishers use spoofed emails and malicious websites to steal the personal information of individuals.

Phishing may be a cyber-attack during which an individual is formed to go to illegal websites and fooled to reveal their hypersensitive data just like the name of the user, bank details, card details, passwords etc. As primary security matters online, phishing has drawn the consideration of many experts and researchers. When there are two similar sites, and knowledge accompanied to the primary page on apprehensive is entered by the user, an alert message should be raised on the second page second. When two sites aren't equivalent, it's absurd that legitimate site is spoofed by the second page, and thus the knowledge can therefore be passed on without an alert that the page obtained is legitimate, supported keywords, by search done employing a program or choosing between a groups of predefined registered pages.

The machine learning approach appears suitable to unravel phishing page detection because this problem is often converted into a task of classification. ML techniques are often wont to develop models to detect phishing activities supported categorizing old sites then these models are often integrated into the browser. Machine learning may be a versatile approach initially utilized in supervised learning to make analytical models. It plays a serious aspect during a broad scope of great applications like image recognition, data processing, skilled systems and image recognition. Consider an example of a user browsing an internet page, ML models will find the legitimate website instantly then forward the output to the user at the opposite end. The vital factor for the success is that the website's features within the input dataset and therefore the availability of adequate websites for the creation of trustworthy analytical models, in developing ML models for automated anti-phishing identification.

There are tools, capital of literature and methods for serving web users to recognise and refrain from phishing sites. a number of these phishing identification techniques are skilled in detecting phishing webpages with extreme accuracy (>99%) while attaining extremely low accuracy of false classifying legitimate web pages. %). Although, a large number of these techniques, which make use of machine learning mainly depends on lots of inert characteristics, chiefly using the bag-of-words approach. The main challenge in phishing detection methods is upholding the labelled data as phishers try to use new methods and their new features in their attacks. Because the phishers mainly target banks, online trading, governments and users of the web, so it becomes a very crucial task to avoid the phishing attacks in its initial phase before it does any damage to an individual. Although, identification of a phishing web page is a laborious task, under the number of advanced approaches used by attackers to step out users of the web. The triumph of phishing web page identification techniques chiefly relies on identifying phishing web pages precisely and within an adequate period. Few new phishing identification methods are proposed to efficiently bypass phishing web pages which act as a substitute solution to already existing phishing webpage identification methods. In the recent past, phishing detection techniques involve Artificial intelligence and advanced machine learning techniques which helps in both efficient and effective detection of predictable phishing web pages.

The motivation in taking up this survey is due to increasing phishing attacks from day to day and during the covid-19 pandemic it has doubled in numbers. Social media is one of the main platforms that phishers use extensively to find their potential targets. Another example is the online classes taken on various video call platforms where there is a high chance of someone posting an unknown link which might lead to phishing.

II. LITERATURE REVIEW

In [1], several machine learning algorithms are used to find the best among them namely Decision tree classifier, k-nearest neighbour, linear svc classifier, Random forest and also a mathematical model which is a collection of correlated decision trees. This mathematical model is based on the bagging technique. In the dataset considered, there are about 30 attributes which have varying amount of relative importance. Based on the accuracy results, it is observed that the random forest algorithm has the highest accuracy among the rest of the algorithms at about 96.87%. There are many tools, methods and capital of literature for the convenience of the web users to identify and avoid phishing websites. The present phishing website identification techniques attain a high accuracy and also achieve the low false classification of legit web pages. The most efficient quality of a phishing website detection system is to precisely and accurately classify a web page in an appropriate amount of time. In the proposed method, feature importance plays a vital role in predicting the class of the feature. At the time of training, the training algorithm treats all the features present in the dataset equally. By processing this dataset, accuracy can be increased. In the considered dataset, the SSL final state and URL of an anchor has the highest feature importance according to the random forest classifier.

In [2], an approach used here is based on a Naïve Bayes algorithm. Together with Naïve Bayes ensemble approach is used which utilizes bagging and stacking approaches. Boosting approach is also used. The best accuracy is achieved using Naïve Bayes with bagging method which gives about 89% accuracy. Boosting and stacking methods used with the Naïve Bayes algorithm provides an accuracy of 85% and 51% respectively. The method can be enhanced by filtering email contents that help to differentiate between a phishing scam and other types of deceptive attacks. The idea behind this approach is to target ad emails that are used by the phishers as an effective way to deceive the users and get sensitive information or login credentials from them. So, repeated set of words are used as a feature with the other set of features to effectively recognize the deceptive emails and as well as alert the users who have received such emails. By creating a substantial list of additional words into the database helps to increase the accuracy of the existing system significantly as the detection framework uses the feature based on the word frequency. The alerting system used here is used to detect phishing emails, ad-email as well as phishing ad-emails.

In [3], the paper uses multiple techniques to classify phishing emails from legitimate ones. Two types of representation used here are term frequency-inverse document frequency(tf-idf) and doc2vec. Algorithms that are used include Decision tree, Naïve Bayes, Ada boost, logistic regression, SVM and Random forest. Using the representation of doc2vec with SVM without header gives an accuracy of 88.4% which is followed by the Random forest algorithm which gives about 87.5%. The SVM model is considered and is tested using test data and checked for true positive, true negative, false positive and false negative. The proposed work aims to develop a supervised classifier that can classify phishing and legitimate emails in a legitimate manner. The proposed methodology relies majorly upon feature selection and as well as feature engineering. This can be further improved in terms of accuracy and efficiency using deep learning methods and can be considered as a prospect concerning the phishing detection system. Future enhancement has great opportunities in this field as the upcoming evolution is based on deep learning methods.

In [4], machine learning techniques are used to identify phishing URLs and extract a certain set of features from the URL's, these include URL length having an IP address, class, web traffic, age of the domain, secure socket layer final state, Server form Handler and request URL. The neural network approach is utilized along with the decision tree and Naïve Bayes. A neural network consists of three layers. Implementation is done using MATLAB scripts. The best accuracy is obtained from pruned decision tree with about 91.5% accuracy and the neural network approach gives about 84.8% accuracy. The main problem in developing a phishing detection system is that there are very few datasets that contain phishing URLs available in the public domain. So, many times the effectiveness of a particular system is reduced by this problem. This particular aim to solve this problem. This is done by comparing the commonly used machine learning algorithms on the same phishing websites. In the dataset which is created using data URL'S have class labels with them. The few limitations of this work are that firstly dataset has a limited number of entries that are 1353 URL's and 9 features are considered for each URL. The commonly used classifiers such as decision trees, Naïve Bayes and rule-based systems are effective if the features are discrete. The accuracy can be further improved by considering a few thousands of URL's and also extracting and considering more features in decision making.

In [5], the Anti-Phishing toolbar is used which helps to effectively differentiate malicious Websites from legitimate ones. Dataset is taken from the UCI repository. The machine learning techniques used here is a Decision tree. The data is classified after finding normalized information gain. The train-test dataset split is in the ratio of 80:20. Email headers are analysed which decreases the misclassification rate which in turn substantially increases the accuracy rate. By automating the process, new features can be found that can be beneficial in finding the new patterns in phishing attacks. In this approach, certain features/qualities are taken from emails. After this, two exploration investigation are rundown that considers the machine taking in phishing URLs. The outcome claims a 95 % identification rate with a low false positivity rate. Extra variables are considered to enhance the predictive nature of the given phishing detection systems. Features that are utilized are analysed which further extends the work that is shown in the particular paper. Creating automated as well as a robotized environment which helps in efficient extraction of new features which are used in the new phishing attacks and their patterns.

In [6], the Phish killer approach is used which mainly aims to mitigate and detect phishing attack attempts on the client-side. This is a very fast as well as an accurate approach that also protects the users or client's privacy and doesn't breach data. A proxy is configured into the client machine which processes the request extracts the URL and sends them into the API. The API contains 3 core modules i.e. Training module, classification module and warning module. Results for using this approach is 97.59% accurate. The Phish killer approach does not require any user input in the verification process. The system of using a proxy is used using python language which is highly portable in the current age of machines. Therefore, is supported in any operating system as well as any browser that has features for the proxy configurations. This featureless approach requires a massive amount of data which can increase the accuracy and also dataset should be properly designed. This approach has high resilience and also the resistance towards newer variants of phishing attacks as it doesn't necessarily depend on features. To further improve this software-defined networking is used which is a centralized controller which helps to expand this on a global scale.

In [7], it means to investigate the area of phishing detection by recognizing the phishing websites by effectively utilizing machine learning algorithms. The proposed system in this paper uses four different machine learning algorithms namely K-nearest neighbor, Random forest, Kernel SVM and Decision tree. Random forest classifier which is an ensemble classifier gives the best accuracy among various machine learning models used with score of 96.82%.

In [8], using UCI machine learning repository datasets are taken in csv form which has about 30 features and a target feature. It contains about 2456 entries which has both phishing as well as legitimate website features contained within the dataset. The linear and non-linear SVM gives an accuracy of about 93.07% and 94.97% respectively. But, out of the selected models, random forest gives the best accuracy which is about 95.11%.

In [9], this approach uses hyperlinks information and Machine Learning Techniques. The various kinds of approaches that have been tested such as Heuristic approach, Machine learning approach, fuzzy rule-based approach, image processing approach and CATINA based approach. Dataset is taken from the DMOZ Directory project and also from YAHOO's directory. The Final Projected accuracy rate is about 98.4%. The accuracy in this method can be further enhanced by considering more features but also increases the cost of the scheme in the process. The selection of hyperlink precise structure is taken from structure. These statements are enough to detect phishing website. Investigational outcomes suggest that this is a highly effective approach concerning the detection of phishing websites. Attacks can be detected from customer reportage image processing, honey pots and other methods. By mining more and more features from the third party the effectiveness of this proposed system can be increased.

In [10], in this approach, they have used deep learning techniques such as MFPD. CNN (Convolutional Neural Network) is used to extract certain features like co-relational features from the convolutional layer. Since the traditional neural network model is not suitable for time series problem, RNN (Recent neural network) is used. Usage of the CNNLSTM algorithm helps to improve the accuracy. It contains three steps namely: Embedded URL representation, Feature Extraction and also Classification. Using these approaches, it is possible to get an accuracy of 98.88%. There is always a contradiction between detection time and accuracy which has to be balanced. This is done by improving the output judgement condition of the

SoftMax classifier in deep learning. New phishing methods that are being used by phishers in the new day and age pose new and tricky challenges to security experts as well as researchers. So, blacklists and whitelists are widely used in this regard to prevent and avoid repetitive attacks. Even Google provides malicious websites in form of alerts and notifications that help an average internet user to be cautious while crawling into unknown websites.

Algorithms Used	**Reference Paper**	**Data Set**	**Language/Tools**	**Conclusion**
Random Forest, Decision Tree, K nearest neighbors ,Linear SVC,SVM	[1]	UCI Repository Machine Learning	Python	Random Forest highest accuracy 96.87%
Naïve Bayes, RMST, MAE	[2]	Not Mentioned	Python	Naïve Bayes with Bagging 89.8%
Naïve Bayes, Random Forest, Decision Tree, K nearest neighbors , Ada Boost, SVM	[3]	ACM international workshop on security and Privacy Analytics	Python	Dov2Vec with SVM obtained 88.4%
Naïve Bayes, Random Forest, Decision Tree, SVM, Neural Network	[4]	IRVINE Machine Learning Repository	Python, MATLAB scripts	Pruned Decision Tree accuracy 91.5%

Decision Tree, SVM	[5]	UCI Repository Machine Learning	Python	Decision Tree accuracy 90%
Natural Language Processing, Phishkiller	[6]	Phish tank archive	Python	Phishkiller accuracy 98.3%.
KNN ,Kernel support vector, Decision tree and random forest	[7]	Phish tank archive	Python	Accuracy of 96.4% is achieved.
Random forest and Support vector machine	[8]	UCI machine learning repository	Python	Accuracy of 90.12% is achieved using random forest
Support vector machines	[9]	DMOZ Open Directory Project	WEKA, MATLAB	SVM obtained 98.39%
Convolutional neural network, MFPD	[10]	Phishtank archive	Dmos Tools.net	Using CNN obtained 96.3%

III. CONCLUSION

Phishing is a critical menace to user’s data nowadays. Detection of phishing websites is a tedious job, as a result, phishers are rapidly increasing. This survey aims to provide a solution to prevent phishing attacks. It is found that phishing attacks are extremely crucial and it's important to urge a mechanism to detect them. As vital and private information of the user is often leaked through phishing websites, it becomes more critical to require care of this issue. This problem is often easily solved by using any of the machine learning algorithms with the classifier. The presence of classifiers gives a good prediction rate of phishing, but after the survey that it will be better to use a hybrid approach for the prediction and additionally enhance the accuracy prediction rate of phishing websites. In [10], the accuracy observed is 96.3%, using Convolution neural networks, which provides the best results comparatively. In future with the structured dataset of phishing, the performance of phishing detection is much faster. The usage of a combination of two or more classifiers can yield maximum accuracy. Exploring various phishing techniques that make use of Lexical features, Network-based features, Content-based features, Web page-based features, HTML and JavaScript features of sites that can improve the performance of the system. In particular, with the implementation of suitable techniques from the above papers, extraction of the features from URLs and pass them through the various classifiers and the result is obtained.

IV. REFERENCES

[1] Gururaj Harinahalli Lokesh, Goutham BoreGowda,” Phishing website detection based on effective machine learning approach ”, Journal Of Cyber Security Technology, 31 Aug 2020.

[2] Gyan Kamal, Monotosh Manna, “Detection of Phishing Websites Using Naïve Bayes Algorithms”, International Journal of Recent Research and Review, Vol. XI, Issue 4, December 2018.

[3] Nidhin A Unnithan, Harikrishnan NB,” Detecting Phishing E-mail using Machine learning techniques”, ACM International Workshop on Security and Privacy Analytics (IWSPA 2018), Tempe, Arizona, USA, 21-03-2018.

[4] Arun Kulkarni, Leonard L. Brown, ” Phishing Websites Detection using Machine Learning”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 7, 2019.

[5] Santhi H, Supraja, “Phishing Detection using Machine Learning Techniques”, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-12S2, October 2019.

[6] Cristian H. Martins de Souza, Marcilio O. O. Lemos, ‘’ On detecting and mitigating phishing attacks through featureless machine learning techniques”, Internet Technology Letters. 2020.

[7] Bhagyashree A V, Anjan K Koundinya, ”Detection of phishing websites using Machine Learning Techniques”, International Journal of Computer Science and Information Security (IJCSIS), Vol. 18, No. 7, July 2020.

[8] S. Jagadeesan, Shashank Kumar,’’ URL Phishing Analysis using Random Forest”, International Journal of Pure and Applied Mathematics, Volume 118 No. 20 2018.

[9] Saad Tayyab, ”Phishing Detection using URLs and Hyperlinks Information by Machine Learning Approach”, International Journal of Computer Science and Mobile Computing, Vol.8 Issue.3, March- 2019, pg. 345-351.

[10] Peng Yang, Guangzhen Zhao, “Phishing Website Detection based on Multidimensional Features driven by Deep Learning”, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN, November 2018.

[11] Deepthi V S, Vagdevi S, “Multiphase Detection and Evaluation of AODV for Malicious Behaviour of a node in MANETs”, Third International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT), 14-15, December 2018