A Machine Learning Approach for Phishing and Its Detection Techniques

Dhananjay Merat[1], Anurag Patil[2], Sourabh Gavsane[3], Vivekanand Jadhav[4], Prof. Himanshu Joshi[5]

Abstract: *As we are moving towards a better future with better technological improvements every year, the risk of credit card details security wise is also increasing. In the recent years, credit card based frauds have increased a lot. This includes hacking of details, phishing and also other wrong and illegal ways to steal data related to one's credit card. In this implementation work, we have implemented the email phishing & URL phishing detection & prevention technique using Machine Learning mechanism which gives the real-time status of the checked URL & fetched Email.*

Keywords: *Software defined networking, Phishing, Cuckoo search, Honey Pots, Random Forest, Machine Learning.*

I. INTRODUCTION

In the cyber-fashion, from the last two set of ten, phishing was spreading. It was observed first with America Online in the year 1995. The words phishing & fishing differs in terms, phishing sticks with the way of fishing in which phisher hooks the victim's private information through lure & fishes. Phishing is described as "one of the scalable shapes of thaumaturgy in which the aiming information is obtained by impersonation".

The major motive of a phishing is getting the attacker's desired action by fooling the recipient through sensitive information like providing login credentials etc. worldwide phishing attacks were developing enormously by 65% increase in 2016 in comparison to its last year. There was a norm growth of 57.53% of phishing attacks each month was observed in 12 years' time (2004-2016) with an all-time high in the financial sector in the year 2016.

Phishing is generally used to gain a person's credit card data or the login id & the login password. People get a phishing e-mail and made to look like as it is given by bank to get user's log-in id and login-password. This is structured to make work simply, but majorly done to collect the log-in data from the dupe of phishing as shown in Fig.1. The users are taken to a fraud link from trust-worthy websites making them misaddress through which the dupes are supposed to use their sensitive login data, thereby phishers acquire the same unlawfully by planning & thereby accomplishing their attacks. Few unsound sites consist the ill-natured code which is to be executed on the user's computed machine where the site is opened by clicking the link of work done.

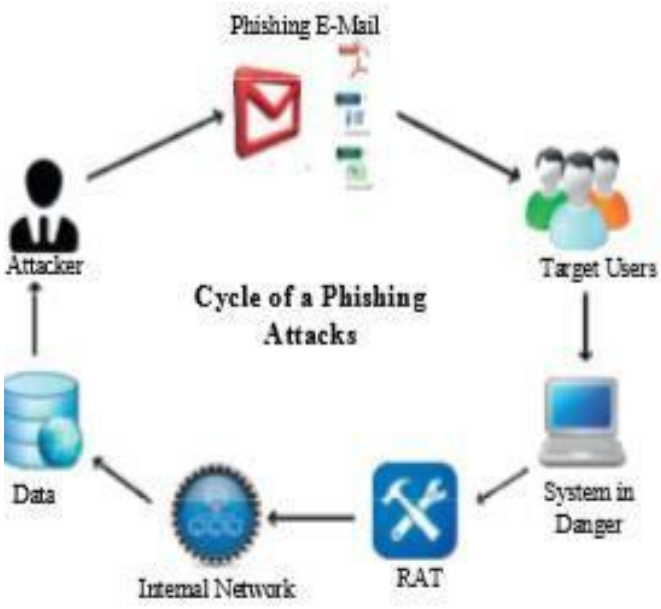

Fig.1: Phishing attack is represented by the processing cycle.

Particularly, by phishing attempt the person's data as their number of the account, user name also the passwords, internet banking data, credit card data etc. However, the attempts are kept by both the researchers in academia & the people in the industry for extenuating these phishing towards the acquisition of anti-phishing.

2. LITERATURE SURVEY

2.1 Vishing:

Vishing is a name given to voice phishing. Here attack is done based on gathering data in the caller's details. We do not require a fake website to perform this attack. Taking the help of fake caller-ID, by giving an appearance that data is got from the trusted organization. These prompts made the user to give their credentials such as account number and PIN there by gathering one's bank details.

2.2 Smishing:

Smishing is the name given to SMS phishing. To reveal the personal information text messages are used

as a tool for inducing people from their mobiles. This is a technique used in this SMS phishing.

2.3 Other methods

Forwarding the user to the bank's legitimate website by placing a popup window thereby requesting their credentials on page top is one of the methods being applied here. Users get message as if bank is requesting the sensitive data.

Tab nabbing

Opening multiple tabs at a time is an advantage of tab nabbing. Redirecting the user to affected site is happening here. Reverse technique is method loaded here that is copying the affected sites into the original site happens here.

Evil twins

This phishing attack is one of the method similar to that of described bank example above, in which the email of user asking the recipient to enter their account credentials.

Generally phishing attacks are now taking place by sending mails to the company either personal or professional. This may be done on the recipient mails. All these happens by giving our details like login id and password to unknown persons.

Spam filters are used to analyse our mails. This will reduce type of phishing attacks being faced by people. These filters use provider-level integration. Other simple way is to avoid phishing mails by using address authentication.

2.4 Phishing is of different types and they are classified:

2.4.1 Spear Phishing

Spear phishing is carried out by sending e-mail to the aimed individual. Phishers mainly get the data of individuals through social media websites as Linked In, Facebook & use of fake addresses for sending e-mails that similarly happens to be the e-mail that was received from anyone of the co-workers. For e.g., Phisher may aim the selected person in finance department by requesting bank transfer of huge amount within a limited amount of time and acts like the target's manager.

2.4.2 Whale Phishing

Whale phishing is implemented when it is done with famous personalities and confidential people. It's one of the forms of phishing which is used to achieve high aims. This sort of phishing usually happens on the company's targeted board members. It's an ease to apply on them because they use only company e-mail ids. As they are using personal e-mail addresses, that will have security & protection methods provided by the company.

2.4.3 Deceptive Phishing

This is one of the most used way of phishing. Attacking the customers for stealing the private data & log-in credentials which happens here. These phishing e-mails mainly are threatening by creating emergency to scare the users into doing the attackers bidding such as Paytm scammers sends an e-mail attack that asks the user to click on the link given for rectifying a mistake in the account. As this link takes to a fake Paytm login page and thereby collect credentials like user's login etc., which will be either used by the attackers or sell this data to other attackers.

3. PROPOSED SYTEM:

A dynamic method for detecting phishing methods is implemented which uses a single layer artificial neural network. In this paper, In the very First step of the method value of six heuristics are calculated using the same algorithm.

In the implementation, a dataset of URLs, in which a combination of phishing & non -phishing URLs are used. Dataset is gathered from UCI Repository achieve. Great accuracy is achieved using NN_PSO models at the lowest RMSE & output layers respectively. Learning ratio is used as a parameter for the result. The accuracy is been compared between both & the highest accuracy was achieved in ANN_PSO.

- TP (True Positive): phishing URLs detected in number.
- FN (False Negative): Incorrect URLs.
- TN (True Negative): correct Legitimate URLs being classified.
- FP (False Positive): Incorrect Phishing URLs which are classified.

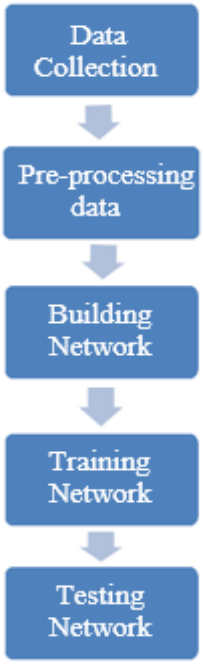

Fig. 2: NN_PSO Model is represented here

The implemented system comprises of email as well as website phishing detection so as to assure the complete secure access. The system makes use of various algorithms first to analyse the accuracy and performance of all the algorithms for classification and then the highest accuracy model will be used for the proposed system. As off now, Random forest is found to have the better performance for the classification problems.

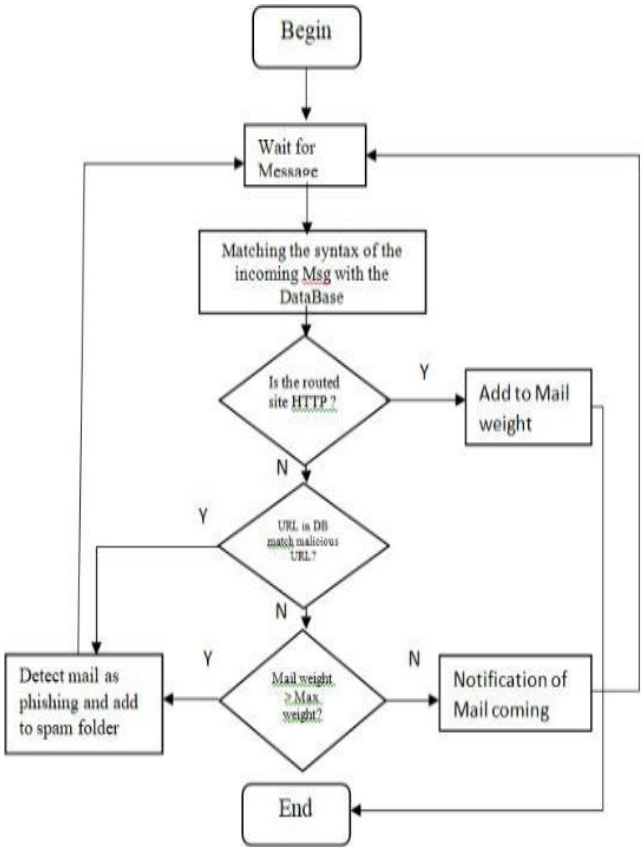

Fig. 3: Flow Chart of the Process

4. METHODOLOGY

The dataset that has been used was synthetically created by us and amalgamation from the internet. It contains 5572 synthetically created records. As this is time consuming process we had to review most of the records to maximise the prediction value. In the dataset there are 747 are spam emails and 4825 are legitimate emails. After creation of the dataset comes tokenization.

4.1 Tokenization

Then the textual data is pre-processed in a process called tokenization. Tokenization is the process of tokenizing or splitting text into list of tokens. Now using Natural Language Processing (NLP) tokenization we get rid of all symbols such as ". ! @ # $ % ^ * ( ) [ ] { } : ; / ? ~ ` _ - + = \ | ". Then the next step is to remove the stop-words such as a, the, of, after, it, hers, have, we, our, while, etc. Stop words are the words which are removed from the text before training machine learning models since stop words occur in abundance, hence providing little to no unique information that can be used for classification or clustering.

4.2 Word Embedding or Word Vectorization

Word to Vector is a methodology in Natural Language Processing (NLP) used to map words from vocabulary to

corresponding vector of a real numbers which is used to find word predictions. This process of converting words to vectors is called Vectorization. This is an integral part of the Natural Language Processing (NLP) as machine learning works on vectors or numbers.

4.3 Classification

Now using Pipeline we vectorise and classify the data using Naïve Bayes. In machine learning we often need to perform series of transformers until fit into final estimator this process is done by a Sci-kit library called Pipeline. Now this pipeline is stored into variable which we split the data into two parts called train and test. We split the data into training and testing datasets. The reason we use training dataset is because to learn the pattern of the data. And the reason we use testing data is to know how it will perform in real world scenario. After splitting the data set we apply the Naïve Bayes algorithm also known as Multinomial NB.

4.4 Testing

After classification is done we check the number of predictions which are correct and which are wrong. In this classification total test cases were 1115 and out of 1115 only 39 were wrong which brings the accuracy to 97%.

	precision	recall	f1-score	support
ham	1.00	0.96	0.98	1014
spam	0.72	1.00	0.84	101
accuracy			0.97	1115
macro avg	0.86	0.98	0.91	1115
weighted avg	0.97	0.97	0.97	1115

Fig 4 Test Results

5. EXPERIMENTAL RESEARCH

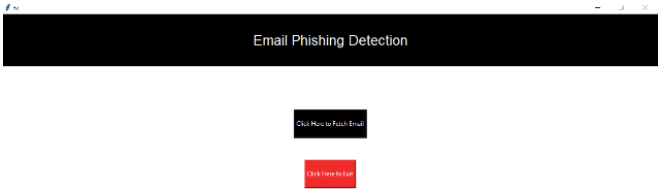

Fig. 5 Home Screen

This is the simplex User Interface (UI) we created using Tkinter Python for email spam detection. In the above image the program collects email from inbox and gives the output according to our trained model for email spam detection

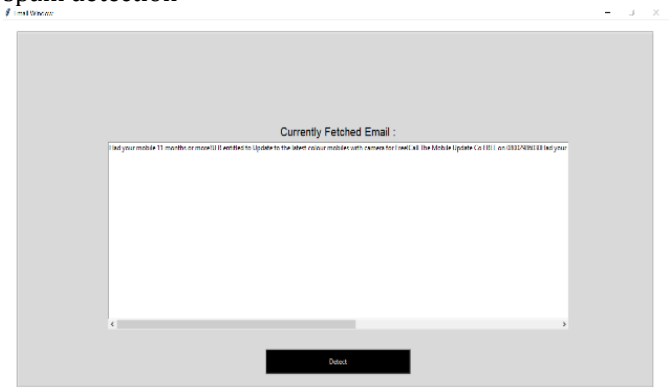

Fig. 6 Email Fetched

This the screen where the email is fetched to our program for classification to either spam or ham. This email is being fetched by IMAP. The topmost email will be fetched the program of the current email address' inbox in the program.

Fig. 7 Email Status

In this screen our model predicts that the above particular text is not spam. This is genuine email according to our classifier model. After the IMAP fetches the email. The words tokenized, cleaned by our classifier and deemed "ham" which means it is not spam.

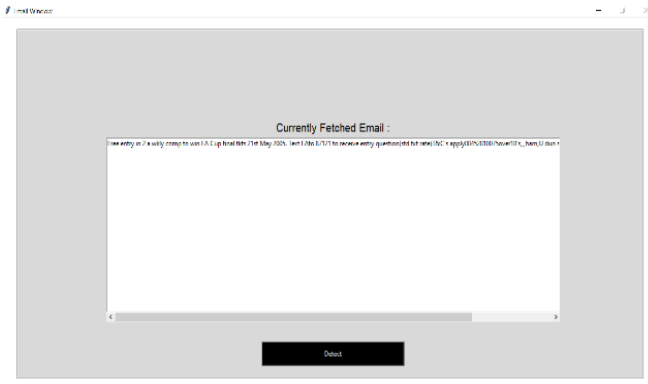

Fig. 8 Another Email Fetched

This the screen where the email is fetched to our program for classification to either spam or ham. This email is being fetched by IMAP. The topmost email will be fetched the program of the current email address' inbox in the program. Then we click the detect button which gives the result.

Fig. 9 Another Email Status

In this screen, we see the Fig 4 email we fetched was spam. In this screen our model predicts that the above particular text as a spam email. This is not a genuine email according to our classifier model. After the IMAP fetches the email. The words tokenized, cleaned by our classifier and deemed "spam" which means it is spam email.

Fig. 10 URL Check

In this screenshot we show that our extension for URL spam detection depicts Facebook as a Safe website.

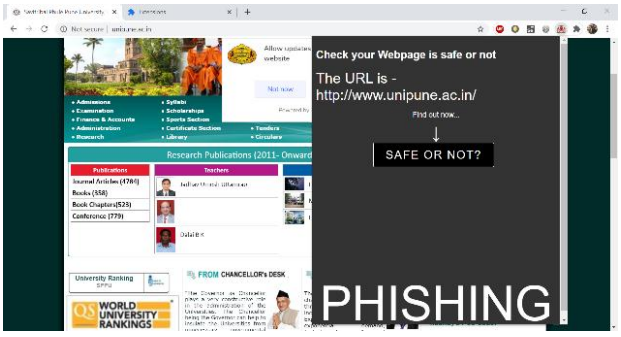

Fig. 11 URL Check

In screenshot we show that our extension for URL spam detection depicts this website as Phishing website. This website is deemed not safe by our extension. In this screenshot we show that our extension for URL spam detection depicts GitHub as a Safe website.

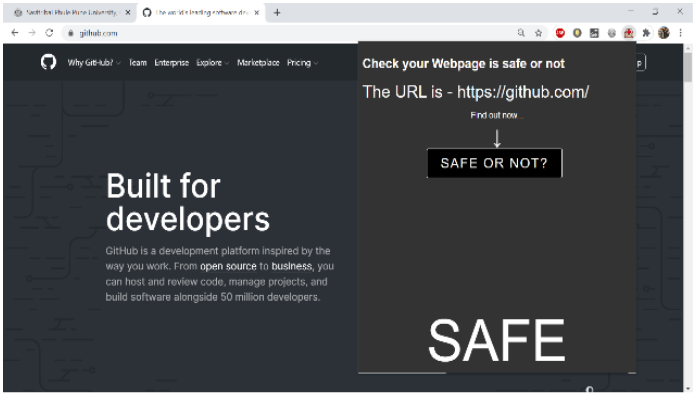

Fig. 12 URL Check

CONCLUSION

The Implemented system can make the general public much more aware and secure regarding the email phishing attacks. Nowadays, internet has become one of the most and major used source to perform phishing attacks. Hence, the implemented system can prevent it's users from such attacks by detecting which email is safe and which is not. The implemented system hence acts an anti-phishing system. It uses Random Forest Algorithm to detect whether the email is phished or a safe and hence provides good accuracy by also protecting the end user to be a victim of email phishing.

REFERENCES

1.Aggarwal S., Kumar V., Sudarsan S. D., "Identification and detection of phishing emails using natural language processing techniques," In Proceedings of the 7th International Conference on Security of Information and Networks 2014.
2.T. Vyas, P. Prajapati and S. Gadhwal, "A survey and evaluation of supervised machine learning techniques for spam e-mail filtering," 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, pp. 1-7, 2015.
3.T.G. Gregory Paul and T. Gireesh Kumar, "A Framework for Dynamic Malware Analysis Based on Behaviour Artifacts" Singapore: Springer Singapore, 2017.
4.Mohammad R. M., Thabtah F. and McCluskey L., 2014 "Predicting phishing websites based on self-structuring neural network," Neural Computing and Applications.
5.M. Khonji, Y. Iraqi & A. Jones, "Phishing detection: a literature survey," Comm. Surveys & Tutorials, vol. 15, no. 4, pp. 2091– 2121, 2013.

6.H. Z. Zeydan, A. Selamat, M. Salleh, "Survey of anti-phishing tools with detection capabilities," In the proceedings of 14 Int. Symposium on Biometrics and Security Technologies ISBAST'2014.
7. Huang Huajun and Qian Liang and Wang Yaojun, "An SVM Based technique to detect phishing URLs," Information Technology Journal, 2012, vol. 11.
8.Kaveh A," Cuckoo search optimization," in Metaheuristic Algorithms for Optimal Design of Structures, 2017.
9.Chandra J Vijaya and Challa Narasimham and Pasupuleti Sai Kiran," A practical approach to E-mail spam filters to protect data from advanced persistent threat," Circuit, Power and Advances Computing Technologies (ICCPCT), 2016 International Conference on, IEEE, 2016.
10. R. M. Mohammad, F. Thabtah, and L. McCluskey, "Intelligent rule based Phishing Websites Classification," 2014.