

We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900

Open access books available

186,000

International authors and editors

200M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



An Emerging Solution for Detection of Phishing Attacks

Prasanta Kumar Sahoo

Abstract

In this era of computer age, as more and more people use internet to carry out their day to day work so as hackers performs various security attacks on web browsers and servers to steal user's vital data. Now Electronic mail (E-mail) is used by everyone including organizations, agency and becoming official communication for the society as a whole in day to day basis. Even though a lot of modern techniques, tools and prevention methods are being developed to secure the users vital information but still they are prone to security attacks by the fraudsters. Phishing is one such attack and its detection with high accuracy is one of the prominent research issues in the area of cyber security. Phisher fraudulently acquire confidential information like user-id, passwords, visa card and master card details through various social engineering methods. Mostly blacklist based methodology is used for detection of phishing attacks but this method has a limitation that it cannot be used for detection of white listed phishing. This chapter aims to use machine learning algorithms to classify between phishing E-mails and genuine E-mails and helps the user in detecting attacks. The architectural model proposed in this chapter is to identify phishing and use J48 decision tree classifier to classify the fake E-mail from real E-mail. The algorithm presented here goes through several stages to identify phishing attack and helps the user in a great way to protect their vital information.

Keywords: security attacks, phishing, fake E-mail, data mining

1. Introduction

It is one of the methods used by the phisher to steal user's most secret information in a fraudulent manner. It is a very serious security problem that the modern world is facing today in cyber space which leads to financial losses for individuals and the society at large. It is an unlawful act, the fraudsters use it to retrieve user's personal and secrete information by betraying them using various social engineering methods. It is becoming one of the major types of frauds where the phisher used to trick the user to reveal their own private information such as user id, password, pin and visa card details. Mostly phishing attack is done by E-mails. Very often a phishing messages may contain a uniform resource locator (URL) that redirect the user to visit an alternate web site. The redirected site is an extremely modified site and when the user clicks on that site, they are directed to enter their personal information which normally transferred to the phishing assailant [1, 2]. It is an offense in which a phisher sends the fake E-mails, that appears to be genuine and come from a trustworthy organization, instruct to enter their personal information such as online banking username, password, mobile number, residential address, details

of the credit card and so forth [3–5]. There are many methodologies used by the phisher to trick the user to deceive them and to steal their personal credentials. Very often phisher used spoofed E-mails and forged websites to deceive the users. Web spoofing is one type of attack where phisher use artificial or forged sites to cheat users and to steal their personal information. The phishing E-mail seems to be a real one and even the website designed for the very purpose which directed the user to enter information looks real one. Mostly fake messages spread through E-mails, short message service (SMS), instant messengers, social networking sites, Voice over Internet Protocol (VoIP), and so forth, but E-mail is the most popular way and 65% of the phishing attack took place due to a click on the hyperlink attached to the E-mail [6]. Spear phishing is one of the methods used by the phisher to dupe organizations and individuals in Business E-mail Compromise (BEC). The very sophisticated spear phishing attacks [7–9] to target selected groups, individuals in an organization. Phishing is a type of attack that is very similar to fishing in a pond or river, but instead of trying to catch a fish, the phisher try to dupe user's most vital information [10, 11]. A user generally follows the authentication procedure by filing login id and passwords. The password should be strong password from security point of view to protect it from the attackers. Many anti-phishing tools were developed to provide stronger security which includes using image as input in the login process and hashing of passwords [12]. The web sites are specially designed by the phisher to looks to be legitimate one for which it is becoming very difficult for the user to detect fake website through their appearance.

1.1 Related work

Tan et al. [13] suggested an anti-phishing method to extract body tags and Meta from the URL. The uniform resource locator (URL) is broken down into tokens and after that the keywords are compared with yahoo search engine. The original domain name is compared against the given domain name and also with the country code of top level domain to check if there is a matching. The country code of top level domain is matched with that of web site and if found correct then it is considered as real web site otherwise fake website. Yan et al. [14] reviewed on Chinese phishing on Ecommerce sites. Sequential minimal optimization algorithm is used for the purpose and the features such as URL and the web features are used for detection of phishing. Genetic algorithm has been used to optimize the features. The data mining tool Waikato Environment for Knowledge Analysis (WEKA) is used to train the model that the system proposes. Li et al. [15] suggested using machine learning to detect phishing web pages. He has used document object model to optimize the features and emphases has given to web image that are extracted from the webpage. The features after optimization are passed into transductive support vector machine to differentiate between fake web site and real web site.

1.2 Existing work on phishing

Gemini is a well known tool used for the authentication process to protect the user against phishing. There were some anti-phishing techniques available today to prevent user from falling prey to the fake web sites by providing a strong secured authentication process. Some of the reputed sites display the security indicator for their sites to convey a message to the user that the site is not a fake website. The presence of URL indicator enables the users to identify the site as a real one [16, 17]. In some cases in the absence of such security indicators, the users avoid themselves from entering the passwords [13]. One of the examples of such is Sitekey [18] which is used by Bank of America for internet banking [19]. The user can choose an image

as input into the login process and when the user trying to login, the system will validate the image. In case the input image is wrong then the user stopped form login and authentication failed. Dhamija et al. [20] in his paper titled “dynamic security skins” proposed to use personal identity for authentication by the remote server that the user can verify. So in this method the web site will be considered as fake web site if the identity of the web site cannot be proved. Parno et al. [21] presented an anti-phishing technique which uses hard ware devices such as smart phones and smart tokens to authenticate. Although a user unknowingly log into a phishing site, this process helps the user to protect the vital information from leaking out to phisher because of this trusted authentication procedure. Gemini does not require the support of other devices in comparison to other existing techniques. There are some anti-phishing techniques such as Antiphish [22] and Webwallet [23] already available to identify the actual intent of users browsing activity which helps the user from falling prey to phishing attacks. This research work takes user name as input to initiate anti-phishing technique which helps the user to protect their vital information whereas other techniques based more on passwords. Yue et al. [24] proposed a technique that is free from any kind of deceit to protect the user credentials being leaked out fraudsters by hiding the actual content from the fake sites. It makes the fraudsters very tough to retrieve user’s secret info before the user identifies the site as fake. Some password management techniques such as PwdHash [19], Password Multiplier [15], and passpet [24] offer password hashing to provide better security strength for passwords. Because of rehashing of passwords and randomly changing the name of web sites a phisher could not make use of the stolen information. Birk et al. [12] suggested a different mechanism to track the identity of the attacker. He has proposed to use of fingerprint credentials to track the stolen information from fake sites.

2. Case studies in phishing

2.1 Case study: website phishing experiment

In this study a website was designed with an exact replica of website www.ahlionline.com, the original Jordan Ahli Bank website. The objective is to misleading the user’s by targeted phishing E-mail attack to giving away their vital information. We intentionally put a lot of known phishing features during web site design to understand the user’s awareness of these kinds of risk after getting authorization from the management. We used Internet Protocol (IP) address instead of domain name, http instead of https, poor design, spelling errors, absence of secure sockets layer (SSL), padlock icon and phony security certificate. We almost achieve our target to attack 120 employees through well planned phishing E-mail, informing them that their e-banking accounts are at high risk of being attacked and requested them to immediately log into their account through fake link attached to our E-mail to verify their balance in the account. We successfully deceive 52 from the group of 120 employees in our organization representing 44% of the sample, who followed the deceiving instructions and give away their actual credentials. The very surprising fact is 8 employees of the IT department and IT auditors are victims out of the 120 representing 7% of the sample. 44 employees from other departments out of 120-targeted victims representing 37% of the sample fell into the trap and give away their information without much hesitation. 28 employees are very cautious and given wrong information representing 23% of the sample and 40 employees choose not to respond at all after receiving the E-mail representing 33% of the sample. The experimental result shows that phishing is extremely dangerous to the whole society

since almost half of the employees who responded were victimized. In particular the very well educated and technically trained people from IT department and IT auditors are also among them. So increasing the awareness of all users who are using e-banking facility regarding this risk factor is highly recommended [25].

2.2 Case study: phone phishing experiment

A group of around 50 employees in an organization were contacted by their female colleagues to lure them into giving away their personal e-banking accounts details such as user id and passwords through friendly conversations with an aim to deceiving them. The results were very surprising as many of the employees fell for the trick. After having friendly conversations for quite for some time with them, the assigned team able to seduce them into giving away their e-banking details such as user id and passwords for false reasons. Some of these lame reasons which were used in the conversations are to check the account integrity, their privileges and accessibility and connectivity issues with the Web server for maintenance purpose. The assigned team managed to deceive 16 out of the 50 employees used for testing purpose into giving away their complete e-banking information such as user id and password, which is about 32% of the sample. Another eight employees (16% of the sample) agreed to give their user name only. The remaining 52% of the sample (26 employees) were very vigilant and decided not to reveal any information over the phone. The summary of the testing results reveals the high risk of the social engineering security factor. The results prove that there is a urgent need to increase the awareness of customers not to fall victims of this kind of threat which can have devastating results [26].

2.3 Case study: business email compromise (BEC)

The Nigeria-based Business E-mail Compromise (BEC) attack hit over 50 countries in 2017, targeting more than 500 businesses predominantly industrial organizations. The phishing scam directed the user to download a malicious file. When these files were downloaded, malware would gain authorized access to their business data and networks [27].

2.4 Case study: shipping information

The internet security company Comodo found a new type of phishing scam specifically to target small businesses in July 2018. E-mails containing phishing spam was sent out to more than 3,000 small businesses firms, mentioning Shipping Information on the subject line. The E-mail was to inform about approaching delivery by United Parcel Service (UPS) and the user were asked to click on the delivery tracking link to get the delivery status. When the user clicked on the delivery tracking link it contained malware, potentially releasing a virus [27].

3. Proposed system architecture

Even though there are several methods exists today to detect phishing but still it has become a very difficult task to detect fake E-mails in the current scenario. Today there are a number of techniques exist for identification of phishing E-mails and some of them are white listing, heuristics, blacklisting and machine learning. A machine learning technique is proposed in this chapter to identify the phishing E-mails and protect the user from revealing their pin, user id and passwords. The objective of

this chapter is to use J48 one of the machine learning algorithms to analyze incoming E-mails and helps in preventing the user from phishing attacks. This chapter presented an architectural model as shown in **Figure 1** below and uses the various sub-processes at different stages to classify between fake E-mail and genuine E-mails.

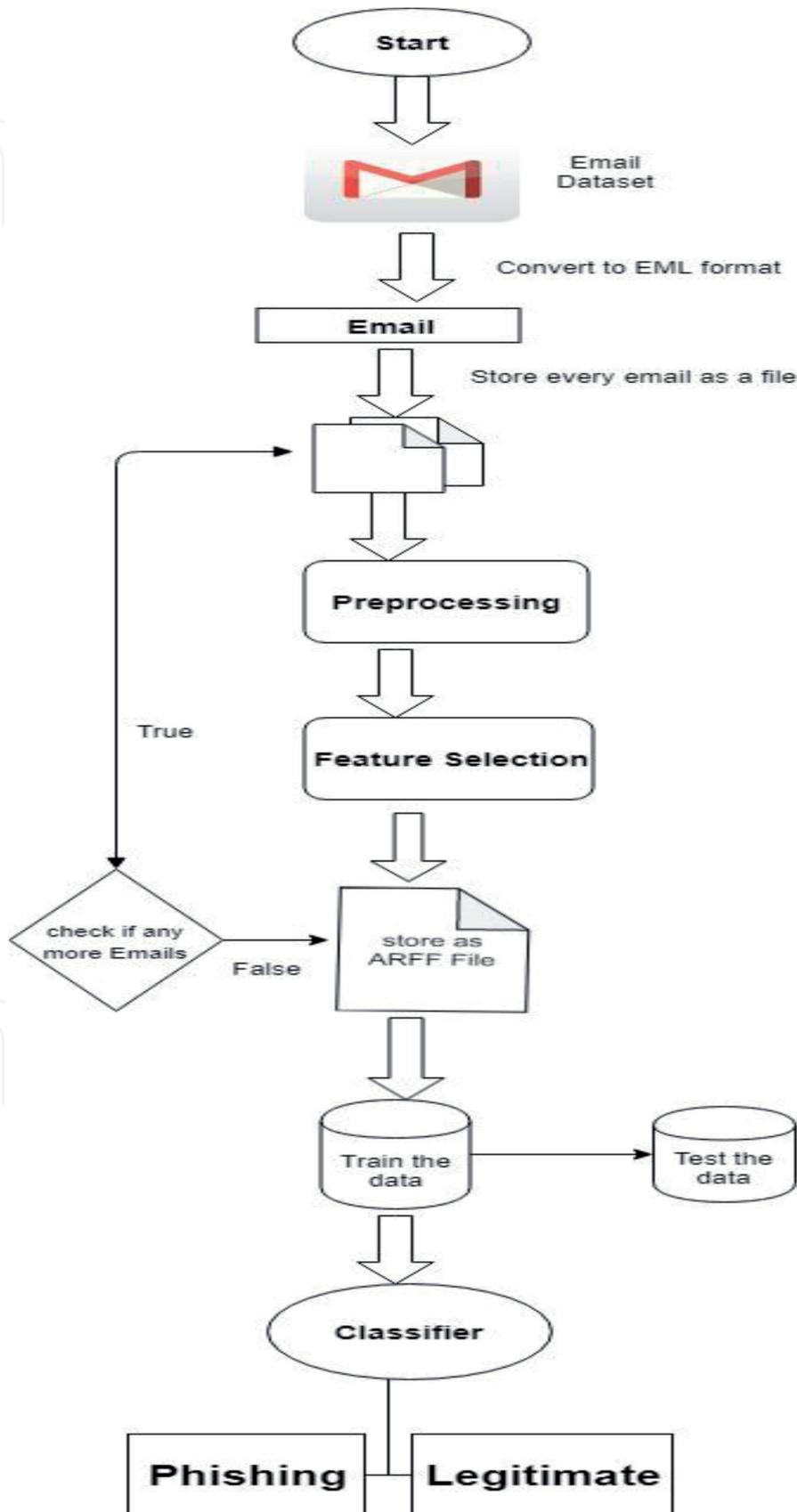


Figure 1.
Shows the architectural model of the proposed work.

3.1 The architectural model

The architectural model presented in the chapter as stated in **Figure 1** consists of seven sub-modules as Input Raw E-mails (data set), Covert to Electronic Mail Format (EML) format, Data Preprocessing, Feature Selection, Training Phase and using the model to classify test data. In the initial stage the system reads the raw E-mails data from Enron dataset. In the second stage convert them into EML (Electronic Mail Format) format and store them as a file. The third stage is data Pre-processing to removes unnecessary words through tokenization. The fourth stage is feature extraction. The features such as body, to, from, URL, carbon copy (Cc), blind carbon copy (Bcc) and the body of the E-Mails that is message are extracted from the input E-mails. In fifth stage the extracted data get converted into Attribute Relation File Format (ARFF). The sixth stage is training phase where model which is used for classification is trained using J-48 classification. The next stage is testing phase and the model is used to classify the E-mails to fake E-mail and real E-mails.

1. The very first step in E-mail classification is to select the suitable E-mail data-set which is a real sample of existing E-mails that includes both phishing and legitimate E-mails.
2. After E-mail data set is selected, splitting each and every E-mail and then converting them into Electronic Mail Format (EML). EML files are normally store each and every message as a single file and attachments may either be in the form of Multipurpose Internet Mail Extensions (MIME) content in the message or can be written off as a separate file.
3. Then data pre-processing is applied on to the above files to remove stop words and unwanted information. Then data reduction technique is applied to reduce the data size that needs to be examined. At the last step in the pre-processing phase lemmatization and stemming technique applied on token of words to convert them into their root forms.
4. After the data pre-processing step is over, then feature selection process starts with the cleaned data to extract different features form the E-mail data set. The features such as to, from, URL, carbon copy (Cc), blind carbon copy (Bcc) and the body of the E-Mails are extracted from the input data set. The process of feature extraction goes on unless the complete data is scanned properly and all the features are extracted. The most important features are E-mail header, Body, Java script and URL as given below.
 - E-mail Header: The header information is extracted from E-mail's data set. The header features are to, from, bcc, and cc fields. Some of the most popular phishing E-mail header includes keywords such as bank, debit, credit, Fwd:, Re:.
 - Body of E-mail: The body part of the E-mail is selected from the E-mails which contains the message part of the E-mail. Mostly phishing E-mail body include keyword such as dear, credit, click, log, identify, information, suspension and verify your account.
 - Java-script: It mainly contains a Java-script code in the email body. A phishing E- mail most of the time contain an On Click event, pop-up window code, or a code that links to an external website.

- URL: The uniform resource locator (URL) contains suspicious URLs. The phishing E-mail mostly contain “@” sign in the URL, port numbers in the URL, presence of an IP address in the URL.
- Network-based: The network-based feature mostly contains packet size and TCP/IP headers.

5. In order to apply classification algorithm to detect phishing E-mail the data needs to be converted into Attribute Relation File Format (ARFF). This chapter has suggested using J48 classifier for the E-mail dataset classification. Decision tree J48 algorithm is the extension of most popular ID3 (Iterative Dichotomise 3). This algorithm is most suitable for E-mail dataset classification where it can handle errors and missing values to some extent.

6. The model is trained in the training phase using the training data set and model is evaluated for its suitability.

7. After the model is thoroughly trained and evaluated properly, it is used to classify the test data set.

8. Finally the E-mail data set are classified into genuine, phishing E-mail and accuracy of the classifier is calculated from the confusion matrix.

3.2 Implementation and discussion on results

Enron data set is used to test the model being proposed by the chapter that includes both genuine E-mails and phishing E-mails. Initially the Data Pre-processing is performed on the data set to remove stop words, superfluous words and also the size of the data is reduced to get better result as shown below in **Figure 2**.

As stated above in **Figure 3**, the chapter is being implemented using J48 classifier for classification genuine E-mails and phishing E-mails with 98% accuracy. In order to measure the efficiency and performance of the proposed algorithm

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
Sno	Message-Id	Date	From	To	Subject	X-From	X-To	X-cc	X-Folder	X-Origin	prediction	predicted content								
1	0 301138621C	20121999	frozensteb frozensteb	'evergree	'daren j fa	'jull meye nan	'darrenfar	'farmerd				1 'congrat 1	'congrat 1 year special cinema pass 2 cell 09061209465 c supman v metrix3 starv							
2	1 203447081	20121999	frozensteb frozensteb	'burg old t	'daren j fa	'brenda f l' mari smit	'darrenfar	'farmerd				1 'ok lar joki	'ok lar joke wif u on!							
3	2 138575151	20121999	frozensteb frozensteb	'januari pr	'daren j fa	'kenneth i nan	'darrenfar	'farmerd				1 'free entri	'free entri 2 wkll comp win fa cup final tkt 21st may 2005 text fa 87121 receiv en							
4	3 19464031C	20121999	frozensteb frozensteb	'hlp 1199	'daren j fa	'kimberli v' anita luor	'darrenfar	'farmerd				1 'u dun say	'u dun say earli hor u c already say'							
5	4 311818821	20121999	frozensteb frozensteb	'meter 58'	'daren j fa	'susan tre nan	'darrenfar	'farmerd				1 'nah dont	'nah dont think goe usf live around though'							
6	5 146427411	09042001	frozensteb frozensteb	'deal 7108'	'daren j fa	'michael c nan	'darrenfar	'farmerd				1 'freemsg i	'freemsg hey darl 3 week word back id like fun still tb ok xxx std chg send 150 rc							
7	6 123545801	05042001	frozensteb frozensteb	'wellhead	'daren j fa	'robert co nan	'darrenfar	'farmerd				1 'even brot	'even brother like speak treat like aid patent'							
8	7 326054211	05042001	frozensteb frozensteb	'fiv payme	'daren j fa	'jo hilliers nan	'darrenfar	'farmerd				1 'per requ	'per request mell mell oru minnaminungint nurungu vettam set callertun caller							
9	8 218906761	04042001	frozensteb frozensteb	'?	'daren j fa	'victor larr nan	'darrenfar	'farmerd				1 'winner va	'winner valu network custom select receivea 900 prize reward claim call 090617							
10	9 25809821	04042001	frozensteb frozensteb	'air produ	'daren j fa	'juliann ke nan	'darrenfar	'farmerd				1 'mobil 11	'mobil 11 month u r entitl updat latest colour mobil camera free call mobil upda							
11	10 300512341	04042001	frozensteb frozensteb	'feb 01 pr	'daren j fa	'katherin l' juli meye	'darrenfar	'farmerd				1 'im gonna	'im gonna home soon dont want talk stuff anymore tonight k ive cri enough toda							
12	11 97948401C	02042001	frozensteb frozensteb	'?	'daren j fa	'buylow b nan	'darrenfar	'farmerd				1 'six chanc	'six chanc win cash 100 20000 pound txt csh11 send 87575 cost 150pday 6day 16 t							
13	12 38414931C	02042001	frozensteb frozensteb	'path que	'daren j fa	'juliann ke nan	'darrenfar	'farmerd				1 'urgent 1	'urgent 1 week free membership 100000 prize jackpot txt word claim 81010 to w							
14	13 52520151C	02042001	frozensteb frozensteb	'mobil be	'daren j fa	'rebecca g nan	'darrenfar	'farmerd				1 'live sear	'live search live search right word thank breather promi wont take help grant fulfil promi w							
15	14 224715401	02042001	frozensteb frozensteb	'fix price s	'daren j fa	'gari w lan nan	'darrenfar	'farmerd				1 'date sunc	'date sunday'							
16	15 240506271	30032001	frozensteb frozensteb	'cpl	'daren j fa	'rebecca g nan	'darrenfar	'farmerd				1 'xxxmobil	'xxxmobilemovieclub use credit click wap link next txt messag click httpwap xx							
17	16 122982231	30032001	frozensteb frozensteb	'tenaska 2'	'daren j fa	'megan pe nan	'darrenfar	'farmerd				1 'oh kim w	'oh kim watch'							
18	17 996088107	29032001	frozensteb frozensteb	'park 1201'	'daren j fa	'dena paw nan	'darrenfar	'farmerd				1 'eh u rem	'eh u rememb 2 spell name ye v naughty make v wet'							
19	18 293663011	28032001	frozensteb frozensteb	'happen t'	'daren j fa	'matt pen nan	'darrenfar	'farmerd				1 'fine way	'fine way u feel way gota b'							
20	19 72850501C	28032001	frozensteb frozensteb	'cpl	'daren j fa	'rebecca g nan	'darrenfar	'farmerd				1 'england	'england v macedonia dont miss goalsteam news txt ur nation team 87077 eg er							
21	20 332771871	28032001	frozensteb frozensteb	'duke	'daren j fa	'mari pool nan	'darrenfar	'farmerd				1 'seriou spi	'seriou spell name'							
22	21 44187841C	28032001	frozensteb frozensteb	'fom hpl n'	'daren j fa	'robert co nan	'darrenfar	'farmerd				1 'im go tri	'im go tri 2 month ha ha joke'							
23	22 105575741	28032001	frozensteb frozensteb	'duke ene	'daren j fa	'megan pe nan	'darrenfar	'farmerd				1 'pay first	'pay first lar da stock comin'							
24	23 53172371C	21032001	frozensteb frozensteb	'central pc	'daren j fa	'gari w lan' aime lanr	'darrenfar	'farmerd				1 'aft finish	'aft finish lunch go str lor ard 3 smth lor u finish ur lunch already'							

Figure 2.
 This shows feature selection process after data preprocessing.

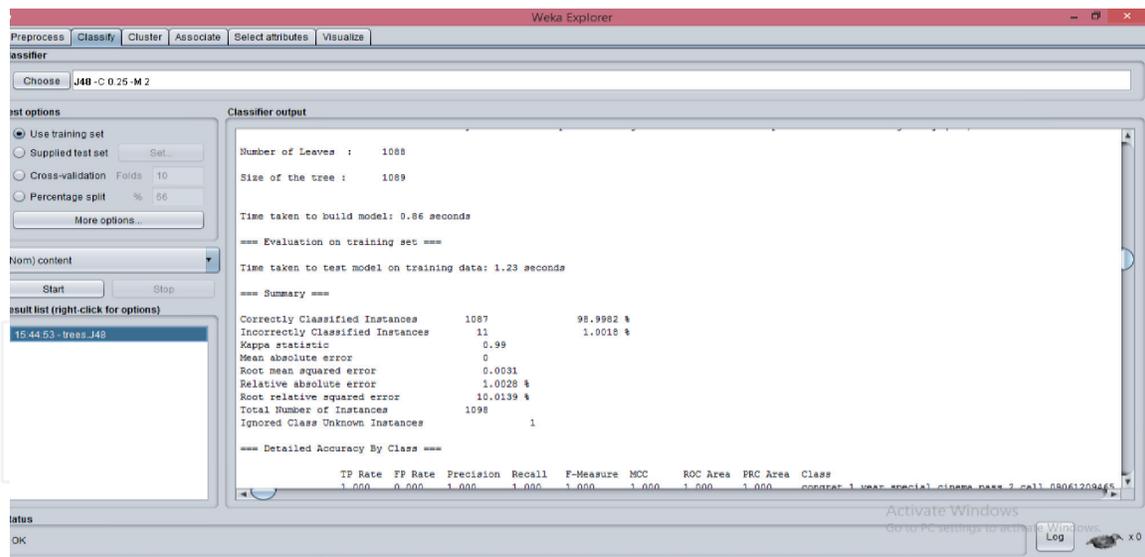


Figure 3.
This figure show E-mails are classified using weka tool.

in detecting phishing E-mails, False Positive (FP), True Positive (TP), True Negative (TN) and False Negative (FN) are computed and considered in the result. Then accuracy, Precision, Recall and F-1 score are computed using the formula given below.

1. **ACCURACY:** Accuracy is used to find the correct values; it is the sum of all true values divided by total values

(True Positive + True Negative)/(True Positive + True Negative + False Positive + False Negative)

$$\text{ACCURACY} = \frac{(TP + TN)}{(TP + TN + FP + FN)}$$

2. **PRECISION:** How often a model predicts a positive value is correct? It is all the true positives divided by the total number of predicted positive values.

(True Positive/True Positive + False Positive)

$$\text{PRECISION} = \frac{(TP)}{(TP + FP)}$$

3. **RECALL:** It used to calculate the models ability to predict positive values. How often does the model actually predict the correct positive values? It is true positives divided by the total number of actual positive values.

(True Positive/True Positive + False Negative)

$$\text{RECALL} = \frac{(TP)}{(TP + FN)}$$

4. **F-1 SCORE:** F1 measure is used when we need to take both Precision and recall.

$$F1 = \frac{2 \times PRECISION \times RECALL}{(PRECISION + RECALL)}$$

4. Conclusion

At this modern era as more and more people use internet for their day to day activities so as hackers on the network to steal their vital data through various security attacks. The objective of this chapter to presents a model using machine learning technique to detect phishing attacks and to prevent users from phishing. This chapter provides a very powerful architectural model in order to identify phishing E-mails. This chapter ends with a conclusion that phishing attacks is very dangerous to everyone in the society including organizations, person and hence must be detected accurately. Many researchers have contributed by giving their ideas to classify phishing E-mails from genuine E-mails but without much success. This chapter used J48 classification algorithm to classify between fake E-mails and genuine E-mails and it was observed that the model able to classify 98% accurately which is a far better result. Hence the model proposed in this chapter is very accurate and efficiently classify and could able to identify phishing E-mails. This chapter would provide a great help for ordinary man in protecting their important information by detecting phishing attacks.

Conflict of interest

I the author of “An Emerging Solution for Detection of Phishing Attacks” states that this research works fully compile with ethical standards as per the Journal.

I have no direct or potential influence or impart bias on this research work.

I have no conflict conflicts of interests that are directly or indirectly related to this research work.

I have no funding from any funding agency or financial support from any organization.

Acronyms and abbreviations

E-mail	Electronic mail
URL	uniform resource locator
EML	Electronic Mail Format
SMS	short message service
VoIP	Voice over Internet Protocol
WEKA	Waikato Environment for Knowledge Analysis
IP	Internet Protocol
SSL	secure sockets layer
BEC	Business Email Compromise
UPS	United Parcel Service
Cc	Carbon copy
Bcc	blind carbon copy
ARFF	Attribute Relation File Format
MIME	Multipurpose Internet Mail Extensions

IntechOpen

IntechOpen

Author details

Prasanta Kumar Sahoo

Department of Computer Science and Engineering, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana, India

*Address all correspondence to: prasantakumars@sreenidhi.edu.in

IntechOpen

© 2021 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] P. Liu and T. S. Moh, "Content Based Spam E-mail Filtering," 2016 International Conference on Collaboration Technologies and Systems (CTS), Orlando, FL, pp. 218-224.
- [2] N. Agrawal and S. Singh, "Origin (dynamic blacklisting) based spammer detection and spam mail filtering approach," 2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC), Moscow, pp. 99-104.
- [3] M. Khonji, Y. Iraqi, and A. Jones, "Phishing detection: a literature survey," 2013 IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2091-2121.
- [4] R. Islam and J. Abawajy, "A multi-tier phishing detection and filtering approach," Journal of Network and Computer Applications, 2013 vol. 36, no. 1, pp. 324-335.
- [5] A. K. Jain and B. B. Gupta, "Comparative analysis of features based machine learning approaches for phishing detection," in Proceedings of the 10th INDIA-COM, New Delhi, India, 2016.
- [6] Kaspersky Lab, "Spam in January 2012 love, politics and sport," 2013, http://www.kaspersky.com/about/news/spam/2012/Spam_in_January_2012_Love_Politics_and_Sport.
- [7] B. Parmar, "Protecting against spear-phishing," Computer Fraud & Security, 2012 vol. 2012, no. 1, pp. 8-11.
- [8] W. Jingguo, T. Herath, C. Rui, A. Vishwanath, and H. R. Rao, "Phishing susceptibility: an investigation into the processing of a targeted spear phishing e-mail," 2012 IEEE Transactions on Professional Communication, vol. 55, no. 4, pp. 345-362.
- [9] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," Communications of the 2007 ACM, vol. 50, no. 10, pp. 94-100.
- [10] C. H. Hsu, P. Wang, and S. Pu, "Identify fixed-path phishing attack by STC," in Proceedings of the 8th Annual Collaboration, Electronic Messaging, Anti-Abuse and Spam Conference (CEAS '11), ACM, Perth, Australia, September 2011, pp. 172-175.
- [11] N. A. G. Arachchilage and M. Cole, "Designing a mobile game for home computer users to protect against phishing attacks," <https://arxiv.org/abs/1602.03929>
- [12] Rosiello, A., Kirda, E., Ferrandif F., et al. "A layoutsimilarity-based approach for detecting phishing pages", In the Proceedings of third International Conference on Security and Privacy in Communication Networks (Secure-Comm), 2007 IEEE, pp. 454-463.
- [13] Choon Lin Tan, Kang Leng Chiew, San Nah Sze, "Phishing Webpage Detection Using Weighted URL Tokens for Identity Keywords Retrieval", in the proceedings of 9th International Conference on Robotic, Vision, Signal Processing and Power Applications, Springer Singapore 2017, pp. 133-139.
- [14] Zhijun Yan, Su Liu, Tianmei Wang, Baowen Sun, Hansi Jiang, Hangzhou Yang, "A Genetic Algorithm Based Model for Chinese Phishing E-commerce Websites Detection in HCI in Business", Government, and Organizations: eCommerce and Innovation, Springer International Publishing, 2016.
- [15] Yuancheng Li, Rui Xiao, Jingang Feng, Liujun Zhao, "A semi-supervised learning approach for detection of phishing webpages," 2013 Optik-International Journal for Light and

Electron Optics, vol. 124, Issue 23, December 2013.

[16] Wenyin, L., Huang, G., Xiaoyue, L., Min, Z., and Deng, X. "Detection of phishing web pages based on visual similarity", In the Special interest tracks and posters of the 14th international conference on World Wide Web (WWW), 2005 ACM, pp. 1060-1061.

[17] Whalent, T., and Inkpen N, K. M. "Gathering evidence: use of visual security cues in web browsers", In the Proceedings of 2005 Graphics Inter- face (GI), Canadian Human-Computer Communications Society, pp. 137-144.

[18] Rsa sitekey solution for enterprise. <http://www.RsaSecurity.com>, 2007. Bank of america, sign up for the sitekey service. <http://www.bankofamerica.com/privacy/passmark/>.

[19] Dhamija, R., and Tygar, J, "The battle against phishing: Dynamic security skins", In the Proceedings of the Symposium on Usable Privacy and Security (SOUPS), ACM 2005, pp. 77-88.

[20] Parno, B., Kuo, C., and Perrig A., "Phoolproof phishing prevention", In the Proceedings of the 10th international conference on Financial Cryptography and Data Security, Springer-Verlag 2006, pp. 1-19.

[21] Kirda, E., and Kruegel, C, "Protecting users against phishing attacks with antiphish", In the Proceedings of the 29th Annual International Computer Software and Applications Conference (COMPSAC), IEEE 2005, pp. 517-524.

[22] Wu, M., Miller, R., and Little, G, "Web wallet: preventing phishing attacks by revealing user intentions", In the Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPS), 2006 ACM, pp. 102-113.

[23] Yee, K., and Sitaker, K., "Passpet: convenient password management and phishing protection", In the Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPS), 2006 ACM, pp. 32-43.

[24] Yue, C., and Wang, G H. Bogusbite, "A transparent protection against phishing attacks", ACM Transactions on Internet Technology (TOIT) 2010 Vol.10 n.2, pp.1-31.

[25] Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Predicting Phishing Websites Using Classification Mining Techniques with Experimental Case Studies. 2010 Seventh International Conference on information technology: New Generations. doi : 10.1109/itng.2010.117.

[26] M. A. Hossain Dept. of Computing University of Bradford Bradford, Predicting Phishing Websites Using Classification Mining Techniques with Experimental" UK, 2010.

[27] <https://smallbiztrends.com/2017/08/phishing-examples-small-business.html>.