PHISHING EMAIL DETECTION

K. Aashish Dubey [#1], *K. Bharath Ganesh* [#2], *V. Gowtham* [#3], *Mr.D. Balakrishnan* [* 4]

[#] *Student , Department of Computer Science and Engineering, Kalasalingam Academy of Research & Education, Krishnankovil, India, 9917004001@klu.ac.in*

[#] *Student , Department of Computer Science and Engineering, Kalasalingam Academy of Research & Education, Krishnankovil, India, 9917004014@klu.ac.in*

[#] *Student , Department of Computer Science and Engineering, Kalasalingam Academy of Research & Education, Krishnankovil, India, 9518004301@klu.ac.in*

[*] *Assistant Professor, Department of Computer Science and Engineering, Kalasalingam Academy of Research & Education, Krishnankovil, India, balakrishnan@klu.ac.in*

***Abstract*— The phishing email is one of the significant threats in the world today and has caused tremendous financial losses. Although the methods of confrontation are continually being updated, the results of those methods are not very satisfactory at existing system. Here, we used Data mining as well as web mining to detect patterns and mine out textual information on web pages. Here, we are using phishing system to detect the unwanted messages that are more susceptible to terrorism and will send to the spam directly to the recipient who is using the system.**

***Index Terms*— Email, Phishing detection, Classification, RCNN, Attention**

I. INTRODUCTION

The rapid development of Internet technologies has immensely changed on-line users' experience, while security issues are also getting more overwhelming. The current situation is that new threats may not only cause severe damage to customers' computers but also aim to steal their money and identity. Among these threats, phishing is a noteworthy one and is a criminal activity that uses social engineering and technology to steal a victim's identity data and account information. According to a report from the Anti-Phishing Working Group (APWG), the number of phishing detections in the first quarter of 2018 increased by 46% compared with the fourth quarter of 2017. According to the striking data, it is clear that phishing has shown an apparent upward trend in recent years. Similarly, the harm caused by phishing can be imagined as well. The report from PhishLabs notes that email and online services overtook financial institutions as the top phishing target. For phishing, the most widely used and influential mean is the phishing email. Phishing email refers to an attacker using a fake email to trick the recipient into returning information such as an account password to a designated recipient. Additionally, it may be used to trick recipients into entering special web pages, which are usually disguised as real web pages, such as a bank's web page, to convince users to enter sensitive information such as a credit card or bank card number and password. Although the attack of phishing email seems simple, its harm is immense. In the United States alone, phishing emails are expected to bring a loss of 500 million dollars per year. According to the APWG, the number of phishing emails increased from 68,270 in 2014 to 106,421 in 2015, and the number of different phishing emails reported from January to June 2017 was approximately 100,000. In addition, Gartner's report notes that the number of users who have ever received phishing emails has reached a total of 109 billion.

II. RELATED WORK

With the emergence of email, the convenience of communication has led to the problem of massive spam, especiallyphishing attacks through email. Various anti-phishing technologies have been proposed to solve the problem of phishingattacks. S. Sheng et al. [1] studied the effectiveness of phishing blacklists. Blacklists mainly include sender blacklists andlink blacklists. This detection method extracts the sender'saddress and link address in the message and checks whetherit is in the blacklist to distinguish whether the email is aphishing email. The update of a blacklist is usually reportedby users, and whether it is a phishing website or not ismanually identified. At present, the two well-known phishingwebsites are PhishTank and OpenPhish. To some extent, theperfection of the blacklist determines the effectiveness of thismethod based on the blacklist mechanism for phishing emaildetection.With the development of AI, phishing email detection hasalso entered the era of machine learning. In particular, thecombination of NLP and machine learning has played asignificant role in phishing email detection. Semantic features [2], syntax feature [3], and contextual features [4]previously have been used in this area. A. Vazhayil et al.[5] started from the most basic machine learning methodsand used decision trees, logistic regression, random forests,and SVM combined with supervised classification to detectphishing emails. I. R. A. Hamid et al. [6] proposed a hybridfeature selection method that combines content and behavior.The detection method for phishing emails using machinelearning mainly uses marked phishing emails and legitimateemails to train the classification algorithm in the machinelearning algorithm to obtain the classifier model for emailclassification. A. Bergholz et al. [7] put forward a series ofthe probability of an email belonging to a specific categoryis achieved by modeling each type of message content. The use of nuclear energy to generate electric power is crucial to meet the high energy demand of a modern economy. In newly constructed nuclear power plants (NPPs), the trend among control systems is to replace the obsolete analog hard-wired systems.

III. TRADITIONAL SYSTEM

The existing detection methods based on the blacklist mechanism mainly rely on people's identification and reporting of phishing links requiring a large amount of manpower and time. The Existing detection method based on deep learning is limited to word embedding in the content representation of the email. These methods directly transferred natural language processing (NLP) and deep learning technology, ignoring the specificity of phishing email detection so that the results were not ideal.

IV. METHODOLOGY

A naive Bayes classifier is an algorithm that uses Bayes' theorem to classify objects. Naive Bayes classifiers assume strong, or naive, independence between attributes of data points. Popular uses of naive Bayes classifiers include spam filters, text analysis and medical diagnosis. These classifiers are widely used for machine learning because they are simple to implement. Naive Bayes is also known as simple Bayes or independence Bayes. Here, this project using the naïve bayes classifier to mining out of common words or stop words from the mail what's the user send. The common words such as, and, then, the, there, or, therefore, hereafter, these, it, is, it's, this, he, she, her, him, etc., This are called preprocessing. In this process we have eliminate these kind out words. From that messages, we are going to highlighting the filteration words.

V. METHODOLOGY

There are two features used in this system that is data mining and web mining. Data mining is a technique used to mine out patterns of useful data from large data sets. Web mining also consists of text mining methodologies that allow us to scan and extract useful content from unstructured data. This system will check the sender messages and whether the message is promoting terrorism. Data mining as well as web mining are used together at times for efficient system development. System will find the unwanted messages that are more susceptible to terrorism and will send directly to the receiver's spam account. It will give more awareness to the users.

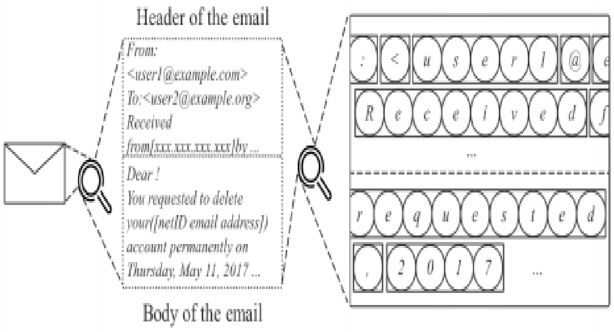
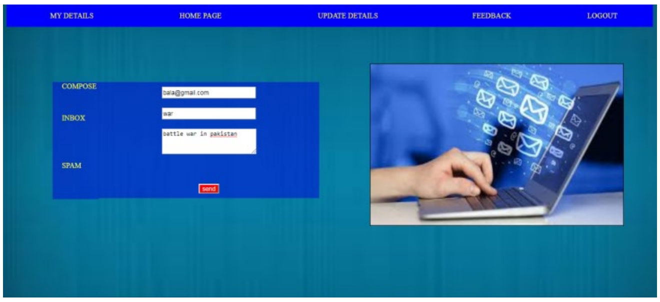


Figure 1: Proposed Methodology

VI. IMPLEMENTATION

Mailing

First, User should Register with their basic details through create an account link. By using that details they need to Login for enter into the system. Then they will receive the message of "success". Here, we are using the system like E-mail. Hence, it contain the features of inbox, sent mail, spam, recent histories, etc., The user can compose the mail with whom to sent. It may be related to terrorism or may something related to common things. Here, the recent history denotes the person who is doing mail recently.



bala@gmail.com

war

battle war in pakistan

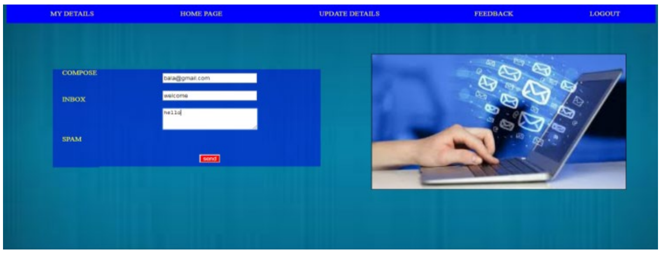
Figure 2: Mailing

Filtering

In this Module, This module have a few data's in Dataset. With that, I will check whether the sent message have contain the filteration words about terrorism or not? This module using Data mining technique to mine out text data from large data sets and make the most use of obtained results. Web mining consists of text mining methodologies. Through that text mining, we can extract the text or content what are all related to terrorism. If the filteration words are match with the sent message means, the receiver receives the mail in his/her spam box or else inbox.

Spam Detection

In this Module, Admin should login first. It will contain the predefined user name and password. Admin side, it will have the features of keywords, spam, analysis, chart. By using Mining concepts Administrator can add few terrorism related words manually in few parameters/ categories. That keywords will also going to add with the existing dataset . In spam, we can see what are all spam messages from starting. In analysis, It contains a mail having how many words in those keyword categories and their total count per each mail.



bala@gmail.com

welcome

hello

Figure 3: Spam Detection

Preprocessing

In this Module, Admin can see all the spam mail sent and receive in this system, whereas, Spam Detection will contain preprocessing which means it will remove all the common words/stop words such as the, and, or, here, there, etc.,

VII. CONCLUSION

To curb and destroy the terrorism and spreading of their activities through online social media through unwanted messages and images to cover the helpless people, we need to use the powerful method or system. That system should be useful to the cops for easily give awareness to common people and find the person who are spreading the harmful words as well as who are all involved in terrorism.

REFERENCES

[1] A.-P. W. Group et al., “Phishing activity trends report 1st quarter 2018,” USA: Anti-Phishing Working Group (APWG), 2018.

[2] PHISHLABS, “2018 phish trends & intelligence report,” https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend %20Report_2018-digital.pdf, 2018.

[3] M. Nguyen, T. Nguyen, and T. H. Nguyen, “A Deep Learning Model with Hierarchical LSTMs and Supervised Attention for Anti-Phishing,” arXiv preprint arXiv:1805.01554, 2018.

[4] A.-P. W. Group et al., “Phishing activity trends report 4th quarter 2016,” USA: Anti-Phishing Working Group (APWG), 2017.

[5] A.-P. W. Group et al., “Apwg attack trends report,” USA: Anti-Phishing Working Group (APWG), 2014.

[6] L. M. Form, K. L. Chiew, W. K. Tiong, et al., “Phishing email detection technique by using hybrid features,” in IT in Asia (CITA), 2015 9th International Conference on, pp. 1–5, IEEE, 2015.

[7] Microsoft, “Microsoft Security Intelligence Report,” https://clouddamcdnprodep.azureedge.net/gdc/gdcVAOQd7/original, 2018.

[8] M. Hiransha, N. A. Unnithan, R. Vinayakumar, and K. Soman, “Deep Learning Based Phishing E-mail Detection,” in Proceedings of the 1st AntiPhishing Shared Pilot at 4th ACM International Workshop on Securityand Privacy Analytics (IWSPA 2018) (A. D. R. Verma, ed.), (Tempe, Arizona, USA), 21-03-2018

[9] C. Coyotes, V. S. Mohan, J. Naveen, R. Vinayakumar, and K. Soman,“ARES: Automatic Rogue Email Spotter,” in Proceedings of the 1stAntiPhishing Shared Pilot at 4th ACM International Workshop on Securityand Privacy Analytics (IWSPA 2018) (A. D. R. Verma, ed.), (Tempe,Arizona, USA), 21-03-2018.

[10] S. Sheng, B. Wardman, G. Warner, L. Cranor, J. Hong, and C. Zhang, “Anempirical analysis of phishing blacklists,” in Sixth conference on emailand anti-spam (CEAS), California, USA, 2009.

[11] R. Verma and N. Hossain, “Semantic feature selection for text withapplication to phishing email detection,” in International Conference onInformation Security and Cryptology, pp. 455–468, Springer, 2013.

[12] G. Park and J. M. Taylor, “Using syntactic features for phishing detection,”arXiv preprint arXiv:1506.00037, 2015.

[13] R. Verma, N. Shashidhar, and N. Hossain, “Detecting phishing emails thenatural language way,” in European Symposium on Research in ComputerSecurity, pp. 824–841, Springer, 2012.

[14] A. Vazhayil, N. Harikrishnan, R. Vinayakumar, and K. Soman, “PED-ML:Phishing Email Detection Using Classical Machine Learning Techniques,”in Proceedings of the 1st AntiPhishing Shared Pilot at 4th ACM International Workshop on Security and Privacy Analytics (IWSPA 2018) (A. D.R. Verma, ed.), (Tempe, Arizona, USA), 21-03-2018.

[15] I. R. A. Hamid and J. Abawajy, “Hybrid feature selection for phishingemail detection,” in International Conference on Algorithms and Architectures for Parallel Processing, pp. 266–275, Springer, 2011.

[16] A. Bergholz, J. De Beer, S. Glahn, M.-F. Moens, G. Paaß, and S. Strobel, “New filtering approaches for phishing email,” Journal of computersecurity, vol. 18, no. 1, pp. 7–35, 2010.

[17] J. Singh, “Detection of Phishing e-mail,” IJCST, vol. 2, no. 1, 2011.

[18] A. Bergholz, J. H. Chang, G. Paass, F. Reichartz, and S. Strobel, “ImprovedPhishing Detection using Model-Based Features.,” in CEAS, 2008.