WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

E-Mail Spam Classification Via Deep Learning and Natural Language Processing

G.Logavarshini[#1], S.Yogalakshmi[#2]

[#1] M.Sc, Department of Computer Science, Kamban College of Arts and Science for Women, Tiruvannamalai-606603 .

[#2] Assistant professor, Department of Computer Science, Kamban College of Arts and Science for Women, Tiruvannamalai- 606603.

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 present. Moreover, phishing emails are growing at an alarming rate in recent years. Therefore, more effective phishing detection technology is needed to curb the threat of phishing emails. In this paper, we first analyzed the email structure. Then based on an improved Recurrent Convolutional Neural Networks (RCNN) model with multilevel vectors and attention mechanism, we proposed a new phishing email detection model named, which is used to model emails at the email header, the email body, the character level, and the word level simultaneously. To evaluate the effectiveness of, we use an unbalanced dataset that has realistic ratios of phishing and legitimate emails. Experimental results show that the. Meanwhile, the ensure that the filter can identify phishing emails with high probability and filter out legitimate emails as little as possible. This promising result is superior to the existing detection methods and verifies the effectiveness of in detecting phishingemails.

KEYWORDS: RCNN , PSHINIG DETECTION

1.INTRODUCTION:

The major issues faced by all the email users are spam mails which contain unwanted information and data and some fake data to spoil the life of the people and also some mails which cause harmful effects. Today, the job issues are faced by fifty percent of the people by both educated and uneducated people. In such a case, these people will get emails about advertisement mails which are completely fake. But by seeing that mail, this people will get interested or have a thought to communicate through the mail for what they are looking into it. More people are affected by this spam mails in similar cases. To reduce this risk and to save the people from this danger of spam mails, we are proposing this system to remove the spam mails. For filtering the spam mails, in this system we are using two filtering model. Namely, Opinion Rank and NLP based n-grams model. By using thesetwo models we will filter the spam mails and non-spam mails. And this system will optimize the data by removing the spam mails and also it calculates the storage of the mails

2.Literature survey:

[1] Anti-phishing aims to detect phishing content/documents in a pool of textual data. This is an important problem in cybersecurity that can help to guard users from fraudulent information. Natural language processing (NLP) offers a natural solution for this problem as it is capable of analyzing the textual content to perform intelligent recognition. In this work, we investigate state-of-the-art techniques for text categorization in NLP to address the problem of anti-phishing for emails (i.e, predicting if an email is phishing or not). These techniques are based on deep learning models that have attracted much attention from the community recently. In particular, we present a framework with hierarchical long short-term memory networks (H-LSTMs) and attention mechanisms to model the emails simultaneously at the word and the sentence level.

[2] With the rapid development of Internet, phishing and other frauds are becoming more and more serious. Criminals posing as banks, electricity providers, social networking sites to send fraudulent information to induce users to log on, steal user information, so that the vast numbers of users and financial institutions suffered property and economic losses. How to accurately and effectively identify phishing related Internet risks has been a major concern of the Internet. This paper analyzes the development history of phishing prevention and control, and presents a Borderline-Smote (Synthetic Minority Over-sampling Technique) DBN (Deeping Belief Network) method to detect phishing. The method uses deep learning phishing detection method based on web documents content and other features to improve 1% on the recognition accuracy. Furthermore the paper uses Borderline-Smote to solve the imbalanced data problem in the training of phishing detection, and further improve 2% on the F-value and recall rate.

[3]. We tackle this problem through the use of a machine learning classifier operating on a large corpus of phishing and legitimate emails. We design

SAFe-PC (Semi-Automated Feature generation for Phish Classification), a system to extract features, elevating some to higher level features, that are meant to defeat common phishing email detection strategies. To evaluate SAFe-PC , we collect a large corpus of phishing emails from the central IT organization at a tier-1 university. The execution of SAFe-PC on the dataset exposes hitherto unknown insights on phishing campaigns directed at university users. SAFe-PC detects more than 70 percent of the emails that had eluded our production deployment of Sophos, a state-of-the-art email filtering tool. It also outperforms SpamAssassin, a commonly used email filtering tool. We also developed an online version of SAFe-PC, that can be incrementally retrained with new samples. Its detection performance improves with time as new samples are collected, while the time to retrain the classifier stays constant.

[4] Anti-phishing aims to detect phishing content/documents in a pool of textual data. This is an important problem in cybersecurity that can help to guard users from fraudulent information. Natural language processing (NLP) offers a natural solution for this problem as it is capable of analyzing the textual content to perform intelligent recognition. In this work, we investigate state-of-the-art techniques for text categorization in NLP to address the problem of anti-phishing for emails (i.e, predicting if an email is phishing or not). These techniques are based on deep learning models that have attracted much attention from the community recently. In particular, we present a framework with hierarchical long short-term memory networks (H-LSTMs) and attention mechanisms to model the emails simultaneously at the word and the sentence level. Our expectation is to produce an effective model for anti-phishing and demonstrate the effectiveness of deep learning for problems in cyber security.

[5] We demonstrate the effectiveness of both approaches on the WMT translation tasks between English and German in both directions. With local attention, we achieve a significant gain of 5.0 BLEU points over non-attentional systems that already incorporate known techniques such as dropout. Our ensemble model using different attention architectures yields a new state-of-the-art result in the WMT'15 English to German translation task with 25.9 BLEU points, an improvement of 1.0 BLEU points over the existing best system backed by NMT and an n-gram reranker.

3. PROPOSED SYSTEM:

With the emergence of email, the convenience of communication has led to the problem of massive spam, especially phishing attacks through email. Various anti phishing technologies have been proposed to solve the problem of phishing attacks. studied the effectiveness of phishing blacklists. Blacklists mainly include sender blacklists and link blacklists. This detection method extracts the sender's address and link address in the message and checks whether it is in the blacklist to distinguish whether the email is a phishing email. The update of a blacklist is usually reported by users, and whether it is a phishing website or not is manually identified.

. According to a report from the Anti-Phishing Working compared with the fourth quarter of 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.

4. METHODOLOGY:

4.1 DATASET

The dataset has been divided into a training set and testing set. Both the training set and the testing set contain emails without header and emails with header. In this paper, we only focus on email data with the header. Due to the irrationality of the segmentation of the training set and the testing set in the original dataset, after merging the two datasets, the training-validation set and the testing set are redivided. The dataset is divided by stratified random sampling; that is, random samples are taken from legitimate email and phishing email at the same proportion. This ensures that the two datasets used in training and testing phases are well.

4.2 USER QUERIES

Users can have queries about the process. This part of project is dedicated to make and get response for queries that are needed to answerable. The major part of the modules is making project as interactive one, queries have been very normally arise to users regarding different details about the process.

4.3 GRAPH ANALYSIS

Graph analysis is the part where admin can knows the statistics about process of details. The data are taken from the project flow and it shows until updated value. The data are gives clear solution to admin that part of improvement and user satisfaction and other factors.

4.4 ANALYSIS

analysis of email structure. a circle represents a character, and a rectangle represents a word. A rectangle is filled with an indefinite number of circles, indicating that the word consists of an indefinite number of characters.

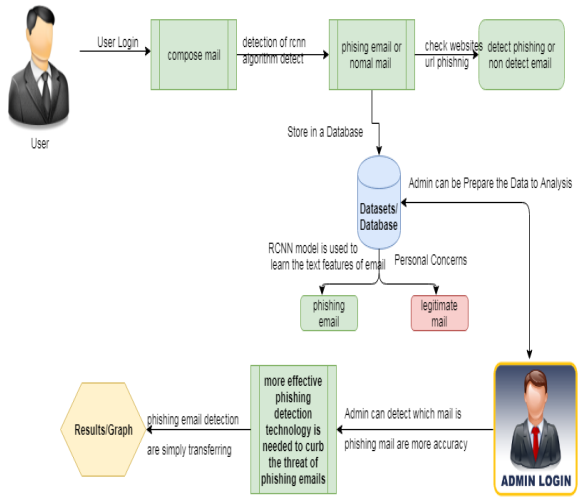
4.5 CYBER ANALYSIS

Cyber threatanalysis is a process in which the knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber-attacks. With respect to cyber security, this threat-oriented approach to combating cyber-attacks represents a smooth transition from a state of reactive security to a state of proactive one. Moreover, the desired result of a threat assessment is to give best practices on how to maximize the protective instruments with respect to availability, confidentiality and integrity, without turning back to usability and functionality conditions. CYPER ANALYSIS.A threat could be anything that leads to interruption, meddling or destruction of any valuable service or item existing in the firm's repertoire. Whether of "human" or "nonhuman" origin, the analysis must scrutinize each element that may bring about conceivable security risk.

4.6 RISKY USER DETECTION

False alarm immunity to prevent customer embarrassment, High detection rate to protect all kinds of goods from theft, Wide-exit coverage offers greater flexibility for entrance/exit layouts, Wide range of attractive designs complement any store décor, Sophisticated digital controller technology for optimum system performance.

5. ARCHITECTURE



6. CONCLUSION:

we use a new deep learning model named to detect phishing emails. The model employs an improved RCNN to model the email header and the email body at both the character level and the word level. Therefore, the noise is introduced into the model minimally. In the model, we use the attention mechanism in the header and the body, making the model pay more attention to the more valuable information between them. We use the unbalanced dataset closer to the real-world situation to conduct experiments and evaluate the model. The model obtains a promising result. Several experiments are performed to demonstrate the benefits of the proposed model. For future work, we will focus on how to improve our model for detecting phishing emails with no email header and only an email body.

7. OUTPUT

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

8.RESULTS:

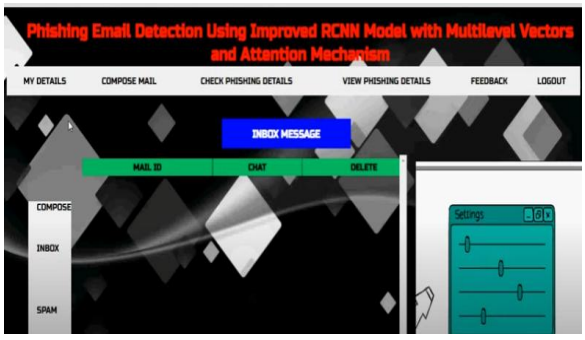


Fig 1: Phishing Email Inbox

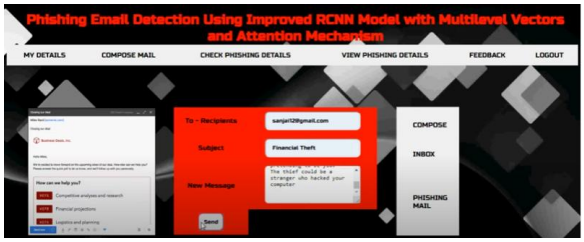


Fig 2: Phishing Email Detection

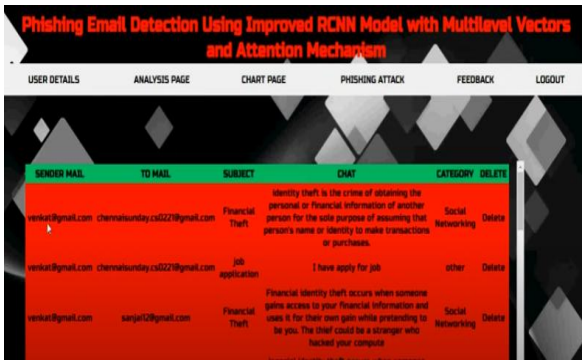


Fig 3: Admin phishing Detection

REFERENCES

[1] Corporate.target.com, "2014 Annual Report | Target Corporate", 2016. [Online]. Available: https://corporate.target.com/annual-reports/2014. [Accessed: 11- Oct- 2015].

[2] J. McHugh, "Testing Intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory", ACM Transactions on Information and System Security, vol. 3, no. 4, pp. 262-294, 2000.

[3] A. J. M. Abu Afza, M. S. Uddin, "Intrusion detection learning algorithm through network mining." In Computer and Information Technology (ICCIT), 2013 16th International Conference on, pp. 490-495, IEEE, Mar. 2014.

[4] J. P. Anderson, "Computer security threat monitoring and surveillance," Technical report, James P. Anderson Company, Fort Washington, Pennsylvania, vol. 17, 1980.

[5] D. Denning, S. Ak, M. Heckman, T. Lunt, M. Morgenstern, P. Neumann and R. Schell, "Views for Multilevel Database Security", IEEE Transactions on Software Engineering, vol. -13, no. 2, pp. 129-140, 1987.

[6] D. E. Denning, "An Intrusion-Detection Model," 1986 IEEE Symposium on Security and Privacy, 1986. [7] J. Quinlan, "Induction of decision trees", Mach Learn, vol. 1, no. 1, pp. 81-106, 1986.

[8] J. Bell, Machine learning: hands-on for developers and technical professionals. Indianapolis: John Wiley & Sons, 2015.

[9] W. Lee, S. J. Stolfo, and P. K. Chan, "Learning patterns from unix process execution traces for intrusion detection," AAAI Workshop on AI Approaches to Fraud Detection and Risk Management, pp. 50–56, Jul. 1997.

[10] T. Lane and C. E. Brodley, "Temporal sequence learning and data reduction for anomaly detection," ACM Transactions on Information and System Security TISSEC ACM Trans. Inf. Syst. Secur., vol. 2, no. 3, pp. 295–331, Jan. 1999.

[11] W. Lee and S. J. Stolfo, "Data mining approaches for intrusion detection," Usenix security, Jan. 1998.

[12] S. Forrest, et al., "A sense of self for unix processes," Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on. IEEE, pp. 120– 128, 1996.

[13] S. Forrest, S. A. Hofmeyr, and A. Somayaji, "Computer immunology," Communications of the ACM, vol. 40, no. 10, pp. 88–96, Oct. 1997.

[14] C. Warrender, S. Forrest, and B. Pearlmutter, "Detecting intrusions using system calls: alternative data models," Proceedings of the 1999 IEEE Symposium on Security and Privacy (Cat. No.99CB36344), pp. 133–145, 1999.

[15] B. C. Rhodes, J. A. Mahaffey, and J. D. Cannady, "Multiple selforganizing maps for intrusion detection," Proceedings of the 23rd national information systems security conference , pp. 16–19, Oct. 2000.

[16] J. Cannady, "Artificial neural networks for misuse detection," National information systems security conference, pp. 368-81, 1998.

[17] K. Julisch, "Mining alarm clusters to improve alarm handling efficiency," Seventeenth Annual Computer Security Applications Conference IEEE, pp. 12–21, Dec. 2001.

[18] F. Cuppens and A. Miege, "Alert correlation in a cooperative intrusion detection framework," Proceedings 2002 IEEE Symposium on Security and Privacy, IEEE, pp. 202–215, 2002.

[19] Y.-A. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks - SASN '03 ACM, pp. 135–147, Oct. 2003.

[20] Z.-S. Pan, et al., "Hybrid neural network and C4. 5 for misuse detection," Machine Learning and Cybernetics, 2003 International Conference on. IEEE, vol. 4, pp. 2463–3467, Nov. 2003.