DETECTION OF PHISHING EMAILS USING AN IMPROVED RCNN MODEL WITH MULTILEVEL VECTORS AND AN ATTENTION MECHANISM

P. Samson Anosh Babu[1], P. Hema Gayathri[2], G. Himaja[3] , J. Jyothi[4] ,A. G M Abhinaya[5]
[1] Associate Professor, Krishna Chaitanya Institute of Technology & Sciences , Markapur, A.P, India
[2,3,4,5] Scholar, Krishna Chaitanya Institute of Technology &Sciences , Markapur, India

ABSTRACT:

Phishing emails are one of the significant threats in today's society and have led to significant financial losses. The results of confrontation approaches are currently not particularly good, despite ongoing improvements. Additionally, the quantity of phishing emails has been rapidly increasing in recent years. More efficient phishing detection technology is needed to lessen the threat presented by phishing emails. In this study, we began by looking at the format of emails. Then, we provide an improved Recurrent Convolutional Neural Networks (RCNN) framework with multilevel vectors and an attention mechanism based on a new Fraud email detection model that concurrently models emails at the email header, email content, character level, and word level.To evaluate how well the recommended method works, we use an unbalanced dataset with real ratios of legitimate and phishing emails. As a consequence of this effort, the filter will have a high likelihood of identifying phishing emails and will exclude as few real emails as possible. The trial's findings were favourable.

Keywords: Phishing E-Mail, RCNN, Multilevel vector

1. INTRODUCTION

Due to the Internet's rapid technological development, online users' experiences have undergone tremendous change, and security concerns are dominating the conversation more and more. New dangers now exist that have the ability to steal money and personal information from customers while also gravely harming their equipment. Among these worries, phishing stands out as a criminal activity that uses social engineering and technology to obtain a victim's account and identification information. According to a research by the Anti-Phishing Working Group (APWG) [1], the number of attacks detections grew by 46% in the first period in 2018 comparable to the fourth quarter of 2017. The shocking figures make it clear that phishing has recently seemed to be on the rise.It is also feasible that phishing might cause harm. The most common phishing targets have shifted from financial institutions to email and internet services, according to data from Phish Labs. The most common and successful phishing technique is the phishing email. An attacker sends phishing emails to trick the recipient into transmitting sensitive information, such as account passwords, to a particular recipient. It may also be used to trick users into visiting certain websites that are usually impersonated as trustworthy ones, such a bank's website, in order to get them to enter sensitive information like a credit card number or bank account password. Phishing emails may cause a lot of harm, even if they seem like a simple attack.It is estimated that phishing emails will cost businesses $500 million yearly in the United States alone. According to the APWG, between January and June of 2017, about 100,000 different phishing emails were found, and the total number of phishing emails increased from 68,270 in 2014 to 106,421 in 2015. Additionally, 109 billion people have at some point in time received phishing emails, according to Gartner data. Microsoft analyses and checks all 470 billion emails sent through Office 365 each month for spam and virus. Between January and December 2018, the proportion of inbound emails that were malicious emails increased by 250 percent. People are now recommended to focus to phishing emails because of the serious impact and rapid increase.As a result, many methods have been proposed for identifying phishing emails.

[2] LITERATURE SURVEY

Due to email's ease of use for communication, there is now a serious spam problem, especially with reference to phishing emails. Several anti-phishing solutions have been developed to solve the problem of phishing attempts. Sheng et al[10] .'s investigation of the efficacy of phishing blacklists. The two types of blacklists that are most often utilised are sender and link blacklists. In order to determine if an email is phishing, this recognition approach pulls the sender's address and the link address from the message and checks to see whether they are on the blacklist. Users frequently note the updating of a blacklist, and whether or not it is a phishing web platform is manually determined.Right present, Phish Tank and Open Phish are the two most well-known phishing websites. The effectiveness of this blacklist-based technique for phishing email detection is partially dependent on how effectively the blacklist functions. With the development of AI, the detection of phishing emails has entered the era of machine learning. The combination of NLP[17] and machine learning[18] has particularly aided the identification of phishing emails. The past has seen the application of contextual characteristics [13], syntactic features [12], and semantic features [11] in this context. Vazhayil et al. [14] used supervised classification together with decision trees, logistic regression, random forests, and SVM to identify phishing emails, starting with the most basic machine learning techniques. Hamid and Abawajy published a hybrid feature selection technique that incorporates both content and behavior[15].

The detection method for phishing emails using machine learning mainly requires tagged phishing emails and genuine emails in order to train the classification algorithm in the machine learning algorithm and develop the classifier model for email classification. Bergholz et al. presented three categories of features: fundamental, latent topic model, and dynamic Markov chain. The essential components of an email could be retrieved without further processing. Topic model features are conceivable qualities that are not apparent in emails. For example, it often comprises of a few words that are related to each other and may appear togetherThe objective of modelling each type of message content is to achieve the goal of capturing the likelihood that an email belongs to a specific category. Dynamic Markov chain characteristics are text features based on the bag-of-words. Since it depends on surface-level text instead of deep semantics, machine learning-based NLP is limited in its ability to identify phishing emails. Therefore, identifying the use of synonyms, modified phrase form, and other variations is a challenge for NLP based on machine learning. Furthermore, the machine learning method largely use feature engineering to develop features that characterise emails and perform tasks based on these features. Both manual feature engineering and blacklisting are required,It decreases the efficacy of detection and calls for a lot of work from experts with the relevant topic expertise.

The studies that come after focus on deep learning strategies[16] to fix the problems with the previous two approaches. A significant deep learning component is included in many NLP and Multi Label Classification applications [19], including text categorization[20], information extraction[21], and machine translation[22],[23], [24] and [25]. Additionally, it can eliminate the requirement for manual email feature extraction by automatically generating helpful features from emails to identify phishing emails. Therefore, the fundamental objective of implementing deep learning for phishing email detection is to describe the email text content more completely and comprehensively. Repke and Krestel restored some structure to free text email dialogues using word embedding and deep learning.Although detecting phishing emails is not the aim of this project, processing emails with deep learning and word embedding is nonetheless instructive. Hiransha et al. recommended using Keras word embedding and convolutional neural network to construct a phishing email detection model (CNN). The Deep Belief Network (DBN) and the Recurrent Neural Network are two other deep learning algorithms that are used (RNN). The disparities between phishing emails and other targets are no longer taken into account by these deep learning approaches for identifying phishing emails, which now focus solely on phishing emails. It ignores certain contextual information. The development of phishing email detection has been hampered by all of these concerns taken together.

[3] SYSTEM ARCHITECTURE

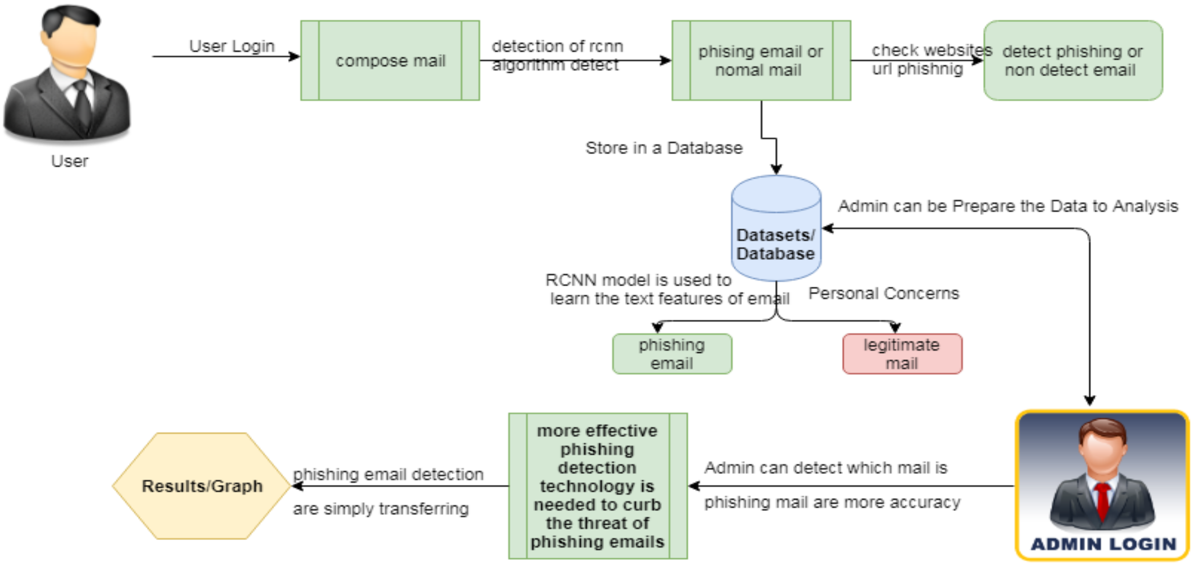

User
User Login
compose mail
detection of rcnn algorithm detect
phising email or nomal mail
check websites url phishnig
detect phishing or non detect email
Store in a Database
Datasets/ Database
Admin can be Prepare the Data to Analysis
RCNN model is used to learn the text features of email
Personal Concerns
phishing email
legitimate mail
ADMIN LOGIN
Admin can detect which mail is
phishing mail are more accuracy
more effective phishing detection technology is needed to curb the threat of phishing emails
phishing email detection
are simply transferring
Results/Graph

Fig1: System architecture

[4] ALGORITHM

4.1 R-CNN Algorithm

Let's quickly go through the three R-CNN family algorithms that we looked at in the first post: R-CNN, Fast R-CNN, and Faster R-CNN. In our implementation phase, we will anticipate the bounding boxes in never-before-seen photographs using this as our foundation (new data). R-CNN extracts several areas from the supplied image using selective search, and then it decides which of these areas contain objects. These regions are first retrieved, then CNN is then used to extract specific features for each zone. Using these features, finding items is then performed. R-CNN is unfortunately quite slow because there are so many different stages to the process.Fast R-CNN receives the entire image after ConvNet develops regions of interest for it (instead of passing the extracted regions from the image). Furthermore, it uses a single model to gather information from the regions, classify them into distinct groups, and generate the bounding boxes rather than three different models (like we saw with R-CNN). Due to the concurrent nature of these operations, it runs more quickly than R-CNN. Fast R-CNN can't process a large dataset quickly since the regions must also be extracted via selective search.

[5] IMPLEMENTATION

5.1 Modules Description

i) Dataset: The dataset was used to build a training set and testing set. Both the training set and the testing set contain emails with and without headers. In this study, we solely focus on email data with the header. Due to the inconsistency of the division of the training set and the evaluating set in the original dataset, the training-validation set and the testing set are reallocated after integrating the two datasets. The dataset is segregated using stratified random sampling, which separates it into equal parts of legitimate and phishing emails. This ensures that the two datasets used for the training and testing phases are accurate.

ii) User Queries: Users may have questions about the process. Creating and receiving replies to questions that must be able to be replied is the aim of this section of the project. The modules' primary objective is to make projects interactive. As a result, queries from consumers about different process details regularly surface.

iii) Graph Analysis: Graph analysis may be used to provide statistics to an administrator about the intricacies of a process. The data, which displays the most current number, is taken from the project flow. The information gives a manager a simple technique to improve customer satisfaction and other factors.

iv) Analysis: Examination of email format. A letter is symbolised by a circle, whereas a word is represented by a rectangle. The word is represented by a rectangle that contains an arbitrary number of circles and has an undetermined number of characters.

5.2 Sample Screenshots

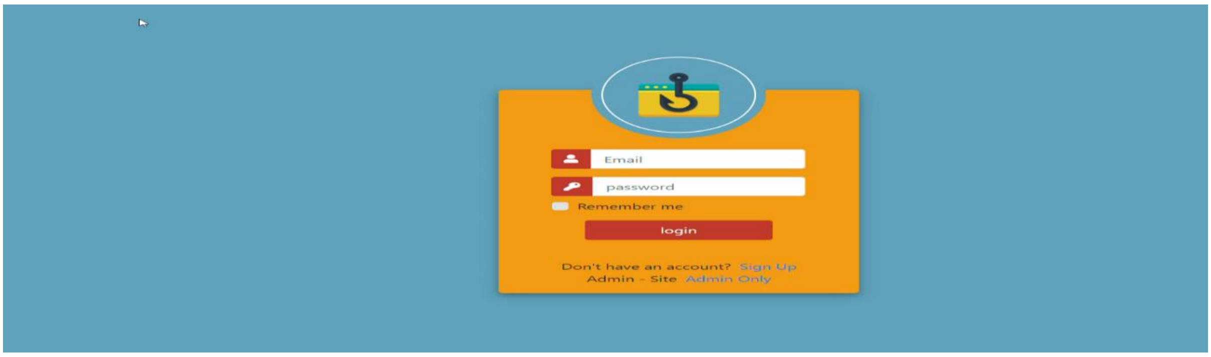
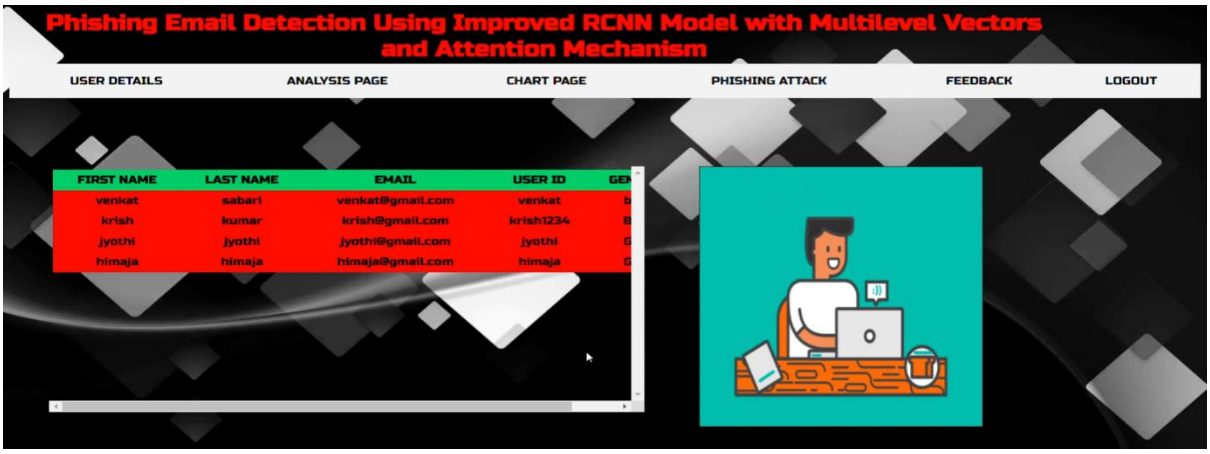
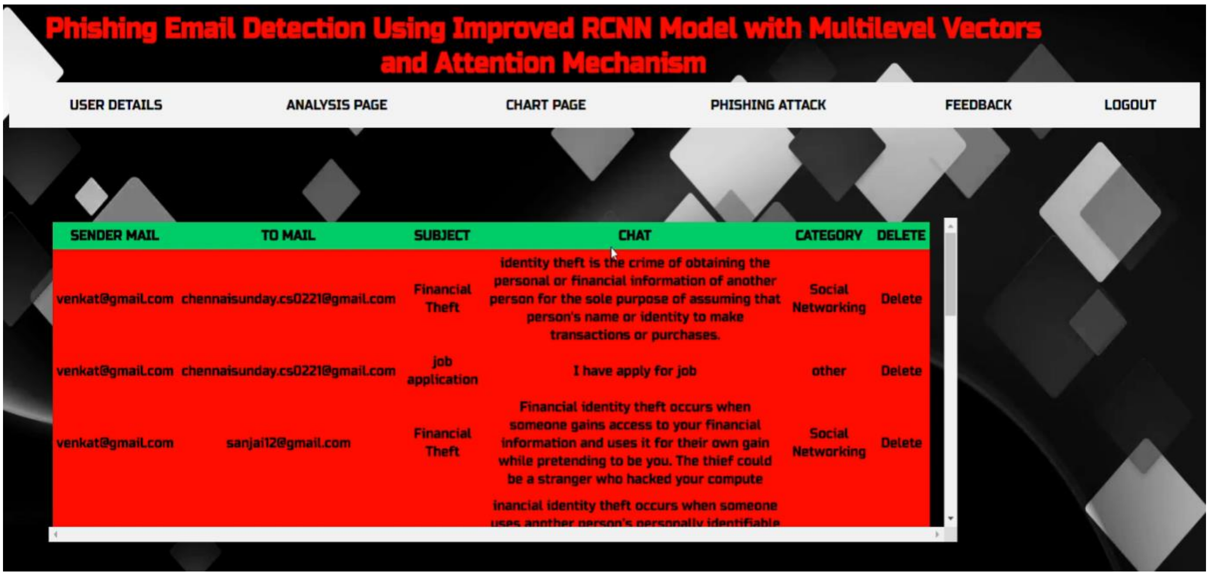


Fig.1: Login page


Phishing Email Detection Using Improved RCNN Model with Multilevel Vectors and Attention Mechanism

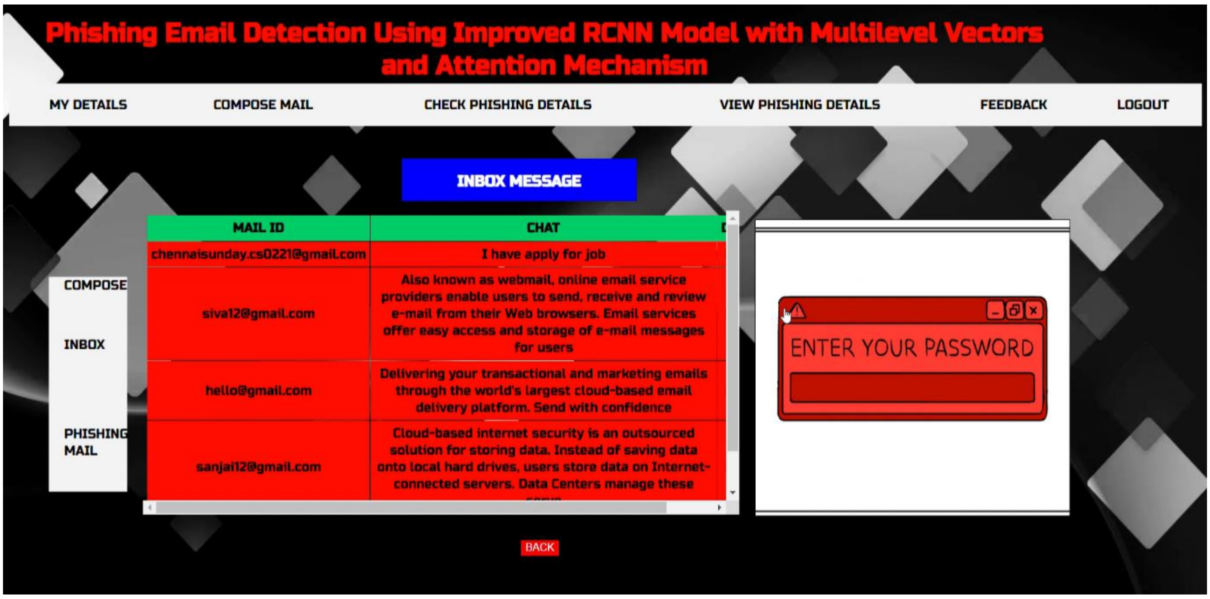
FIRST NAME	LAST NAME	EMAIL	USER ID	GEN
venkat	sabari	venkat@gmail.com	venkat	b
krish	kumar	krish@gmail.com	krish1234	B
jyothi	jyothi	jyothi@gmail.com	jyothi	G
himaja	himaja	himaja@gmail.com	himaja	G

Fig. 2: User details


Phishing Email Detection Using Improved RCNN Model with Multilevel Vectors and Attention Mechanism

SENDER MAIL	TO MAIL	SUBJECT	CHAT	CATEGORY	DELETE
venkat@gmail.com	chennaisunday.cs0221@gmail.com	Financial Theft	identity theft is the crime of obtaining the personal or financial information of another person for the sole purpose of assuming that person's name or identity to make transactions or purchases.	Social Networking	Delete
venkat@gmail.com	chennaisunday.cs0221@gmail.com	job application	I have apply for job	other	Delete
venkat@gmail.com	sanjai12@gmail.com	Financial Theft	Financial identity theft occurs when someone gains access to your financial information and uses it for their own gain while pretending to be you. The thief could be a stranger who hacked your compute	Social Networking	Delete
			inancial identity theft occurs when someone uses another person's personally identifiable		

Fig.3 Analysis and Phishing



MAIL ID	CHAT
chennaisunday.cs0221@gmail.com	I have apply for job
siva12@gmail.com	Also known as webmail, online email service providers enable users to send, receive and review e-mail from their Web browsers. Email services offer easy access and storage of e-mail messages for users
hello@gmail.com	Delivering your transactional and marketing emails through the world's largest cloud-based email delivery platform. Send with confidence
sanjai12@gmail.com	Cloud-based internet security is an outsourced solution for storing data. Instead of saving data onto local hard drives, users store data on Internet-connected servers. Data Centers manage these

Fig.4 Phishing and Checking

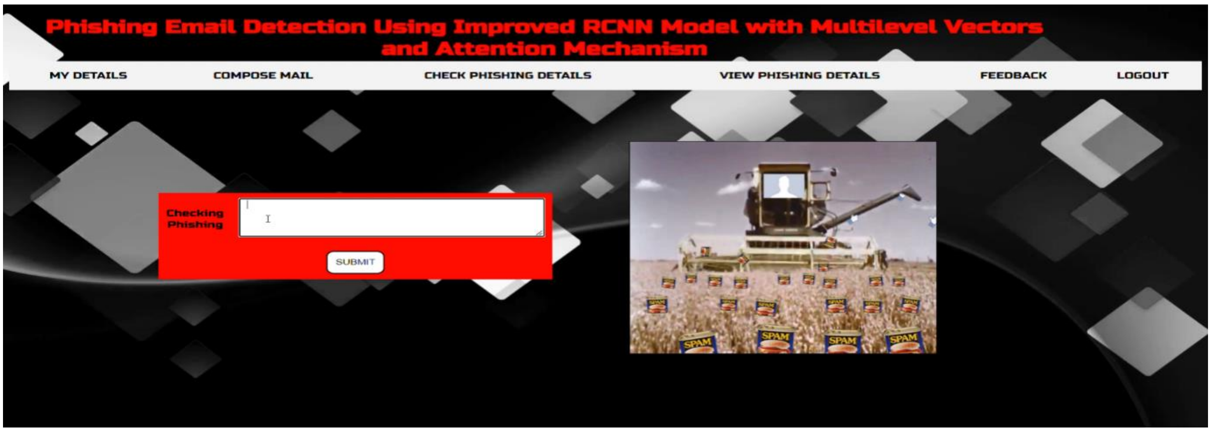


Fig. 5 Checking

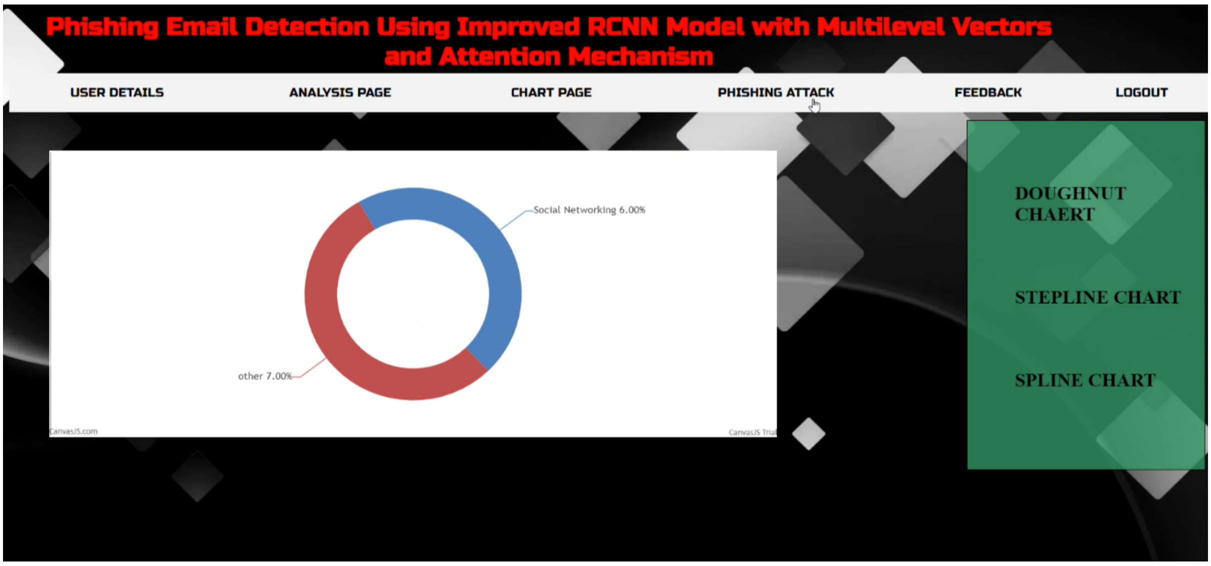


Fig. 6 Graphical Analysis

[6] CONCLUSION AND FUTURE WORK

We use a deep learning system to detect phishing emails. The model takes use of an updated RCNN to model the email text and header at both the character and word levels. Therefore, the model only slightly adds noise. We use the model's attention mechanism to force the model to pay greater attention to the information that is between the header and the body. We use the unbalanced dataset, which is more indicative of the real-world scenario, to conduct tests and evaluate the model. The model produces a promising result. Several experiments are used to demonstrate the benefits of the proposed paradigm.The following research aims to improve our model's capacity to identify phishing emails that consist only of an email body.

References

[1] Anti-Phishing Working Group. (2018). Phishing Activity Trends Report 1st Quarter 2018. [Online]. Available: http://docs.apwg.org/ Preports/apwg_trends_report_q1_2018.pdf

[2] PhishLabs. (2018). 2018 Phish Trends & Intelligence Report. [Online]. Available: https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend %20Report_2018-digital.pdf

[3] M. Nguyen, T. Nguyen, and T. H. Nguyen.(2018). ‘‘A deep learning model with hierarchical LSTMs and supervised attention for anti-phishing.’’[Online]. Available: https://arxiv.org/abs/1805.01554

[4] Anti-Phishing Working Group. (2016). Phishing Activity Trends Report 4th Quarter 2016. [Online]. Available: http://docs.apwg.org/ reports/apwg_trends_report_q4_2016.pdf

[5] Anti-Phishing Working Group. (2015). Phishing Activity Trends Report 1st-3rd Quarter 2015. [Online]. Available: http://docs.apwg.org/Preports/ apwg_trends_report_q1-q3_2015.pdf

[6] L. M. Form, K. L. Chiew, S. N. Sze, and W. K. Tiong, ‘‘Phishing email detection technique by using hybrid features,’’ in Proc. 9th Int. Conf. IT Asia (CITA), Aug. 2015, pp. 1–5.

[7] Microsoft. (2018). Microsoft Security Intelligence Report.[Online]. Available: https://clouddamcdnprodep.azureedge.net/gdc/gdcVAOQd7/original

[8] M. Hiransha, N. A. Unnithan, R. Vinayakumar, and K. Soman, ‘‘Deep learning based phishing e-mail detection,’’ in Proc. 1st AntiPhishing Shared Pilot 4th ACM Int. Workshop Secur. Privacy Anal. (IWSPA), A. D. R. Verma, Ed. Tempe, AZ, USA, Mar. 2018.

[9] C. Coyotes, V. S. Mohan, J. Naveen, R. Vinayakumar, and K. P. Soman, ‘‘ARES: Automatic rogue email spotter,’’ in Proc. 1st AntiPhishing Shared Pilot 4th ACM Int. Workshop Secur. Privacy Anal. (IWSPA), A. D. R. Verma, Ed. Tempe, AZ, USA, Mar. 2018.

[10] S. Sheng, B. Wardman, G. Warner, L. Cranor, J. Hong, and C. Zhang, ‘‘An empirical analysis of phishing blacklists,’’ in Proc. 6th Conf. Email Anti-Spam (CEAS), Sacramento, CA, USA, 2009, pp. 1–10.

[11] R. Verma and N. Hossain, ‘‘Semantic feature selection for text with application to phishing email detection,’’ in Proc. Int. Conf. Inf. Secur.Cryptol. Cham, Switzerland: Springer, 2013, pp. 455–468,

[12] G. Park and J. M. Taylor. (2015). ‘‘Using syntactic features for phishing detection.’’ [Online]. Available: https://arxiv.org/abs/1506.00037

[13] R. Verma, N. Shashidhar, and N. Hossain, ‘‘Detecting phishing emails the natural language way,’’ in Proc. Eur. Symp. Res. Comput. Secur. Berlin, Germany: Springer, 2012, pp. 824–841.

[14] A. Vazhayil, N. B. Harikrishnan, R. Vinayakumar, and K. P. Soman, ‘‘PED-ML: Phishing email detection using classical machine learning techniques,’’ in Proc. 1st AntiPhishing Shared Pilot 4th ACM Int. Workshop Securss. Privacy Anal. (IWSPA), A. D. R. Verma, Ed. Tempe, AZ, USA, 2018, pp. 1–8.

[15] I. R. A. Hamid and J. Abawajy, ‘‘Hybrid feature selection for phishing email detection,’’ in Proc. Int. Conf. Algorithms Archit. Parallel Process. Berlin, Germany: Springer, 2011, pp. 266–275.

[16] Y Sri Lalitha, SK Althaf Hussain Basha, Ayesha Mariyam, S Viswanadha Raju, "A Brief Research On Deep Learning Models", International Journal of Computer Engineering and Applications, Volume 13, Issue 6, November 2020, ISSN2321-3469.

[17] Sk. Althaf Hussain Basha, Sreedhar Jinka,Baijnath Kaushik, D.Praveen Kumar, A Jagan, “NLP: Context Free Grammars and Parse Trees for Disambiguiting Telugu Language Sentences”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT) Volume 2 , Issue 7 , pp.332-337, 2017, ISSN : 2456-3307

[18] Ayesha Mariyam, SK Althaf Hussain Basha,, S Viswanadha Raju, “A Literature Survey On Recurrent Attention Learning For Text Classification”, 2nd International Conference on Machine Learning, Security and Cloud Computing (ICMLSC2020), Springer Conference 18th & 19th December2020.

[19] SK Althaf Hussain Basha, Ayesha Mariyam, and S Vishwanadha Raju "Applications of Multi- Label Classification", International Journal of Innovative Technology and Exploring Engineering(IJITEE),pp.86-89,ISSN:2278-3075,Volume-9, Issue-4S2, March 2020.

[20] Ayesha Mariyam, SK Althaf Hussain Basha Sk, and Viswanadha Raju S , “A Brief Literature Survey on Text Classification Applications”, International Conference on Devices, Intelligent Systems & Communications (DISC)2020.

[21] Venkata Pavan Kumar Savala, Sk Althaf Hussain Basha, Ranganath P, P V Ravi Kumar, “Information Inclusion: The Modern Rank and The Approach Forward”, International Journal of Computer Engineering and Applications(IJCEA), Volume 13, Issue 6 , December. 20, ISSN2321-3469.

[22] Sreedhar Jinka, Sk. Althaf Hussain Basha, Suresh Dara, Baijnath Kaushik, “Sequence Labelling for Three Word Disambiguation in Telugu Language Sentences”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT) Volume 2 , Issue 7 , pp.311-315, 2017, ISSN :2456-3307.

[23] Baijnath Kaushik, Sk. Althaf Hussain Basha, Sreedhar Jinka, D Praveen Kumar, “ Sequence Labelling for Two Word Disambiguation in Telugu Language Sentences”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT) Volume 2 , Issue 7 , pp.321-327, 2017, ISSN :2456-3307.

[24] Sreedhar Jinka, Sk. Althaf Hussain Basha, Baijnath Kaushik, D. Praveen Kumar, A. Jagan, “ Empirical Analysis of Context Sensitive Grammars and Parse Trees for Disambiguiting Telugu Language Sentences”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT) Volume 2 , Issue 7 , pp.328-331, 2017, ISSN :2456-3307.

[25] GNR Prasad , SK Althaf Hussain Basha, Mallikharjuna Rao K M GnanaVardhan “A Review of Predictive And Descriptive Data Mining Techniques In Higher Education Domain, International Journal of Computer Engineering and Applications(IJCEA),Volume 13, Issue 6, January. 21, ISSN2321-3469.