RESEARCH ARTICLE OPEN ACCESS

Enhancing User Security Through Phishing Email Detection With Bi-Lstm

Annie Florance V [1], Fathima G [2]

[1]M.Sc, Department of Computer Science and Engineering, Dr. MGR Educational and Research Institute, Chennai, India

[2] Faculty, Centre of Excellence in Digital Forensics, Dr. MGR Educational and Research Institute, Chennai, India

ABSTRACT

Cybercriminals have efficiently invaded many important statistical structures through phishing e-mails, causing heavy losses. Detection of phishing from the big-email data has attracted the public attention. However, the camouflage era of phishing email disguises is becoming increasingly sophisticated, and current detection techniques cannot cope with the growing number of phishing techniques and growing diversity of emails. A phishing detection method was proposed in this paper and this method is mainly based on LSTM for big e-mail data. However, the camouflage technology of phishing mail is becoming more and more complex, and the existing detection methods are unable to confront the increasingly complex deception methods and the growing number of emails. In this project proposed a Bidirectional LSTM-based phishing detection method for big email data. The preprocessed data is then used to train the LSTM model. Finally, based on the trained model, the phishing emails are classified. This experiment evaluates the performance of the proposed method, and the experimental results show that the accuracy of our detection method for phishing e-mails can reach 95 percent.

Keywords: Phishing E-mail, RNN, Bidirectional LSTM, Accuracy

I. INTRODUCTION

In recent years, cyber security incidents have frequently occurred. In most of these incidents, attackers have used phishing e-mail as a counterattack to successfully penetrate government systems (such as the US State Department and the White House),[1] famous companies (like Google and RSA), and politicians' websites and social organizations in many countries (such as John Podesta and DNC)[2]. This series of high-profile incidents highlights phishing attacks growing popularity and strength. Expression data is called a Microarray database. On the one hand, phishing emails often cause economic losses to companies. On the other hand, phishing emails leak personal information, causing damage to industries and even the country.

These technologies are primarily used to prevent phishing scams that redirect users to fake websites via embedded links in emails and do not easily scale for distribution and receipt. active form. Machine learning is an effective way to tackle phishing attacks when incorporated into phishing email detection in complex environments. However, this idea faces many difficulties in practical implementation. [3] It is important to note that in practice, phishing e-mails can be classified into several types depending on their means of disguise, such as disguising public domain names, cloning IP addresses, using links, etc. short conclusions, etc. Each type of phishing e-mail has different characteristics

Although these methods mentioned above can detect phishing e-mails to a certain extent, for identity forgery and cloud attachment, methods such as feature extraction and sandbox are invalid In addition, there is a huge difference between the various open-source datasets used for Internet research and the actual data used in practical applications, which seriously affects the generalization of the model and detection effect. Therefore, first propose a sample labeling method in our paper. So this method can use clustering algorithms to accurately label existing email samples on big e-mail data that is not marked precisely

Meanwhile, it can also expand the email Samples and solve the problems caused by insufficiently accurately labeled data. Secondly, since we need to classify according to the message body, it uses the LSTM (LongShort-TermMemory Network) a neural network model for training, mainly owing to the excessive length of the message body. The LSTM neural network can effectively process information through three gate units and solve the problem of vanishing gradients caused by excessive context length. Therefore, can train the LSTM neural network model to detect phishing emails, effectively solving the above problems and achieving effective phishing email detection.

II. REVIEW OF LITERATURE

Najwa Altwaijry, Isra Al-Turaiki, et al., 24 March [4] Advancing Phishing Email Detection: A Comparative Study of Deep Learning Models. In this section, they proposed and suggested the use of deep learning (DL) and machine learning (ML) to mitigate the risks of phishing attacks. The proposed 1D-CNNPD (1-Dimensional Convolutional Neural Networks) model, a one-dimensional CNN-based approach, has been

improved to address phishing attacks. They used some of the models for testing the datasets, including LSTM (long short-term memory), Bi-LSTM (Bidirectional Long Short-Term Memory), GRU (gated recurrent unit), and Bi-GRU (Bidirectional gated recurrent unit). The standard datasets were used to evaluate the models' performance. The results show how the extensions significantly improved the performance of the baseline 1D-CNNPD (1-dimensional Convolutional Neural Network) model. Advanced 1D-CNNPD with Leaky RELU and Bi-GRU achieved 100% accuracy, 99.68% precision, 99.66% F1 score, and 99.32% recall rate. The performance of these models demonstrates their potential to enhance cybersecurity solutions against email phishing attacks

Jay Doshi, Kunal Parmar, et al., October [5]. A comprehensive dual-layer architecture for phishing and spam email detection. In this paper, They proposed that they should focus on classifying spam and phishing e-mails, often attackers are used to theft confidential information by impersonating authorized sources. It should alarm the scale of attacks that have resulted in significant financial in-depth such as stealing banking, technology, healthcare, and other business sectors.+++Using ANN (artificial neural networks), RNN (recurrent neural network generators), and CNN (convolutional neural networks). The double-layer architecture classifies data instances into some of their respective classes, layer 1 classifies phishing e-mail as magnificence, and layer 2 classifies spam elegance. This comprehensive approach was used for deep learning techniques, text classification, and analysis results showing superior accuracy, recall, precision, and F1 score, reaching 99.50%, 99.67%, 99.4%, and 99.50%, respectively. These results show that this method can improve the security system in e-mail communication, detecting and classifying malicious emails with significant errors, this will be used to avoid phishing attacks Therefore protecting against cyberattacks is the most important

S.Mani, Dr.G.Gunasekaran, et al., 04, April,[6] E-mail Spam -Detection Using Gated Recurrent Neutral Network In this article, the result in email spam was increasing, resulting in losses of 5 million per year, requiring the use of advanced techniques such as machine learning (ML) based language modeling and RNN (recurrent neural units) these algorithms are used to Categorize unwanted emails. They used some of the GRU (Gated recurrent unit) algorithms used in this study to classify phishing e-mails, demonstrating high accuracy rates in non-bailout scenarios. The large volume of spam generated globally from botnets impacts mailbox capacity, communication space loss, and personal mail safety. So Identifying spam e-mails remains an arduous task due to the prevalence of spam emails. The author of this article created a GRU-RNN algorithm to detect spam and phishing emails, achieving an accuracy rate of 97.6% using a spam-based dataset. These methods will show the accuracy of legitimate phishing e-mails

China Moulali Shaik, Narasimha Murthy Penumaka, et al., February [7] Bi-LSTM and Conventional Classifiers for Email Spam FilteringIn those days, emails played a main role in absolutely everyone's everyday existence. the wide variety of humans using electronic mail is swiftly developing. due to this, the hackers are taking benefit of the opportunity to apply the emails as their secret weapons in opposition to the e-mail users. the hackers send a bulk of emails at a time with an unmarried click on. the general public of unsolicited mail consists of advertisements or promotions for numerous activities, utilities, home equipment, and so forth. a single spam email outcomes in an internet loss for the person. In this research paper ML (Machine Learning) and DL (Deep Learning) gain knowledge of algorithms which include naive Bayes classifier, random forest, synthetic neural network, guide vector machine, lengthy brief-time period memory, and bidirectional-lengthy short-term reminiscence is used to perceive which model is greater correct to categorize the emails as spam or ham

Zainab Alshingiti, Rabeah Alaqel, et al., 3 January,[8] A Deep Learning-Based Phishing Detection System Using CNN, LSTM, and LSTM-CNN The proposed phishing detection method demonstrated by the CNN-based system is superior. Attackers gather information about the users by mimicking original websites that are indistinguishable from the eye. Sensitive information about the users may be accessed and they might be subject to financial harm or identity theft They develop Three distinct deep learning-based techniques are proposed in this paper to identify phishing websites, including long short-term memory (LSTM) and convolutional neural network (CNN) for comparison, and lastly an LSTM–CNN-based approach. Experimental findings demonstrate the accuracy of the suggested techniques, i.e., 96.2%, 95.6%, and 99.8% for CNN, LSTM–CNN, and LSTM, respectively.

Qi Li; Mingyu Cheng Junfeng Wang, et al., 01 February [9]: LSTM-Based Phishing Detection for Big Email Data. They proposed some phishing-avoiding techniques in this article they told now that nowadays Cybercriminals increasingly use phishing e-mails to intrude information on systems, causing significant damage. To combat this, an LSTM-based phishing detection method is proposed for big e-mail data. There are some stages to detect phishing testing stage and expansion stage. In the sample expansion stage, KNN and K-Means are combined to expand the training data set for deep learning. In the testing stage, samples are per-processed for generalization, word segmentation, and word vector generation.

Umer Ahmed Butt, Rashid Amin, et al., 02 June [10] Cloud-based E-mail phishing attack using machine and deep learning algorithm. In this paper they proposed to use different legitimate and phishing data sizes, to avoid phishing and spam e-mails to detect new emails, and use different features and algorithms for classification A revised data set is created after measuring existing data. created a CSV file and feature-extracted label file and applied Support Vector Machine

(SVM), naive Bayes (NB), and Long Short-Term Memory (LSTM)algorithms. This experiment treats phishing email recognition as a classification problem. According to the comparison and implementation, the performance of SVM, NB, and LSTM is better and more accurate in detecting email phishing attacks. Classifying email attacks using SVM, NB, and LSTM classifiers achieved the highest accuracy of 98.62%, 96%, and 97% respectively.

III. RESEARCH METHODOLOGY

In this section, the overall approach and tools used to execute the phishing email detection task are described in detail. Generally, any NLP task consists of five main phases: data collection, data processing, feature extraction, Dataset extraction, and prediction[11].Fig.1 shows the flow for those phases. Hence, in this feature, feature extraction will be done automatically as part of the deep learning model training

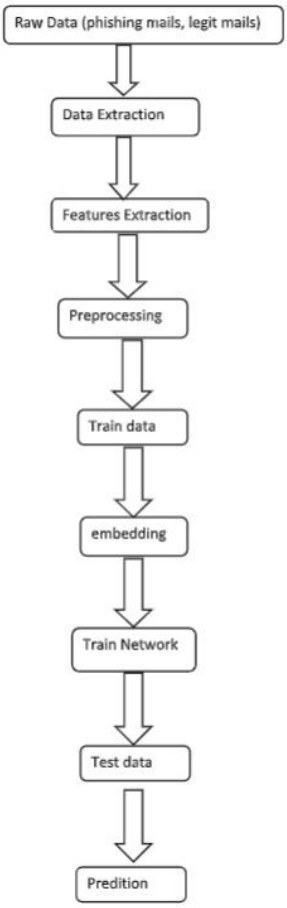

Fig. 1. General Flow of Main Phases for NLP Task

Cybersecurity incidents have occurred frequently Attackers attackers have used phishing emails as a knock-directly to correctly invade authorities' systems. Therefore, designed a phishing email detection method based on the Bidirectional LSTM neural network This research aims to build a a architecture for email spam detection employing the neural network. In Recurrent Neural Network(RNN), Bidirectional Long-Short Term Memory(Bi-LSTM). The proposed Methods include two important stages, the sample expansion stage and the testing stage under sufficient samples this sample stage combined KNN with K-Means to expand the data sets, so the size of training samples can meet the needs of in-depth learning speeded up training time involving Reccurent Nural Network (RNN) before the Bi-LSTM network and also extract higher level features of texts using this network within less time compared to straight LSTM network First, should have to preprocess these samples, including generalization, word segmentation, and word vector generation in the testing stage Apart from this, demonstrate eleven Features to Detect phishing e-mails Then, the preprocessed data is used to train a Bi -LSTM model eventually, primarily based on the educated version.

A. *Dataset collection:*

Phishing emails are collected from different unknown users and Legitimate emails are collected from open source platforms.

B. *Data preprocess:*

Dimension is huge so the computation time takes will take more time. That is why it sampled the data moreover the dataset is imbalanced because the good label is higher than the bad label which will affect our accuracy[12]. Removed duplicate values in our dataset and did some exploratory data analysis to gather insights from the collected dataset. In this project detecting phishing our data will be in the text so have to do some text preprocessing and natural language processing using the NLTK tool.in nltk, use regex tokenizer for tokenization with regex it is useful for nothing but removing unwanted symbols and numbers, etc, and then the stopword removing process and then finally stemming the words

C. *Feature extraction:*

To cluster and categorize the emails from each author, the suggested model uses Deep learning techniques. The development of a feature set is a crucial component of achieving this. The actual writing style of each author is based on the particular ways in which they create and display their knowledge. These details serve as the foundation for the extraction of style measurement features for each author taken into account in the email dataset. Fig 2 shows the disguising and separating the phishing e-mails

phish_url_1	phish_url_2	phish_url_3	phish_url_4	HTML_presence	Black_List_content	Black_List_subject	Label
1	0	0	1	1	1	1	1.0
1	0	0	1	1	1	1	1.0
1	0	0	1	1	1	1	1.0

Fig. 2 After the feature extraction of phishing e-mail.

D. *Dataset extraction:*

Split the dataset into after performing training, validation, and checking outsets. The training set is used to train the Bi-

LSTM model, the validation set is used to tune hyperparameters and monitor model performance during training, and the testing set is used to evaluate the final performance of the trained model on unseen data.

E. *Prediction:*

This paper analyzes the existing phishing email detection methods and finds that the traditional detection methods are difficult to accurately detect phishing emails[13]. Therefore, designed a phishing email detection method based on a Bidirectional LSTM neural network (Bi-LSTM). At the same time, when designing the model, the problem of the phishing e-mail did not have an accurately labeled dataset. So the phishing email feature extraction algorithm extracts the characteristics of the email and then uses the extracted features to cluster the emails after the feature extraction, to achieve accurate labeling of phishing emails. Eventually, train the model and compare the proposed method with the traditional phishing email detection method by the experiment. Our method performed datasets better than the existing phishing email detection method, So it improves accuracy and reduces the false positive rate and false negative rate.

These technologies are primarily used to prevent phishing scams that redirect users to fake websites via embedded links in emails and do not easily scale for distribution and receipt. Active form. Machine learning is an effective way to tackle phishing attacks when incorporated into phishing email detection in complex environments. However, this idea faces many difficulties in practical implementation. It is important to note that in practice, phishing e-mails can be classified into several types depending on their means of disguise, such as disguising public domain names, cloning IP addresses, using links, etc. short conclusions, etc. Each type of phishing e-mail has different characteristics.

The code starts by importing necessary libraries and loading a dataset (final_process.csv) containing preprocessed email data[14]. Have to click the show originals and copy the subejects Text data (email subjects) are tokenized using one-hot encoding and padded to ensure uniform length for input to the deep learning model. Numeric features are scaled using Min-Max scaling and combined with the text data for model training. Fig 3 shows whether the email header in the email is legitimate or a phishing email.

Fig. 3. . Imitating linked phishing emails and email headers.

Therefore, first propose a sample labeling method in our paper. Use a clustering algorithm to accurately label the existing email samples on big email data that are not marked precisely. Meanwhile, it can also expand the email samples and solve the problems caused by insufficiently accurately labeled data. Secondly, since, needs to be classified according to the message body, this uses the Bi- LSTM (Bi-directional Long Short-Term Memory Network) neural network model for training, mainly owing to the excessive length of the message body. The LSTM neural network can effectively process information through the comparison of the existing data of three gate units, and solve the problem of gradient disappearance caused by the excessive length of context. So, it can train an- LSTM neural network model to detect phishing emails, which effectively solves the problems mentioned above and achieves effective detection of phishing email

Nowadays, phishing email attack methods are mainly divided into two categories and show malicious-link-based phishing emails and the email's header, which involves constructing a similar domain name or imitating a domain name to attack the recipient, and the recipient will be attacked once the link is clicked then have to understand the difference between legit mail and phishing e-mail. As shown in Fig 4 The malicious attachment phishing e-mail and the email's header, mainly involve inducing the recipient to download and open the malicious attachment of the email and using the malicious attachment to attack the victim.

Fig. 4. The example of legitimate email and phishing email

Should have to predict that legitimate emails, when passed through the Bidirectional LSTM model, are more likely to produce a lower probability of being classified as phishing. This model learns the patterns from the text, subject, and other extracted features of legitimate emails that are indicative of their authenticity. These patterns might include linguistic characteristics, formatting styles, and content topics commonly found in legitimate communications and should have to predict that phishing emails, on the other hand, are more likely to exhibit patterns that trigger a higher probability of being classified as phishing by the Bidirectional LSTM model as shown in fig 5. These patterns may include deceptive language, urgent calls to action, suspicious URLs or attachments, and attempts to mimic legitimate senders.

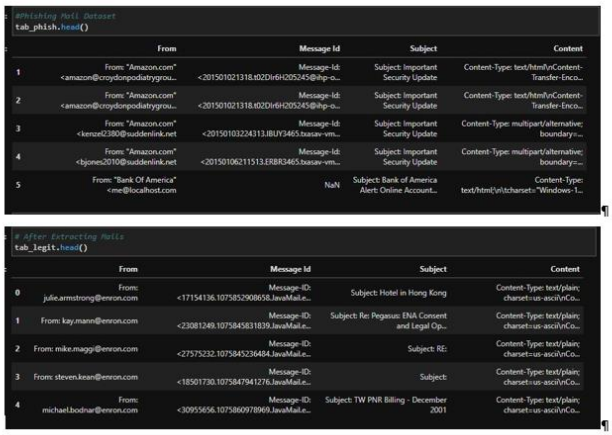

Fig 5 After extracting the phishing and legitimate e-mails

In this project, the processed datasets by the Bidirectional LSTM model, phishing emails are expected to generate a probability score closer and give accurate accuracy compared to the existing phishing Detection. The model's output reflects the higher likelihood assigned to the email being classified as phishing based on the presence of features associated with fraudulent or deceptive content. After analyzing the accuracy of different existing approaches, it has been found that the ensemble model that uses both- LSTM and RNN performed better with an accuracy of 92% and precision is 95% respectively which is far better than the existing solutions. as shown in Fig 6.

TABLE 1
The Number of sAMPLES in Dataset

Dataset	Positive samples		Negative samples		Total samples	Ratio of the positive samples and negative samples
	Type A	Type C	Type B	Type D		
DS1	93080	56920	10271	39729	2000000	3:1
DS2	76414	56920	10271	56395	2000000	2:1
DS3	43080	56920	10271	89729	2000000	1:1
DS4	9746	56920	10271	123063	2000000	1:2
DS5	0	56920	10271	132809	2000000	1:3

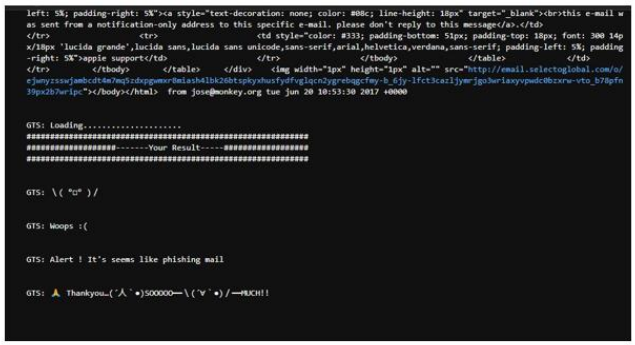

Fig 6 Comparison of both existing and results of present

IV. CONCLUSION

This article analyzes the existing phishing email detection methods and finds that the traditional detection methods are difficult to accurately detect phishing emails. Therefore, this proposed system designed a phishing email detection method based on the LSTM neural network. At the same time, when it designed the model, the problem of the phishing email did not have an accurately labeled dataset. So, used phishing feature extraction techniques and user-defined functions to extract the characteristics of the e-mail, to achieve accurate labeling of phishing emails. In the end, trained the version. This method is to perform better than the existing phishing email detection method. To memorize the contextual meaning and the sequential property of a sentence, adopted the Bidirectional LSTM network which makes the model very accurate giving improved performance accuracy of about 98.99%

REFERENCES

[1] "US State Department hack has major security implications," SecurityIntelligence, 2019. [Online]. Available: https://securityintelligence.com/us-state-department-hack-has-major-security-implications/

[2] V. Gandhi and P. Kumar, "A Study on phishing: Preventions and anti-phishing solutions," Int. J. Sci. Res., vol. 1, no. 2, pp. 68–69, 2012.

[3] Altwaijry N, Al-Turaiki I, Alotaibi R, Alakeel F. Advancing Phishing Email Detection: A Comparative Study of Deep Learning Models. Sensors (Basel). 2024 Mar 24;24(7):2077

[4] Doshi, J., Parmar, K., Sanghavi, R., & Shekokar, N. (2023). A comprehensive dual-layer architecture for phishing and spam email detection.Computers & Security,133,103378.

[5] S.Mani, "Email Spam Detection Using Gated Recurrent Neural Network", *IJPREMS, vol. 03, Issue 04, April 2023, pp: 90-99*

[6] C. M. Shaik, N. M. Penumaka, S. K. Abbireddy, V. Kumar and S. S. Aravinth, "Bi-LSTM and Conventional Classifiers for Email Spam Filtering," *2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, Coimbatore, India, 2023, pp. 1350-1355

[7] Alshingiti, Z., Alaqel, R., Haq, Q. E., Saleem, K., & Faheem, M. H. (2022).A Deep Learning-Based Phishing Detection System Using CNN, LSTM, and LSTM-CNN.*Electronics*,*12*(1),232.

[8] Q. Li, M. Cheng, J. Wang, and B. Sun, "LSTM Based Phishing Detection for Big Email Data" in *IEEE Transactions on Big Data*, vol. 8, no. 01, pp. 278-288, 2022

[9] Butt, U.A., Amin, R., Aldabbas, H.*et al.*Cloud-based email phishing attack using machine and deep learning algorithms.*Complex Intell. Syst.***9**, 3043–3070 (2023)

[10] K. Zetter, L. Matsakis, I. Lapowsky, G. Graff, E. Dreyfuss, and L. Newman, "Researchers uncover RSA phishing attack, hiding in plain sight," WIRED, 2018. [Online]. Available: https://www.wired.com/2011/08/how-rsa-got-hacked

[11] L. Matsakis, I. Lapowsky, G. Graff, E. Dreyfuss, and L. Newman, "Why the DNC thought a phishing test was a real attack," WIRED, 2018. [Online]. Available: https://www.wired.com/story/dncphishing- test-boatbuilder

[12] M. Alsharnouby, F. Alaca, and S. Chiasson, "Why phishing still works: User strategies for combating phishing attacks," Int. J. Hum.-Comput. Stud., vol. 82, pp. 69–82, 2015. [Online]. Available: 10.1016/j.ijhcs.2015.05.005.

[13] Jagatic, Tom & Johnson, Nathaniel & Jakobsson, Markus & Menczer, Filippo. (2007). Social phishing. Commun. ACM. 50. 94-100. 10.1145/1290958.1290968.

[14] Arachchilage, Nalin. (2016). Phishing threat avoidance behavior: An empirical investigation. Computers in Human Behavior. 60. 185–197. 10.1016/j.chb.2016.02.065.