Kanniappan Elumalai[1]

Dr. Duraimutharasan Bose[2]

Advancement of Phishing Attack Detection Using Machine Learning

Abstract: - Phishing attacks continue to pose significant threats to individuals and organizations, necessitating the development of advanced detection mechanisms. This study, propose a novel approach to phishing attack detection leveraging Machine Learning (ML) techniques, focusing on the analysis of features extracted from phishing emails or URLs. The given labeled dataset is datasets containing both malicious and non-malicious instances, supervised ML models on which we demonstrate the effectiveness of this approach in accurately predicting the nature of incoming emails or URLs. Key advanced attributes such as alias symbol, URL length, and presence of advanced characters in URLs are extracted and utilized as features for classification. Various ML Algorithms, including Support Vector Machine, Logistic Regression and Artificial Neural Network are evaluated to identify the most effective classifier for this task. Experimental results on real-world datasets show the proposed approach's high accuracy, precision, and recall rates in detecting phishing attacks.

Keywords: PHISHING ATTACK, MACHINE LEARNING, CYBERSECURITY, URLS, SUPERVISED ML MODELS

.

1. Introduction

5.35 billion People used the internet globally as of January 2024, making up 66.2 percent of the world's population. Of this total, 5.04 billion people, or 62.3 percent of the global populace, used the internet to communicate [1]. With the massive usage and development of the internet, then network attacks also increased. This brings many challenges to network security. This research focuses on phishing attacks, which are a type of network attack utilizing computer technology and social engineering to get individuals' sensitive personal data. Attackers induce people to click on phishing URLs by sending those misleading emails, SMS messages, or messages on social media [2].

When the phishing attack is to be perform the attackers has to make some preliminary steps they are:

1. Collecting the data of both users (Internal and External) Organization information.

2. Setting up the infrastructure, which includes establishing counterfeit domain names and websites, building message-sending botnets, and developing malware.

3. Sending emails that contain malicious software attachments (such as archives, jpeg, pdf, or Microsoft Office files) or URLs that point to fake or compromised websites.

4. Obtaining the desired outcome such as financial gain and gaining user credentials [3].

Some of the different methodologies used to study this kind of attack.

Anti-Phishing: solutions are being developed to combat the rise in phishing attacks. These solutions can be classified into several following approaches.

Heuristic-based: uses features like IP address, '@' symbol, right click disabled, and pop-up windows for passwords to classify URLs.

Content-based : compare two web pages based on similar content, using Term Frequency/Inverse document Frequency (TF-IDF) or screen shots.

[1] Research Scholar, Department of Information Technology, Academy of Maritime Education and Training (AMET University), Chennai-India

* Correspondence: kanniappan1maha@gmail.com

[2]Professor, Head, Department of Information Technology, Academy of Maritime Education and Training (AMET University), Chennai-India

Blacklist-based: include websites declared as spam, like Google's PageRank value, which may not detect newly created phishing URLs.

Machine learning: Extract features and classify those using algorithms, with the accuracy varying based on the chosen algorithm.

Hybrid approaches: Combine different techniques to detect fake or real websites, such as heuristics and blacklisting URLs [4].

2. Related work

To get people to react in a way that suits them, phishing attackers play on their fears, curiosities, or enthusiasm. Some of the attackers frequently create a sense of shortage or urgency to persuade people to act without fully thinking through the repercussions [5]. To give their requests more legitimacy, phishing attackers frequently pose as authoritative individuals like bank employees or IT managers. People are more likely to comply with demands without questioning those who they consider to be in a position of power [6].

People fall for phishing emails because they highlight how design factors, such as visual deception and interpersonal signs, can affect an individual's susceptibility to phishing [7].Incident response emphasizes the need for effective integration of CTI (Cyber Threat Intelligence) for early threat detection, situation awareness, and response orchestration [8].

Collecting tweets containing URLs, extracting features from the URLs and associated tweets, and applying machine learning algorithms to classify them as phishing or legitimate[9].The methodology involves extracting features from website URLs and web page content, such as domain characteristics and HTML attributes, and training classifiers to differentiate between legitimate and phishing sites[10].Analyzing existing research literature to identify and categorize different approaches, including heuristic-based detection, content-based analysis, and machine learning-based classification[11].

Detecting phishing websites using supervised learning techniques and efficient feature selection methods and compares the performance of different feature selection techniques, such as Information Gain and Chi-Square, in improving the accuracy of phishing detection models[12].Analyze website content and classify webpages as legitimate or phishing based on textual and visual feature[13].

Analyze email headers, content, and attachments and identify phishing emails[14].Analyzing web page content and extracting features using machine learning techniques such as logistic regression and k-nearest neighbors (KNN)[15].Investigate patterns such as email click rates, response times, and interaction with malicious links to develop behavioral models for phishing detection[16].Hybrid approach that combines URL-based features with webpage content analysis to classify websites as legitimate or phishing based on a combination of textual and structural features[17].

3. Materials and Methods

Dataset: In this work used a dataset called the "Kaggle Full Legitimate Phishing Dataset," which consists of 10,000 entries and includes 50 characteristics (features). Among these entries, 5,000 are categorized as benign, meaning they are considered safe or legitimate. The other 5,000 entries are labeled as malicious, indicating they are associated with phishing attempts or malicious activity.

The dataset was split into two portions. The larger portion, comprising 80% of the data, was used for training the model. The remaining 20% was reserved for testing the model's performance.

4. PROPOSED METHODOLOGY

In order to improve the quality and dependability of the dataset, preprocessing involved fixing errors, inconsistencies, or missing values.

When the dataset is subjected to dimensionality reduction techniques such as principal component analysis

(PCA), normalization becomes crucial in order to keep features with large sizes from influencing the variance computation. By transforming the data into a consistent scale or range, the PCA
Method helps to maintain consistency across features and mitigate variations [20].

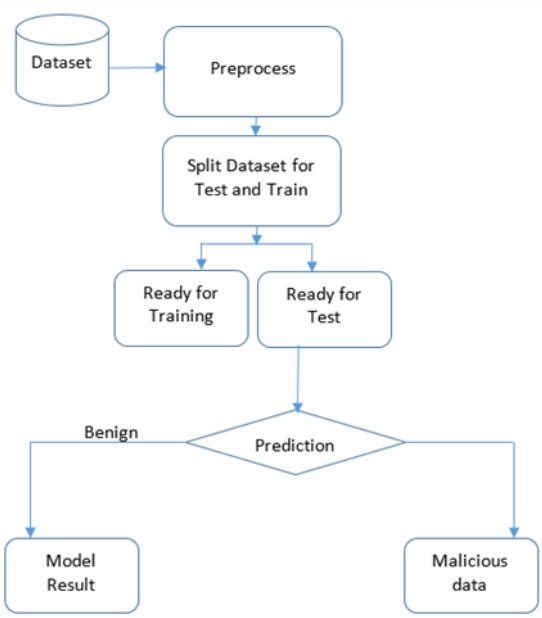

Figure 1. Data Flow Diagram

5. Results and Discussions

In the realm of cyber-attacks, perpetrators often choose their targets strategically, focusing on sectors such as finance, healthcare, or industry. Attackers employ familiar tactics like email spoofing, social engineering, and deceptive URLs to carry out their malicious activities.

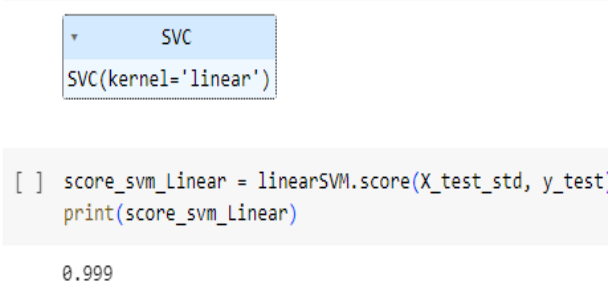

Figure 2. SVM Prediction Score

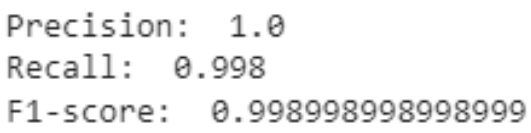

Figure 3. SVM predictions Scores

On the testing set, the first technique, the Support Vector Model, exceeded expectations with an accuracy of 0.999. Here, Figure 3 illustrates how the Support Vector Machine model achieved the highest possible results in F1-Score, Precision, and Recall.

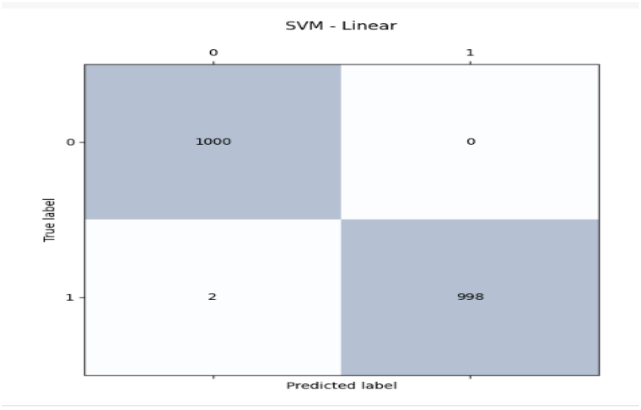

Figure 4. SVM Confusion Matrix

Figure 4 displays the SVM Confusion Matrix result. Of the 1000 tests, there were two False Positives and no False Negatives.

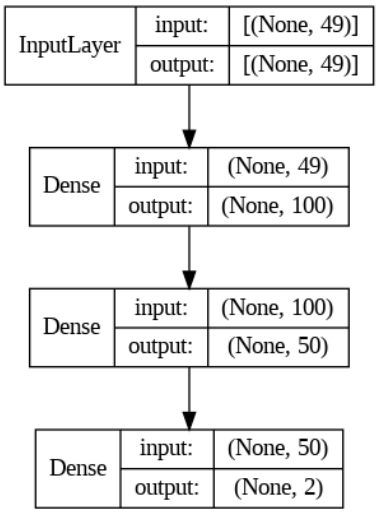

Figure 4. Dense Layer

Deep Neural networks have emerged as powerful tools for solving complex classification problems by learning intricate patterns and relationships within data. Dense layers, also known as fully connected layers, are fundamental building blocks of neural networks. Figure 4 illustrates how 3 density layers were employed in this work to obtain the highest prediction.

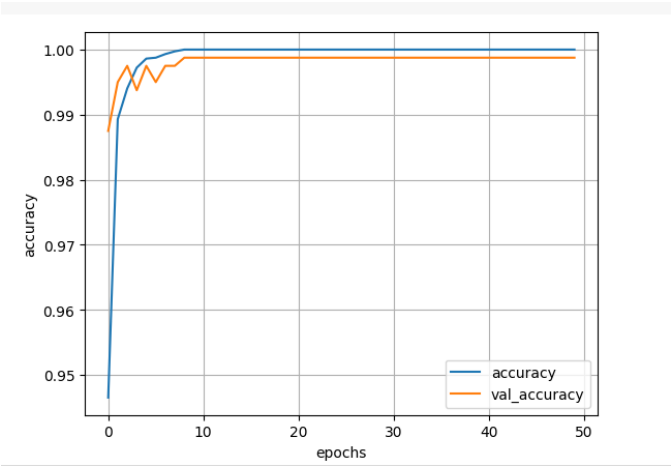

Figure 5. Deep Neural Network Accuracy

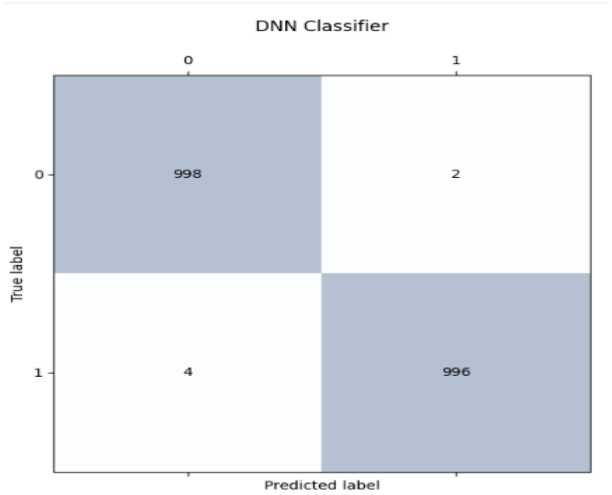

Figure 6. DNN Classifier Confusion Matrix

In figure 5 shows the prediction accuracy graph. Figure no.6 is the confusion matrix for Deep Neural Network. The result shows there is two False Negatives and four False Positives. When compared with Support Vector Machines, SVM gives the best prediction, but when applied to a large dataset, it has some drawbacks like computational Complexity, Memory Usage, and Overfitting

Accuracy: Calculates the ratio of the model's correct predictions to its total number of predictions.

Precision: The ratio of true positives to all predicted positives, which represents the accuracy of the model's positive predictions.

$$\text{Pr} = \frac{TP}{TP+FP} \qquad (2)$$

Recall: This applies to the ratio of true positives to all actual positives, which indicates how well the model identified all pertinent events in the dataset.

$$R = \frac{TP}{TP+FN} \qquad (3)$$

F1 Score: An accurate evaluation of the model's performance based on the harmonic mean of precision and recall [22].

$$\text{F} = \frac{Pr \times R \times 2}{\text{Pr} + R} \qquad (4)$$

Confusion Matrix: To evaluate the model's classification accuracy in detail, this tool tabulates predictions that are true positive, true negative, false positive, and false negative [20].

6. Conclusion

This study offered valuable insights into common phishing strategies and demonstrated the importance of real-time data on the latest phishing techniques. Future research should focus on enhancing the speed with the same accuracy level of phishing detection systems by utilizing the most recent datasets with limited features. Applying machine learning models will improve the identification of complex phishing attempts, especially those targeting new platforms and technological innovations.

References

[1] https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=Worldwide%20digital%20population%202024&text=As%20of%20January%202024%2C%20there,population%2C%20were%20social%20media%20users.

[2] Tang, L.; Mahmoud, Q.H. A Survey of Machine Learning-Based Solutions for Phishing Website Detection. Mach", MDPI 2021, 3, 672–694. https://doi.org/ 10.3390/make30300034

[3] Michael A. Ivanov,et.al2021," Phishing Attacks and Protection Against Them", 4,2021 at 04:17:06 UTC from IEEE Xplore, 978-1-6654-0476-1/21.

[4] Srushti Patil,et.al., “A Methodical Overview on Phishing Detection along with an Organized Way to Construct an Anti-Phishing Framework”, 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), 978-1-5386-9533-3/19/ ©2019 IEEE

[5] 555Luisa Franchina,et.al.2021,” Detecting phishing e-mails using Text Mining and features analysis”, https://www.researchgate.net/publication/357053201.

[6] H. Abroshan,.et.al2021, "Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process," in IEEE Access, vol. 9, pp. 44928-44949, 2021, doi: 10.1109/ACCESS.2021.3066383.

[7] Z. Wang, H. Zhu and L. Sun, "Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods," in IEEE Access, vol. 9, pp. 11895-11910, 2021, doi:10.1109/ACCESS.2021.3051633.

[8] Rachna Dhamija,et.al,2006,” Why Phishing Works”, Conference on Human Factors in Computing Systems, April 2006

[9] D. Schlette, M. Caselli and G. Pernul, "A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective," in IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2525-2556, Fourth quarter 2021, doi: 10.1109/COMST.2021.3117338.

[10] Aggarwal, Anupama & Rajadesingan, Ashwin & Kumaraguru, Ponnurangam. (2013). “PhishAri: Automatic Realtime Phishing Detection on Twitter”. eCrime Researchers Summit, eCrime. 10.1109/eCrime.2012.6489521.

[11] Dutta AK. “Detecting phishing websites using machine learning techniques”. PLoS One. 2021 Oct 11;16(10):e0258361. doi: 10.1371/journal.pone.0258361. PMID: 34634081; PMCID: PMC8504731.

[12] Basit, A., Zafar, M., Liu, X.. A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommun Syst 76, 139–154 (2021). https://doi.org/10.1007/s11235-020-00733-2.

[13] Almseidin, M., Abu Zuraiq, A., Al-kasassbeh, M. & Alnidami, N. (2019). Phishing Detection Based on Machine Learning and Feature Selection Methods. International Association of Online Engineering https://www.learntechlib.org/p/216410/.

[14] S. Singh, M. P. Singh and R. Pandey, "Phishing Detection from URLs Using Deep Learning Approach," 2020 5th International Conference on Computing, Communication and Security (ICCCS), Patna, India, 2020, pp. 1-4, doi: 10.1109/ICCCS49678.2020.9277459.

[15] L. Shalini, S. S. Manvi, N. C. Gowda and K. N. Manasa, "Detection of Phishing Emails using Machine Learning and Deep Learning," 2022 7th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2022, pp. 1237-1243, doi: 10.1109/ICCES54183.2022.9835846.

[16] M. Korkmaz Et Al. , "A Hybrid Phishing Detection System Using Deep Learning-based URL and Content Analysis," Elektronika ir Elektrotechnika , vol.28, no.5, pp.80-89, 2022

[17] Li, Y., Xiong, K., & Li, X. . (2019). Applying Machine Learning Techniques to Understand User Behaviors When Phishing Attacks Occur. EAI Endorsed Transactions on Security and Safety, 6(21), e3. https://doi.org/10.4108/eai.13-7-2018.162809

[18] M. Korkmaz Et Al. , "A Hybrid Phishing Detection System Using Deep Learning-based URL and Content Analysis," Elektronika ir Elektrotechnika , vol.28, no.5, pp.80-89, 2022 [here 5 to 18 is the only for related works

[19] Tang, L.; Mahmoud, Q.H. A Survey of Machine Learning-Based Solutions for Phishing Website Detection. Mach. Learn. Knowl. Extr. 2021, 3, 672-694. https://doi.org/10.3390/make3030034[20]