PHISHNET: Intelligence System For Phishing Attacks Using Machine Learning

Mr Prasanna K S *1, Dhanyashri B G *2,Nagashree patgar *3,Varshini N *4,Niharika G J *5

*1.Guide ,Department of Computer Science & Engineering ,Malnad College of Engineering,Hassan,Karnataka,India

*2,3,4,5 Student,Department Of Computer Science & Engineering ,Malnad College of Engineering,Hassan,Karnataka,India

***Abstract*-- Phishing attacks remain a significant threat to cybersecurity, targeting individuals and organizations alike. This paper introduces PHISHNET, a comprehensive threat intelligence system that leverages machine learning techniques to detect and mitigate phishing attacks across two communication vectors: URLs, emails. The system employs Gradient Boosting for URL detection, achieving an accuracy of approximately 98%, while Random Forest algorithms are utilized for email, attaining accuracies of approximately 97% and 96%, respectively. By analyzing various features related to URLs and extracting content from emails, PHISHNET provides users with actionable insights to enhance their security posture against phishing threats.**

Keywords - Feature Extraction, URL Analysis, Real-Time Detection, Cybersecurity, Building Classification, Machine Learning

I. INTRODUCTION

The Phishing attacks have emerged as one of the most prevalent threats in the digital landscape, targeting individuals and organizations alike. These malicious attempts often involve deceptive tactics designed to trick users into revealing sensitive information, such as passwords, credit card numbers, and personal identification details. As cybercriminals continuously evolve their strategies, traditional security measures frequently fall short, necessitating the development of more sophisticated detection systems.

In response to this growing challenge, machine learning techniques have gained traction as effective tools for enhancing phishing detection capabilities. By analyzing patterns in data, these algorithms can identify potential phishing attempts with greater accuracy than conventional methods. This paper presents PHISHNET, a comprehensive threat intelligence system that employs machine learning to detect phishing attacks across various communication channels, including URLs, emails.

In email phishing for example, the hacker sends a link via email to the user. When the user clicks on the link and enters their details, the hacker gains access to the entire user's information. According to Google's Transparency Report 2020 and (APWG), new phishing websites were detected every week. Phishing attacks have progressed and enhanced their techniques as the technology progress and research does not stop at developing or improving its techniques in cybersecurity to detect and classify phishing attacks, by developing several techniques. Many researches have demonstrated that approaches used artificial intelligence (AI) specifically,machine learning with the goal to strengthen system security and prevent any network intrusion .

In recent years, most studies has concentrated on applying machine learning and deep learning methods in cybersecurity, as well as, developing new features selection techniques. As a result, several machine learning techniques have proven to be effective in accurately identifying phishing attacks such as: Decision Tree, Random Forest, SVM, Naïve Bayes, Neural Network and so on, PHISHNET aims to enhance user trust and engagement. Additionally, addressing the cold start problem—where new users lack sufficient data for accurate predictions is crucial for maintaining system efficacy.

Moreover, then temporal aspect of phishing detecti on plays a vital role in ensuring relevance and accuracy.

As new phishing tactics emerge and old ones become obsolete, it is essential for detection systems to adapt accordingly. By implementing mechanisms that account for the age of data and user interactions, PHISHNET strives to provide timely recommendations that reflect current threats. In summary, this paper outlines the development phishing attacks using advanced machine learning techniques

II. LITERATURE REVIEW

The landscape of phishing detection has evolved significantly, with numerous studies exploring various methodologies and techniques to enhance the identification and mitigation of phishing threats. This literature survey reviews key contributions in the field, focusing on machine learning approaches, spam detection, and the challenges faced in phishing detection systems.

In 2022, Adarsh Mandadi et al. presented a study on phishing website detection using various machine learning models, highlighting the impact of feature selection and optimization for improved accuracy. This research was shared at the IEEE 7th International Conference for Convergence in Technology (I2CT), where the authors compared the performance of several algorithms in detecting phishing sites. The study revealed that machine learning models provide superior detection rates over traditional methods by emphasizing tailored feature selection and optimized models.

Mustafa Aydin et al. proposed a classification algorithm for phishing website detection by extracting websites' URL features and analyzing subset based feature selection methods. It implements feature extraction and selection methods for the detection of phishing websites. The extracted features about the URL of the pages and composed feature matrix are categorized into five different analyses as Alpha-numeric Character Analysis, Keyword Analysis, Security Analysis, Domain Identity Analysis and Rank Based Analysis. Most of these features are the textual properties of the URL itself and others based on third parties services.

A 2021 review by Ammar Odeh et al. discussed the challenges and advantages of different machine learning techniques for phishing detection. Presented at the IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), this study reviewed multiple algorithms used in phishing detection, stressing the importance of a combined approach for achieving high detection rates and adapting to emerging threats.

In their 2023 study, V. Dharani et al. investigated spam detection in email using machine learning classifiers. Presented at the 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), their research emphasized the significance of feature extraction and model training for accurately distinguishing legitimate from fraudulent messages. The study underscored that these steps are crucial for effective phishing and spam detection.
In 2021, Kerin Pithawala et al. focused on phishing URL detection using classification techniques, presented at the 12th International Conference on Computing Communication and Networking Technologies (ICCCNT). Their research highlighted that robust classification algorithms significantly enhance the identification of phishing attempts, particularly through feature selection based on URL characteristics.

S. Marchal et al., (2017) proposed this technique to differentiate Phishing website depends on the examination of authentic site server log knowledge. An application Off-the- Hook application or identification of phishing website. Free, displays a couple of outstanding properties together with high preciseness, whole autonomy, and nice language-freedom, speed of selection, flexibility to dynamic phish and flexibility to advancement in phishing ways.

H. Huang et al., (2009) proposed the frameworks that distinguish the phishing utilizing page section similitude that breaks down universal resource locator tokens to create forecast preciseness phishing pages normally keep its CSS vogue like their objective pages.

N. Choudhary b, K. Jain, S. Jain: This study emphasizes the significance of only using attributes from the URL. Both the Kaggle and Phishtank websites make it easy to get the dataset used in this study. The researchers used a hybrid approach that combined Principal Component Analysis (PCA) with

Support Vector Machine (SVM) and Random Forest algorithms to reduce the dataset's dimensionality while keeping all important data, and it produced a higher accuracy rate of 96.8% compared to other techniques investigated.

Overall, recent literature illustrates the value of machine learning in enhancing phishing and spam detection systems. Studies underscore the importance of feature extraction, algorithm selection, and model optimization, all of which are essential to improve detection accuracy in a landscape where phishing and spam techniques continue to evolve.

III. METHODOLOGY

In response to the growing sophistication of phishing attacks, we propose a comprehensive phishing detection system named PHISHNET. This system is designed to leverage advanced machine learning techniques and incorporate multiple data sources to enhance the accuracy and effectiveness of phishing detection across various communication channels, including URLs, emails. The proposed system aims to address key challenges such as personalization, cold start problems, and the temporal relevance of data.

A. DATASET

The datasets utilized in this project are obtained from Kaggle and encompass three specific domains: email spam detection and phishing link detection.

The email spam detection dataset consists of 5,559 email messages, each labeled as either spam or non-spam. Each entry contains the text of the message along with a binary label—1 indicating spam and 0 denoting legitimate emails. By analyzing the textual features and patterns within this dataset, classifiers can be developed to effectively distinguish between spam and non-spam messages.

In each field of based on learning approach, the choice of the dataset is considered an important first step to start building the proposed model. The choice of the dataset must take several considerations such as the amount of data, diversity of emails representing phishing and benign and the quality and relevance . The dataset used for this study is available and sourced from Kaggle. It contains two types of features:

- Email Text: is the content of the email
- Email Type: The classification of the email, indicating whether it is a Phishing email or a safe email.

The phishing link detection dataset comprises 11,054 URLs and includes 32 features related to URL composition, webpage attributes, and external link indicators. These features are categorized into three main types: URL-based characteristics (such as URL length and presence of an IP address), webpage content indicators (including HTML structure and form handling), and external factors (like page rank and traffic metrics). Each URL is labeled with a binary target feature—1 for phishing links and 0 for legitimate links. The dataset also includes binary values indicating phishing indicators alongside numeric values reflecting risk levels. Preprocessing was conducted to eliminate any missing values, followed by a division into 75% training data and 25% testing data. This dataset allows for an analysis of critical factors that contribute to effective phishing detection.

FEATURE EXTRACTION

PHISHNET utilizes through a feature extraction process specifically designed for each type of phishing vector. For URLs, the extracted features encompass various elements such as the length of the URL, the presence of special characters, the age of the domain, and whether HTTPS is used. In the case of email phishing, key features include the sender's email address, an analysis of the subject line, relevant keywords found within the content, and details from the email header. This tailored approach ensures that each phishing vector is effectively addressed through targeted feature extraction.

B. MACHINE LEARNING MODELS

PHISHNET implements three distinct machine learning models, each optimized for addressing different types of phishing threats. The URL Detection Model utilizes Gradient Boosting algorithms to classify URLs as either safe or malicious. This model is trained on a comprehensive dataset that includes both known phishing URLs and legitimate ones, allowing it to learn from a wide array of features extracted from the URLs. By analyzing characteristics such as URL length, the presence of special characters, and domain age, the model can effectively differentiate between phishing and non-phishing links.

$$Accuracy = \frac{Numberofcorrectpredictions}{Totalnumberofpredictions} \quad (1)$$

Fig 1. Architecture Diagram

For email phishing detection, PHISHNET employs the Email Detection Model, which is based on Random Forest algorithms. This model analyzes the content of email messages to classify them as spam or legitimate (ham). It leverages machine learning techniques to understand the context and semantics of the email text, considering features such as the sender's email address, subject line, and specific keywords within the message. This approach enables

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (2)$$

the model to accurately identify phishing attempts disguised as legitimate emails.

Overall, PHISHNET's approach combines advanced machine learning techniques with tailored models for different phishing vectors, enhancing its ability to detect and mitigate various forms of phishing attacks.

C. EVALUATION OF MODEL

In this stage we evaluate the models by entering the dataset with predictor variables to each model, then the models will predict the targeting variable according to the prediction results and we will compare it with real values. In Fig. 2 there is a learning model of the proposed work.

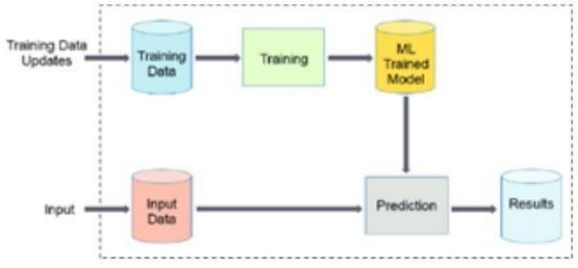
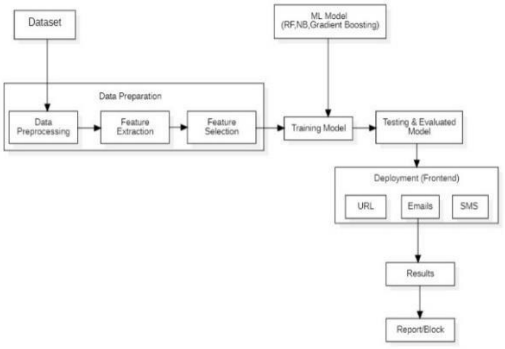


Fig. 2. Learning model from prposed system.

IV. EXPERIMENTAL RESULTS

To validate the machine learning models developed for phishing detection in our project, we utilized accuracy as the primary metric for evaluation. Accuracy is a widely recognized measure in classification tasks due to its simplicity and ease of interpretation. It provides a clear indication of a model's performance by calculating the proportion of correct predictions made



by the model. The formula for accuracy can be expressed as follows:

In a more detailed context, accuracy can also be calculated using the following equation:
Where:

- TP*TP* represents True Positives,
- FP*FP* denotes False Positives,
- TN*TN* stands for True Negatives,
- FN*FN* indicates False Negatives.

In this project, we trained models for two distinct types of phishing detection: URLs, emails. Each model was evaluated based on its ability to accurately classify instances as phishing or legitimate. The experimental evaluation yielded the following results:

1. **URL Detection Model**: Implementing Gradient Boosting algorithms, this model achieved an approximate impressive accuracy of **98%** in identifying phishing URLs.

2. **Email Detection Model**: Utilizing Random Forest algorithms, this model successfully classified emails with an approximate accuracy of **97%**, effectively distinguishing between spam and legitimate messages.

These results demonstrate the effectiveness of the selected algorithms in accurately identifying phishing threats across different communication channels, highlighting the robustness of our approach in combating phishing attacks.

V. CONCLUSIONS AND FUTURE WORK

In this project, we developed and evaluated machine learning models for detecting phishing threats across two distinct channels: URLs, emails. The results demonstrated that our models achieved high accuracy rates approximately—98% for URL detection using Gradient Boosting, 97% for email detection with Random Forest. These findings underscore the effectiveness of machine learning techniques in identifying phishing attempts and enhancing cybersecurity measures. The successful implementation of these models indicates that they can serve as valuable tools for organizations seeking to protect their users from phishing attacks. By leveraging advanced algorithms and comprehensive feature extraction methods, we have laid the groundwork for a robust phishing detection system that can adapt to evolving threats. Looking ahead, there are several avenues for future work. First, we plan to expand the datasets used for training to include a broader range of phishing Examples, which could improve the models' generalizability and robustness. Incorporating more diverse features—such as behavioral analysis of users interacting with emails could also enhance detection capabilities. Additionally, exploring ensemble methods that combine multiple algorithms may yield even better performance by capitalizing on the strengths of different classifiers. Implementing real-time detection systems could further increase the practical applicability of our models, allowing organizations to respond swiftly to potential threats. Finally, ongoing research into adversarial machine learning techniques will be essential to ensure that our models remain effective against increasingly sophisticated phishing tactics. By continuously updating our models and methodologies in response to emerging threats, we can contribute to a safer digital environment for all users.

REFERENCES

[1] Adarsh Mandadi, Saikiran Bopanna, Vishnu Ravella, Dr. R Kavitha, Phishing Website Detection Using Machine Learning , 2022
IEEE 7th International conference for Convergence in Technology (I2CT).

[2] Edward Wijaya, Gracella Noveliora, Kharisma Dwi Utami , Rojali, Ghinaa Zain Nabiilah ,Spam Detection in Short Message
Service (SMS) Using Naïve Bayes, SVM, LSTM, and CNN , 2023 10th International Conference on Information Technology, Computer
and Electrical Engineering (ICITACEE) .

[3] Ammar Odeh , Ismail Keshta , Eman Abdelfattah, Machine Learning Techniques for Detection of Website Phishing: A Review for Promises and Challenges , 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC).

[4] V Dharani, Divyashree Hegde, Mohana, Spam SMS (or) Email Detection and Classification using Machine Learning , 2023 5th
International Conference on Smart Systems and Inventive Technology (ICSSIT).

[5] Kerin Pithawala, Sakshi Jagtap and Preksha Cholachgud , Detecting Phishing of Short Uniform Resource Locators using
classification techniques , 2021 12th International Conference on Computing Communication and Networking Technologies
(ICCCNT).

[6] M.Rubin Julis et al. Spam Detection in SMS Using Machine Learning Through Text Mining, International journal of scientific& technology research, vol 9, Issue 02, 2020.

[7]. Safa Alrefaai , Ghina Ozdemir, Afnan Mohamed , Detecting Phishing Websites Using Machine Learning , 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA).

[8]. Bhagyashree A V , Anjan K Koundinya , Detection of phishing websites using Machine Learning Techniques . International Journal of Computer Science and Information Security (IJCSIS), Vol. 18, No. 7, July 2020.

[9] Mustafa Aydin et al,Ashritha Jain R,Chaitra kulal,deekshitha s,Mrs Mangala kini proposed a review paper on Detection of phishing websites using machine learning (IJERT) 2019.