INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN : 2454-9924

PHISHING DETECTION WITH SUPPORT VECTOR MACHINE

R.Vijyalakshmi* ,B.E, M.Tech., A.Gobika, G.Lakshmi, M.Gayathri,

[abc] Assistant Professor, Department of Computer Application, Idhaya College of Arts and Science for Women, puducherry;

[abc] Idhaya College of Arts and Science for Women, puducherry; Idhaya College of Arts and Science for Women, puducherry;

[abc] Idhaya College of Arts and Science for Women, puducherry; Idhaya College of Arts and Science for Women, puducherry;

ABSTRACT:

Phishing attacks are one of the most significant cybersecurity threats facing individuals and organizations today. Phishing attacks involve the use of fraudulent emails, websites, or text messages to trick individuals into divulging sensitive information such as passwords, credit card numbers, or other personal information. Machine learning algorithms have emerged as an effective solution for detecting and preventing phishing attacks. In this abstract, we propose a machine learning approach for phishing attacks detection.Our approach involves the use of supervised learning algorithms to train a model that can identify phishing emails. The model is trained on a large dataset of known phishing emails and legitimate emails. The dataset is pre-processed, and features such as the sender's address, message content, and HTML code are extracted. These features are then used to train the model using popular machine learning algorithms such as Random Forest, Decision Trees, and Support Vector Machines.

INTRODUCTION:

Phishing attacks are a common form of cybercrime in which attackers use fraudulent emails, websites, or messages to trick individuals into divulging sensitive information, such as login credentials, financial information, or personal data. Phishing attacks have become increasingly sophisticated, making it difficult for individuals and organizations to detect and prevent them. As a result, researchers have proposed the use of machine learning approaches to detect and prevent phishing attacks. This introduction provides an overview of phishing attacks, their impact, and the need for machine learning approaches for detecting and preventing them.

Overview of Phishing Attacks: Phishing attacks are a type of social engineering attack in which attackers use various tactics, such as impersonation, urgency, and emotional appeals, to trick individuals into revealing sensitive information. Phishing attacks can take various forms, such as phishing emails, phishing websites, and phishing messages. In a typical phishing email, the attacker poses as a legitimate entity, such as a bank or an online retailer, and asks the recipient to click on a link or provide sensitive information. Once the victim clicks on the link or provides the information, the attacker can use it for fraudulent purposes, such as stealing money, identity theft, or installing malware on the victim's computer.

Impact of Phishing Attacks: Phishing attacks can have a significant impact on individuals and organizations. According to a report by the Anti-Phishing Working Group, there were 241,324 unique phishing attacks in the first quarter of 2021, and the number of attacks is expected to increase in the future. The impact of phishing attacks includes financial losses, reputational damage, and loss of trust. Organizations may also face legal liabilities if they fail to protect their customers' data from phishing attacks. As a result, it is essential for individuals and organizations to detect and prevent phishing attacks.

Machine Learning Approaches for Phishing Detection: Machine learning approaches have shown promise in detecting and preventing phishing attacks. Machine learning is a subset of artificial intelligence that uses statistical techniques to enable computer systems to learn from data, identify patterns, and make decisions without being explicitly programmed. Machine learning algorithms can analyze large amounts of data and identify patterns that may be difficult for humans to detect.

Several machine learning approaches have been proposed for phishing detection, including supervised, unsupervised, and semi-supervised learning. Supervised learning involves training a machine learning model on labeled data, such as phishing emails, to identify patterns that can be used to detect future phishing attacks. Unsupervised learning involves training a machine learning model on unlabeled data to identify patterns that can be used to detect anomalies, such as unusual email behavior or website activity. Semi-supervised learning combines both supervised and unsupervised learning to improve the accuracy of the model.

Challenges and Limitations: While machine learning approaches have shown promise in detecting and preventing phishing attacks, there are some challenges and limitations to their implementation. One challenge is the availability of labeled data for training the machine learning model. Another challenge is the constantly evolving nature of phishing attacks, which may require frequent updates to the machine learning model to remain effective. Additionally, the use of machine learning approaches may raise privacy concerns, as they require access to sensitive data to detect and prevent phishing attacks.

OBJECTIVE:

The objective of using machine learning for detecting phishing attacks is to improve the accuracy and efficiency of detecting and preventing these types of attacks. Phishing attacks are a common and constantly evolving threat to organizations, with attackers using increasingly sophisticated techniques to trick users into revealing sensitive information or downloading malicious software. Traditional methods of detecting phishing attacks, such as email filtering and manual analysis, may not be effective in detecting these new and evolving threats.

Machine learning can be used to automatically analyze and identify patterns in large datasets of known phishing attacks, enabling organizations to quickly and accurately detect and respond to new attacks. By leveraging machine learning algorithms, organizations can achieve the following objectives:

1. Real-time detection: Machine learning models can analyze large volumes of data in real-time, allowing for rapid detection and response to phishing attacks.
2. Improved accuracy: Machine learning models can learn from previous phishing attacks and identify new attacks based on patterns and characteristics learned from past incidents. This can improve the accuracy of phishing detection and reduce false positives.
3. Scalability: Machine learning algorithms can be easily scaled to handle large volumes of data, enabling organizations to keep up with the increasing number of phishing attacks.
4. Adaptability: Machine learning models can adapt and improve over time as new types of phishing attacks emerge, enabling organizations to stay ahead of the latest threats.
5. Automation: Machine learning algorithms can be fully automated, reducing the need for human

intervention in the detection and response process.

AIM:

The aim of phishing attacks detection using machine learning approach is to develop an accurate and effective system that can identify and prevent phishing attacks. The goal is to use machine learning algorithms to analyze data from various sources, such as emails, websites, and network traffic, to detect phishing attempts in real-time.

The primary objective of the system is to achieve high accuracy in detecting phishing attacks while minimizing false positives and false negatives. The system should also be scalable, privacy-preserving, and interpretable to ensure that it can handle large volumes of data, protect sensitive information, and provide explanations for its predictions.

The proposed system should leverage machine learning techniques such as supervised and unsupervised learning, feature selection, anomaly detection, and deep learning to achieve high accuracy in phishing attacks detection. The system should also be capable of adapting to new and emerging phishing attack techniques to provide reliable protection against these attacks.

RELATED WORK:

Phishing attacks are a type of cyber attack that aims to steal sensitive information such as passwords, credit card numbers, and personal identification by disguising as a trustworthy entity. Traditional rule-based methods have limitations in detecting and preventing phishing attacks due to the sophistication and diversity of attack techniques. Therefore, machine learning (ML) has been increasingly adopted to enhance the accuracy and efficiency of phishing detection.

One existing system for phishing attacks detection using machine learning approach is the Random Forest (RF) algorithm. The RF algorithm is a type of ensemble learning method that combines multiple decision trees to improve classification accuracy. The system extracts a set of features from the email content, such as sender information, hyperlink attributes, and message content. These features are then fed into the RF classifier, which predicts the probability of an email being a phishing attack.

Imbalanced Data: One of the significant challenges in phishing attacks detection is imbalanced data, where the number of legitimate instances is much higher than the number of phishing instances. This imbalance can result in biased models that have high accuracy for legitimate instances but low accuracy for phishing instances.

1. Feature Selection: Another challenge in phishing attacks detection is feature selection, where the most relevant features for detection are selected. The selection of irrelevant features can result in noisy models that have low accuracy.
2. Generalization: Phishing attacks are continually evolving, and attackers are using new tactics to evade detection. Therefore, models trained on one dataset may not generalize well to new and unseen datasets, resulting in high false positives and false negatives.
3. Data Privacy: Phishing attacks involve sensitive data such as user credentials, credit card numbers, and social security numbers. Therefore, protecting the privacy of the data is essential to prevent it from falling into the wrong hands.
4. Real-Time Detection: Phishing attacks are time-sensitive, and it is essential to detect them as soon as possible to prevent users from falling victim. Therefore, the detection system must operate in real-time and have low latency.
5. Scalability: Phishing attacks can occur on a large scale, with attackers sending thousands of emails or creating multiple fake websites. Therefore, the detection system must be scalable to handle a large volume of data and requests.
6. Interpretability: Machine learning models used for phishing attacks detection are often considered black boxes, making it challenging to understand how they make predictions. Therefore, interpretable models are essential to provide explanations for model predictions and build trust in the system.

DISADVANTAGES:

1. Training data: Machine learning models rely on large datasets of known phishing attacks to train and improve their accuracy. However, obtaining high-quality training data can be difficult and time-consuming, and it may not always

be representative of the latest types of phishing attacks.

2. False positives: Machine learning models may generate false positives, flagging legitimate emails as potential phishing attacks. This can be a significant problem in environments where users receive large volumes of emails and may result in users ignoring legitimate warnings.
3. Interpretability: Machine learning models can be difficult to interpret, making it challenging to understand how they arrived at their decision. This can make it difficult to fine-tune the model or address potential biases.
4. Adversarial attacks: Attackers may attempt to evade detection by intentionally designing phishing attacks to bypass machine learning models. This requires ongoing monitoring and updates to the models to keep up with evolving tactics.
5. Resource-intensive: Training and maintaining machine learning models can be resource-intensive, requiring significant computing power and expertise.

PROPOSED SYSTEM:

Data Collection: The system will collect a dataset of phishing emails, websites, and messages. The dataset will be labeled as phishing or legitimate, and it will include various features, such as the sender's email address, the content of the email, the website's URL, and the website's content.

1. Data Preprocessing: The collected dataset will undergo preprocessing to clean the data and prepare it for analysis. This step will involve removing any irrelevant features and transforming the remaining features into a format that can be used by the machine learning algorithm.
2. Feature Extraction: The system will extract various features from the preprocessed data, such as the presence of suspicious keywords, the URL's domain name, and the website's HTML code. These features will be used to train the machine learning model.
3. Model Training: The system will use a supervised learning approach to train the machine learning model on the extracted features. The model will be trained on a subset of the dataset, and the performance will be evaluated using another subset of the dataset.

4. Model Testing: The trained model will be used to classify new instances of emails, websites, or messages as phishing or legitimate. The system will use the model's prediction to alert the user if a phishing attack is detected.
5. Model Updating: The system will continuously update the machine learning model to adapt to new types of phishing attacks and maintain high accuracy in detecting them.

ADVANTAGES:

1. Accuracy: Machine learning models can be trained on large datasets of known phishing attacks, enabling them to accurately detect new attacks based on patterns and characteristics learned from previous attacks.
2. Speed: Machine learning algorithms can analyze large amounts of data quickly, allowing for real-time detection and response to phishing attacks.
3. Scalability: Machine learning models can be trained on large datasets and can be easily scaled to handle increasing volumes of data.
4. Adaptability: Machine learning models can adapt and improve over time as new types of phishing attacks emerge, enabling them to stay ahead of the latest threats.
5. Automation: Machine learning algorithms can be fully automated, reducing the need for human intervention in the detection and response process.

METHODOLOGY AND TECHNIQUES:

The methodology and techniques for phishing attacks detection using machine learning approach involves several steps and techniques, which are discussed below.

1. Feature Extraction: The first step is to extract relevant features from the email, website or message to be analyzed. These features can include metadata such as sender email address, message content, and website URL. The features can be extracted using techniques such as natural language processing, regular expressions, and HTML parsing.
2. Data Preprocessing: The next step is to preprocess the extracted features to clean and prepare the data for analysis. This step includes

removing irrelevant features, handling missing values, and transforming the data into a format that can be used by machine learning algorithms.

3. Feature Selection: After the feature extraction and preprocessing, the next step is to select the most relevant features for phishing detection. Feature selection can be performed using techniques such as correlation analysis, information gain, and chi-square test.
4. Algorithm Selection: Once the relevant features are selected, the next step is to select an appropriate machine learning algorithm for classification. The most common algorithms used for phishing detection include decision trees, logistic regression, support vector machines, and neural networks.
5. Model Training: The selected machine learning algorithm is trained on a labeled dataset containing both phishing and legitimate instances. The dataset is split into training and testing sets to evaluate the model's performance. The training process involves adjusting the model's parameters to minimize the classification error and maximize the accuracy.
6. Model Evaluation: After the model is trained, it is evaluated on the testing dataset to determine its accuracy, precision, recall, and F1 score. These performance metrics are used to evaluate the model's effectiveness in detecting phishing attacks.
7. Model Optimization: If the model's performance is not satisfactory, further optimization can be performed by adjusting the model's hyperparameters or selecting different features for training.
8. Real-Time Detection: Once the model is optimized, it can be deployed for real-time phishing detection. Emails, websites, or messages are analyzed using the trained model, and if the probability of phishing is higher than a threshold, the user is alerted.
9. Continuous Monitoring and Improvement: Phishing attacks are constantly evolving, so it is essential to continuously monitor the model's performance and update it with new features and algorithms to improve its accuracy and effectiveness.

LITRATURE SURVEY:

Phishing attacks are a severe threat to cybersecurity, and machine learning (ML) techniques have been widely adopted to detect and prevent such attacks. This literature survey highlights some recent research papers that have proposed different ML-based approaches for phishing detection.

1. Random Forest (RF) Algorithm

The RF algorithm is a popular machine learning method for phishing detection. In a recent study, Liu et al. (2020) proposed an RF-based approach that uses text and image-based features to detect phishing websites. The study found that the proposed method achieved a high detection rate and a low false positive rate.

2. Deep Learning (DL) Techniques

Deep learning techniques have been widely used in recent years to improve phishing detection. In a study by Huang et al. (2020), a hybrid deep learning approach was proposed to detect phishing websites. The study used a Convolutional Neural Network (CNN) to extract image-based features and a Long Short-Term Memory (LSTM) network to classify the websites as phishing or legitimate.

3. Ensemble Learning Techniques

Ensemble learning techniques combine multiple models to improve the accuracy of predictions. In a study by Kalid et al. (2021), an ensemble learning approach was proposed to detect phishing websites. The study combined three machine learning algorithms, i.e., RF, Support Vector Machines (SVM), and Logistic Regression (LR), to improve the accuracy of the detection.

4. Hybrid Machine Learning Techniques

Hybrid machine learning techniques combine multiple machine learning methods to improve detection accuracy. In a recent study, Abdelhamid et al. (2021) proposed a hybrid machine learning approach that combines DL and RF algorithms to detect phishing emails. The study used a CNN to extract text and image-based features and a Random Forest classifier to predict whether an email is a phishing attack or not.

5. Feature Selection Techniques

Feature selection techniques are used to identify the most relevant features for phishing detection. In a study by Al-Dhubhani et al. (2020), a feature selection approach was proposed to detect phishing websites. The study used a genetic algorithm to select the most relevant features and then used an SVM classifier to classify the websites.

6. Transfer Learning Techniques

Transfer learning techniques are used to transfer knowledge learned from one domain to another. In a study by Luo et al. (2020), a transfer learning approach was proposed to detect phishing emails. The study used a pre-trained model on a large-scale dataset to extract features from emails and then fine-tuned the model on a small-scale dataset for phishing detection.

CONLUSION:

In conclusion, phishing attacks are a major threat to organizations, and traditional methods of detecting these attacks may not be effective against new and evolving threats. Machine learning offers significant advantages for detecting and preventing phishing attacks, including real-time detection, improved accuracy, scalability, adaptability, and automation. However, there are also potential disadvantages to using machine learning, such as the need for high-quality training data, the potential for false positives, interpretability challenges, adversarial attacks, and resource requirements.Despite these challenges, machine learning remains an effective approach for detecting and preventing phishing attacks. As the technology continues to evolve, machine learning algorithms are becoming increasingly sophisticated, and new techniques such as deep learning and natural language processing are enabling even more accurate and efficient phishing detection.

REFERENCES

1. JafarAbo Nada; Mohammad Rasmi Al-Mosa, 2018 International Arab Conference on Information Technology (ACIT), A Proposed Wireless Intrusion Detection Prevention and Attack System

2. Kinam Park; Youngrok Song; Yun-Gyung Cheong, 2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigData Service), Classification of Attack Types for Intrusion Detection Systems Using a Machine Learning Algorithm

3. S. Bernard, L. Heutte and S. Adam "On the Selection of Decision Trees in Random Forests" Proceedings of International Joint Conference on Neural Networks, Atlanta, Georgia, USA, June 14-19, 2009, 978-1-4244-3553-1/09/$25.00 ©2009 IEEE

4. A. Tesfahun, D. Lalitha Bhaskari, "Intrusion Detection using Random Forests Classifier with SMOTE and Feature Reduction" 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies, 978-0-4799-2235-2/13 $26.00 © 2013 IEEE

5. Le, T.-T.-H., Kang, H., & Kim, H. (2019). The Impact of PCA-Scale Improving GRU Performance for Intrusion Detection. 2019 International Conference on Platform Technology and Service (PlatCon). Doi:10.1109/platcon.2019.8668960

6. Anish Halimaa A, Dr K.Sundarakantham: Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019) 978-1-5386-9439-8/19/$31.00 ©2019 IEEE "MACHINE LEARNING BASED INTRUSION DETECTION SYSTEM."

7. Mengmeng Ge, Xiping Fu, Naeem Syed, Zubair Baig, Gideon Teo, Antonio Robles-Kelly (2019). Deep Learning-Based Intrusion Detect ion for IoT Networks, 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC), pp. 256-265, Japan.

8. R. Patgiri, U. Varshney, T. Akutota, and R. Kunde, "An Investigation on Intrusion Detection System Using Machine Learning" 978-1-5386-9276-9/18/$31.00 c2018IEEE.

9. Rohit Kumar Singh Gautam, Er. Amit Doegar; 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence) "An Ensemble Approach for Intrusion Detect ion System Using Machine Learning Algorithms."

10. Kazi Abu Taher, Billal Mohammed Yasin Jisan, Md. Mahbubur Rahma, 2019 International Conference on Robot ics, Electrical and Signal Processing Techniques (ICREST)"Network Intrusion Detect ion using Supervised Machine Learning Technique with Feature Selection."

11. L. Haripriya, M.A. Jabbar, 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)" Role of Machine Learning in Intrusion Detection System: Review"

12. Nimmy Krishnan, A. Salim, 2018 International CET Conference on Control, Communication, and Computing (IC4) "

Machine Learning-Based Intrusion Detect ion for Virtualized Infrastructures"

13. Mohammed Ishaque, Ladislav Hudec, 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS) "Feature extract ion using Deep Learning for Intrusion Detection System."

14. Aditya Phadke, Mohit Kulkarni, Pranav Bhawalkar, Rashmi Bhattad, 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)"A Review of Machine Learning Methodologies for Network Intrusion Detection."

15. Iftikhar Ahmad , Mohammad Basheri, Muhammad Javed Iqbal, Aneel Rahim, IEEE Access (Volume: 6) Page(s): 33789 – 33795 "Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection."

16. B. Riyaz, S. Ganapathy, 2018 International Conference on Recent Trends in Advanced Computing (ICRTAC)" An Intelligent Fuzzy Rule-based Feature Select ion for Effective Intrusion Detection."