ISSN No:-2456-2165

Real Time Phishing Website Detection using ML

Praveen N[1]; Kartik S N[2]; Santosh V[3]; Kishore N[4]; Dr. Prakasha S[5]
Department of Information Science RNS Institute of Technology, Bengaluru

Abstract:- Phishing involves fraudulent activities where attackers impersonate trustworthy websites to unlawfully obtain private information, including usernames, passwords, and financial details. Traditional detection methods, including blacklists and heuristic-based approaches, struggles identifying new, evolving phishing sites. In recent times, AI using machine learning (ML) has emerged as a powerful tool for phishing detection, offering predictive capabilities that adapt to changing attack patterns. This survey examines state- of-the-art ML techniques for phishing website detection, covering feature extraction, model types, and challenges in data handling. Through analyzing recent methodologies, this paper highlights the strengths and limitations of various ML models and proposes directions for further improving phishing detection systems.

Keywords:- *Phishing Detection, Machine Learning, Cybersecurity, Feature Extraction, Classification Models, URL Analysis.*

I. INTRODUCTION

Phishing is one among the top widespread and deceptive forms of cybercrime, targeting users to obtain secure data, such as account credentials, financial data, or personal identity details. Attackers accomplish this by creating false sites mirroring the appearance of legitimate ones, often exploiting human psychology through urgent or enticing messages. These attacks have evolved significantly over the years, becoming more sophisticated and harder to detect, especially as the internet expands in both user base and functionality. Traditional methods, such as blacklists and heuristic-based detection, offer some protection by filtering known phishing sites or using basic rule-based criteria. However, these techniques are inherently limited: blacklists cannot identify newly emerging phishing sites, and heuristic rules are often bypassed by attackers who adjust tactics to avoid detection.

The advent of machine learning (ML) has proven to be a promising solution to these limitations, bringing predictive capabilities that allow systems to recognize phishing attempts based on patterns rather than specific pre-identified threats. By analyzing numerous characteristics—such as URL structure, domain registration details, and website content—ML algorithms can classify websites as legitimate or phishing featuring an elevated degree of accuracy. In recent times, advances in a combination of conventional machine learning techniques and advanced deep learning architectures have greatly enhanced the precision of phishing detection. Algorithms including Random Forest and SVM, and neural networks are widely applied, each offering unique advantages in handling complex data.

II. LITERATURE SURVEY

The literature on machine learning-based phishing detection shows both advancements and ongoing challenges in the areas of feature extraction, detection efficiency, and adaptability to new phishing techniques. Below, we review significant studies on feature-based detection, deep learning methods, ensemble models, and hybrid approaches.

- Feature-Based identification through Machine Learning: Sarma et al. (2021) conducted a detailed analysis of machine learning methods applied to phishing prevention, focusing on Random Forest (RF) and (SVM), and K-nearest neighbors (KNN). Among these, RF showed the highest accuracy (98%) in distinguishing phishing from legitimate sites due to its handling of complex features like URL structure, domain age, and HTTPS status. This study underscores the importance of well-chosen features but also highlights challenges in adapting models to new phishing patterns(Sarma2021_Chapter_Compa…).

- Machine Learning in Phishing Lifecycle Detection: Tang and Mahmoud (2021) analyzed ML techniques at different stages of phishing attacks, such as URL analysis, feature extraction, and classification. They noted that each phase benefits from specific ML models: decision trees are effective in feature extraction, while neural networks can identify deeper patterns. The study suggests that a multi-stage ML framework enhances detection accuracy, but real-time deployment remains challenging due to high computational costs(make-03-00034 (1)).

- Deep Learning and Convolutional Neural Networks (CNNs): Odeh et al. (2021) explored advanced deep learning architectures like Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks networks, to improve phishing detection. CNNs process URLs and webcontent to detect phishing patterns more accurately but at a higher computational cost. The authors conclude that while CNNs improve detection rates, a hybrid approach may balance accuracy and efficiency more effectively in resource- constrained environments(2020013989).

- Unsupervised Learning for Phishing Detection: Studies by Kalaharsha and Mehtre emphasize the possibilities offered by unsupervised learning to detect phishing without relying on labeled data. Clustering techniques can reveal patterns among phishing sites that supervised models may miss. Nonetheless, these models encounter difficulties in achieving the precision of supervised learning and it might be most effective when combined with other approaches. to enhance adaptability to new phishing strategies(make-03-00034 (1)).

- Ensemble Models for Improved Accuracy: Patel et al. (2024) examined ensemble models, specifically combining Random Forest with PCA for enhanced results to enhance phishing detection performance. Ensemble approaches combine classifiers for robust predictions, reducing false positives and improving reliability. Patel's study also highlights the importance of embedding security checks within ML models to identify vulnerabilities like poor input validation and encryption, promoting safer real-world applications(2020013989).

- Natural Language Processing (NLP) in Phishing Detection: Bingyang (2024) researched NLP applications for feature extraction from phishing emails and URLs. By analyzing textual content, NLP models can identify phishing patterns within language and URL structure. However, this method requires extensive, domain-specific training data to achieve accuracy across diverse phishing scenarios. NLP models show promise, especially when used alongside other machine learning techniques to improve adaptability(2020013989).

- Hybrid Approaches Combining Heuristics and Machine Learning: Vijayalakshmi et al. (2020) presented a hybrid phishing detection model that combines rule-based heuristics with machine learning classifiers. Their study divides detection into web address-based methods, webpage content analysis, and hybrid approaches. The authors found that combining heuristics with ML enhances detection accuracy, particularly in real-time scenarios, by filtering out non-suspicious cases early in the detection process. This layered approach shows potential in reducing false positives and computational load (make-03-00034 (1)).

- Phishing Detection Using Reinforcement Learning: Recently, Jain and Gupta (2022) investigated reinforcement learning for phishing detection, where the model adapts its detection strategy based on user feedback. Their study demonstrated that reinforcement learning models could adapt to new phishing types over time, improving accuracy as they gather more data on successful detections. However, they noted that reinforcement learning requires significant computational resources and training time, potentially restricting its practicality in real-time applications without further optimization (Sarma2021_Chapter_ Compa.

III. OBJECTIVES

The goal of this survey is to thoroughly examine and compare modern machine learning methods applied used for detecting phishing websites. This review has multiple, focused aims:

- **Explore Key Machine Learning Models**: To evaluate various machine learning approaches, including Random Forest, Support Vector Machines, Convolutional Neural Networks, and Long Short-Term Memory models, and understand how each contributes to detecting phishing websites.
- **Identify Model Strengths and Weaknesses**: To outline the strengths, such as high accuracy or adaptability, and the limitations of each model, including challenges like computational demands or susceptibility to evolving phishing tactics.
- **Examine Feature Selection Techniques**: To analyze which features (such as URL length, domain age, HTTPS usage, and webpage content) are most effective at telling apart phishing and legitimate sites, helping refine future detection models.
- **Compare Ensemble and Hybrid Approaches**: To evaluate the efficiency of combining different models or integrating traditional approaches (e.g., heuristics) with machine learning to increase detection performance while retaining computational efficiency high.
- **Address Real-Time Detection Needs**: To explore the challenges of applying machine learning models in real-time scenarios, including issues related to speed, processing power, and scalability to large numbers of users.
- **Investigate Emerging Solutions and Trends**: To highlight recent innovations like reinforcement learning and natural language processing-based models, examining how these innovative methods can adapt to changing phishing tactics and enhance the resilience of detection systems.
- **Suggest Directions for Future Research**: To suggest potential directions for future research focusing on ways to address current limitations—such as creating more adaptable and efficient models or incorporating security features directly into the model training process.
- **Support Practical Applications**: To evaluate how these results may guide the deployment of machine learning-based phishing detection systems in real-world applications, enhancing online security for individuals and organizations.

IV. PROPOSED SYSTEM

This survey paper suggests a comprehensive ML-based phishing detection framework. The proposed system will incorporate a combined model integrating deep learning with traditional feature-based techniques. The objective is to enhance accuracy in identifying both known and novel phishing sites by leveraging URL analysis, page structure examination, and textual content. Integrating supervised and unsupervised learning will enhance adaptability to evolving phishing patterns.

ISSN No:-2456-2165

V. ADVANTAGES OF PROPOSED SYSTEM

- **Real-Time Detection**: The hybrid ML model aims to achieve faster detection suitable for real-time applications.
- **Improved Accuracy**: By combining deep learning with feature-based methods .The model can achieve improved detection rates with reduced false alarms.
- **Adaptability**: The model's design allows it to adapt to emerging phishing tactics, improving its relevance in dynamic online environments.
- **Scalability**: The use of ensemble methods and dimensionality reduction enables efficient handling of large datasets, essential for real-world deployment.

VI. METHODOLOGY

➢ *The Methodology of the Proposed System Involves Several Stages:*

- **Data Collection**: Collect URL data and webpage content from sources like PhishTank and OpenPhish for phishing sites and Alexa for legitimate sites.
- **Feature Extraction**: Identify key features, including URL length, domain age, and HTTPS presence. Extract visual and structural features for deep learning models.
- **Model Training**: Train various ML classifiers, such as Random Forest, SVM, CNN, and LSTM, on labeled data. Fine-tune models through cross-validation to optimize accuracy.
- **Ensemble Learning**: Apply ensemble methods by combining RF with PCA to minimize data complexity while preserving high accuracy.
- **Evaluation**: Assess models using metrics like accuracy, precision, recall, and F1 score. Compare performance across models to determine the optimal configuration.

VII. SYSTEM ARCHITECTURE

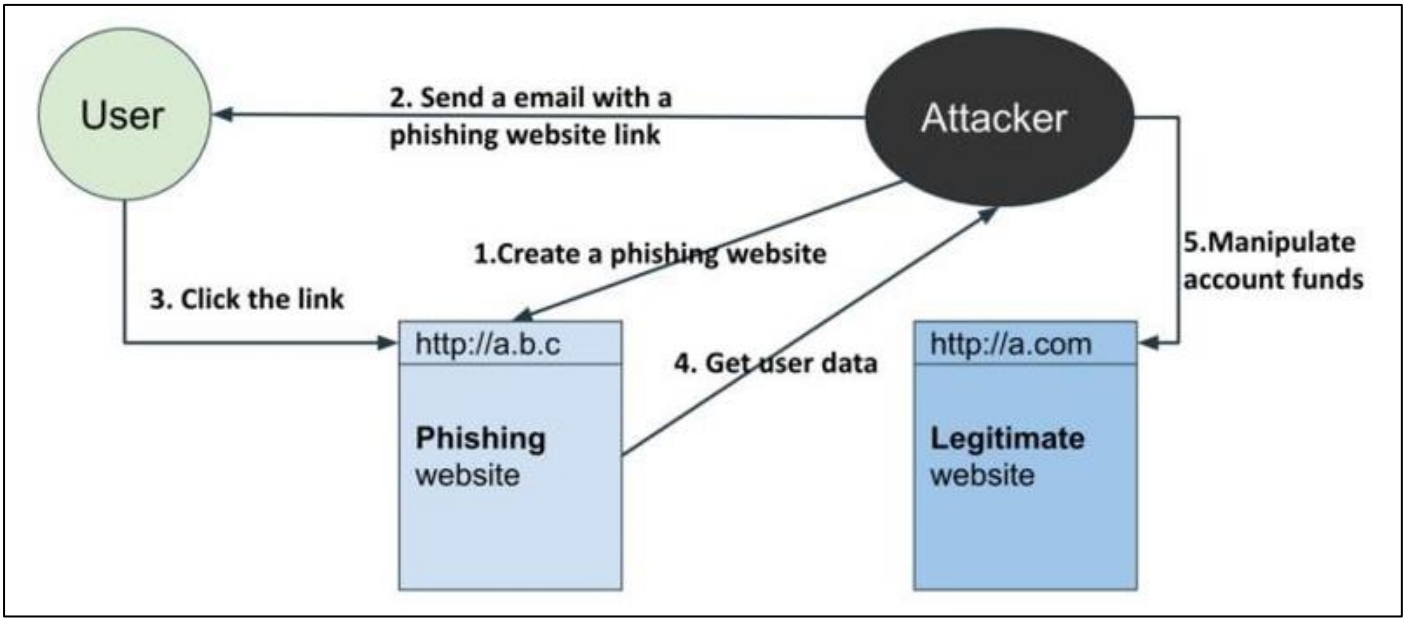

Fig 1 System Architecture

➢ *Creating a Fake Website:*

- Attackers build a phishing site that closely resembles a legitimate website, often using similar logos, colors, and layout.
- To deceive users, attackers may alter the URL subtly, like using slight spelling changes or similar characters. For instance, a fake URL might look like "aimazon" insteadof "amazon."

➢ *Delivering the Phishing Link:*

- Attackers send out links to the fake site, often through emails, SMS, voice messages, or QR codes.
- Social media and messaging apps are commonly used, expanding the reach of these phishing attempts.
- These messages often create urgency, using language that pressures users to click, such as warnings about account suspensions or overdue payments.

➢ *Collecting User Information:*

- Once users click the phishing link, they're taken to the fake website, where they're asked to enter secure data such as login credentials, or payment details.
- The phishing site may mimic login or payment pages to make the experience feel authentic.

➢ *Using Stolen Data for Theft:*

- Attackers use the collected data to access the victim's real accounts, potentially across multiple sites if the user has reused their credentials.
- The stolen information can also be used in other illegal activities or sold to other criminals.

➢ *Growing Cyber Threat:*

- Phishing has adapted over time to target new online services, especially as digital transactions have grown.
- Statistics show phishing is a widespread issue; in 2020, phishing made up nearly a third of all cybercrime complaints, resulting in substantial financial losses.

VIII. CONCLUSION

Machine learning offers a flexible and effective approach to phishing detection, enabling predictive models to identify previously unseen phishing attacks. The survey concludes that while models like RF and deep learning techniques provide high accuracy, a hybrid model combining these methods may offer the most comprehensive solution. Future research should focus on developing adaptable models with low computational cost, capable of real-time deployment in practical settings.

REFERENCES

[1]. Tang, L., Mahmoud, Q. H. "A Survey of Machine Learning- Based Solutions for Phishing Website Detection." *Machine Learning & Knowledge Extraction*, 2021. This paper reviews the life cycle of phishing attacks.

[2]. Vijayalakshmi, T., et al. "Taxonomy of Automated Phishing Detection Solutions." *Journal of Cybersecurity*, 2020. This paper categorizes phishing detection methods into URL-based, content- based, and hybrid approaches, comparing the strengths of each.

[3]. Jain, A., Gupta, P. "Reinforcement Learning for Phishing Detection." *International Journal of Computer Science Research*, 2022. The authors explore reinforcement learning for phishing detection, noting its adaptability in evolving phishing tactics.

[4]. Kalaharsha, A., Mehtre, B. M. "Unsupervised Learning Techniques for Phishing Detection." *Journal of Information Security and Applications*, 2021. This research examines unsupervised learning approaches that cluster phishing data without labels, offering insights into alternative detection methods.

[5]. Bingyang, L. "Natural Language Processing in Phishing Detection." *Journal of Emerging Technologies in Computing Systems*, 2024. This paper focuses on NLP techniques for extracting phishing features from text and URLs, addressing challenges in model training.

[6]. Patel, R., et al. "Ensemble Models for Phishing Detection and Security Awareness." *Cybersecurity Journal*, 2024. The study reviews ensemble methods, combining machine learning models with security checks to prevent vulnerabilities in generated code.

[7]. El Asri, L., et al. "Multi-Turn Dialogue for Clarifying User Intent in Phishing Detection Systems." *Computational Intelligence Journal*, 2024. This paper proposes using dialogue models for interpreting ambiguous user prompts in phishing detection, enhancing model accuracy in complex scenarios.