e-ISJN: A4372-3114
p-ISJN: A4372-3115

ISSN: 2321-7782 (Online)
ISSN: 2347-1778 (Print)
Impact Factor: 6.012

Volume 12, Issue 11, November 2024

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

A Monthly Double-Blind Peer Reviewed, Refereed, Open Access, International Journal - Included in the International Serial Directories

ML-Based Phishing Detection: The key to protecting your data

Savarnika Ravulapelly[1]
Student, Department of Information Technology,
Stanley College of Engineering and Technology for Women,
Hyderabad, Telangana, India.

Paladugu Gayathri[2]
Student, Department of Information Technology,
Stanley College of Engineering and Technology for Women,
Hyderabad, Telangana, India.

Zainab Farooq[3]
Student, Department of Information Technology,
Stanley College of Engineering and Technology for Women,
Hyderabad, Telangana, India.

T.C Swetha Priya[4]
Assistant Professor, Department of Information Technology,
Stanley College of Engineering and Technology for Women,
Hyderabad, Telangana, India.

DOI: https://doi.org/10.61161/ijarcsms.v12i11.2

Abstract: Internet dragged more than half of the world's population into the cyber world. Unfortunately, with the increase in internet transactions cybercrimes also increase rapidly. With the anonymous structure of the internet, attackers attempt to deceive the end-users through different forms namely phishing, malware, system tunneling, ransom ware etc. Amongst them, phishing is the most deceiving attack that exploits the vulnerabilities in the end-users. Phishing is often done through emails and malicious websites to lure the user by posing themselves as a trusted entity. Security experts have been proposing many anti-phishing techniques. Till today there has been no single solution that can mitigate all the vulnerabilities. This paper gives an overview of a systematic review of current trends in web phishing detection techniques. The objective of this study is to acknowledge the status of current research in automated web phishing detection and evaluate their performance. This study also discusses the research avenues for future investigation.

Keywords: Attack, Security threats, Phishing, Cyber-attack, Internet security, Machine learning.

I. INTRODUCTION

The Internet has significantly transformed our world today due to its versatility. With its advanced infrastructure, people can perform transactions like shopping and banking at any time and from anywhere. While the internet offers numerous advantages, it also presents various security and privacy challenges. The anonymous and decentralized nature of the internet creates a fertile ground for cyber-attacks, including phishing, malware distribution, and privacy breaches. As a result, end-users face serious threats from these attacks. Among the various types of cyberattacks, phishing is the most prevalent, primarily targeting individuals by exploiting their vulnerabilities rather than directly attacking computers. Phishing is a cyber tactic that employs social engineering and technical tricks to steal users' identity data and financial account credentials by posing as a trusted entity. To ensnare their targets, attackers create fraudulent websites and send emails that appear to be from legitimate sources. The main objective of phishing is to capture sensitive information such as usernames, passwords, bank account details, and credit card numbers. Attackers engage in phishing for various reasons, including financial gain, stealing personal information, damaging the reputation of organizations, or sometimes simply for notoriety. AI-driven phishing detection utilizes machine learning algorithms to analyze a wide array of factors in emails, URLs, websites, and other communication channels to assess their potential maliciousness. Unlike traditional rule-based methods, machine learning systems learn from extensive datasets and can identify subtle patterns that may suggest phishing attempts. By recognizing features such as unusual text, suspicious URL formats, and abnormal sender behavior, AI can more accurately flag potential phishing threats compared to conventional techniques. Machine learning methods for phishing detection are varied and include supervised learning where models are trained on labeled data.

II. Literature Survey

Lizhen Tang et al., [1] has proposed a survey on machine learning solutions for detecting phishing websites. This survey highlights that phishing attacks have become increasingly sophisticated, rendering traditional detection methods largely ineffective. The study explores various approaches, including supervised learning, unsupervised learning, and deep learning, which can achieve high accuracy when applied to large datasets and complex pattern recognition. Different algorithms, such as SVM, LR, and ANN, were utilized to evaluate the accuracy of phishing detection. The findings indicate significant improvements in phishing detection accuracy when machine learning techniques are employed, but they also emphasize the need for more diverse datasets with relevant features to further enhance model performance. Future research should focus on strengthening the robustness of these models while reducing false positives and negatives. It is crucial to gather datasets with a wider range of information and more robust features to boost the effectiveness of these models. Major future research directions should aim to refine the models to minimize false positives and negatives, ensuring the reliability and effectiveness of AI-based phishing detection systems.

Abdul Basit et al. [2] have presented a Comprehensive Survey of AI-Enabled Phishing Attacks Detection Techniques. This survey delves into various methods for detecting phishing attacks using AI, with a particular emphasis on machine learning approaches. The authors note that phishing attacks are becoming more sophisticated, rendering traditional detection methods less effective. Machine learning models, both supervised and unsupervised, enhance accuracy by analyzing extensive datasets and recognizing intricate patterns. The paper reviews the application of various datasets and URL characteristics for training these models and assesses their performance through algorithms such as support vector machines (SVM), logistic regression (LR), and artificial neural networks (ANN). The findings indicate notable improvements in phishing detection accuracy with machine learning techniques, while also highlighting the necessity for diverse datasets and features to boost model performance. Future research avenues include enhancing model robustness and minimizing false positives and negatives. By utilizing machine learning strategies like supervised, unsupervised, and deep learning, the paper demonstrates significant advancements in detection accuracy, adaptability to emerging phishing tactics, and overall efficiency. The study emphasizes the critical role of varied datasets and feature sets, such as URL length and domain age, in training these models. The results reveal that machine learning algorithms, including SVM, LR, and ANN, provide greater accuracy and lower false positive rates compared to traditional methods. The authors call for continued research to strengthen model robustness, decrease false positives and negatives, and adapt to evolving phishing strategies, ultimately aiming to sustain and enhance the reliability of AI-driven phishing detection systems.

Rasha et al., [3] has done a survey on the Detection of Phishing Websites which describes the multiple detection methods for phishing websites that can be characterized as a serious threat for online security. It also separates some detection techniques into different approaches such as blacklist-based methods, heuristic-based methods, machine learning-based methods, and visual similarity-based methods, respectively highlighting their strengths and weaknesses. This paper also discusses some hybrid approaches that combine multiple techniques to improve the accuracy of detection. Among the key challenges this field faces, the evolving nature of phishing attacks, the threat of false positives versus false negatives, and the inevitable evasive strategy used by the attackers abound. In general, this survey yields fertile insights on the state-of-the-art in phishing detection and the associated research endeavors to combat this emerging threat.

Zamir et al., [4] has proposed diverse Machine Learning Algorithms to detect Phishing that investigates how various machine learning techniques can be used to identify phishing websites. It offers a thorough analysis of different algorithms, including Decision Trees, Random Forests, Support Vector Machines (SVM), K-Nearest Neighbors (KNN), and Neural Networks, and compares their effectiveness in detecting phishing sites. The paper highlights the importance of feature extraction methods, such as URL-based features, domain name characteristics, and HTML content, which are essential for training machine learning models. It also discusses the strengths and weaknesses of each algorithm, pointing out how ensemble methods and hybrid models can enhance detection accuracy. Additionally, the study addresses the challenges faced in phishing website detection, such as the constantly changing nature of phishing attacks, and the trade-offs between model complexity, performance, and interpretability. Overall, the research demonstrates how a variety of machine learning approaches can be utilized to improve phishing detection systems.

Mehmet Korkmaz et al., [5] has proposed a Machine Learning based on URL Analysis which examines the use of machine learning techniques to identify phishing websites through the analysis of URLs. The authors investigate how different characteristics of URLs—such as domain names, length, the presence of special characters, and suspicious keywords—can be extracted and utilized to train machine learning models for classification purposes. The study compares various machine learning algorithms, including Decision Trees, Random Forests, and Support Vector Machines (SVM), evaluating their effectiveness in accurately detecting phishing websites based on URL features. The authors emphasize the advantages of URL analysis in phishing detection, especially during the initial phases of an attack, as it tends to be less resource-intensive and quicker than more complex methods like content-based analysis. Additionally, the paper addresses challenges such as the ever-changing nature of phishing URLs and the necessity for ongoing model adjustments to keep pace with new phishing strategies. In summary, the research illustrates the potential of machine learning-based URL analysis in combating phishing threats.

Lior Shamir et al., [6] has proposed analysis and prevention of AI-Based Phishing Email Attacks which analyzes the increasing phishing attacks seemingly backed by Artificial Intelligence. They delved into the ways attackers have started using AI techniques, in particular natural language processing and machine learning, to improve the crafting of phishing emails with more convincing, personalized messages, eluding detection by the traditional systems as well. The paper discusses most of the AI-driven methods available today, which make phishing emails more effective. Further on in the text, defense mechanisms in the current state are also discussed and advanced detection strategies proposed for AI-generated phishing attempts, along with machine learning models trained on large datasets of phishing and legitimate emails and behavioral analysis during anomalous email interaction patterns. By this rationale, the paper calls for an update of how anti-phishing systems are to be done continuously due to the fact that AI technologies evolve rapidly and are capable of evading the traditional detection methods. At its core, the study calls for a combination of artificial intelligence-based detection tools with human awareness and response strategies in a bid to effectively detect AI-driven phishing attacks.

Asadullah Safi et al., [7] has done a systematic review that classifies the existing phishing website detection by focusing on methods like blacklist-based, heuristic-based, machine learning-based, and hybrid approaches. The limitations and the strengths of each approach were outlined based on the URL pattern, page content, as well as the characteristics of the domain. More recent trends included the use of deep learning techniques and visual similarity-based detection in an attempt to achieve improved accuracy and robustness in phishing detection systems. The authors discuss the most stringent challenges currently faced in the area-cumulation in phishing attacks, false positives, and the critical need for real-time detection. Overall, the survey provides insightful information on what is happening about phishing website detection but also establishes deficits and areas for further research in this quintessential cybersecurity domain.

Daniel Nahmias et al., [8] has proposed Prompted Contextual Vectors for Spear-Phishing Detection which presents a novel method for identifying spear-phishing attacks. Unlike general phishing, spear-phishing targets specific individuals or organizations with personalized attacks that often use contextual information to appear more credible. The prompted contextual vectors is a technique that employs machine learning to capture and analyze contextual details from email content and sender behavior. By training models on the semantic meaning and context of communications, this method enables the detection system to better differentiate between legitimate emails and spear-phishing attempts. The approach focuses on context-aware analysis, taking into account not just specific email characteristics (such as sender domain or subject line) but also the wider context of previous communication patterns, relationships, and relevant organizational data. The paper illustrates how this technique enhances detection accuracy and minimizes false positives, offering a more advanced solution for recognizing spear-phishing attempts. Overall, the study underscores the significance of contextual awareness in strengthening phishing detection systems against increasingly targeted and personalized threats.

Yazan Ahmad et al., [9] has proposed a Meta-Learners and Extra-Trees Algorithm for the Detection of Phishing Websites which delves into the use of advanced machine learning techniques to improve the detection of phishing websites. The AI meta-learners integrate various learning algorithms to enhance predictive performance that can be effectively utilized for identifying phishing sites. They emphasize the Extra-Trees algorithm, an ensemble learning method that relies on random decision trees, to classify websites as either legitimate or phishing. The study demonstrates that the combination of these techniques, which leverage a variety of feature sets including URLs, domain characteristics, and website content, can significantly enhance detection accuracy while minimizing false positives. Additionally, the authors evaluate the performance of their proposed model against other conventional machine learning methods, revealing that their approach yields better results in terms of accuracy and robustness. The paper concludes that the integration of AI meta-learners and Extra-Trees presents a promising strategy for advancing phishing detection systems, particularly in response to the constantly evolving tactics used in phishing attacks.

Tajamul Shahzad et al., [10] have proposed a study titled "Unveiling the Efficacy of AI-based Algorithms in Phishing Attack Detection," which explores the effectiveness of phishing attack detectors developed using AI-backed algorithms. The phishing landscape is continuously evolving, with AI and machine learning algorithms enhancing the detection capabilities against modern phishing attacks. Traditional methods that rely heavily on human intervention are proving inadequate against the sophisticated evasion techniques employed by contemporary phishing technologies. This study assesses the performance of various AI-based algorithms in identifying phishing URLs and email content, including SVM, Random Forest, and deep learning models. The research emphasizes how AI-driven approaches can automate and streamline the identification of phishing attempts. It also discusses the roles of techniques like NLP and neural networks in recognizing patterns in phishing emails and websites. The authors present empirical results from their experiments, detailing how each algorithm performed in real-world scenarios regarding detection accuracy and overall effectiveness. The conclusion highlights that AI-based systems significantly reduce false positives and enhance detection rates compared to traditional methods, making them a crucial component of cybersecurity defense frameworks.

Arun et al., [11] have introduced the Next Generation of Phishing Attacks Using AI-Powered Browsers. This new wave of phishing attacks highlights the evolving nature of cyber threats, particularly those driven by AI-enhanced browsing experiences. The argument is made that the growing integration of AI technology into everyday browsing is enabling more sophisticated phishing tactics. While traditional phishing methods remain prevalent, they are rapidly adapting due to advancements in AI, allowing attackers to automate personalized and convincing schemes. The paper explores how AI-powered browsers utilize features like predictive text and personalized search results, as well as automated page rendering based on user behavior. Although these features aim to improve user experience, they also create vulnerabilities that attackers can exploit. The authors provide several case studies illustrating how AI-enabled browsers can be manipulated to display fraudulent web pages, dynamically change content, and evade standard detection techniques. Furthermore, the paper addresses future threats, particularly the use of machine learning algorithms that can anticipate user preferences and behaviors, which attackers could leverage to craft more effective phishing lures. The authors advocate for improved security protocols and real-time monitoring solutions to combat this emerging cybersecurity threat, emphasizing the need for better collaboration between browser developers and security experts.

Salah Eddine Elgharbi et al.[12] has proposed a heuristic-based machine learning framework for detecting phishing attacks online. This framework aims to identify phishing threats in digital environments. However, the tactics used by attackers are constantly evolving, which often leaves traditional security measures lagging. The authors present an innovative system that combines heuristic analysis with machine learning techniques for real-time detection and mitigation of phishing threats. The framework focuses on key features such as URL structure, site behavior, and email content, employing various machine learning algorithms, including Decision Trees, Logistic Regression, and K-Nearest Neighbors. The heuristic rules enhance the system's ability to adapt to new phishing strategies. The paper outlines the architecture of the proposed framework, which integrates real-time data analysis with a comprehensive feature set to improve detection rates while minimizing false positives. Additionally, the authors provide empirical results from testing the framework on a large dataset of phishing URLs and legitimate websites, drawing conclusions about the findings of their research. They highlight the improved detection accuracy of the heuristic-based approach compared to traditional machine learning models and emphasize the need for further research into adaptive algorithms capable of addressing more complex phishing attacks.

Peter K. et al., [13] have proposed a Hybrid Security Framework for Phishing Awareness, Education, and Defense. This framework aims to boost phishing awareness through education while enhancing defense mechanisms. As phishing attacks become increasingly complex, it is evident that relying solely on technical solutions is not enough. The authors conclude that a combination of technical measures and comprehensive user education is essential to effectively mitigate phishing threats. The proposed hybrid framework incorporates multiple layers of protection, including AI-driven phishing detection systems, interactive awareness training, and real-time user feedback mechanisms. The educational aspect of the framework equips users with the knowledge and skills needed to recognize phishing attempts, while the defense mechanisms employ machine learning and heuristic-based strategies to identify and block such attacks. The study emphasizes the importance of conducting periodic phishing simulations and assessments to improve vigilance and response times. Empirical results indicate that organizations that integrate education with technical defenses experience fewer successful phishing attacks compared to those that depend solely on technical solutions. The authors recommend that future frameworks should further incorporate AI tools for personalized phishing training and adaptive security responses.

Ashit Kumar Dutta et al., [14] has proposed a method for identifying phishing websites using a machine learning algorithm. As internet and cloud technology continue to advance, electronic transactions have surged, leading to a rise in phishing attacks. These attacks aim to trick users into providing sensitive information, such as login credentials, financial data, and personal details, by using malicious websites that closely mimic legitimate ones. The increase in online trading and transactions has left consumers more vulnerable to these threats. Traditionally, detection methods have relied on blacklists and heuristic-based systems, but these approaches have not proven effective enough. The anonymous and decentralized nature of the internet allows phishing attacks to persist, and many existing security solutions struggle to keep up with the evolving sophistication of these techniques. Therefore, there is a pressing need for intelligent and adaptive methods to effectively detect and prevent such attacks. In this paper, Ashit Kumar Dutta presents a phishing URL detection system utilizing a machine learning approach. The proposed framework is based on a recurrent neural network (RNN), which serves as the model for this system. The RNN's primary function involves analyzing the structure of URLs to differentiate between phishing and legitimate sites. To demonstrate the accuracy of this method in identifying phishing web pages, the author tested the system against a dataset of 7,900 malicious URLs. The results indicated that applying machine learning significantly improves phishing detection rates compared to traditional methods.

Fatima Salahdine et al., [15] have proposed a method for detecting phishing attacks using a machine learning approach. Phishing attacks, which are a prevalent form of social engineering, target users' email accounts to fraudulently obtain confidential and sensitive information. These attacks can potentially lead to deeper intrusions into corporate or government networks, causing significant damage. Despite the development of various anti-phishing techniques over the past decade, many existing methods have shown inefficiencies and inaccuracies. This highlights the need for improved detection techniques that offer greater reliability. The paper presents a novel method for identifying phishing attacks through machine learning algorithms. The authors collected over 4,000 targeted emails sent to the University of North Dakota's email service. To model the attacks, they identified 10 key features that were instrumental in creating a comprehensive dataset, which was then used for training, validation, and testing of different machine learning algorithms. Four performance evaluation metrics were employed in this study: probability of detection, probability of miss-detection, probability of false alarm, and overall accuracy. The experimental results indicate that the use of artificial neural networks (ANN) has significantly enhanced phishing detection performance, outperforming traditional methods. This research underscores the importance of leveraging machine learning techniques to develop effective defenses against phishing attacks, ensuring better security measures for protecting sensitive information in digital communication.

III. Comparison of Phishing Detection Techniques

S. No	Algorithms	Remarks/Drawbacks
1.	Support Vector Machines (SVM), Logistic Regression (LR), and Artificial Neural Networks (ANN) for phishing website detection.	It provides a comprehensive overview of the advancements in AI-enabled phishing detection, making a compelling case for the adoption of machine learning techniques.
2.	The algorithms used in the study are Support Vector Machines (SVM), Logistic Regression (LR), and Artificial Neural Networks (ANN). These models enhance phishing detection by analyzing large datasets and identifying complex patterns.	It emphasizes the importance of diverse datasets and robust features for enhancing model performance and reducing false positives and negatives.
3.	List-Based Detection: Blacklist Approach, Whitelist Approach, Similarity-Based Detection: Content Similarity Detection, URL Similarity Matching. Decision Tree Classifier, Support Vector Machine (SVM), Random Forest, Neural Network-Based Detection.	Phishing attacks demand advanced detection to safeguard users and brands. List-based, similarity-based, and machine learning methods each offer unique strengths but reveal gaps for improvement against evolving tactics.
4.	Stacking Model (ensemble technique combining multiple classifiers for improved detection) Decision Tree, Random Forest, Support Vector Machine (SVM), Naive Bayes, K-Nearest Neighbors (KNN)	Phishing poses a significant risk across sectors by mimicking legitimate websites to steal sensitive information. This stacking model framework enhances detection accuracy by combining diverse algorithms, addressing the adaptability and complexity of phishing techniques.
5.	Machine Learning Algorithms: Decision Tree, Random Forest, Support Vector Machine (SVM), Naive Bayes, Logistic Regression, K-Nearest Neighbors (KNN), Neural Networks, Gradient Boosting, Detection Techniques: Blacklist-based, Rule-based, Anomaly-based	The proposed machine learning-based phishing detection system using URL analysis demonstrates strong performance in identifying phishing websites.
6.	Model Selection: Choose machine learning models (e.g., Random Forest, SVM, or Deep Learning models	This algorithm effectively combines natural language processing and machine learning techniques to identify phishing emails. It provides a scalable solution for adapting to new phishing tactics through continuous learning.
7.	List-Based, Visual Similarity, Heuristic, and Machine Learning-based approaches. Among these, the most frequently used algorithm is the Random Forest Classifier, with Convolutional Neural Networks (CNN) achieving the highest accuracy of 99.98% for phishing website detection.	The study provides a comprehensive comparison of various phishing website detection techniques, with a particular emphasis on the effectiveness of machine learning and deep learning methods. Notably, the use of Convolutional Neural Networks (CNN) shows outstanding performance, achieving nearly perfect accuracy in phishing detection.
8.	Supervised Machine Learning Model: The document vectors are fed into a downstream supervised machine learning model to classify emails, with a focus on detecting spear-phishing emails.	This approach innovatively uses LLMs for document vectorization, capturing persuasive elements in spear-phishing emails for accurate detection. The method demonstrates strong performance, achieving a 91%

		F1 score in identifying LLM-generated spear-phishing emails.
9.	Meta-Learner Models: The study utilizes four meta-learner models—AdaBoost-Extra Tree (ABET), Bagging-Extra Tree (BET), Rotation Forest-Extra Tree (RoFBET), and LogitBoost-Extra Tree (LBET)—using the Extra Tree base classifier to detect phishing websites.	The proposed meta-learner models demonstrate superior detection accuracy and minimal false positives compared to existing methods. These models offer an effective approach to combating the evolving nature of phishing attacks with AI-based countermeasures.
10.	Support Vector Machines (SVM), Random Forests, and Naive Bayes to improve phishing email detection.	It makes a significant contribution to the field of phishing detection by showcasing the advantages of hybrid machine learning approaches.
11.	Support Vector Machines (SVM), Random Forest, and deep learning models for phishing detection. It highlights the use of natural language processing (NLP) and neural networks for enhanced pattern recognition in phishing emails and websites	It provides a timely and important contribution to the field of cybersecurity by showcasing the potential of AI and ML in combating phishing attacks.
12.	Support Vector Machines (SVM), Random Forest, and Neural Networks for detecting AI-powered phishing attacks.	It sheds light on the emerging threats posed by AI-enhanced phishing tactics, highlighting a critical area of concern in the cybersecurity landscape
13.	Decision Trees, Logistic Regression, and K-Nearest Neighbors, combined with heuristic rules to enhance phishing detection.	It addresses a critical gap in phishing detection by combining heuristic analysis with machine learning.
14.	Random Forest, Support Vector Machines (SVM), and Gradient Boosting for phishing website detection.	It underscores the importance of leveraging machine learning in the fight against sophisticated phishing attacks.
15.	Support Vector Machines (SVM) and Random Forest for phishing detection, along with heuristic-based approaches. It also explores AI tools for personalized phishing awareness training.	It highlights a critical and often overlooked aspect of cybersecurity: the importance of user education alongside technical defenses.
16.	Neural Networks and Natural Language Processing (NLP) models to detect phishing emails by analyzing features like email headers, body content, and URL patterns.	It provides a timely and relevant contribution to the field of cybersecurity, particularly in the context of email threats.
17.	Long Short-Term Memory (LSTM) networks for detecting phishing attacks by analyzing sequential data. This AI-based approach improves the accuracy of phishing detection and addresses limitations of existing security methods	It can expand the understanding of phishing beyond traditional methods, emphasizing the importance of considering the entire attack lifecycle.
18.	Recurrent Neural Network (RNN) model to detect phishing websites by analyzing URL structures and patterns.	It highlights the critical need for advanced detection techniques in the face of evolving phishing threats.
19.	K-means clustering for feature selection and Artificial Neural Networks (ANN) for classifying emails as phishing or legitimate.	Feature selection and ANN for classification demonstrates a thoughtful approach to enhancing detection capabilities.
20.	Artificial Neural Networks (ANN) to detect phishing attacks, significantly improving detection performance compared to traditional methods.	It underscores the urgent need for improved phishing detection methods, given the persistent vulnerabilities in email systems.

IV. Conclusion

AI-based phishing detection using machine learning (ML) is becoming an essential tool in combating cyber threats. Phishing attacks, which trick individuals into revealing sensitive information like passwords, credit card numbers, or personal details, are constantly evolving, rendering traditional rule-based or blacklist methods less effective. ML algorithms can tackle this issue by analyzing large datasets, identifying patterns, and spotting anomalies that indicate phishing attempts. These algorithms can be utilized across various domains, including website detection (by examining URLs, domain names, and web content), email phishing detection (by scrutinizing email metadata, text, and sender behavior), and even social media phishing (by recognizing suspicious interactions and profiles). Techniques in machine learning, such as decision trees, support vector machines, random forests, and deep learning, have demonstrated superior performance compared to traditional methods in terms of accuracy, scalability, and adaptability to new phishing tactics. AI models can identify phishing attempts in real time and adjust as phishing strategies change, making them more resilient against the latest threats. However, challenges persist, such as managing large data volumes, reducing false positives, and ensuring the models are applicable across various platforms and types of phishing. Despite these hurdles, the integration of AI and ML in phishing detection systems provides a more proactive, efficient, and automated way to safeguard users and organizations from increasingly sophisticated and targeted phishing attacks.

References

1. Tang, L., & Mahmoud, Q. H. (2021). A survey of machine learning-based solutions for phishing website detection. Machine Learning and Knowledge Extraction, 3(3), 672-694.
2. Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommunication Systems, 76, 139-154.
3. R. Zieni, L. Massari and M. C. Calzarossa, "Phishing or Not Phishing? A Survey on the Detection of Phishing Websites," in IEEE Access, vol. 11, pp. 18499-18519, 2023, doi: 10.1109/ACCESS.2023.3247135.
4. Zamir, A., Khan, H. U., Iqbal, T., Yousaf, N., Aslam, F., Anjum, A., & Hamdani, M. (2020). Phishing web site detection using diverse machine learning algorithms. The Electronic Library, 38(1), 65-80.
5. Korkmaz, M., Sahingoz, O. K., & Diri, B. (2020, July). Detection of phishing websites by using machine learning-based URL analysis. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-7). IEEE.
6. Eze, C. S., & Shamir, L. (2024). Analysis and prevention of AI-based phishing email attacks. Electronics, 13(10), 1839.
7. Safi, A., & Singh, S. (2023). A systematic literature review on phishing website detection techniques. Journal of King Saud University-Computer and Information Sciences, 35(2), 590-611.
8. Nahmias, D., Engelberg, G., Klein, D., & Shabtai, A. (2024). Prompted contextual vectors for spear-phishing detection. arXiv preprint arXiv:2402.08309.
9. Alsariera, Y. A., Adeyemo, V. E., Balogun, A. O., & Alazzawi, A. K. (2020). Ai meta-learners and extra-trees algorithm for the detection of phishing websites. IEEE access, 8, 142532-142542.
10. Shahzad, T., & Aman, K. (2024). Unveiling the Efficacy of AI-based Algorithms in Phishing Attack Detection. Journal of Informatics and Web Engineering, 3(2), 116-133.
11. Arun, A., & Abosata, N. (2024). Next Generation of Phishing Attacks using AI powered Browsers. arXiv preprint arXiv:2406.12547.
12. Elgharbi, S. E., Yahia, M. A., & Ouchani, S. (2024, June). Online Phishing Detection: A Heuristic-Based Machine Learning Framework. In 2024 13th Mediterranean Conference on Embedded Computing (MECO) (pp. 1-4). IEEE.
13. Loh, P. K., Lee, A. Z., & Balachandran, V. (2024). Towards a Hybrid Security Framework for Phishing Awareness Education and Defense. Future Internet, 16(3), 86.
14. Dutta, A. K. (2021). Detecting phishing websites using machine learning technique. PloS one, 16(10), e0258361.
15. Salahdine, F., El Mrabet, Z., & Kaabouch, N. (2021, December). Phishing attacks detection a machine learning-based approach. In 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 0250-0255). IEEE.

How to cite this article?

Ravulapelly, S., Gayathri, P., Farooq, Z., & Priya, T. C. S. (2024). ML-Based Phishing Detection: The key to protecting your data. *International Journal of Advance Research in Computer Science and Management Studies, 12*(11), 9–17. https://doi.org/10.61161/ijarcsms.v12i11.2