# EVALUATING MACHINE LEARNING APPROACHESFOR PHISHING WEBSITE DETECTION

**[1]MOHAMMAD ALANAZI, [2]FUHIDALANAZI**

College of Computer and Information SciencesFaculty of Computer and Information Systems
Imam Mohammad Ibn Saud Islamic University Islamic University of Madinah
Riyadh, Saudi ArabiaMadinah 42351, Saudi Arabia
E-mail: [1]alanazi@gmail.com

**Abstract -** Phishing is a deceptive and fraudulent attack where spammers and malicious actors impersonate trusted and legitimate sources to trick internet users into revealing their personal information, such as bank details, passwords, usernames, and credit card information. These attackers often send emails with malicious links, text messages, and even make phone calls to steal valuable data. Despite various solutions being proposed and implemented to protect online users from these scams, many unsuspecting individuals still fall victim to these tactics.
This study aims to evaluate the effectiveness of prominent Machine Learning (ML) algorithms in detecting and classifying websites as either phishing or legitimate based on structural attributes extracted from their URLs. The research includes two ML algorithms: Support Vector Classifier (SVC) and Logistic Regression along with two ensemble techniques: Random Forest Classifier (RFC) and Gradient Boosting Classifier (GBC).

**Keywords** - Machine Learning, Phishing, SVC, RFC, GBC.

## I. PROBLEM STATEMENT

To ensure the protection of personal and organizational information, it is crucial to detect phishing websites, preventing them from ensnaring unsuspecting internet users into revealing their sensitive data. Traditional methods for identifying phishing sites primarily rely on heuristic approaches and blacklists of known malicious websites (Alrefaai, 2019). A significant drawback of these methods is the latency between the creation of a new phishing site and its classification as malicious after being reported.

During this lag, internet users remain vulnerable to these phishing threats (Nagunwa, 2022).
To counteract the attempts of malicious actors to steal valuable information from individuals and organizations, several innovative technologies have emerged. Among these, machine learning (ML) has become one of the most powerful tools for developing robust and versatile artificial intelligence (AI)-based anti-phishing software (Wang, 2021; Balogun, 2021). ML's ability to analyze vast amounts of data and extract meaningful insights allows it to examine website content, URLs, and previously blacklisted phishing sites, enabling the system to identify patterns indicative of potential phishing attempts, even for newly created websites (Gopalaswamy, 2017).

Supervised ML algorithms can be trained on labeled datasets that contain extensive information about both phishing and legitimate websites. During the training phase, the algorithm learns to recognize the distinguishing features of both categories and can subsequently classify newly created websites as either phishing or legitimate.

## II. OBJECTIVES

This study aims to evaluate the performance of leading machine learning algorithms in classifying and detecting phishing websites by analyzing URL features. The objective is to assess the effectiveness, robustness, and accuracy of these algorithms by considering the structural characteristics of both legitimate and phishing websites. By learning from these features, the study seeks to apply this knowledge to timely detect potential phishing attempts.

The primary focus is on assessing the performance of Logistic Regression, Support Vector Classifier (SVC), Random Forest (RF) classifier, and Gradient Boosting Classifier (GBC) in identifying phishing websites through a detailed examination of their URLs. The algorithms will be evaluated using various performance metrics, including Accuracy, Precision, Recall, F1 Score, and ROC AUC values. These metrics are essential for assessing the effectiveness, specificity, and sensitivity of the machine learning algorithms employed.

This study will also implement several data preprocessing steps essential for improving the performance of machine learning models. These steps include feature engineering, feature selection, and feature scaling.

Feature engineering involves creating appropriate features for the model, while feature selection aims to reduce the dataset's dimensionality. Feature scaling adjusts the values of attributes to a specific range, minimizing the impact of outlier data points and enhancing model effectiveness.

## REFERENCES


[1] S. Alnemari and S, Alshammari, (April 2023)," Detecting Phishing Domains Using ML", Taif University – collage of Computer and Information and technology, https://doi.org/10.3390/app13084649

[2] Alrefaai, S., Özgörmiş, G., & Mohamed, A. (2019, December). A comprehensive Review on phishing website detection using ML and deep learning techniques. International Conference on Artificial Intelligence Systems and ML.

[3] Anderson, H. S., Woodbridge, J., &Filar, B. (2018). DeepDGA: Adversarially-tuned domain generation and detection. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS), 1467-1481. doi:10.1145/3243734.3243768

[4] Balogun, A.O., Akande, N.O., Usman-Hamza, F.E., Adeyemo, V.E., Mabayoje, M.A., Ameen, A.O. (2021). Rotation Forest-Based Logistic Model Tree for Website Phishing Detection. In: Gervasi, O., et al. Computational Science and Its Applications – ICCSA 2021. ICCSA 2021. Lecture Notes in Computer Science, vol 12957. Springer, Cham. https://doi.org/10.1007/978-3-030-87013-3_12

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

[6] Basit, A., Zafar, M. H., Liu, X., Javed, A. R., Jalil, Z., Sultana, S., & Srivastava, G. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommunication Systems, 76(4), 1-22. doi:10.1007/s11235-021-00778-7

[7] Buczak, A. L., &Guven, E. (2016). A survey of data mining and ML methods for cybersecurity intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176. doi:10.1109/COMST.2015.2494502

[8] Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ...&Bengio, Y. (2014). Generative adversarial nets. Advances in Neural Information Processing Systems (NeurIPS), 2672-2680.

[9] Gopalaswamy, M. Shankar, N. & Srinivas agamurthy, N. (2017, December), "Phishing detection using ML: A survey". International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 1025-1030).

[10] Huang, W., & Stokes, J. W. (2016). Mtnet: A multi-task neural network for dynamic malware classification. Proceedings of the 2016 International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA), 399-418. doi:10.1007/978-3-319-40667-1_20

[11] Sarri, A., Paggio, V., &Bafoutsou, G. (2021). CYBERSECURITY FOR SMES–Challenges and Recommendations. European Union Agency for Cybersecurity, ENISA, Heraklion, Greece.

[12] L. Tang and Q H. Mahmoud, 2021, "A Survey of ML-Based Solutions for Phishing Website Detection", DOI: 10.3390/make3030034

[13] Thomas, Nagunwa, (2022), Fast Detection of Zero-Day Phishing Websites Using ML. Doctoral thesis, Birmingham City University. https://www.open-access.bcu.ac.uk/id/eprint/13635

[14] Umbrella, C. (2022). Cybersecurity threat trends-phishing, crypto top the list.

[15] Verma, R., & Hossain, N. (2017). Hybrid phishing attack detection using URL features. Proceedings of the 2017 IEEE International Conference on Privacy, Security and Trust (PST), 199-203. doi:10.1109/PST.2017.00031

[16] Wang, Haonan, c. m. (2021). Phishing detection using ML. (Doctoral Dissertation). Colorado State University. http://hdl.handle.net/10217/234216


★★★