A Real-Time Phishing Detection System: A Web-Based Solution for Enhanced Cybersecurity

Chitturu Sudheer, Sridevi Sakhamuri, Gaadhe Naveen and Sala Vidwath Sai
Department of Electronics and Computer Science, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur District, Andhra Pradesh, India

Keywords: Phishing Detection, Machine Learning, Gradient Boosting Classifier, URL Classification, Cybersecurity.

Abstract: Phishing is a deceptive online scam where attackers trick users by sending fake messages that seem to be from reliable sources. These messages usually contain URLs or attachments intended to steal confidential details or compromise systems with malware upon interaction. While conventional phishing techniques relied on mass spam campaigns targeting a broad audience, modern approaches have become more sophisticated. To combat phishing effectively, machine learning provides a powerful approach by categorizing URLs as either malicious or safe. By examining different URL attributes, algorithms such as SVM, DL architectures like Neural Networks, along with Random Forest and Decision Trees, and XGBoost have been employed in detection systems. This study proposes a gradient boosting classifier-based method for real-time phishing URL detection. The approach leverages distinct URL characteristics to distinguish genuine links from fraudulent ones, demonstrating significant effectiveness in accurately identifying phishing attempts in real-time scenarios.

1 INTRODUCTION

Phishing, which takes use of human weaknesses and deceptive tactics to trick users into disclosing private information like passwords and bank account information, has emerged as one of the most persistent challenges in the realm of cybersecurity. These deceptive schemes often manifest as fraudulent messages, websites, or content that appear authentic, making them hard to detect (S. A. Murad et al. 2023). As the frequency and complexity of phishing attacks continue to rise, enhanced detection mechanisms have become paramount.

The ever-changing tactics used by attackers make it especially difficult to identify phishing websites or URLs. Although somewhat successful, traditional techniques like blacklisting are unable to keep up with the speed at which new dangerous URLs are created. This problem has prompted academics to investigate cutting-edge AI and ML techniques, which provide flexible and scalable answers. (S. A. Murad et al. 2023),(K. Dutta et al. 2021). For instance, models incorporating Recurrent Neural Networks (RNNs) and transformer-based architectures have demonstrated remarkable potential in analyzing large datasets and identifying malicious patterns [(K. Dutta et al. 2021).

Phishing URL detection leverages a variety of approaches, including URL structure analysis, domain reputation checks, and content-based evaluations. These techniques intention to identify anomalies and suspicious traits that distinguish phishing web sites from legitimate ones (J. Misquitta et al. 2023),(R. Mourya et al. 2021). Machine learning plays a crucial role by automating the detection process, using algorithms to learn and recognize patterns indicative of phishing (V. A. Onih et al, 2024).

This study's goal is to provide a machine learning-based algorithm that can recognize phishing URLs with accuracy. By addressing limitations such as false positives and negatives and improving detection efficiency, this research aims to enhance online security and mitigate the impact of phishing attacks on users and organizations.

Sudheer, C., Sakhamuri, S., Naveen, G. and Sai, S. V.
A Real-Time Phishing Detection System: A Web-Based Solution for Enhanced Cybersecurity.
DOI: 10.5220/0013891000004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 3*, pages 19-25
ISBN: 978-989-758-777-1

2 LITERATURE SURVEY

Phishing attacks, which take advantage of users' weaknesses to trick users and steal private data, have become a serious problem in the field of cybersecurity. In response, a great deal of research has been done to create effective detection methods, and machine learning is essential to thwarting these kinds of attacks.

In this section, a selection of research studies that utilize the algorithms mentioned above are reviewed, and their findings are summarized:

Marwa Abd Al Hussein Qasim and Dr. Nahla Abbas Flayh (2025) examined machine learning techniques for phishing website identification. In order to identify phishing websites using characteristics like URL architecture and website content, the study focuses on techniques like Support Vector Machines (SVM), Decision Trees, and Random Forests. In order to improve detection accuracy, the researchers stress the importance of feature selection and dimensionality reduction methods like PCA. They also discuss the importance of dataset preprocessing and performance evaluation metrics. This review underscores the potential of hybrid models in mitigating phishing threats and providing efficient solutions to protect users from cyberattacks.

R. Jayaraj, A. Pushpalatha, K. Sangeetha, T. Kamaleshwar, S. Udhaya Shree, Deepa Damodaran (2023) examined machine learning for phishing website identification. They emphasize the application of Hybrid Ensemble Feature Selection (HEFS), which successfully selects features by combining function perturbation and data perturbation techniques. The study introduces the Cumulative Distribution Function gradient (CDF-g) algorithm to improve feature subset generation and reduce overfitting. The authors emphasize the importance of feature engineering and reducing classifier complexity to enhance phishing detection accuracy. Their findings suggest that hybrid approaches provide robust solutions for phishing threat mitigation.

Machikuri Santoshi Kumari, Chiguru Keerthi Priya, Gondhi Bhavya, Haridas Tota, Monisha Awasthi, Surendra Tripathi (2023) examined machine learning for phishing URL detection. To improve detection accuracy, they suggest a methodology that combines blacklisting and boosting strategies. A sizable dataset of annotated URLs is used to train the method, and metrics like precision, recall, and F1 score are used to assess its effectiveness. The authors emphasize the importance of data collection, URL preprocessing, feature extraction, and blacklisting in the detection system. They suggest future improvements, such as leveraging deep learning and expanded datasets, to enhance the robustness of phishing detection.

Ameya Chawla (2022) examined machine learning for phishing website identification. The study examines typical characteristics of phishing websites and creates a model to identify them. A dataset was used to train a number of classifiers, such as Random Forest, Decision Tree, Logistic Regression, K Nearest Neighbors (KNN), and Artificial Neural Networks (ANN). A Max Vote Classifier that combined Random Forest, ANN, and KNN had the greatest accuracy of 97.73%; Decision Tree and ANN also performed well. A web application that uses the trained model to analyze input URLs and identify phishing websites is one practical way to implement the suggested solution.

Sibel Kapan and Efnan Sora Gunal (2023) reviewed machine learning for phishing attack detection. They created a new phishing dataset, combining Alexa and PhishTank URLs. The study found that URL and HTTP features provided the best performance, with the decision tree classifier achieving an F1-score of 0.99. The paper highlights the significance of feature engineering and classifier choice in enhancing phishing detection.

Arathi Krishna V, Anusree A, Blessy Jose, Ruthika Anilkumar, and Ojus Thomas Lee (2021) reviewed phishing detection models using machine learning-based URL analysis. The performance and accuracy of many machine learning methods used for phishing URL identification are examined in this research. It highlights that Random Forest often outperforms other models but notes that performance varies depending on factors like dataset, train-test split ratio, and feature selection. The authors mention the importance of further research to optimize detection models for accuracy and efficiency.

Jinu Kulkarni and Leonard L. Brown III (2019) examined machine learning for phishing website identification. The study looked at a number of methods for increasing the precision of phishing detection. Neural networks and support vector machines (SVM) were tested on a dataset of 1,353 URLs that were classified as phishing, suspicious, or legitimate. According to their research, these classifiers had an accuracy of over 90%, and features like SSL, web traffic, and URL length were crucial for detection. The authors underlined the necessity to address problems like overfitting in Decision Tree classifiers to increase robustness and the growing significance of machine learning in distinguishing authentic websites from phishing ones.

Keerthana Shankar, U. Rithika, Sathya M., Shishani Chitapur, and Tejaswini J. (2024) looked into phishing website identification using machine learning. Their proposed model utilized the Gradient Boosting Classifier (GBC), leveraging feature sets extracted from phishing and legitimate websites. They emphasized feature engineering, including URL structure, subdomain length, and website attributes, to differentiate phishing sites. The system achieved 97% accuracy and integrated tools like Flask and Fast API for deployment and scalability. The authors highlighted the importance of continuous monitoring and retraining to adapt to evolving phishing tactics.

Sundar et al. (2024) created a phishing detection model using machine learning that extracted features from a dataset of 89 variables and used Lasso regression and recursive feature reduction to choose the best features. The study created a web-based solution for real-time detection and used Random Forest, AdaBoost, Gradient Boosting, and XGBoost to categorize phishing URLs. Their approach focuses on linguistic and URL-based feature analysis, enhancing resilience against adversarial attacks. In contrast, our study, "Real-Time Phishing Detection System: A Web-Based Solution for Enhanced Cybersecurity," improves real-time usability, automating feature selection and leveraging advanced ensemble models for better phishing classification.

Yau and Chia (2024) Using deep learning architectures including Autoencoder, XGBoost, and Random Forest (RF), examined phishing detection by combining list-based and ensemble learning techniques for two-tier security. Using the wrapper technique for feature selection, they discovered that Random Forest performed exceptionally well in managing complex data and class imbalances, achieving 97.03% accuracy. Their work highlights the need for model adaptation and the role of ensemble techniques for robustness. In comparison, our study, "Real-Time Phishing Detection System: A Web-Based Solution for Enhanced Cybersecurity," expands on real-time detection and usability, leveraging advanced ensemble models and web-based implementation for enhanced phishing prevention.

3 METHODOLOGY

By discovering trends in data, machine learning has proven to be useful in spotting phishing websites. This methodology employs supervised learning techniques, leveraging a dataset of website features to classify websites as phishing or legitimate.

3.1 Data Description

The dataset consists of 11,054 samples with 30 features extracted from website URLs. These features include structural properties, domain-based information, and behavioral patterns. The target variable classifies each website as:

- "1" for phishing websites.
- "-1" for legitimate websites.

3.2 Feature Engineering

The development of a strong machine learning framework for identifying phishing websites heavily relies on feature engineering. It entails selecting, extracting, and refining features that encapsulate the core attributes of phishing websites. In this study, we emphasize three main categories of features: URL-based, Page-based, and Domain-based. These characteristics help distinguish genuine websites from phishing ones by capturing important behavioral patterns and oddities. (V. Shahrivari et al. 2020). Figure 1 Shows the Flow Diagram of Phishing Detection System.

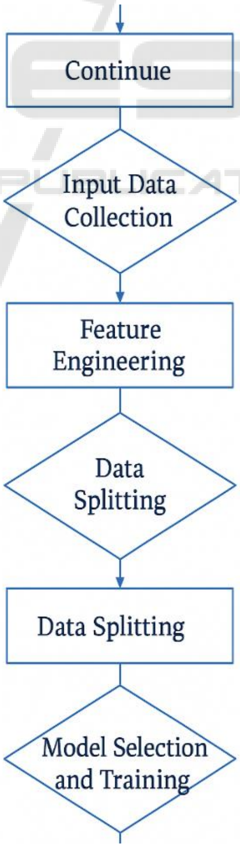

Figure 1: Flow Diagram of Phishing Detection System.

3.2.1 URL: Based Features

Phishing URLs often exhibit anomalies like longer lengths, special characters, and multiple subdomains to mimic legitimate sites. Additionally, they frequently use obscure TLDs or embed IP addresses in URLs to deceive users.

3.2.2 Page: Based Features

Phishing pages mimic legitimate websites but often lack valid SSL certificates or host mismatched favicons. They also redirect links to unexpected domains and include suspicious content such as pop-ups and excessive advertisements.

3.2.3 Domain: Based Features

Phishing domains are often newly registered, lack complete WHOIS information, or use free hosting services Legitimate domains can be distinguished from one another thanks to their extensive DNS records and greater popularity.

3.2.4 Selection of Features

We used the following methods to decrease dimensionality and increase model efficiency:

- **Correlation Analysis**: Features with high correlation (>0.8> 0.8>0.8) were identified and removed to avoid redundancy.
- **Mutual Information:** Assesses the relationship between features and the dependent variable. Features with insignificant mutual information were discarded.
- **Recursive Feature Elimination (RFE):** Gradually removes less important features based on their influence on model accuracy.

3.3 Algorithms Used

Advanced machine learning algorithms are used in phishing detection to recognize and categorize fraudulent websites. Important methods include Logistic Regression (LR) for statistical analysis, Support Vector Machines (SVM) for decision boundary creation, and Random Forest (RF) for improving prediction accuracy. Additionally, Gradient Boosting techniques such as XGBoost incrementally reduce errors, while neural networks uncover intricate relationships within data. Probabilistic methods like Naïve Bayes (NB) further enhance classification by utilizing prior knowledge. These approaches collectively strengthen phishing mitigation efforts.

3.3.1 Logistic Regression (LR)

- A probabilistic model that predicts the likelihood of a website being phishing:

$$P(y=1|X)=\frac{1}{1+e^{-(\beta 0+\beta 1X1+\beta 2X2+\cdots+\beta nXn)}} \quad (1)$$

- **Objective:** Minimize the logistic loss function to determine the optimal weights β.

3.3.2 Support Vector Machines (SVM)

- A discriminative classifier that separates data using a hyperplane:

$$f(x)=sign(w\cdot x+b) \qquad (2)$$

- **Kernel Trick:** Maps data into higher dimensions for non-linear classification.

3.3.3 Decision Tree (DT)

A rule-based model that splits the data into homogenous subsets:

- **Splitting Criterion:** Gini Index or Entropy
- Formula for Gini Index:

$$G=1-\sum_{i=1}^{n}{p_i}^2 \qquad (3)$$

3.3.4 Random Forest (RF)

Using a group of decision trees to increase resilience:

- Combines predictions from multiple trees using majority voting.
- Reduces overfitting compared to a single decision tree (Ali, W. (2017).

3.3.5 Gradient Boosting (e.g., XGBoost)

An iterative algorithm that optimizes weak learners (trees) by minimizing a loss function:

$$F_{m+1}(x)=F_m(x)+\gamma h_m(x) \quad (4)$$

3.3.6 k-Nearest Neighbors (k-NN)

A distance-based algorithm:

- Predicts the class based on majority voting among k-nearest neighbors.
- **Common distance metric:** Euclidean Distance.

3.4 Model Evaluation

Performance metrics used to evaluate models:

- Accuracy:

$$Accuracy = \frac{TP+TN}{TP+FP+FN+TN} \quad (5)$$

- **Precision:** Measures true positives among predicted positives.
- **Recall (Sensitivity):** Measures true positives among actual positives.
- **F1 Score:** precision and recall harmonic mean.
- **ROC-AUC:** Assesses model discrimination.

3.5 Comparison of Results

The performance of various machine learning models in phishing website identification is thoroughly examined in this section. Important performance metrics, such as accuracy, F1 score, recall, and precision, are used to evaluate these models.

Finding the most efficient model for spotting phishing websites is the main goal. Table 1 Shows the Evaluation Metrics.

The following steps are employed to compare model performance:

- Dividing the dataset into training (80%) and testing (20%) subsets.
- Hyperparameter tuning using Grid Search or Random Search.
- Evaluating on the test set using the above metrics.
- Selecting the best-performing model based on F1 Score and AUC-ROC.

Table 1: Evaluation Metrics.

S. No	ML Model	Accuracy	F1 Score	Recall	Precision
1	Gradient Boosting Classifier	0.974	0.974	0.988	0.989
2	CatBoost Classifier	0.972	0.972	0.990	0.991
3	Random Forest	0.967	0.971	0.993	0.990
4	Support Vector Machine	0.964	0.968	0.980	0.965
5	Multi-layer Perceptron	0.963	0.963	0.984	0.984
6	Decision Tree	0.962	0.966	0.991	0.993
7	K-Nearest Neighbors	0.956	0.961	0.991	0.989
8	Logistic Regression	0.934	0.941	0.943	0.927
9	Naive Bayes Classifier	0.605	0.454	0.292	0.997

3.5.1 Best Model

The Gradient Boosting Classifier emerged as the best-performing model, achieving the highest accuracy (97.4%) and F1 score (97.4%). It also demonstrated a strong balance between recall (98.8%) and precision (98.9%), making it the most effective model for detecting phishing websites.

3.5.2 Confusion Matrix

An important tool for determining how well a categorization model works is the confusion matrix. It displays counts of cases that were properly and erroneously classified, including true positives, true negatives, false positives, and false negatives, in order to visually depict the model's predictions.

This Table 2 is the Gradient Boosting Classifier's confusion matrix:

Table 2: Confusion Matrix.

Actual \ Predicted	Phishing (Positive)	Non-Phishing (Negative)
Phishing (Positive)	True Positives (TP)	False Negatives (FN)
Non-Phishing (Negative)	False Positives (FP)	True Negatives (TN)

- **True Positives (TP):** The count of phishing websites correctly identified as phishing.
- **False Negatives (FN):** The count of phishing websites incorrectly classified as non-phishing.

- **False Positives (FP):** The count of non-phishing websites incorrectly classified as phishing.
- **True Negatives (TN):** The count of non-phishing websites correctly identified as non-phishing. Confusion Matrix Shown in Figure 2.

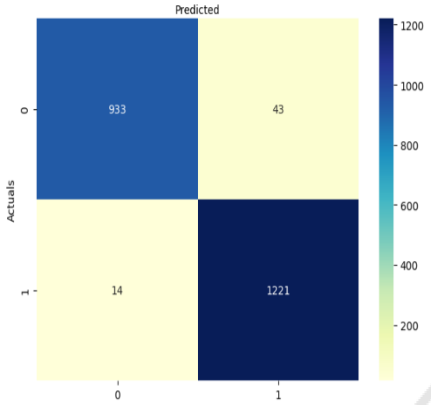

Figure 2: Confusion Matrix.

The Gradient Boosting Classifier demonstrated its efficacy in differentiating between phishing and authentic websites by achieving a noteworthy number of true positives and true negatives. The occurrence of FP and FN was minimal, highlighting the model's capacity to reduce errors.

The proposed approach seamlessly integrates feature engineering with ML architectures to enhance phishing website detection. By analyzing multiple algorithms, we ensure better classification performance, strengthening efforts to combat phishing attacks.

4 RESULTS

The goal of the phishing website detection study was to assess how well various machine learning architectures could detect fraudulent websites using a dataset of 11,054 samples with 30 features. With the highest accuracy of 97.4% and an F1 score of 97.4%, the results showed that ensemble approaches in particular, the Gradient Boosting Classifier performed better than other models. This model performed exceptionally well in maintaining minimum FP and FN by striking a balance between recall (98.8%) and precision (98.9%).

With accuracies of 96.7% and 97.2%, respectively, other models like Random Forest and CatBoost also performed well, but more straightforward models like Logistic Regression and k-Nearest Neighbors produced results that were mediocre. Despite having a high precision (99.7%), Naive Bayes fared poorly, with a correctness of 60.5%. This was mainly because it was unable to detect phishing websites with perfect accuracy (low recall of 29.2%). The Gradient Boosting Classifier's confusion matrix demonstrated a high proportion of true positives and true negatives with little misclassifications, further confirming the model's resilience.

The experiment demonstrated the value of feature engineering and exploratory data analysis (EDA) in enhancing detection accuracy, in addition to model performance. Features such as "HTTPS," "Anchor URL," and "Website Traffic" were identified as key contributors in differentiating phishing sites from legitimate ones.

Correlation analysis and visualizations provided deeper insights into feature relationships and their impact on model performance. Overall, the study highlights the value of machine learning in combating phishing attacks, with ensemble methods like as Gradient Boosting showing itself to be the most effective approach. To further increase accuracy and adaptability, future research could concentrate on real-time detection systems, more feature integration, and the use of deep learning models.

5 CONCLUSIONS

In this study, a Gradient Boosting Classifier has been proposed for a highly effective real-time phishing detection, showing the best accuracy level of 97.4% and high F1 scores. Integration of URL along with page-based and domain-based features significantly improves the model in distinguishing between phishing and legitimate sites. Ensemble models outperformed traditional methods in phishing detection tasks, as confirmed from comparative analysis. Feature Engineering and Dimensional Reduction were critical to enhancing classification speed. In conclusion, the proposed framework contains automated and scalable web solution for mitigating cyber threats from phishing attacks.

REFERENCES

A. K. Dutta, "Detecting phishing websites using machine learning technique," PLoS One, vol. 16, no. 10, p. e0258361, Oct. 2021. DOI:10.1371/journal.pone.0258361. PMCID: PMC8504731, PMID: 34634081.

A. Krishna V, A. A, B. Jose, K. Anilkumar, and O. T. Lee, "Phishing detection using machine learning based URL analysis: A survey," IJERT, vol. 9, no. 13, Paper ID: IJERTCONV9IS13033, Aug. 2021.

A. Chawla, "Phishing website analysis and detection using Machine Learning," Int. J. Inf. Syst. Appl. Eng., vol. 2022, pp. 1-10, 2022, doi: 10.18201/ijisae.2022.262.

Ali, W. (2017). Phishing website detection based on supervised machine learning with wrapper features selection. International Journal of Advanced Computer Science and Applications (IJACSA), 8(9)

Arun Kulkarni and Leonard L. Brown III, "Phishing Websites Detection using Machine Learning," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 10, no. 7, pp. 1-7, 2019, doi: 10.14569/IJACSA.2019.0100702.

J. Misquitta and A. K., "A Comparative Study of Malicious URL Detection: Regular Expression Analysis, Machine Learning, and VirusTotal API," Research Article, Dec. 2023. DOI: 10.21203/rs.3.rs-3685949/v1.

Keerthana Shankar, K., Rithika, U., Sathya, M., Chitapur, V., and Tejaswini, J., "Detection of Phishing Website using Machine Learning," TIJER - International Research Journal, vol. 11, no. 5, May 2024, pp. b651. ISSN 2349-9249.

M. Santoshi Kumari, C. Keerthi Priya, G. Bhavya, H. Neha, M. Awasthi, and S. Tripathi, "Viable detection of URL phishing using machine learning approach," E3S Web of Conferences, vol. 430, p. 01037, 2023, doi: 10.1051/e3sconf/202343001037.

M. A. A. H. Qasim and N. A. Flayh, "Phishing Website Detection Using Machine Learning: A Review," Wasit Journal for Pure Sciences, vol. 2, no. 2, p. 270, 2025.

R. Jayaraj, A. Pushpalatha, K. Sangeetha, T. Kamaleshwar, S. Udhaya Shree, and D. Damodaran, "Phishing website detection using novel machine learning fusion approach," Measurement, vol. 203, p. 101003, 2023, doi: 10.1016/j.measen.2023.101003.

R. Mourya, A. R. Khan, P. Jain, and S. K. Singh, "Phishing URL Detection Using Machine Learning," IRE Journals, vol. 7, no. 8, pp. 198-202, Feb. 2024. DOI: 1705486.

S. Kapan and E. S. Gunal, "Improved phishing attack detection with machine learning: A comprehensive evaluation of classifiers and features," Appl. Sci., vol. 13, no. 24, p. 13269, Dec. 2023, doi: 10.3390/app132413269.

S. A. Murad, N. Rahimi, and A. J. M. Muzahid, "PhishGuard: Machine Learning-Powered Phishing URL Detection," in Proceedings of the IEEE International Conference on Computing Sciences & Computer Engineering (CSCE), Hattiesburg, MS, USA, 2023, pp. 371 375. DOI:10.1109/CSCE60160.2 023.00371.

Sudar, K.M., Rohan, M. & Vignesh, K. Detection of adversarial phishing attack using machine learning techniques. Sādhanā 49, 232 (2024). https://doi.org/10 .1007/s12046-024-02582-0

V. Shahrivari, M. M. Darabi, and M. Izadi, "Phishing Detection Using Machine Learning Techniques," arXiv preprint arXiv:2009.11116, Sep. 2020.

V. A. Onih, "Phishing Detection Using Machine Learning: A Model Development and Integration," International Journal of Scientific and Management Research, vol. 7, no. 4, pp. 1-10, 2024.

Yau, J.X., Chia, K.L. (2024). Machine Learning-Based Phishing Website Detection: A Comparative Analysis and Web Application Development. In: Ghazali, R., Nawi, N.M., Deris, M.M., Abawajy, J.H., Arbaiy, N. (eds) Recent Advances on Soft Computing and Data Mining. SCDM 2024. Lecture Notes in Networks and Systems, vol 1078. Springer, Cham.https://doi.org/10. 1007/978-3-031-66965-1_18