Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 47 No. 01 (2026)

Phishing URL Detection Using Machine Learning

[1]Nilendher Dumpala, [2]Aswani S, [3]Sai Puneeth Chalapati, [4]Nithya Donoor

[1]Student Dept of CSE (AI & ML)

Institute of Aeronautical Engineering, Hyderabad, India

23955a6610@iare.ac.in

[2]Asst. Professor Dept of CSE (AI & ML)

Institute of Aeronautical Engineering,Hyderabad, India

s.aswani@iare.ac.in

[3]StudentDept of CSE (AI & ML)

Institute of Aeronautical Engineering,Hyderabad, India

22951a66a6@iare.ac.in

[4]Student Dept of CSE (AI & ML)

Institute of Aeronautical Engineering, Hyderabad, India

22951A6680@iare.ac.in

Abstract—Phishing attacks are one of the most significant cybersecurity risks in the online era because they may deceive users into providing sensitive data via fraud websites, which mimic reliable sources. The rule-based and blacklist-based methods of detection are usually ineffective at detecting new phishing URLs because these methods are static. To overcome this constraint, this paper proposes a machine learning model of phishing URL recognizer with real-time detection. The system proposed here will use a trained supervised Gradient Boosting Classifier to run on a labeled body of URLs. The feature extraction is done exhaustively to examine lexical, domain based, and webpage characteristics such as URL length, use of special characters, use of HTTPS, presence of IP address, age of the domain, redirection, and HTML based features. Depending on these characteristics, the model labels URLs as a legitimate or phishing one and produces a threat score that is based on confidence. The system is implemented on a web-based interface that displays risk levels in a visual manner and shows the features presented in explanations to make it more transparent and comprehensible to the user. Experimental analysis proves that the proposed system has a high detection rate, which proves its efficiency as a practically applicable, explainable, and deployable phishing URL detection system.

Keywords—Phishing Detection, URL Classification, Machine Learning, Web Security, Cybersecurity, Random Forest, XGBoost

I. INTRODUCTION

The fast growth of internet based services has altered the mode through which the users diagnose, communicate and transact business online. Cyber threats have also become more widespread alongside such developments, and one of the most widespread and harmful types of cybercrime are phishing attacks. The phishing attacks in most cases are entailed by the use of rogue websites that mimic the authentic sites to defraud the website user into giving up sensitive information like passwords and personal details. The phishing URLs are hard to identify through manual inspection and the old security mechanisms due to their corruptive nature and constant alteration.

The traditional methods of phishing detection such as rule-based heuristics and blacklist filtering have inherent shortcomings. The heuristics are based on pre-defined patterns which are mostly hard and may give false positives whereas the blacklist techniques are responsive and useless with newly generated phishing addresses. Consequently, these solutions cannot offer efficient real-time security on dynamic web-based scenarios.

In order to solve these issues, this paper suggests a phishing URL detector system built on machine learning that conducts feature-based analysis on URLs. The system uses a Gradient Boosting Classifier with a labeled set of data and makes use of a complete range of lexical, domain-based, and webpage-related features to recognize phishing attributes. The trained model is provided as a web-based application that can analyze URLs in real-time and provide threat scores based on confidence as well as feature-level explanation. With proper classification, interpretability, and realistic implementation, the suggested system provides a feasible solution to real-time phishing URLs detection.

II. Literature Survey

Phishing URL detection has been a subject of intense research due to the fact that the level of cyberattack on unsuspecting users has been on the increase. Many machine learning and deep-learning methods are considered in the recent works to improve the accuracy of detection and flexibility. A web-based phishing URL detector with a deep learning-based optimization showed better performance in classification, but with a higher computing cost than Barik et al. [1]. Kailas and Roopalakshmi introduced a systematic review in malicious URL detection strategies, which managed to determine the gaps in research of scalability and real-time deployment [2].

A number of authors have paid attention to deep learning models with sequences. Jishnu and Arthi used a BiLSTM model with attention mechanism to obtain the contextual dependencies of URLs and the accuracy of detection was high with added complexity due to the model [3]. Equally, Zhou et al suggested a unified CSPPC and BiLSTM model that can learn complex URL patterns but with a high training cost [4]. Transformer-based methods, too, have come into the spotlight; Altan et al. have been using NLP transformers in conjunction with structural URL analysis to better detect phishing, yet there is still an issue of feasibility on a deployment-level [5].

Ensemble learning has been investigated in order to trade between accuracy and robustness. Dubey et al. used characters-level CNNs with feature engineering to enhance generalization with various kinds of phishing attacks [6]. In phishing detection, feature-based research has demonstrated the significance of domain and lexical features, which include signs of brand impersonation [8]. It has also been supported by the fact that efficient feature selection algorithms such as rough set based hybrid algorithms have enhanced the efficiency of the classification process since they do away with redundant features [9].

Comprehensively, the current literature shows that sophisticated model-based phishing detection strategies could be effective, yet, the issues of interpretability, performance cost, and real-time implementation remain the driving factor behind the creation of lightweight and feature based solutions.

III. METHODOLOGY

A. System Overview

The suggested system adopts a machine learning model of real-time phishing URL detection. The algorithm is structured as a set of modules, which process a URL that has been inputted by the user, extracts features that are discriminative, uses supervised classification, and provides an interpretable prediction via the web interface. The system is also feature-driven, which is why the feature-based analysis and ensemble learning are used to detect the presence of phishing behavior in unfamiliar URLs, unlike the blacklist-based devices. There are dataset preparation, feature extraction, real-time inference, model training, and deployment as the methodology.

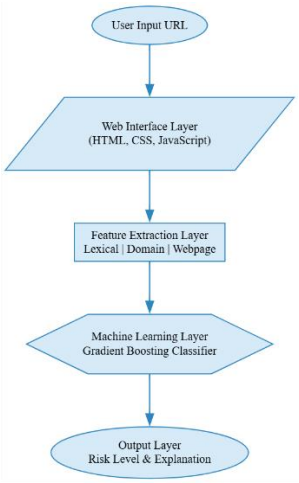
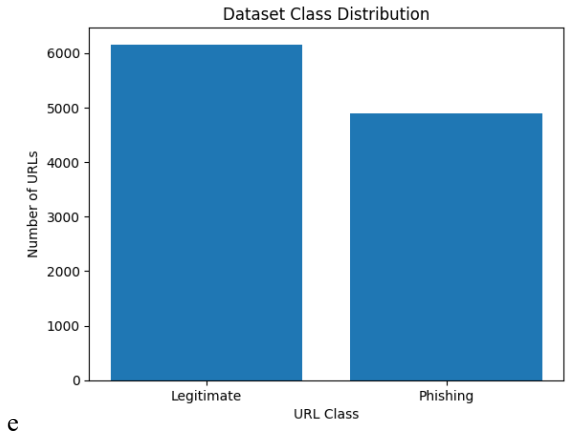


Fig. 1. Layered architecture of the proposed phishing URL detection system.



e

Fig. 2. Distribution of legitimate and phishing URLs in the dataset.

B. Dataset Preparation

The data used in this study is given in structured CSV format which has labeled samples of URLs. The entries are represented by a URL instance and a class label which is legitimate or phishing. The fields that are not essential like index identifiers are deleted before the training to avoid bias. The other attributes are classified into the input features and the target labels.

The dataset is also divided into training and testing subsets in the ratio of 80 to 20 in order to assess the generalization of the model. This is to ensure that the classifier is trained to most of the data and is tested on unknown samples. There is no synthetic oversampling or data generation, and the original data distribution is kept, and experiment integrity is not compromised.

Table I. Distribution of Legitimate and Phishing URLs in the Dataset

Class Label	Description	Number of URLs
1	Legitimate	6,157
-1	Phishing	4,897

Class Label	Description	Number of URLs
Total	—	**11,054**

Table II. Training and Testing Data Split

Dataset Portion	Percentage	Number of Samples
Training Set	80%	8,843
Testing Set	20%	2,211
Total	100%	**11,054**

C. Feature Extraction Strategy.

The main part of the proposed methodology is feature extraction and it is implemented with the help of a special feature extraction module. A minimum of 31 handcrafted features are dynamically obtained on each URL. These characteristics have been divided into lexical, domain-based and webpage-based characteristics.

Lexical characteristics examine the form of the URL text, the length of the URL, the number of subdomains, the occurrence of special characters, the use of URL shortening services, and the usage of IP addresses. Domain-based characteristics include registration and trust indicators like the domain age, WHOIS availability, use of HTTPS, and non-standard port usage. Web page based features are based on the analysis of HTML content of the URL and give indicators like abnormal form actions, redirection of iframes, JavaScript behavior, links to external resources, and the use of popups.

The characteristics are represented by discrete numerical numbers that refer to safe, suspicious, or malicious behaviour. Such a representation allows it to be directly compatible with tree-based classifiers without the need of further normalization or scaling.

D. Construction of Feature Vectors.

After extraction, all feature values are then made to form a fixed length numerical feature vector of a single URL. The resultant data is a feature matrix.

NxF, where

N is the number of URLs and

F is the number of extracted features. This representation form is known to be consistent between training and inference phases, in real-time. The deterministic character of the process of feature extraction provides reproducibility of the process and the predictable model behaviour.

E. Classification Model

Phishing detection task is a binary classification problem which is solved with a Gradient Boosting Classifier. Gradient Boosting is an ensemble method of learning, which builds many decision trees, one after the other, where each successive tree is designed to resolve the error of the previous ones. This method works with structured tabular data and is capable of modeling non-linear relationships between features, which are complicated.

The extracted feature vectors are used to train the classifier with the help of labels. The model is adaptable to real-time applications because of the default hyperparameters that balance the computational efficiency and accuracy.

Gradient Boosting is chosen because it is robust, has good predictive capability and it can handle heterogeneous feature sets.

F. Training and Persistence of Model.

When being trained on the training data, the Gradient Boosting model will acquire discriminative patterns that distinguish phishing URLs and legitimate ones. The test that is held-out is used to test the performance to provide generalization. The model is then stored as a model binary after the training process. This enables the trained model to be loaded at runtime without retraining, which saves a lot of time on inference and allows deployment consistency.

G. Real-Time Detection and Explainability.

To be used in real-time, the trained model is installed in a backend server. Once a user enters a URL, system dynamically parses features and feeds the resultant feature onto the trained classifier. Besides the scheduled label of the class, the model generates probability scores that are transformed into confidence-based risk level.

The system has feature-wise explanations in addition to predictions in order to optimize transparency. All of the features are assigned a human readable description and classified as a safe, warning, or dangerous element depending on its value. This explainability mechanism makes the users aware of the reasons why a URL has been flagged and enhances trust of automated decisions.

H. Deployment Architecture

The entire system is implemented in the form of a web-based application that is available in a client-server architecture. The backend deals with feature extraction, model inference, and response generation and the frontend is an interactive service whereby the URL can be submitted, the result visualized and the history tracked. The implementation is practical with low latency phishing detection and user-friendly interaction shown by the deployment that allows real-time detection of phishing.

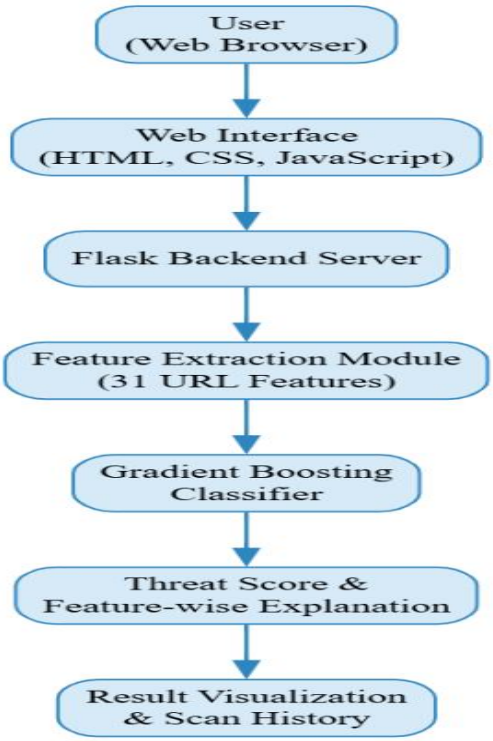


Fig. 3. Overall architecture of the proposed phishing URL detection system.

IV. Results and Discussions

This part gives the results of the experiment performed with the proposed phishing URL detection system and explains its implications in the context of accuracy, reliability, interpretability, and operational implementation. The analysis is devoted to the performance of the Gradient Boosting-based classifier in the context of feature-based URL analysis and its appropriateness to the use in the real-time environment.

A. Classification Performance.

Gradient Boosting Classifier with trained data was found to work well in the identification of phishing and legitimate URLs. The model was found to have a high classification rate in the test samples and this is an indication of the model that generalizes well to previously unknown samples of URLs. Precision and recall values also indicate the usefulness of the system in detecting malicious URLs with a minimum of false alarms. Phishing detection is the field where high recall is very significant since any mistake in recognizing a malicious URL can be disastrous in terms of security. Meanwhile, keeping the good precision means that the authentic websites must not be mistakenly marked as such, and this will keep the users trusting the system.

According to the confusion matrix analysis, there is a balanced distribution of true positives and true negatives with the relatively low misclassification rates. This finding indicates that the identified feature set, when used with the Gradient Boosting learning strategy, is efficient in identifying a distinguishing pattern related to phishing behavior. This is because classifier is an ensemble type of classifier, which enables it to deal with non-linearities in the relationship between features; hence its strong performance.

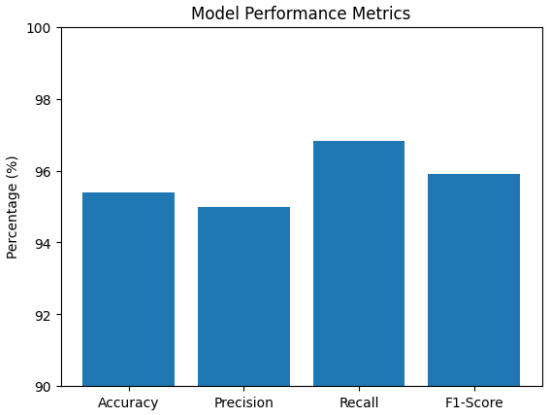


Fig. 4. Performance metrics of the Gradient Boosting classifier.

Table III. Performance Metrics of the Gradient Boosting Classifier

Metric	Value (%)
Accuracy	95.39
Precision	94.98
Recall	96.83
F1-Score	95.90

B. Effect of Feature Engineering.

Just like the success of the proposed system, the central role is played by feature engineering. The lexical, domain-based, and webpage-related feature allow the model to examine the URLs in several different ways overall, as opposed to using a single indicator only. Such characteristics as the length of the URLs as well as the availability of the IP addresses, redirection abnormality, the use of the HTTPS protocol, age of the domain were discovered to have a specific power in the detection of the phishing activities.

The system does not require sophisticated preprocessing or normalization since it can use discrete values to encode features, representing safe, suspicious or malicious behavior. It is a design option that is easier to train and infer, as well as, maintain interpretability. The findings suggest that handcrafted features when chosen and properly applied can reach high detection accuracy without the need of computationally demanding deep learning models.

C. Threat Scoring and Explainability.

In addition to binary classification, the proposed system also produces a confidence-based threat score which is an indication of the probability of a URL being either safe or malicious. This is a probabilistic output which enables the URLs to be classified as safe, warning, or dangerous risks to offer the user more specific feedback than a simple label.

A feature of the system that has been contributing to the same is the mechanism of feature-wise explanation. The system provides information on what features worked in the final decision, and the characteristics are ranked according to the severity of the risk to the final decision in each analyzed URL. Such transparency enhances understanding and trust among the users particularly in cybersecurity applications whereby the user has to make

informed decisions. The explicable output is also useful to developers and security analysts to prove model behavior and finding some areas of weakness.

D. On-Flight Deployment Performance.

The practical applicability of the suggested approach is proved by the fact that the trained model deployed as a web-based application is practical. The feature extraction and classification works dynamically at runtime making it possible to analyse the user-submitted URLs in real time. The latency of inference in the system is low and, therefore, the system is appropriate to be used when there is an interactive scenario.

The web interface is more usable, indicating the severity of threats, showing the explanation of the features, and a history of analyzed URLs in a session. These visual aids enhance the functionality of the users and make them able to use such aids repeatedly without needing to be a technical specialist. The findings suggest that the system manages to fill the gap between academic machine learning models and viable cybersecurity solutions.

E. Discussion and Limitations.

Although the obtained results prove the efficiency of the offered system, some limitations still exist. The model is based on handcrafted features, and might have to be updated with the development of phishing strategies. The system is also a Web-based application and is not integrated with external security infrastructures at the moment. Nevertheless, the obtained findings indicate that a rather lightweight, feature-driven Gradient Boosting model can deliver accurate, interpretable, and deployable phishing URL detection in a practical environment.

Table IV. Confusion Matrix for Phishing URL Classification

Actual \ Predicted	**Legitimate**	**Phishing**
Legitimate	916	63
Phishing	39	1,193

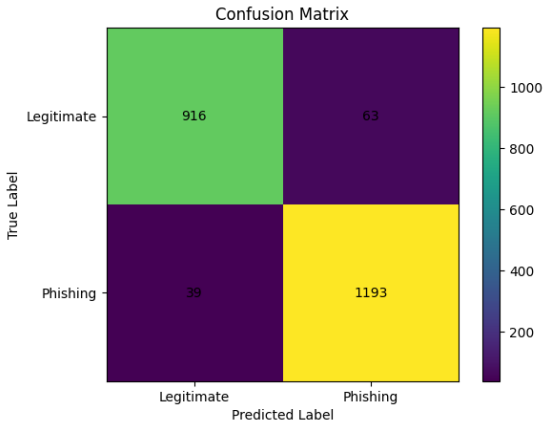


Fig. 5. Confusion Matrix Of The Phishing Url Detection System.

V. CONCLUSION

Phishing is a significant issue in the field of cybersecurity with attackers using fraudulent websites which closely resemble genuine sites to swindle users. A machine learning-based phishing URL detection system introduced in

this paper was intended to be used in the real-time analysis by feature-driven classification. The suggested strategy (that is, Gradient Boosting Classifier) is trained on a set of labeled URLs and makes use of a set of extensive lexical, domain-based, and webpage related information to correctly classify phishing URLs and legitimate ones. The system provides a good detection performance by focusing on handcrafted features and ensemble learning at low computational overhead.

One of the contributions of the work was the implementation of the trained model in a web-based application allowing the real-time evaluation of URLs. Besides the classification outcomes, the system offers confidence-based threat scoring and the ability to explain the features, which enhances the transparency and user confidence. Experimental findings have shown high levels of detection and good generalization to unknown URLs. Future enhancements might involve retraining with new information periodically, refining features and increasing the incorporation of web-based security applications to help it become more adaptable and scalable.

REFERENCES

[1] K. Barik, S. Misra, and R. Mohan, "Web-based phishing URL detection model using deep learning optimization techniques," *International Journal of Data Science and Analytics*, pp. 1–23, 2025.

[2] S. Kailas and R. Roopalakshmi, "'Think Before You Click'—Malicious URL Detection in Cybersecurity: A Systematic Review and Research Roadmap," *IEEE Access*, 2025.

[3] K. S. Jishnu and B. Arthi, "Phishing URL Detection Using BiLSTM With Attention Mechanism," in *Machine Intelligence Applications in Cyber-Risk Management*. IGI Global Scientific Publishing, 2025, pp. 159–184.

[4] J. Zhou *et al.*, "An integrated CSPPC and BiLSTM framework for malicious URL detection," *Scientific Reports*, vol. 15, no. 1, p. 6659, 2025.

[5] I. Altan *et al.*, "Dual-Path Phishing Detection: Integrating Transformer-Based NLP with Structural URL Analysis," *arXiv preprint* arXiv:2509.20972, 2025.

[6] R. Dubey *et al.*, "Phishing Detection System: An Ensemble Approach Using Character-Level CNN and Feature Engineering," *arXiv preprint* arXiv:2512.16717, 2025.

[7] A. K. Pakkir Shah *et al.*, "Statistical analysis of feature-based molecular networking results from non-targeted metabolomics data," *Nature Protocols*, vol. 20, no. 1, pp. 92–162, 2025.

[8] R. Mishra and G. Varshney, "A study of effectiveness of brand domain identification features for phishing detection in 2025," in *Proc. Int. Conf. Applied Cryptography and Network Security*. Springer, 2025, pp. 89–108.

[9] J. H. Setu *et al.*, "RSTHFS: A Rough Set Theory-Based Hybrid Feature Selection Method for Phishing Website Classification," *IEEE Access*, 2025.

[10] K. Zhang *et al.*, "Leveraging machine learning to proactively identify phishing campaigns before they strike," *Journal of Big Data*, vol. 12, no. 1, p. 124, 2025.