PhishCure: AI Powered Phishing Link Detection

Jesy Jeff Laura E[1], Aditi Gupta[2]
[1,2]*Student, Dept. of CSE (IoT & Cyber Security Including Blockchain Technology), Bangalore Institute of Technology, Bengaluru-560004, India*

***Abstract* — Phishing attacks are fraudulent communication techniques used to deceive users into revealing sensitive information by impersonating trusted entities. These attacks are commonly delivered through email and Short Message Service (SMS), leading to identity theft, financial loss, malware infections, and reputational damage. This paper presents PhishCure: Phishing Detection with Artificial Intelligence, a web-based system that leverages machine learning to identify malicious Uniform Resource Locators (URLs). The system is trained on a dataset containing legitimate and confirmed phishing URLs collected from various sources. Important features such as domain characteristics, Internet Protocol (IP) address usage, domain age, security protocol, and structural URL attributes are extracted and analyzed. A Random Forest classifier is employed to evaluate the likelihood of a URL being malicious. Based on the prediction results, the system provides warning alerts for suspicious URLs and trust indicators for legitimate ones. The proposed solution enhances cybersecurity defenses by enabling real-time phishing detection and protecting users from online threats.**

***Index Terms*— Artificial Intelligence, Cybersecurity, Machine Learning, Phishing Detection, Random Forest, URL Analysis.**

I. INTRODUCTION

Phishing has emerged as one of the most dangerous cyber threats in today's digital world. Cybercriminals create misleading websites, fake login pages, and deceptive URLs to obtain confidential information from unsuspecting users. With the rapid expansion of online banking, e-commerce platforms, cloud services, and digital communication systems, phishing attacks have significantly increased in both frequency and sophistication.

Conventional phishing protection mechanisms such as blacklist-based filtering and signature-based detection systems are no longer sufficient.

Attackers continuously generate new phishing domains and exploit URL obfuscation techniques to evade traditional security systems. Since many phishing websites are temporary, they often bypass existing detection solutions. Therefore, intelligent and adaptive systems capable of identifying unseen malicious URLs are required.

To address this issue, PhishCure is proposed as an AI and ML-based solution for real-time phishing detection. The system extracts intrinsic URL characteristics such as length, structure, protocol type, domain age, redirection behaviour, and special character patterns. These features are analysed using machine learning models to classify URLs as legitimate or malicious.

II. LITERATURE REVIEW

Phishing attacks have been one of the most enduring forms of cyber threats, which are mainly driven by the use of deceptive Uniform Resource Locators (URLs) to trick victims into revealing their confidential information.

Conventional blacklisting solutions have been found to be inadequate, as the attackers have been constantly changing the URL patterns to evade detection. This has resulted in the use of Machine Learning (ML) and Deep Learning (DL) techniques, which are adaptive and data-driven.

[1] Phishing URL Detection Using Machine Learning Methods

Shaik et al. propose a machine learning-based framework for detecting phishing URLs using lexical and host-based features [1]. The study evaluates multiple classification algorithms and highlights the effectiveness of feature engineering in improving detection accuracy. Their work demonstrates that ML-based systems outperform traditional blacklist approaches in identifying newly generated phishing URLs.

[2] Phishing Attack Detection Using LightGBM and SVM Algorithm
This study compares Support Vector Machine (SVM) and LightGBM for phishing detection [2]. The results indicate that LightGBM achieves higher accuracy and faster prediction time due to its gradient boosting architecture and optimized histogram-based learning method.

[3] Comparative Study of CatBoost, XGBoost, and LightGBM for Enhanced URL Phishing Detection
The authors present a comparative analysis of advanced boosting algorithms for phishing URL classification [3]. Among the evaluated models, LightGBM demonstrated superior computational efficiency and competitive predictive performance, making it suitable for real-time applications.

[4] Towards Lightweight URL-Based Phishing Detection
This research emphasizes the need for lightweight phishing detection systems capable of operating in resource-constrained environments [4]. The study suggests that optimized feature selection and efficient classifiers significantly reduce memory consumption while maintaining accuracy.

[5] Phishing Detection Using Machine Learning Techniques
This paper explores traditional machine learning techniques such as Decision Tree, Random Forest, and Naive Bayes for phishing detection [5]. The findings confirm that ensemble methods provide better resilience against noisy and imbalanced datasets.

[6] Detection of Phishing Attack Using LightGBM and XGBoost
The study compares gradient boosting frameworks and reports that LightGBM achieves faster inference and lower computational cost while maintaining high detection accuracy [6].

[7] A Novel Phishing Website Detection Model Based on LightGBM and Domain Name Features
Zhou et al. propose a phishing detection model that integrates domain name features with LightGBM classification [7]. Their approach improves detection rates by leveraging structural URL characteristics and domain-related attributes.

[8] Machine Learning Based Phishing Detection from URLs
Sahingoz et al. develop a URL-based phishing detection system using supervised learning techniques [8]. The study demonstrates the importance of lexical feature extraction in improving classification performance.

[9] Phishing Website Detection Using Machine Learning: A Survey
This survey provides a comprehensive overview of phishing detection methods, categorizing them into blacklist-based, heuristic-based, and machine learning-based approaches [9]. The authors conclude that ML techniques offer superior adaptability against evolving phishing tactics.

[10] Improved Phishing Attack Detection with Machine Learning
This work focuses on improving classification performance using feature optimization and ensemble methods [10]. The study reports enhanced precision and recall metrics compared to baseline models.

[11] Detecting Phishing Domains Using Machine Learning
The authors present a domain-focused phishing detection framework [11]. By analyzing domain registration features and structural URL patterns, the model achieves strong detection accuracy.

[12] Phishing Website Detection Using Machine Learning
This study evaluates various classifiers for phishing detection and emphasizes the importance of dataset balance and cross-validation in improving model generalization [12].

The literature highlights the growing adoption of machine learning techniques for phishing URL detection due to their ability to learn complex patterns and adapt to evolving attack strategies. Studies consistently demonstrate that ensemble methods, particularly gradient boosting algorithms such as LightGBM, provide superior accuracy, efficiency, and robustness compared to traditional classifiers. Feature engineering, especially lexical and domain-based attributes, plays a critical role in enhancing detection performance. Furthermore, lightweight and deployable systems are emphasized for real-time cybersecurity applications.

Overall, existing research establishes a strong foundation for applying optimized boosting algorithms and structured feature extraction in phishing detection systems, motivating the development of PhishCure as a scalable and efficient real-time solution.

III. DESIGN AND METHODOLOGY

This section describes the architectural design and methodology of PhishCure, a lightweight and scalable system designed for real-time phishing URL classification. The system has a modular pipeline architecture with five main components: User Interface, Feature Extraction Engine, Machine Learning Classifier, Backend API, and Deployment Server. The system design focuses on efficiency, scalability, security, and easy deployment with accurate classification using the Light Gradient Boosting Machine (LightGBM) model.

1. System Architecture

PhishCure has a sequential processing system architecture that processes a submitted URL by the user to produce a classification output. The system starts with the User Interface (UI), where the user enters a suspected URL.

The URL is sent to the backend server for validation of the URL format before proceeding to feature extraction. The extracted features are sent to the trained LightGBM model for prediction. The prediction output is sent back to the UI for display to the user.

The system architecture is modular, providing flexibility for individual component updates without affecting the system performance. The system architecture is suitable for real-time processing and cloud deployment for worldwide accessibility.

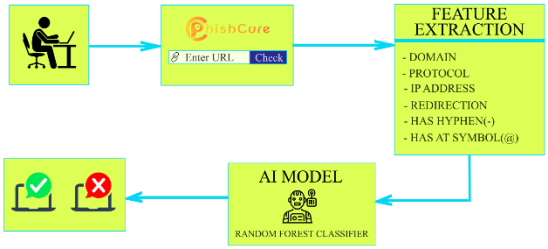

Figure 3.1: System Architecture of PhishCure

2. User Interface

The User Interface is the main interaction point between the user and the system. It is implemented as a responsive web application that enables users to:

- Input a URL for analysis
- Make the request
- Display classification results (Secure/ Phishing)

The interface provides results in the form of textual feedback and color indicators for better usability. The simplified interface makes it accessible to both technical and non-technical users.

3. Feature Extraction Engine

The Feature Extraction Engine is responsible for extracting a set of numerical features from the input URL without actually loading the webpage, making it safe and fast. The extracted features include:

- URL length
- Presence of IP address
- Domain age
- Redirection count
- Special characters (@, -)
- URL depth
- Protocol type (HTTP/HTTPS)

The features are a set of lexical and host-based features that are generally linked to phishing activity. The feature vector is used as input to the classification model.

4. Model Selection

Selecting an appropriate machine learning algorithm is essential for accurate phishing URL detection. Since the problem is binary (phishing = 1, legitimate = 0), classification algorithms were employed to categorize URLs based on extracted features. The following models were evaluated:

- Random Forest: An ensemble of decision trees that improves accuracy and reduces overfitting.
- Decision Tree: An interpretable tree-based model suitable for structured data.
- Support Vector Machine (SVM): Identifies an optimal separating hyperplane and handles high-dimensional data effectively.
- Naive Bayes: A probabilistic classifier that is computationally efficient and suitable for feature-based classification.
- Gradient Boosting: A sequential ensemble method capable of modeling complex feature interactions with high accuracy.

These algorithms were selected due to their complementary strengths in interpretability, robustness, and predictive performance. Comparative evaluation enabled identification of the most suitable classifier for phishing URL detection.

ML_Models	Accuracy
RandomForestClassifier	86
DecisionTreeClassifier	83.8
SupportVectorClassifier	83.7
GradientBoostingClassifier	83.7
NaiveBayesClassifier	83.5

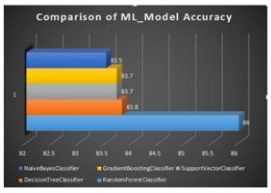

Figure 3.2: Model Comparison Table and Graph of PhishCure

5. Model Training

The classification component uses LightGBM, a gradient boosting library that is renowned for its high accuracy and efficiency. LightGBM uses leaf-wise tree growth and histogram-based optimization to achieve faster training and prediction. Several algorithms were tested during the experiment, but LightGBM was chosen because of the following reasons:

- High accuracy of classification
- Fast prediction speed
- Low memory usage
- Scalability for cloud computing

The classifier makes a binary prediction:

- 0 – Genuine
- 1 – Phishing

This allows for instantaneous detection of threats, including unknown malicious URLs.

6. Backend API

The Backend Application Programming Interface (API) is responsible for communication between the user interface and the machine learning model. The API performs the following tasks:

- Input URL validation
- Activation of feature extraction
- Transmission of features to the classifier
- Formatting of prediction results

The modular design of the backend API ensures efficient handling of multiple concurrent requests and system stability.

7. Deployment Server

PhishCure is implemented on a cloud-based server infrastructure, which provides for continuous availability and scalability. The server supports:

- The trained LightGBM model
- Backend logic
- Full web interface

Cloud deployment provides for improved availability, remote accessibility, and real-time processing capabilities without the need for local infrastructure.

8. Use Case Overview

The interaction with the system is simple and user-friendly. The main actor in the system is the User, who follows the following sequence of actions:

- Enter URL
- Submit request
- Get prediction result

The system checks the URL, identifies the relevant features, and applies them to the ML model for classification result display.

IV. RESULTS AND PERFORMANCE EVALUATION

1. Model Testing and Evaluation

Model testing was conducted to check the generalization ability of the trained LightGBM classifier. As phishing patterns keep changing, the model was tested on new datasets to check its predictability.

- Evaluation Metrics

Various evaluation metrics were employed to ensure a complete analysis of the LightGBM classifier's performance:

→ Accuracy: It measures the overall correctness of the classification.
→ Precision: It measures the number of correctly classified phishing URLs.
→ Recall: It measures the proportion of correctly identified phishing URLs.
→ F1-Score: It is the harmonic mean of precision and recall, which is ideal for imbalanced datasets.
→ ROC-AUC: It measures the discriminative power of the classifier.
→ Confusion Matrix: It is used to analyze the true positives, true negatives, false positives, and false negatives.

- Cross-Validation

K-fold cross-validation was employed to check the stability of the LightGBM classifier on different data splits. This ensured that the performance was not biased towards a single train-test split.

- Generalization Testing

The LightGBM classifier was further tested on new datasets containing sophisticated phishing patterns such as:

→ Use of excessive subdomains
→ Use of obfuscation techniques
→ Use of shortened URLs
→ Use of homograph attacks

The LightGBM classifier performed exceptionally well on the generalization test and showed excellent predictability.

2. Web Integration

The final system combines the trained LightGBM model with a web interface. The user can input a URL and get instant classification results, which are either:

→ Secure (Legitimate)
→ Unsecure (Phishing)

Figure 4.1: Web Interface Output for a Secure URL

Figure 4.2: Web Interface Output for a Phishing URL

This system offers an end-to-end real-time phishing detection solution with user-friendly interaction.

3. Model Performance

LightGBM (Light Gradient Boosting Machine) performed well as a predictive model because of its tree-based boosting structure and histogram optimization methods. The important performance aspects are:

→ High accuracy rate
→ Low misclassification rate
→ Fast processing time
→ Excellent performance on imbalanced datasets

These aspects make LightGBM an ideal model for cybersecurity and real-time detection applications.

4. Website Performance Analysis

The web interface was analyzed using Google Lighthouse. The analysis checked performance, accessibility, SEO, and best practices.

Figure 4.3: Lighthouse Performance Result

- Lighthouse Scores

→ Performance: 86
→ Accessibility: 63
→ Best Practices: 100
→ SEO: 73

- Important Performance Metrics

→ First Contentful Paint (FCP): 1.2 s
→ Largest Contentful Paint (LCP): 2.0 s
→ Speed Index: 1.6 s
→ Total Blocking Time (TBT): 0 ms
→ Cumulative Layout Shift (CLS): 0.003

These performance metrics show that the system loads quickly, has a stable layout, and executes JavaScript efficiently.

- Strengths Identified

→ No security threats found
→ Fast CSS and JavaScript loading
→ No console errors

- Areas for Improvement

→ Large image sizes, which increase page size
→ Missing accessibility attributes (alt tags and ARIA attributes)
→ Missing meta descriptions for SEO

V. CONCLUSION

PhishCure provides an effective solution in the ongoing fight against phishing attacks. By integrating machine learning algorithms, the system is capable of detecting phishing websites with high accuracy (86%).

The proposed approach strengthens cybersecurity by enabling real-time URL classification and reducing potential threats. Overall, PhishCure enhances digital safety for both individuals and organizations, contributing to a more secure online environment.

REFERENCES

[1] B. Swarna Jyothi, M. Akshaya, K. Anjum, A. Bhavana, and K. Sreemukha, "URL Based Phishing Detection using Machine Learning," *Proc. of the 4th Int. Conf. on Information Technology, Civil Innovation, Science, and Management (ICITSM)*, EAI, 2025, doi:10.4108/eai.28-4-2025.2358166. (EUDL)

[2] A. U. Rehman, I. Imtiaz, S. Javaid, and M. Muslih, "Real-Time Phishing URL Detection Using Machine Learning," *Eng. Proc.*, vol. 107, no. 1, pp. 108, 2025, doi:10.3390/engproc2025107108. (MDPI)

[3] C. F. Mohd Foozy, M. A. I. Anuar, A. Maslan, H. A. Mohd Adam, and H. Mahdin, "Phishing URLs Detection Using Naïve Bayes, Random Forest and LightGBM Algorithms," *Int. Journal of Data Science*, vol. 5, no. 1, pp. 56-63, 2024, doi:10.18517/ijods.5.1.56-63.2024. (International Journal of Data Science)

[4] Jingxian Zhou et al., "A Novel Phishing Website Detection Model Based on LightGBM and Domain Name Features," *Symmetry*, vol. 15, no. 1, Art. 180, 2023, doi:10.3390/sym15010180. (MDPI)

[5] Adel A. Albishri and M. M. Dessouky, "A Comparative Analysis of Machine Learning Techniques for URL Phishing Detection," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 18495-18501, 2024, doi:10.48084/etasr.8920. (ETASR)

[6] P. Chakradhar Reddy et al., "Comparative Analysis of Machine Learning Algorithms for Phishing Detection Using URL Features," *Proc. of ICITSM*, 2025, doi:10.4108/eai.28-4-2025.2357976. (EUDL)

[7] Saritha Banoth et al., "Detecting Phishing URL using Random Forest Classifier," *Scholars Repository*, 2025, doi:10.30574/wjarr.2025.25.2.0360. (Scholars Repository)

[8] M. Fahri, "Implementation of the Random Forest Algorithm for Phishing Detection on Websites," *JITSI: Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 6, no. 2, pp. 186-194, 2025, doi:10.62527/jitsi.6.2.472. (Jurnal ITSI)

[9] N. Fahad Almujahid, M. A. Haq, and M. Alshehri, "Comparative Evaluation of Machine Learning Algorithms for Phishing Site Detection," *PeerJ Computer Science*, 10.7717/peerj-cs.2131, 2024. (PeerJ)

[10] "URL Based Phishing Detection using Machine Learning," *IJRASET Journal for Research in Applied Science and Engineering Technology*, 2023, doi:10.22214/ijraset.2023.52342. (IJRASET)

[11] "Real Time Phishing URL Detection Using Machine Learning Algorithms," International Journal of Research Publication and Reviews, vol. 6, no. 6, 2025, doi:10.5281/zenodo.16314488. (Zenodo)

[12] "Comparative Study of CatBoost, XGBoost, and LightGBM for Enhanced URL Phishing Detection," *Journal of Internet Services and Information Security*, vol. 13, no. 4, 2023, doi:10.58346/JISIS.2023.I4.001. (JISIS)