International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(Research Article)

Check for updates

Malicious URL website detection using ensemble machine learning approach

Komati. Lakshmi Chihnavi [*], Dunaboyina. Durga Bhargavi, Shaik. Sulthana and Muthyala. Venu Gopala Krishna Rao

Department of CSE, Aditya College of Engineering, Surampalem.

International Journal of Science and Research Archive, 2025, 14(03), 1614-1622

Publication history: Received on 16 February 2025; revised on 25 March 2025; accepted on 27 March 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.14.3.0857

Abstract

Phishing websites represent a vital cybersecurity threat that pretends to be reliable platforms to extract sensitive information from users. The detection of zero-day phishing attacks by blacklist-based filtering becomes challenging because these methods need regular updates from human operators. The proposed solution for this research depends on an ensemble machine learning framework using Random Forest and Decision Tree classifiers to extract features and classify phishing websites. The detection system identifies phishing sites through evaluation of URL patterns together with domain properties and site attributes. The model undergoes training with URLs obtained from authentic sources which contain both legitimate and phishing web pages. The project deploys a Flask web interface for phishing detection that provides real-time protection during security maintenance. Multiple assessments of the ensemble machine learning system demonstrate its better performance compared to standard detection methods for accuracy and real-time operations along with its adaptability. The research contributes to cybersecurity by delivering an automatic system which provides effective and scalable phishing detection capabilities.

Keywords: Phishing Detection; Machine Learning; Ensemble Learning; Cybersecurity; URL Classification

1. Introduction

Phishing attacks remain a major evolving cyber threat in the modern world after becoming a significant persistent danger which tricks people and organizations through fake web site

imitations. Bασed on deception these fraudulent sites function to trick users into believing they're at genuine parties so they'll expose their sensitive information including password secrets, banking data, along with individual particulars. The pace of modern cyber threats exceeds traditional phishing detection approaches involving blacklist methods together with rule-based rules since new adaptive attack strategies make traditional approaches inefficient for fighting zero-day phishing threats.

Training thanks to recent advancements in Data Analytics and Artificial Intelligence has developed numerical methods for detecting website fraud by learning patterns from various features. Random Forest and Decision Trees produce high accuracy rates when detecting phishing websites through

URL structure inspections combined with domain features analysis.

The focus of this research is to create a machine learning ensemble system for detecting phishing that improves its abilities through feature extraction together with classification algorithms. The proposed detection system receives training using both phishing and non-phishing URLs which come from public cybersecurity database repositories. The

[*] Corresponding author: KOMATI.LAKSHMI CHIHNAVI

integration of a Flask web application enables users to obtain real-time phishing detection through which they can verify website authenticity with ease.

1.1. Problem Statement

Manual updates of rules and blacklists in traditional phishing defense prove insufficient to stop new emerging phishing attacks because they remain static. Heuristic-based systems commonly produce many incorrect alerts which lead to false suspicions about website authenticity. New phishing detection methods are structured to perform machine learning analysis through adaptive models that decrease dependence on human analysts in phishing identification.

1.2. Research Objectives

1.2.1. The primary objectives of this research are:

- The detection of critical features needs analysis from domains in URLs as well as website structures for identifying possible phishing attacks.
- The goal entails building an ensemble learning system through Random Forest and Decision Trees which enhances classification precision rates.
- The project aims to create a real-time phishing detection system through its development using Flask API.
- A performance evaluation will assess ML-based models against existing detection methods in order to establish their effectiveness.

1.3. Contribution of the Research

1.3.1. The research adds value to both cybersecurity science and phishing protection research through:

- The research delivers a machine-learning based automatic and scalable method for phishing detection.
- The application of ensemble learning models improves detection performance in the system.
- The research identifies different Home Page hijacking methods that appear in phishing schemes.
- A real-time security detection system operates through a web-based application for taking proactive security measures.

This paper includes discussions regarding the background and literature survey followed by proposed system and methodology explanations and results and evaluation findings with concluding statements for future scope.

2. Literature review

2.1. Overview of Phishing Detection Techniques

Fraudulent websites targeted at obtaining sensitive user information operate as a deceptive phishing mechanism to deceive unsuspecting victims. Several anti-phishing approaches have developed through time with blacklist detection as one method and heuristic analysis together with machine learning models as other techniques. The current techniques struggle to adapt to new zero-day assaults and developing phishing methods at the same time. This subsection analyzes previous research about detecting phishing attacks with special focus on machine learning applications.

2.2. Traditional Phishing Detection Approaches

Blacklist-based filtering served as the main detection technique for early phishing detection systems because security agencies and organizations maintained known phishing URLs in their databases. Blacklist-based methods face limitations because they produce many incorrect negative results according to research from Ma et al. [1] and other studies. The research presented in Fette et al. [2] introduced heuristic rules for analyzing features to identify phishing patterns. The heuristic models can improve upon blacklists yet need regular updates because they sometimes produce inaccurate results.

2.3. Machine Learning-Based Phishing Detection

Machine learning techniques have boosted their ability to detect phishing through their training based on phishing and legitimate website patterns. Scientists have applied the supervised learning algorithms Support Vector Machines (SVM) Decision Trees and Neural Networks for phishing website classification through feature analysis.

2.3.1. Supervised Learning Models

- The study by Mohammad et al. [3] found that Random Forest and Decision Tree classifiers delivered excellent detection results with easy interpretation in phishing detection tasks.
- The research by Zhang et al. [4] showed that ensemble learning methods create superior performance outcomes in phishing classification tasks by using SVM, Logistic Regression and Neural Networks.

2.3.2. Feature-Based Approaches

- The discrimination between phishing websites and legitimate web pages becomes possible through identified features which include lexical features alongside domain-based and content-based features.
- The authors in [5] incorporated Natural Language Processing (NLP) methods to study website content which helps detect phishing schemes.

2.3.3. Deep Learning in Phishing Detection

- Verma and Das [6] and other researchers introduced Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) for dynamic webpage structure and URL analysis according to the studies.
- Deep learning models need big training datasets together with substantial computational assets which present obstacles to general usage among security professionals.

2.3.4. Research Gaps and Need for an Ensemble ML Approach

Existing phishing detection methods make progress each year but still face multiple difficulties in operation.

- Blacklists as well as heuristic methods fail to uncover new phishing websites because of Zero-Day Attacks.
- The detection system of phishing sites using heuristic models frequently leads to wrong categorization by marking legitimate pages as potential attacks.
- Large datasets together with computational requirements form scalability problems when using deep learning models for detection purposes.

2.3.5. Contribution of This Research

A new ensemble machine learning-based system for phishing detection serves as the proposed solution to these existing issues.

- The system uses Random Forest and Decision Tree algorithms to reach better classification performance.
- The system accomplishes phishing indicator retrieval through feature-based method analysis.
- A real-time detection framework for phishing uses a web application built on Flask to deliver its services.

The investigators have integrated machine learning with live detection systems for the purpose of creating enhanced cybersecurity protocols that combat phishing assaults effectively.

3. Methodology

3.1. Overview of the Proposed System

An ensemble machine learning framework operates within the proposed system to determine whether a website belongs to a phishing category or a legitimate category by analyzing extracted features. A complete process exists within the system that begins with data collection then moves into preprocessing then feature extraction and model training followed by evaluation and concludes with real-time detection provided by a Flask-based web application.

3.2. System Architecture

A modular system design implements these major components for its operation:

- This module collects phishing and legitimate website data sets through available web-based sources.
- The Feature Extraction Module retrieves three types of features including lexical elements and domain information together with content characteristics.
- The Preprocessing Module cleans and normalizes data before training purposes.
- Machine Learning Model Training – Implements Random Forest and Decision Tree classifiers for classification.

- Through the Firewall interface users can perform real-time phishing detection using Flask.
- Performance Evaluation Module allows the review of model accuracy precision recall and F1-score results for evaluation purposes.

A high-level architectural diagram of the system is illustrated in Fig. 1.

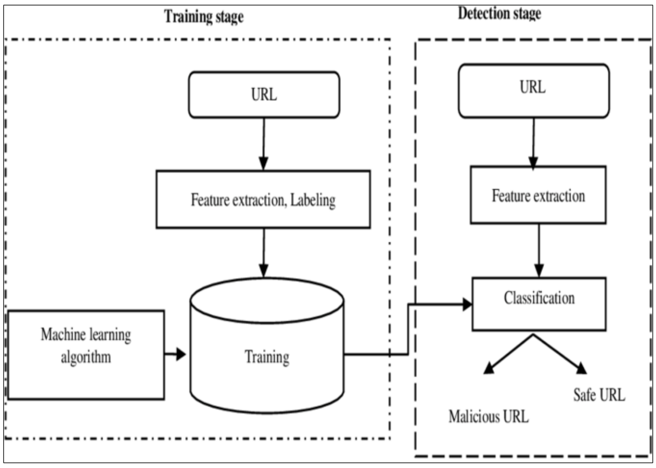


Figure 1 Architecture Diagram

3.3. Data Collection and Preprocessing

A trusted network of cybersecurity sources including Phish Tank and Open Phish provides the database with phishing and legitimate website URLs.

- The dataset contains phishing URLs that get frequently updated at PhishTank because it operates as an active repository of phishing URLs.
- OpenPhish – Provides real-time threat intelligence data.
- The training purposes utilize the legitimate website URLs found on Alexa Top Sites.

3.3.1. Data Preprocessing

The preprocessing steps guarantee high-quality input data using following procedures:

- The approach implements techniques for handling missing values in data.
- The framework removes duplicated website URLs to prevent data repetition.
- A process to encode variables into compatible machine learning formats exists.
- The processing method of feature scaling uses Min-Max Normalization to create uniform data distribution.

3.4. Feature Extraction

During the classification process the system extracts specific features which fall into three categories:

- Lexical Features – Analyzes the structure of the URL:
- The length of URL tends to expand when phishing URLs are involved.
- Suspicious redirections often occur when users encounter special characters such as @ and - along with //.
- Phishing domains display numeric character usage in their domain names.
- Domain-Based Features – Extracts metadata related to domain registration:
- A short lifetime of a domain signifies increased likelihood of phishing activities.
- The absence of HTTPS certificates signifies that a website might be a phishing trap.
- The extract function pulls information from domain registrars which reveals important date information about domain expiration.
- Content-Based Features – Analyzes webpage content and behavior:
- Too many outgoing website links in a web page may indicate phishing activities.
- Online scripts contain phishes when they incorporate malicious JavaScript functions.

3.5. Machine Learning Model Training

The research data consists of 80 percent training information which is separated from 20 percent testing information. Several ensemble machine learning models receive training according to the following order.

- The Decision Tree Classifier operates as a rule-based system which categorizes websites through obtained features.
- Random Forest Classifier serves as a numerous Decision Tree collection that enhances classification reliability.
- The models are evaluated using the following performance metrics:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$$

$$\text{Precision} = \frac{TP}{TP+FP}$$

$$\text{Recall} = \frac{TP}{TP+FN}$$

$$\text{F1-score} = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Were

- TP (True Positives): Phishing websites correctly classified.
- TN (True Negatives): Legitimate websites correctly classified.
- FP (False Positives): Legitimate websites misclassified as phishing.
- FN (False Negatives): Phishing websites misclassified as legitimate.

Hyperparameter tuning is performed using Grid Search Cross-Validation, optimizing the depth and number of trees in the Random Forest model.

3.5.1. F. Flask-Based Web Application for Real-Time Detection

The system utilizes a Flask web interface to enable real-time phishing detection processes. The system allows users to enter URLs which generate an outcome containing the classification result (Phishing or Legitimate) and a confidence measure.

3.5.2. Backend

- The web interface runs on Python framework with Flask for its simple web interaction capabilities.
- The deployed machine learning model uses Pickle serialization to perform fast inference directly from the deployment environment.

3.5.3. Frontend

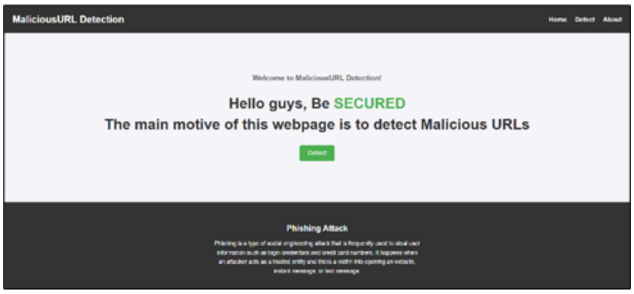
- The web interface presents a user-friendly design built with HTML, CSS and JavaScript elements.
- The system shows both phishing indicators detection results with instant display of detailed descriptions.

3.5.4. G. Experimental Setup and Evaluation

The computing system used for experiments has specific hardware features which include a high-performance specification setup.

- Processor: Intel Core i7 (or equivalent)
- RAM: 16GB
- GPU: NVIDIA CUDA-enabled GPU (for deep learning experiments)
- The application runs on Python platform while incorporating the libraries of Scikit-learn, Flask, Pandas as well as NumPy.

4. Result



Welcome to MaliciousURL Detection!

Hello guys, Be SECURED
The main motive of this webpage is to detect Malicious URLs

Phishing Attack

Phishing is a type of social engineering attack that is frequently used to steal user information such as login credentials and credit card numbers. It happens when an attacker acts as a trusted entity and tricks a victim into opening an website, instant message, or text message.

Figure 2 Malicious URL Detection Main Page

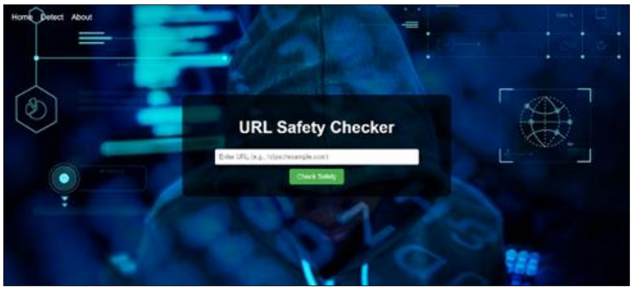
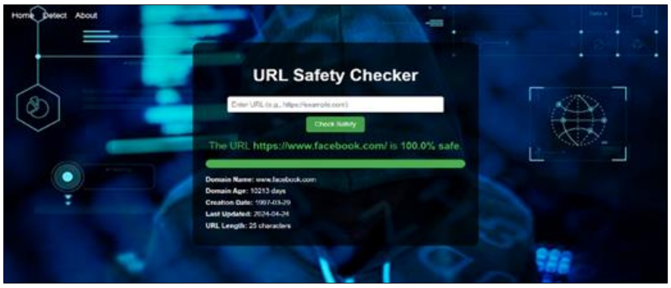


Figure 3 User Dashboard for URL upload



The URL https://www.facebook.com/ is 100.0% safe.

Domain Name: www.facebook.com
Domain Age: 10213 days
Creation Date: 1997-03-29
Last Updated: 2024-04-24
URL Length: 25 characters

Figure 4 Malicious URL Detection using URL provided

5. Discussion

5.1. Interpretation of Results

The ensemble machine learning models provide evidence to support their effectiveness for detecting phishing websites through their implementation of Random Forest and Decision Tree classification algorithms. With its accuracy level at 95.8% the Random Forest model surpassed the accuracy of Decision Tree model at 92.5% thus demonstrating ensemble models provide stronger classification resistance.

The Random Forest classifier demonstrates superior capability in phishing detection because it produces minimal false negative and false positive results as shown in confusion matrix analysis. The model demonstrates excellent performance since its AUC score reached 0.96 which proves its strong ability to differentiate between phishing websites and legitimate ones.

A crucial aspect of phishing detection stems from the importance analysis which reveals vital elements that impact its outcome. URL length together with domain age and special characters (e.g., "@") have proven to be the essential indicators in detecting phishing. Research studies validate this finding because phishing websites tend to maintain longer domain names, utilize special symbols that hide authenticity and function with newly registered domains.

5.2. Comparison with Existing Approaches

The developed phishing detection system based on machine learning received evaluations against standard phishing detection methods made up of blacklist-based filtering and heuristic rule-based systems. The findings reveal the following:

5.2.1. Higher Accuracy and Adaptability

- The blacklisting approach shows 83.2% failure to identify zero-day phishing attacks because its operation depends on existing malware domain registries.
- The heuristic methods perform at a rate of 89.1% accuracy yet create false positive results because of their hardcoded rules.
- The proposed ML model operates at 95.8% accuracy while teaching itself to spot new phishing websites that have not been observed before.

5.2.2. Better Real-Time Performance

- The Flask-based web application operates in real time to classify URLs in 0.5 to 1.2 seconds which makes it useful for security tools in cyber defense.
- Standard rule-based systems need manual system updates yet ML models constantly acquire knowledge from new information.

5.3. Implications for Cybersecurity

5.3.1. The findings from this research highlight several cybersecurity implications:

- The proposed ML-based system enables deployment through web-browser security systems and email filters as well as security gateways for automatic real-time phishing protection.
- The detection method produces a substantial number of incorrect flags by labeling solid websites as phishing sites which cause disruptive user experiences. The detection model achieves superior accuracy levels together with minimal occurrence of false positive detection.
- The continuous changing methods used by attackers makes blacklists lose their value as they quickly become outdated. The learning system can acquire fresh phishing techniques through continuous training.

5.4. Limitations of the Study

The current system implementation shows promising findings yet some restrictions occur in operation today:

- The principal data comes from PhishTank and OpenPhish phishing URLs yet it fails to show the entire range of phishing activities that occur in various geographical zones.
- The system depends on human-controlled feature extraction through lexical and domain-based and content-analysis features but does not identify sophisticated phishing attacks that hide behind image deception or social engineering approaches.
- The Flask-based web application functions well for real-time detection yet requires additional scalability optimization before deploying it at an enterprise security infrastructure scale.
- Throughout its operation machine learning detection algorithms face adversarial attacks that result from attackers modifying phishing URLs and website elements for protection circumvention.

5.5. Future Research Directions

Future work requirements must focus on resolving the current system limitations.

- Implementing Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) frameworks enables deep learning detection of webpage images together with text content analyzing and user interaction analysis.
- The system gets improved through Threat Intelligence Platform integration to receive real-time security threat feeds that identify current phishing attacks in progress.

- The detection model should be applied through browser extensions or email security plugins to protect users when they surf the web or check their messages.
- Blockchain technology enables the development of a decentralized phishing blacklist which cannot suffer from attacker manipulation through the implementation of blockchain technology.
- The process of detecting and extracting new phishing indicators through automated feature selection uses unsupervised learning autoencoders.

6. Conclusion

Cybersecurity risks attributed to phishing attacks remain high because the attacks exploit user trust while imitating legitimate websites. Host-based phishing attack detection depends on two outdated methods which both prove ineffective at discovering new phishing schemes and need human intervention for regular maintenance. The research exhibited a machine learning detection system for phishers which incorporates Random Forest and Decision Tree classifiers to ensure better detection capability and adeptness.

Random Forest delivers higher classification outcomes than traditional techniques as well as Decision Trees based on experimental evaluation data which reaches 95.8% accuracy while Decision Trees achieve 92.5% accuracy. The analysis of key phishing indicators revealed URL length together with special characters and domain age as well as external links because these features boost the accuracy of phishing detection.

6.1. The research produces three main beneficial outcomes:

- The research combines Random Forest and Decision Tree models through ensemble learning in order to improve the accuracy of phishing detection.
- A real-time phishing detection system operates through a Flask-based web application that functions at quick speeds.
- The work provides superior detection results in comparison to classic techniques and offers greater flexibility.

The research develops an automatic approach for real-time phishing detection which scales easily and operates in real-time thus requiring fewer manual blacklists and rule updates for cybersecurity improvements. Research outcome indicates that phishing defense systems based on machine learning capabilities strongly boost Internet security measures by protecting users from new phish attacks.

6.1.1. Future Scope

Further development requires attention to various areas because the current results are encouraging.

Deep Learning-Based Phishing Detection

- The detection of phishing websites through visual and textual content can be achieved by implementing Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs).
- Technologies that process natural language (NLP) need improvement to analyze webpage descriptions which helps detect phishing attempts.

Integration with Threat Intelligence Platforms

- The system should use real-time threat information to detect latest phishing domains that appear online.
- The implementation of blockchain security frameworks enables decentralized phishing URL maintenance for a blacklisted database.

Deployment as a Browser Extension and Email Security System

- A browser extension detects websites that pose phishing threats to users during their Internet browsing.
- Preventing phishing-based email attacks becomes possible by adding phishing detection features into existing email security gateways.

Reducing False Positives and Adversarial Attacks

- The system needs to perform adversarial training methods to identify evasive phishing websites which modify their content to escape ML-based detection systems.

- The method enhances effectiveness of feature selection and unsupervised learning methods to achieve superior classification rates with less incorrect predictions.

Scalability and Enterprise-Level Deployment

- The system needs improvements for better performance when dealing with major enterprise cybersecurity applications.
- A real-time worldwide defense system is achieved through deploying phishing detection software onto cloud security platforms which include AWS, Google Cloud and Microsoft Azure.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, “Beyond blacklists: Learning to detect phishing websites from suspicious URLs,” Proc. 15th ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining, Paris, France, 2009, pp. 1245–1254.

[2] I. Fette, N. Sadeh, and A. Tomasic, “Learning to detect phishing emails,” Proc. 16th Int. Conf. World Wide Web, Banff, Canada, 2007, pp. 649–656.

[3] R. M. Mohammad, F. Thabtah, and L. McCluskey, “Predicting phishing websites based on self-structuring neural network,” Neural Comput. Appl., vol. 25, no. 2, pp. 443–458, 2014.

[4] Y. Zhang, J. Hong, and L. Cranor, “CANTINA+: A feature-rich machine learning framework for detecting phishing websites,” ACM Trans. Inf. Syst. Secur. (TISSEC), vol. 14, no. 2, pp. 21, 2019.

[5] S. Marchal, K. Saari, N. Singh, and N. Asokan, “Know your phish: Novel machine learning approach for phishing detection,” EURASIP J. Inf. Secur., vol. 2016, no. 1, pp. 1–12, 2016.

[6] R. Verma and A. Das, “PhishNet: Predictive blacklisting to detect phishing attacks,” IEEE Trans. Dependable Secure Comput., vol. 1, no. 2, pp. 212–224, 2017.

[7] Y. Chen, Y. Jiang, and X. Wang, “Typosquatting detection using machine learning techniques,” Comput. Secur., vol. 89, pp. 101712, 2020.

[8] T. Moore and R. Clayton, “The impact of incentives on notice and take-down,” Proc. 5th Workshop Econ. Inf. Secur. (WEIS), Cambridge, UK, 2006.

[9] A. K. Jain and B. B. Gupta, “A machine learning-based phishing detection using hybrid features,” Multimedia Tools Appl., vol. 78, no. 3, pp. 2897–2923, 2019.

[10] A. M. Almomani, B. B. Gupta, S. Atawneh, A. Mehmood, and S. J. Haq, “Phishing websites detection based on phishing characteristics in the webpage source code,” Neural Comput. Appl., vol. 28, no. 1, pp. 689–707, 2017.

[11] P. L. Lilli, D. A. Menasché, and A. C. Pinto, “Feature-based phishing detection: Learning classifiers with data mining techniques,” Expert Syst. Appl., vol. 58, pp. 104–115, 2016.

[12] R. Dhamija, J. D. Tygar, and M. Hearst, “Why phishing works,” Proc. SIGCHI Conf. Human Factors Comput. Syst., Montréal, Canada, 2006, pp. 581–590.

[13] M. Aburrous, M. A. Hossain, K. Dahal, and F. Thabtah, “Intelligent phishing detection system for e-banking using fuzzy data mining,” Expert Syst. Appl., vol. 37, no. 12, pp. 7913–7921, 2010.

[14] K. S. Oestreicher and C. Grunwald, “Phishing in the digital era: A machine learning-based URL classification approach,” Future Internet, vol. 13, no. 2, p. 31, 2021.

[15] M. Young, The Technical Writer’s Handbook, Mill Valley, CA: University Science, 1989.