IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, May 2025
Impact Factor: 7.67

Phishing Website Detection Using Random Forest Algorithm

Age Yuvraj B., Bandagar Varsha S., Rewanwar Anurag A., Saindane Jayesh J.
Department of Information Technology Engineering
NBN Sinhgad Technical Institutes Campus, Pune, India

Abstract: *The Internet has become an integral part of everyday life, but it has also paved the way for cybercriminal activities such as hacking. Phishers employ social engineering tactics and fraudulent websites to deceive users and steal sensitive information, including account credentials, usernames, and passwords from both individuals and organizations. Phishing is a form of online identity theft where attackers manipulate users into revealing confidential data by leveraging website spoofing and psychological manipulation. This stolen data is often used for illicit financial transactions, such as unauthorized online banking activities or fraudulent purchases.*

The Internet serves as a crucial communication tool for people worldwide, but it has also become a medium for cybercriminals to exploit personal information with minimal risk of detection. Phishing, a deceptive practice, poses a major threat to the e-commerce industry by eroding consumer confidence in online shopping and causing financial losses to service providers. Therefore, a deeper understanding of phishing mechanisms is essential. Despite the introduction of various methods to detect phishing websites, cybercriminals continuously refine their techniques to bypass these defenses. Machine learning has emerged as a powerful approach for identifying such malicious activities, as phishing attacks often exhibit recurring patterns that can be analyzed effectively..

Keywords: Phishing, Classification, Machine Learning, Cybersecurity, Fraud Detection

I. INTRODUCTION

Online services have greatly enhanced convenience in everyday life, enabling seamless access to information and reducing operational costs for service providers. For instance, online banking has become an essential tool for both financial institutions and customers, streamlining transactions and reducing the need for physical interactions. However, many online services, including banking applications, require a certain level of technical understanding, which not all users possess. This lack of familiarity has made many individuals vulnerable to phishing attacks—cyber threats designed to exploit unsuspecting users for financial gain.

Phishing is a deceptive form of online identity theft that combines social engineering tactics with website spoofing to manipulate users into disclosing sensitive information. A common phishing attack involves an attacker distributing a large number of fraudulent emails that appear to originate from a trusted institution, such as a bank. These emails typically urge recipients to update their personal details, often under the pretense of security verification or account maintenance. To create a sense of urgency, they may include threats of account suspension if the recipient fails to comply. Such scare tactics are a well-known aspect of social engineering and effectively persuade users into taking action.

When a victim follows the link embedded in the phishing email, they are redirected to a counterfeit website controlled by the attacker. This fraudulent site is carefully crafted to resemble the legitimate organization's web page, mimicking its logos, color schemes, icons, and other branding elements. Believing the site to be authentic, the victim enters their credentials—such as a username and password—allowing the attacker to gain unauthorized access to their account. This can result in financial fraud, unauthorized transactions, or further exploitation of personal information.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, May 2025
Impact Factor: 7.67

Despite increasing awareness of phishing due to media coverage, these attacks continue to be highly successful. Cybercriminals consistently refine their strategies, making their fraudulent attempts more sophisticated. For instance, many phishing emails now claim to request personal details for "security reasons," falsely assuring victims that their financial institution is taking steps to protect them. This evolving nature of phishing underscores the need for robust detection mechanisms to safeguard users from such threats.

II. METHODOLOGY

Random Forest is a widely used machine learning algorithm for fraud detection. It operates as an unsupervised learning method that detects fraudulent activities by identifying anomalies within a dataset. By randomly partitioning features, the algorithm generates shorter decision paths for fraudulent data points, making them distinguishable from legitimate ones.

In the proposed system, a user logs in using their credentials, including a user ID and password. Upon successful authentication, they are directed to the homepage, where they can input a potentially suspicious URL for verification. The system then first checks whether the entered URL is already present in the database and has been previously flagged as phishing. If a match is found, the system retrieves the corresponding classification result and presents it to the user via the graphical interface. However, if the URL is not in the database, it undergoes classification using a machine learning approach. The Random Forest algorithm, a well-established classification technique, is applied to determine whether the URL is legitimate or fraudulent. If the system classifies the URL as a phishing site, the results are displayed in the user interface accordingly.

Dataset Collection and Preprocessing

The dataset consists of labeled URLs, with attribute values represented as integers: -1 for legitimate sites, 0 for suspicious or doubtful cases, and 1 for phishing websites. Before classification, the dataset is preprocessed to structure the data into a suitable format. It is then divided into two subsets: training data and testing data. The implementation, which is carried out using Java, applies the Random Forest algorithm to detect phishing websites efficiently.

Random Forest Classification

The dataset is split into training and testing sets, with 80% allocated for training the model and the remaining 20% for testing. Furthermore, a portion of the training set (25%) is used for additional validation. Random Forest, a robust machine learning classification algorithm, operates by constructing multiple decision trees. Each tree is trained on a subset of the dataset using randomly selected features, reducing the risk of overfitting and improving model performance.

To apply Random Forest for phishing detection, a dataset containing labeled URLs (either phishing or legitimate) is required. Various attributes, such as URL length, number of subdomains, presence of specific keywords, and other structural characteristics, are extracted. These extracted features serve as input to the Random Forest model for classification.

Prediction Process

The following steps outline how the trained Random Forest model predicts whether a given URL is phishing or legitimate:

Feature Extraction: The system analyzes the new URL, extracting key attributes such as URL length, number of subdomains, and presence of suspicious keywords. The preprocessing follows the same procedure applied during training.

Input to the Model: The extracted features are then fed into the trained Random Forest model for analysis.

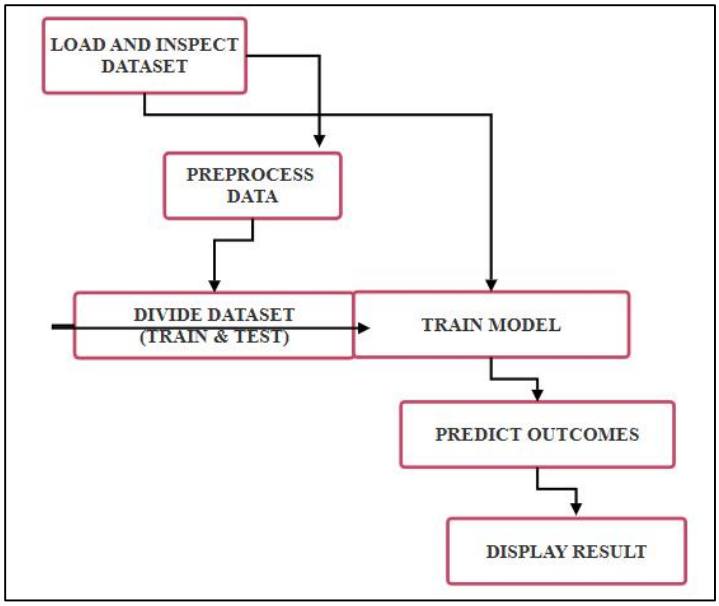
Classification: The model processes the input and predicts whether the given URL is phishing (1), suspicious (0), or legitimate (-1).

Result Interpretation: Based on the model's output, if the label is 1, the system classifies the URL as phishing; if it is 0, the URL is considered suspicious; and if it is -1, the URL is classified as safe.

This structured approach allows for effective detection of phishing websites using machine learning, providing a secure environment for users against fraudulent online threats.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, May 2025
Impact Factor: 7.67

III. IMPLEMENTATION



1. Load and Inspect Dataset

The dataset is loaded into a data processing framework such as **Pandas** (Python) or **Hadoop** (Big Data).

The dataset is inspected for its structure, including:

Number of rows and columns.

Data types of each column.

Presence of missing or incorrect values.

An initial exploratory analysis is conducted to understand the distribution of data and detect potential inconsistencies.

2. Preprocess Data

Cleaning: Remove duplicate, missing, or irrelevant entries.

Feature Extraction: Extract relevant features (e.g., URL length, domain name, presence of suspicious keywords).

Feature Engineering: Convert categorical data into numerical format (e.g., encoding website domain types).

Normalization/Scaling: Standardize feature values to improve model performance.

Handling Imbalanced Data: Use oversampling/undersampling techniques if necessary.

3. Divide Dataset (Train & Test)

The dataset is split into two parts:

Training set (70-80%): Used to train the model.

Test set (20-30%): Used to evaluate the model's performance.

The split ensures the model learns from one portion of data and generalizes well to unseen data.

A stratified split is used if class distribution is imbalanced.

4. Train Model

The selected machine learning model (e.g., **Random Forest, SVM, or Neural Network**) is trained using the training dataset.

The model learns patterns and relationships from input features.

Hyperparameters are optimized using techniques like **Grid Search or Random Search** to improve accuracy.

Cross-validation is applied to ensure the model performs well on different subsets of the training data.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, May 2025
Impact Factor: 7.67

5. Predict Outcomes

The trained model is tested using the test dataset.

The model predicts outcomes (e.g., phishing or legitimate URLs).

The performance of the model is measured using evaluation metrics such as **Accuracy, Precision, Recall, F1-score, and ROC-AUC**.

If performance is not satisfactory, model tuning is performed to enhance predictions.

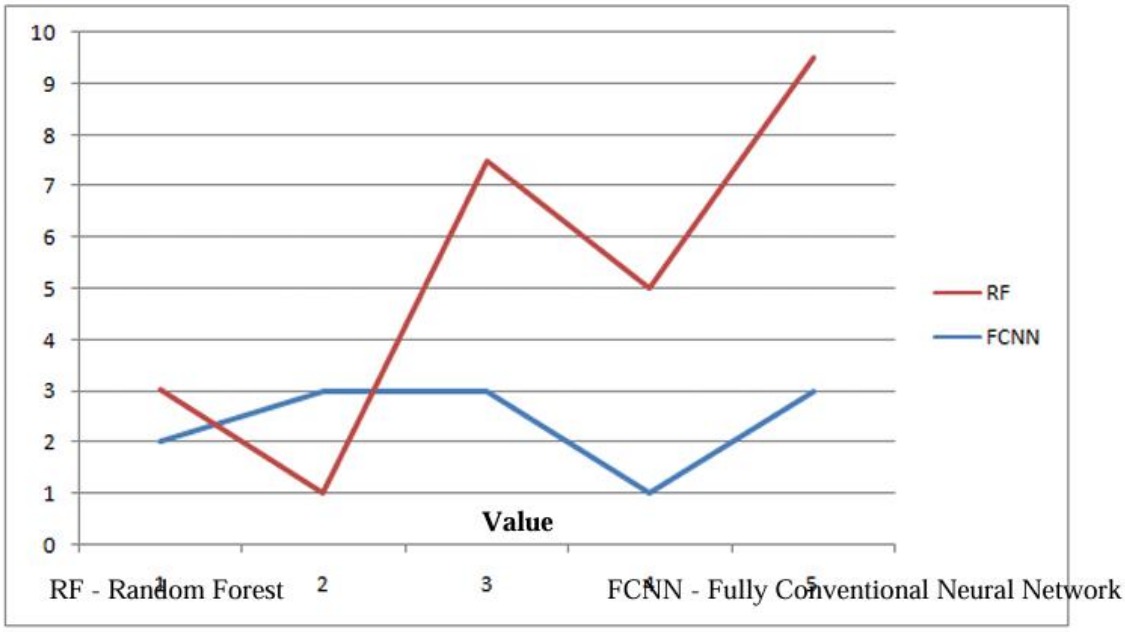
6. Display Results

The final prediction results are visualized using tables, graphs, and classification reports.

The model's accuracy, confusion matrix, and precision-recall curves are displayed.

The results highlight the effectiveness of the model in detecting phishing attacks.

Insights and recommendations are provided based on findings.



Accuracy

III. CONCLUSION

With the increasing importance of privacy protection and cybersecurity, phishing detection has become a critical area of research. Various techniques have been developed to classify websites and identify phishing attempts using machine learning models. Among these, URL-based classification has proven to be an effective approach, significantly improving detection speed. Machine learning algorithms, particularly those optimized for classification tasks, have demonstrated high performance in identifying phishing websites.

This paper explores phishing detection methods and reviews the latest research in this domain. Our proposed approach enhances phishing detection by leveraging machine learning technology. Specifically, we employed the **Random Forest algorithm**, achieving a **97.14% detection accuracy** while maintaining a **low false positive rate**. Our results indicate that classifiers perform better when trained on larger datasets, highlighting the importance of comprehensive training data in improving detection accuracy.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, May 2025
Impact Factor: 7.67

For future work, we aim to develop a **hybrid phishing detection system** that integrates **machine learning with blacklist-based approaches**. By combining the **Random Forest algorithm** with **blacklist techniques**, we anticipate further improvements in detection accuracy and real-time phishing prevention. This hybrid approach will strengthen cybersecurity defenses against evolving phishing threats.

REFERENCES

[1] A. F. Al-Qahtani and S. Cresci, ''The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19,'' *IET Inf. Secur.*, vol. 16, no. 5, pp. 324–345, Sep. 2022, doi: 10.1049/ise2.12073.
[2] APWG, "Phishing Activity Trends Reports." Accessed: Sep. 28, 2022. [Online]. Available: https://apwg.org/trendsreports/
[3] N. Q. Do, A. Selamat, O. Krejcar, E. Herrera-Viedma, and H. Fujita, ''Deep learning for phishing detection: Taxonomy, current challenges, and future directions,'' *IEEE Access*, vol. 10, pp. 36429–36463, 2022, doi: 10.1109/ACCESS.2022.3151903.
[4] Phishing Websites Features.pdf. Accessed: Sep. 28, 2022. [Online]. Available: http://eprints.hud.ac.uk/id/eprint/24330/6/
[5] UCI Machine Learning Repository: Phishing Websites Data Set. Accessed: Oct. 1, 2022. [Online]. Available: https://archive.ics.uci.edu/ml/datasets/phishing+websites
[6] S. Al-Ahmadi, "PDMLP: Phishing Detection Using Multilayer Perceptron." Rochester, NY, USA, 2020. Accessed: Sep. 1, 2022. [Online]. Available: https://papers.ssrn.com/abstract=3624621
[7] PhishTank, "Join the Fight Against Phishing." Accessed: Oct. 1, 2022. [Online]. Available: https://phishtank.org/
[8] Q. Li, M. Cheng, J. Wang, and B. Sun, ''LSTM-based phishing detection for big email data,'' *IEEE Trans. Big Data*, vol. 8, no. 1, pp. 278–288, Feb. 2022, doi: 10.1109/TBDATA.2020.2978915.
[9] A. Odeh, I. Keshta, and E. Abdelfattah, "Efficient Detection of Phishing Websites Using Multilayer Perceptron." *International Association of Online Engineering*, 2020. Accessed: Sep. 30, 2022. [Online]. Available: https://www.learntechlib.org/p/217754/
[10] Y. Lin, "Phishpedia: A Hybrid Deep Learning-Based Approach to Visually Identify Phishing Webpages." Accessed: Sep. 30, 2022. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/lin
[11] S. Kiranyaz, O. Avci, O. Abdeljaber, T. Ince, M. Gabbouj, and D. J. Inman, ''1D convolutional neural networks and applications: A survey,'' *Mech. Syst. Signal Process.*, vol. 151, Apr. 2021, Art. no. 107398, doi: 10.1016/j.ymssp.2020.107398.
[12] A. Lakshmanarao, P. S. P. Rao, and M. M. B. Krishna, ''Phishing website detection using a novel machine learning fusion approach,'' *Int. Conf. Artif. Intell. Smart Syst. (ICAIS)*, Mar. 2021, pp. 1164–1169, doi: 10.1109/ICAIS50930.2021.9395810.
[13] G. H. Lokesh and G. BoreGowda, ''Phishing website detection based on an effective machine learning approach,'' *J. Cyber Security Technol.*, vol. 5, no. 1, pp. 1–14, Jan. 2021, doi: 10.1080/23742917.2020.1813396.
[14] A. Ozcan, C. Catal, E. Donmez, and B. Senturk, ''A hybrid DNN–LSTM model for detecting phishing URLs,'' *Neural Comput. Appl.*, vol. 33, pp. 1–17, Aug. 2021, doi: 10.1007/s00521-021-06401-z.
[15] A. Butnaru, A. Mylonas, and N. Pitropakis, ''Towards lightweight URL-based phishing detection,'' *Future Internet*, vol. 13, no. 6, p. 154, Jun. 2021, doi: 10.3390/fi13060154.
[16] Y. Wei and Y. Sekiya, ''Feature selection approach for phishing detection based on machine learning,'' in *Proc. Int. Conf. Appl. Cyber Security (ACS)*, 2021, pp. 61–70, doi: 10.1007/978-3-030-95918-0_7.
[17] S. Mahdavifar and A. A. Ghorbani, ''DeNNeS: Deep embedded neural network expert system for detecting cyber attacks,'' *Neural Comput. Appl.*, vol. 32, no. 18, pp. 14753–14780, 2020, doi: 10.1007/s00521-020-04830-w.
[18] W. Wei, Q. Ke, J. Nowak, M. Korytkowski, R. Scherer, and M. Wozniak, ''Accurate and fast URL phishing detector: A convolutional neural network approach,'' *Comput. Netw.*, vol. 178, Sep. 2020, Art. no. 107275, doi: 10.1016/j.comnet.2020.107275