iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.77759

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

AI-Driven Cybersecurity Framework for Phishing Website Detection Using Optimized Machine Learning Models

Leena Sanjay Pelne[1], Prof. Yamini Laxane[2], Prof. Bhagyashree Kumbhare[3]
Smt. Radhikatai Pandav College of Engineering, Nagpur ,India

Abstract: ***Phishing attacks remain one of the most critical cybersecurity threats, exploiting users through fraudulent websites to obtain sensitive information such as credentials and financial data. Traditional rule-based detection systems often lack adaptability to evolving attack strategies. This study proposes an AI-driven cybersecurity framework for phishing website detection using supervised machine learning models. The UCI Phishing Website Dataset consisting of 1353 instances and 10 security-related attributes was used for experimentation. Three classifiers—Logistic Regression, Support Vector Machine (SVM), and Random Forest—were implemented and comparatively evaluated. Hyperparameter optimization using GridSearchCV with 5-fold cross-validation was performed to enhance predictive performance. The dataset was split into 70% training and 30% testing subsets. Performance evaluation was conducted using accuracy, precision, recall, F1-score, and confusion matrix analysis. Experimental results show that the optimized Random Forest model achieved approximately 91% accuracy, outperforming Logistic Regression and SVM models. Feature importance analysis highlights that attributes such as SFH and SSLfinal_State significantly influence classification outcomes. The findings demonstrate that ensemble-based AI techniques strengthen phishing detection systems and provide scalable, intelligent cybersecurity defense mechanisms.***
Keywords: artificial intelligence, cybersecurity, machine learning, phishing detection, random forest.

I. INTRODUCTION

Phishing is a deceptive cyberattack technique aimed at stealing sensitive user information by impersonating legitimate websites. As internet usage increases, phishing attacks have become more sophisticated and difficult to detect. Traditional blacklist and rule-based detection systems are limited in their ability to adapt to evolving phishing strategies. Artificial Intelligence (AI) and machine learning techniques provide intelligent and adaptive mechanisms for automated phishing detection. This study proposes an AI-driven cybersecurity framework that leverages supervised learning algorithms to classify websites as legitimate or phishing. The objective is to compare multiple machine learning classifiers and identify the most effective model for accurate phishing detection.

II. DATASET DESCRIPTION

The experiments were conducted using the UCI Phishing Website Dataset containing 1353 instances with 10 relevant features. The dataset includes URL-based, domain-based, and security-related attributes such as:

1) SFH
2) SSLfinal_State
3) popUpWidnow
4) Request_URL
5) URL_Length
6) web_traffic
7) age_of_domain
8) having_IP_Address

The dataset was divided into 70% training data and 30% testing data to ensure reliable evaluation and prevent overfitting.

III. PROPOSED METHODOLOGY

A. Data Preprocessing

The dataset was examined for inconsistencies and prepared for supervised classification. Feature-label separation was performed, and categorical values were encoded where necessary.

B. Machine Learning Models

Three classification algorithms were implemented:

1) Logistic Regression: A linear classification model used as a baseline classifier.
2) Support Vector Machine (SVM): A margin-based classifier effective in high-dimensional spaces.
3) Random Forest: An ensemble-based learning method combining multiple decision trees to improve accuracy and reduce overfitting.

C. Hyperparameter Optimization

GridSearchCV with 5-fold cross-validation was applied to tune Random Forest hyperparameters. This optimization improved model generalization and predictive performance.

D. Performance Evaluation Metrics

Model performance was evaluated using:

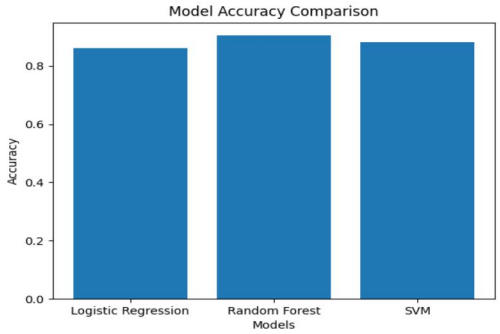
1) Accuracy
2) Precision
3) Recall
4) F1-score
5) Confusion Matrix

These metrics provide a comprehensive assessment of classification performance.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

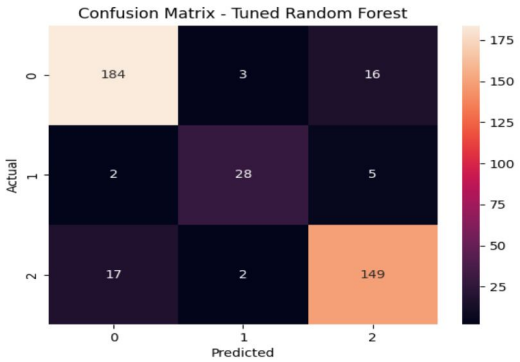
The optimized Random Forest classifier achieved the highest accuracy of approximately 91%, outperforming Logistic Regression (≈86%) and SVM (≈88%).

Fig. 1. Accuracy Comparison of AI Models



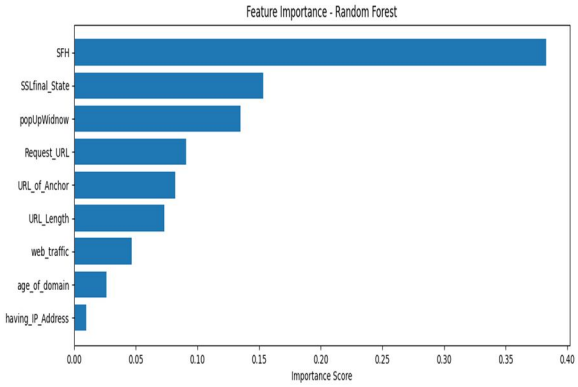
Confusion matrix analysis indicates strong classification capability with minimal false positives and false negatives.

Fig. 2. Confusion Matrix of Tuned Random Forest



Feature importance analysis reveals that SFH and SSLfinal_State are dominant predictors, emphasizing the importance of security-related attributes in phishing detection.

Fig. 3. Feature Importance Analysis



The experimental findings confirm that ensemble-based machine learning models provide enhanced detection capability compared to traditional linear models.

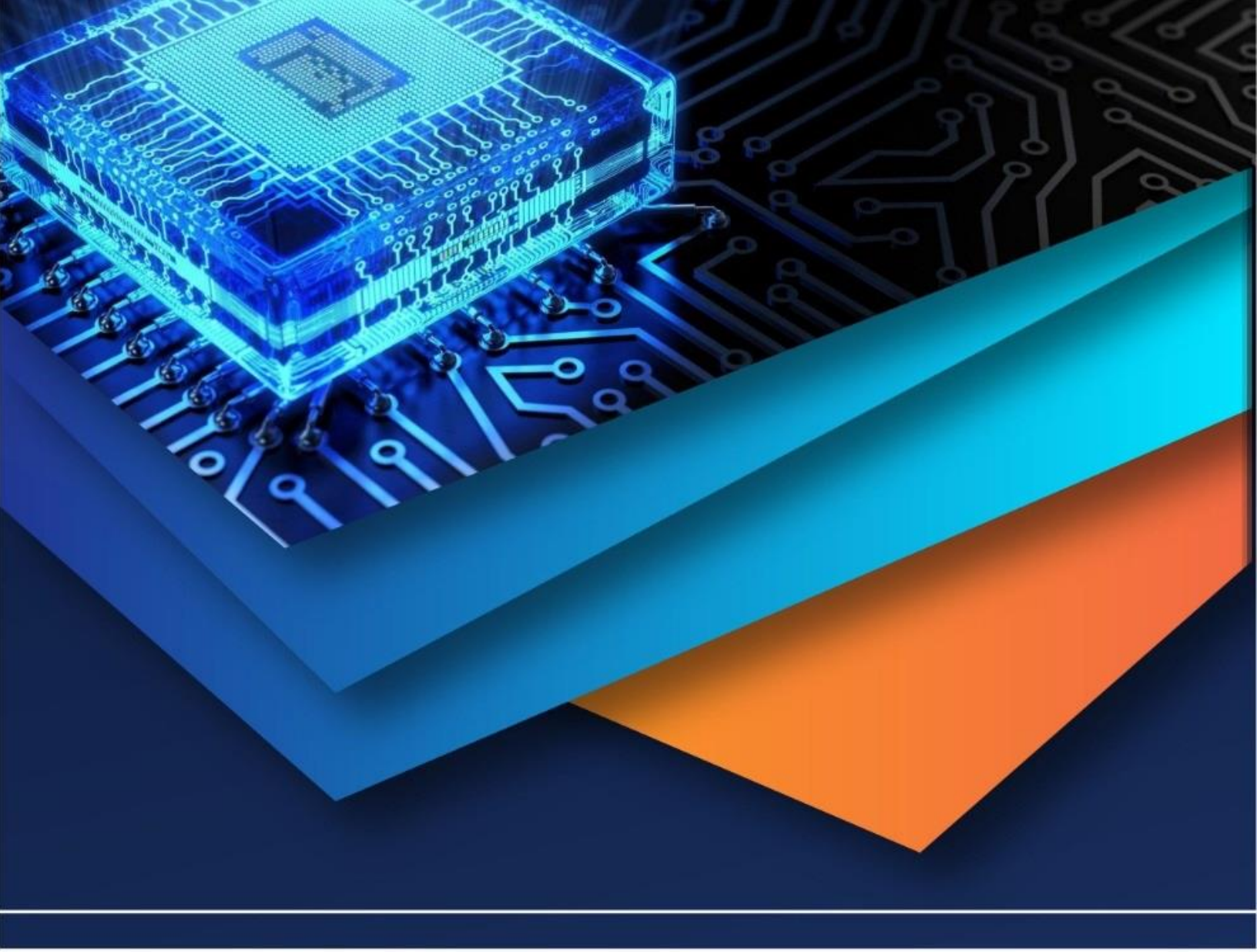
V. CONCLUSION

This research presented an AI-driven cybersecurity framework for phishing website detection using optimized machine learning models. Comparative analysis demonstrated that the Random Forest classifier achieved superior accuracy and robustness. Feature importance evaluation improved interpretability and understanding of critical phishing indicators.

The proposed framework offers scalability and adaptability for real-world cybersecurity systems. Future work may involve integration of deep learning techniques, real-time deployment in browser-based environments, and expansion to larger phishing datasets for improved generalization.

REFERENCES

[1] UCI Machine Learning Repository, “Phishing Website Dataset.”
[2] https://www.kaggle.com/datasets/tlhcelik/website-phishing-dataset
[3] https://ieeexplore.ieee.org/document/11011572
[4] https://www.sciencedirect.com/science/article/abs/pii/S0167404820303965



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY