Detecting Phishing Websites using Machine Learning Algorithms: A Comparative Study of Random Forest and SVM

# Abstract

Phishing attacks are among the most prevalent cyber threats, targeting users to steal sensitive information by mimicking legitimate websites. Traditional detection methods are increasingly ineffective against rapidly evolving phishing techniques. This research applies machine learning (ML) algorithms—Random Forest and Support Vector Machine (SVM)—to detect phishing websites using the UCI Phishing Dataset containing 11,000 entries and 30 features. Performance was evaluated using accuracy, precision, and F1-score. The results showed that Random Forest outperformed SVM, achieving a 96.4% accuracy. This study demonstrates the effectiveness of ML models in cybersecurity and highlights the importance of automated phishing detection.

# 1. Introduction

Phishing is a deceptive technique used to fraudulently acquire sensitive data such as login credentials, credit card numbers, and personal information. Cybercriminals often use spoofed websites and social engineering techniques. Due to the dynamic and ever-changing nature of phishing attacks, rule-based and signature-based detection methods are no longer sufficient. Machine learning presents a scalable solution to detect phishing websites by analyzing features extracted from URLs and website metadata. This study evaluates two widely used ML models—Random Forest and SVM—on the UCI Phishing dataset.

# 2. Literature Review

Several studies have attempted to address phishing detection using ML:  
- Mohammad et al. (2012) proposed a hybrid ML model using heuristic and blacklist features.  
- Jain and Gupta (2018) implemented ensemble learning for robust detection with improved precision.  
- A recent study by Rao et al. (2020) applied deep learning on URL embeddings for phishing classification.

However, challenges remain in feature interpretability, latency in real-time detection, and generalization to unseen attack patterns.

# 3. Methodology

3.1 Dataset  
- Source: UCI Machine Learning Repository  
- Entries: ~11,000 URLs  
- Features: 30 features such as having\_IP\_Address, URL\_Length, SSLfinal\_State, etc.  
- Target: -1 (Phishing) and 1 (Legitimate)

3.2 Data Preprocessing  
- Removed missing values  
- Converted categorical features to numerical (binary or ordinal)  
- Normalized numerical features using MinMaxScaler  
- Split data into 80% training and 20% testing sets

3.3 Algorithms Used  
- Random Forest: An ensemble learning technique using multiple decision trees and majority voting  
- SVM: A supervised classifier that finds the hyperplane separating classes with maximum margin

# 4. Evaluation Metrics

- Accuracy: Correct predictions / total predictions  
- Precision: True Positives / (True Positives + False Positives)  
- F1 Score: Harmonic mean of Precision and Recall

# 5. Results and Analysis

Model Performance:

| Model | Accuracy | Precision | F1 Score |  
|---------------|----------|-----------|----------|  
| SVM | 93.1% | 92.0% | 92.8% |  
| Random Forest | 96.4% | 95.9% | 96.3% |

Random Forest showed better generalization, less overfitting, and handled noisy data more effectively. Feature importance (from Random Forest) indicated that URL\_Length, having\_At\_Symbol, and HTTPS\_token were the most influential features.

# 6. Discussion

The comparative analysis shows that Random Forest is more accurate and robust for phishing website detection than SVM. The ensemble nature of Random Forest helps in reducing variance and handling feature interactions better. Although SVM is theoretically powerful, it is sensitive to parameter tuning and feature scaling. The dataset's simplicity and binary classification nature suit Random Forest’s capabilities.

# 7. Conclusion and Future Work

This study confirms that machine learning, particularly Random Forest, is effective in detecting phishing websites with high accuracy. Future research can explore:  
- Deep learning models (LSTM for sequential URL patterns)  
- Real-time browser extension integration  
- Cross-language phishing detection  
- Continual learning to handle evolving phishing techniques

# 8. References

1. UCI Machine Learning Repository. “Phishing Websites Data Set.”  
2. Mohammad, R. M., Thabtah, F., & McCluskey, L. (2012). Predicting phishing websites based on self-structuring neural networks.  
3. Jain, A., & Gupta, B. B. (2018). Comparative analysis of phishing detection techniques using machine learning.  
4. Rao, R., & Ali, S. (2020). Deep learning approach for phishing URL classification using hybrid features. Computers & Security.