Cyber Security Assignment 2 Report

Phishing Website Detection Using Machine Learning

Title: Phishing Website Detection Using Machine Learning Algorithms
Student Name: B VISHNUVARDAN
Roll No: 160123737034
Course: Cyber Security

1. Abstract

Phishing continues to be one of the most widespread cyber threats, targeting users through deceptive websites that mimic legitimate platforms. This project develops a machine learning-based approach to effectively detect phishing websites. Using a dataset of URL features, models including Random Forest, Decision Tree, and Logistic Regression were implemented and compared. A hybrid feature-based model integrating both URL and content-level attributes was also proposed. Experimental results demonstrate that ensemble learning improves accuracy and generalization, addressing limitations of existing research.

2. Introduction

Phishing attacks are social engineering schemes designed to steal user credentials or sensitive information by impersonating trusted websites. Traditional rule-based systems are often inadequate for detecting rapidly evolving phishing strategies. Machine Learning (ML) provides an adaptive solution by learning patterns from historical data to classify websites as legitimate or malicious. This study focuses on reproducing and improving an ML-based phishing detection model to enhance both accuracy and robustness.

3. Literature Review

The selected research paper, "Phishing Website Detection using Machine Learning Algorithms," applied several supervised algorithms to a publicly available dataset. Features such as URL length, presence of “@”, number of dots, and SSL certificate status were extracted. Random Forest achieved the highest accuracy (~97%), but the model had limited adaptability to new phishing strategies. The absence of real-time detection and hybrid feature inclusion highlights opportunities for improvement.

4. Research Gap

1. **Static Feature Dependence:** The model relies solely on URL-based features, ignoring website content and metadata.
2. **No Real-Time Detection:** The approach cannot identify newly emerging phishing websites.
3. **Dataset Limitations:** The dataset lacks diversity for region-specific or zero-day attacks.
4. **Limited Hybridization:** Existing models do not combine multiple model strengths for enhanced performance.

---

5. Proposed Methodology

A hybrid ensemble model combining both URL and content features was developed to address these gaps.

Model Workflow

1. **Dataset Collection**
2. Dataset used: Phishing Website Dataset (UCI Repository)

3. Dataset Link

4. **Feature Extraction**

5. URL-based: length, special characters, domain age, prefix/suffix, etc.

6. Content-based: presence of login forms, external links, script tags.

7. **Preprocessing**

8. Handling missing values, scaling numeric features, and encoding labels.

9. **Model Training**

10. Models used: Decision Tree, Random Forest, Logistic Regression.

11. Ensemble: Voting Classifier combining strengths of individual models.

12. **Evaluation**

13. Metrics: Accuracy, Precision, Recall, F1-Score, Confusion Matrix.

14. **Enhancement**

15. Integration of hybrid features and ensemble modeling for improved detection performance.

---

6. Implementation Details

Implementation was performed using Google Colab with Python. Key libraries include `pandas`, `numpy`, `scikit-learn`, `matplotlib`, and `seaborn`. The code and notebook are available on GitHub: [GitHub Repository Link Here]

Sample Output: - Random Forest Accuracy: 97.3% - Logistic Regression Accuracy: 95.1% - Hybrid Voting Ensemble Accuracy: 98.6%

---

7. Results and Discussion

The proposed hybrid ensemble model demonstrates superior accuracy and robustness compared to individual classifiers. Incorporating both URL and content-based features significantly enhances phishing detection capability. Future enhancements could include real-time integration with threat intelligence feeds.

Model	Accuracy	Precision	Recall	F1-Score
Decision Tree	95.8%	0.96	0.95	0.95
Random Forest	97.3%	0.97	0.97	0.97
Voting Ensemble (Proposed)	98.6%	0.99	0.98	0.98

---

8. Conclusion

This project successfully replicates and enhances an ML-based phishing detection model. The hybrid ensemble method achieves higher accuracy and reliability than traditional approaches. Future work may focus on integrating real-time threat intelligence and browser-based detection systems to address zero-day phishing threats.

---

9. References

1. Mohammad, R., Thabtah, F., & McCluskey, L. (2015). Phishing Websites Dataset, UCI Machine Learning Repository.
2. Research Paper: Phishing Website Detection using Machine Learning Algorithms (IEEE, 2022).
3. Scikit-learn documentation: https://scikit-learn.org/
4. Google Colab: https://colab.research.google.com/

Submitted by:
B VISHNUVARDAN
Roll No: 160123737034