Project Proposal

Project Title :

Detecting Phishing Websites Using Machine Learning and URL-Based Features

Introduction :

Phishing attacks remain a prevalent and dangerous cybersecurity threat, where malicious actors deceive users into revealing sensitive information by masquerading as legitimate entities. One of the most common phishing attack vectors is the use of fraudulent websites. This project focuses on leveraging machine learning techniques to classify websites as phishing or legitimate using features extracted from URLs. By focusing on this lightweight and easily accessible information, we aim to build an efficient and scalable model that can be integrated into web browsers or email clients for real-time phishing detection.

Literature Review :

1. Abdelhamid, N., Ayesh, A., & Thabtah, F. (2014). “Phishing detection based on hybrid feature selection approach.” International Journal of Computer Applications.
This paper demonstrates how feature selection enhances phishing detection accuracy when machine learning models are applied to URL-based and site-based features.

2. Rao, R. S., & Ali, S. (2015). “Phishing websites detection using machine learning.” Procedia Computer Science.
Explores a range of ML classifiers and URL-based features, validating their effectiveness for phishing detection.

3. Mohammad, R. M., Thabtah, F., & McCluskey, L. (2015). “Intelligent phishing detection system for e-banking using fuzzy data mining.” Expert Systems with Applications.
Investigates fuzzy and rule-based systems in phishing detection and emphasizes the usefulness of feature-level analysis.

Dataset to Be Used :

We will use the Phishing Websites Dataset available on the UCI Machine Learning Repository. This dataset contains 30+ features extracted from URLs and web page metadata, labeled as either phishing or legitimate.

Source: UCI Phishing Websites Dataset
Format: CSV
Features: Includes characteristics like presence of “@” symbol, length of URL, SSL certificate status, domain registration length, etc.
Label: Phishing (1) or Legitimate (-1)

Proposed Methodology & Approach :

1. Data Preprocessing :
- Load and clean the dataset.
- Encode categorical labels and normalize numerical features.
- Handle missing values if present.
- Split dataset into 80% training and 20% testing sets.

2. Model Building :
- Implement and compare multiple machine learning algorithms:
  - Logistic Regression
  - Decision Trees
  - Random Forests
- Use Scikit-learn for model development and experimentation.

3. Attack Simulation :
- Simulate simple evasion techniques (e.g., modifying URL length or obfuscating characters) to test model robustness.
- Measure changes in prediction accuracy under such conditions.

4. Evaluation :
- Evaluate models using: Accuracy, Precision, Recall, F1 Score, Confusion Matrix.
- Use K-fold cross-validation for result reliability.
- Analyze feature importance to explain decisions.

Expected Results & Evaluation :

Expected Contribution:
The project will deliver a lightweight, explainable, and highly accurate phishing detection model that can be applied in real-time settings without relying on heavy feature extraction or third-party services.

Key Performance Indicators (KPIs):
- Accuracy ≥ 90%
- Precision and Recall ≥ 85%
- False Positive Rate < 10%
- Time to predict per URL ≤ 50 ms
- Feature importance visualization to support interpretability

Tools & Software :

- Programming Language: Python
- Frameworks: Scikit-learn, Pandas, NumPy
- Environment: Jupyter Notebook
- Visualization Tools: Seaborn, Matplotlib

Research Problem :

Phishing attacks using deceptive URLs continue to bypass traditional detection systems. Many existing solutions rely on blacklists or complex content inspection, which are often too slow or not generalizable.

Research Question :

Can a machine learning model trained solely on URL-based features accurately and efficiently classify phishing websites?

Hypothesis :

URL-based features alone are sufficient to build an effective phishing detection model using traditional machine learning techniques.

Hypothesis :

Cyber defense using AI