ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 11, Issue 3, March 2026

Automated Phishing Email and Url Detection System Using Machine Learning and Gemini API

[1] K.Jeevitha, [2] M.Jayashree, [3] J.Abinaya, [4] M.Kamalika, [5]Dr.N.Shunmuga Karpagam
[1] [2] [3] [4] Dept. of Computer Science and Engineering, Er. Perumal Manimekalai College of Engineering, Hosur, Tamilnadu, India.
[5] Assistant Professor, Department of Computer Science and Engineering Er. Perumal Manimekalai College of Engineering, Hosur

Abstract: ***This project titled "Automated Phishing email and url detection system" focuses on building an intelligent security solution that helps users identify harmful emails and suspicious web links before any damage occurs, the proposed system uses machine learning techniques along with feature extraction methods to analyze the content of emails and the structure of urls. Various characteristics such as keywords, sender details, link patterns, and text structure are examined to decide whether the given input is safe or malicious. The system is designed to be simple, user-friendly, and efficient so that even non-technical users can benefit from it. By automating the detection process, the project aims to reduce human errors and improve overall cyber safety. The final outcome is expected to be a reliable tool that significantly reduces the risk of phishing attacks and malicious website access***

Keywords : Phishing detection ,Gemini API ,LLM ,Naive bayes ,logistics regression, Tokenization, TF-IDF, Real-time Detection

I. INTRODUCTION

Email is one of the most common way to communicate with people in today's digital world. It's used for both business and personal communication and business interaction. However emails are used by so many people because of its major business needs and also as a personal medium,also it is a major target for cyber attacks. Phishing emails uses people's trust by pretending to be real businesses, coworkers, or service providers. These emails often have urgent messages, misleading links, fake security alerts, or links that aren't real that make people feel like they need to act immediately Most traditional email security systems use keyword matching, blacklists, or predefined filtering rules that have already been set up. These methods can find threats that are already known, but they don't work against new phishing attacks that use changed language and social engineering techniques. Because attackers change their attacking methods often, current security systems fail to recognize when new attacks are happening. Machine learning is another option because it lets systems learn patterns directly from data. Machine learning models can find strange patterns or text that set phishing emails apart from real ones, rather than just following the rules that are already in place. This project is about making a phishing email detection system that uses machine learning to look at the content and URLs of emails to see if they are safe or not. The goal is to make email safer and cut down on the number of phishing attacks that users are exposed to.

II. LITERATURE SURVEY

[1]Rishikesh Mahajan, Irfan Siddavatam , International Journal Computer Applications , October 2018. “Phishing Website Detection using Machine Learning Algorithms”. This paper says how Phishing is the most straightforward method of receiving sensitive information from unsuspecting consumers. The goal of attackers is to get sensitive data such as usernames, passwords, and bank account numbers. People working in cyber security are increasingly seeking for reliable and consistent detection strategies for phishing websites. The purpose of this work is to use machine learning to detect phishing URLs by extracting and evaluating various aspects of authentic and phishing URLs. Phishing websites are detected using Random Forest ,Decision Tree, algorithms. The goal of the study is to detect phishing URLs and reduce the attacks using machine learning method by analysing each algorithm's accuracy rate. Using machine learning technologies, this article tries to improve the detection mechanism for phishing websites. In addition, the results prove that classifiers perform better when more data is utilized as training data

[2] Large Language Models for Cybersecurity: A Systematic Review by Zhang et al. (2023) presents a comprehensive review of the role of Large Language Models (LLM) in improving cybersecurity applications. The study analyzes how advanced natural language processing techniques can be applied to detect and overcome cyber threats such as phishing attacks. . One of the key findings of the paper is that LLMs have strong semantic understanding capabilities, allowing them to analyze the context, intent, and meaning of textual data rather than relying only on keyword-based detection methods. This makes them identifyphishing emails and

misleading communication patterns that traditional rule-based systems often fail to detect. However, the authors also discuss certain challenges including high processing demand, potential bias in training datasets. Overall, the paper features that integrating LLM technologies into cybersecurity frameworks can enhance threat detection and response mechanisms, making them highly relevant for modern phishing detection systems

III. PROBLEM STATEMENT

Phishing emails and malicious URLs have become major cybersecurity with the rise in the number of internet users and online services. Phishing emails and malicious URLs are used by attackers to trick the victim into revealing their sensitive information such as usernames, passwords, credit card information, and so on. Phishing attacks result in huge losses in terms of money, identity, and privacy for the victim.

The existing security measures such as junk mail filters and rule-based detection tools that are not effective in detecting phishing emails and malicious URLs. Phishing attackers are changing their tactics by sending emails with complicated URLs, short URLs, spoofed email addresses, and socially engineered emails that ignore conventional email filters and detection tools. Manually detecting malicious emails and URLs by the user is not a reliable option since the user may not be aware of the tactics used by attackers to trick the victim.

There exists a great need for the development of a smart and intelligent system that can efficiently detect phishing emails and malicious URLs exactly. This project aims at detecting phishing emails and malicious URLs efficiently by applying machine learning algorithms to solve the problem.

IV. PROPOSED METHODOLOGY

The Phishing Email and Malicious URL Detection System is divided into several functional modules. Each module performs a specific task to ensure accurate and efficient detection of phishing attacks.

1: User Input

This module allows the user to provide input in the form of email content or a URL. The system accepts text-based email messages and website links for analysis. Verification is performed to ensure that the input is in the correct format before the process done

2: Data Preprocessing

The preprocessing module cleans and prepares the input data for analysis. It removes unwanted characters, HTML tags, punctuation, and stop words from email content. The dataset was pre-processed by converting all URLs into a consistent, standard format. This step improves the accuracy and efficiency of feature extraction and classification.

3: Feature Extraction

In this module, important features are extracted from the preprocessed data. For emails, features include suspicious keywords, sender information, malicious entries and link count. For URLs, features include URL length, presence of special characters, presence of keywords use of IP addresses, symbol changes and domain details. These features help identify phishing patterns.

4: Machine Learning Model

This module applies machine learning algorithms trained on labeled phishing and legitimate datasets. The model learns patterns and combinations from the extracted features to distinguish between malicious and safe inputs.

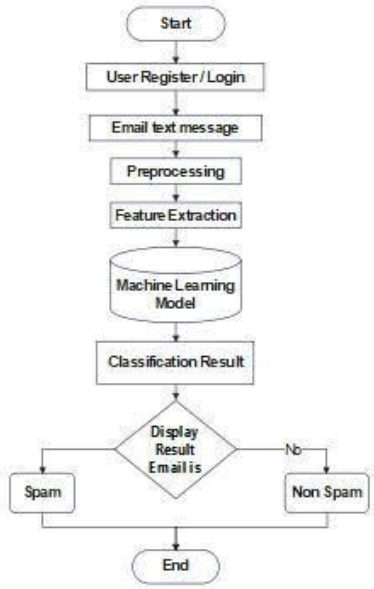
5: Classification

The classification module uses the trained model to test whether the given input is phishing or legitimate. The prediction is based on learned patterns and calculated probabilities.

6: Result Display

This module displays the final classification result to the user. If phishing is detected, a warning message is shown; otherwise, the input is marked as safe. The output is presented in a clear and user-friendly format.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 11, Issue 3, March 2026

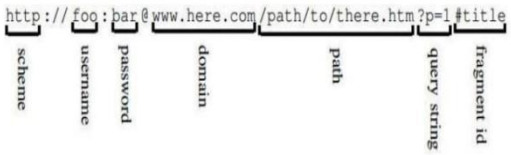


V. PARAMETER USED

A. Email-Based Parameters

- Presence of phishing-related keywords
- Sender email domain mismatch
- Use of urgent or threatening words
- Number of hyperlinks in email
- Presence of HTML forms
- Use of shortened URLs

B. URL-Based Parameters



- Length of the URL
- Number of dots (.) in URL
- Presence of IP address instead of domain name
- Use of special characters (@, -, %)
- HTTPS availability
- Domain age and reputation

C. Text Processing Parameters

- Token count
- Term Frequency (TF)
- Inverse Document Frequency (IDF)
- N-gram features

D. Model Parameters

- Training and testing data ratio
- Learning rate
- Kernel type (for SVM)
- Maximum depth (for Decision Tree)

VI. ALGORITHM USED

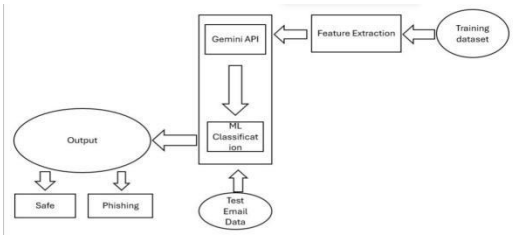
The Phishing Email and Malicious URL Detection System uses machine learning algorithms to classify inputs as phishing or legitimate. These algorithms are chosen for their effectiveness in text and URL-based classification tasks.

1. Naïve Bayes Algorithm
Naïve Bayes is a probabilistic classification algorithm based on Bayes' Theorem. It assumes independence among features and calculates the probability of an email or URL being phishing based on feature occurrence.
Reason for Selection:
Fast and efficient
Suitable for large datasets

2. Support Vector Machine (SVM)
Support Vector Machine is a supervised learning algorithm that separates phishing and legitimate data using an optimal hyperplane. It performs well in high-dimensional feature spaces.
Reason for Selection:
High classification accuracy
Effective for complex patterns
Suitable for URL structure analysis

3. Logistic Regression
Logistic Regression is a binary classification algorithm that predicts the probability of an input being phishing or legitimate.
Reason for Selection:
Simple and interpretative
Efficient for real-time systems
Produces probability-based outputs

4. Decision Tree (Optional)
Decision Tree uses rule-based decisions to classify data based on feature conditions.
Reason for Selection:
Easy to understand
Visual representation of decisions.

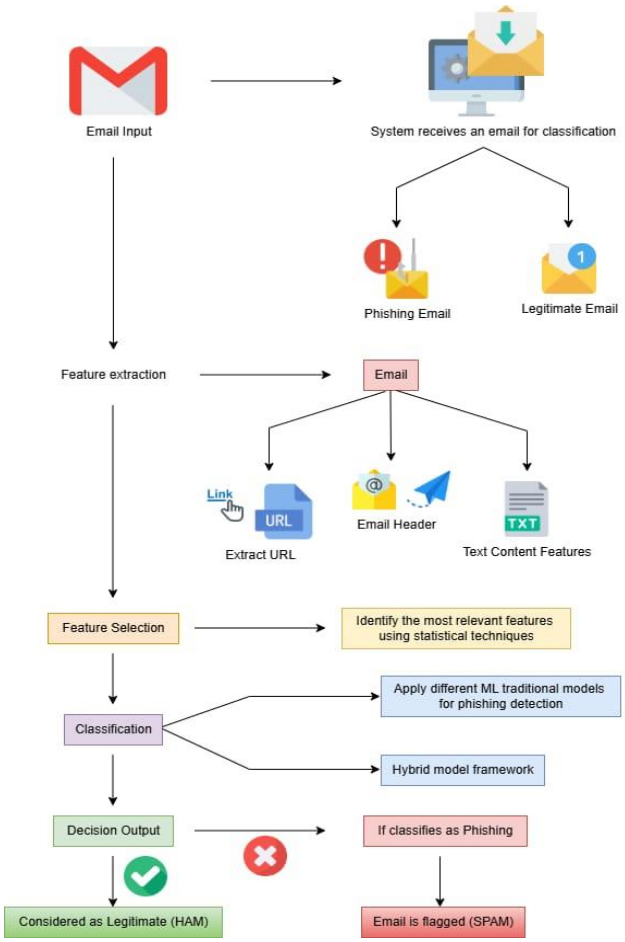


VII. EXPERIMENTAL EVALUATION

The dataset used in the Phishing Email and Malicious URL Detection System consists of labeled email messages and URLs categorized as phishing or legitimate. The data is collected from publicly available cybersecurity datasets and trusted online sources. It includes real-world phishing samples as well as genuine emails and safe website links to ensure balanced learning. Each email sample contains attributes such as senders address, email subject, body content, attachments, and embedded links. URL samples include features like URL length, number of special characters, presence of IP addresses, domain age,

subdomains path and parameters and protocol information. Before training, the dataset undergoes preprocessing to remove the noise and irrelevant data.

The dataset is divided into two parts : training data and testing data. Typically, 80% of the dataset is used for training the machine learning models, while the remaining 20% is used for testing and validation. This split helps evaluate the performance and accuracy of the proposed system. A well-prepared dataset improves noise labeling ,detects accuracy and reduce error in results



VIII. ADVANTAGE

- Provides automated detection of phishing emails and malicious URLs
- Reduces dependency on user awareness and manual inspection
- Improves detection accuracy using machine learning techniques
- Identifies both known and unknown phishing patterns
- Reduces false positives and false negatives compared to rule-based systems
- User-friendly interface with quick response time
- Scalable and adaptable for real-world security systems

IX. LIMITATION

- Requires large and updated datasets for better accuracy
- Performance depends on the quality of training data
- May not detect completely new phishing techniques initially

- Limited effectiveness against highly sophisticated social engineering attacks

IX. CONCLUSION

The Phishing Email and Malicious URL Detection System provides an effective solution to detect and prevent phishing attacks using machine learning techniques. By analyzing email content and URL features, the system accurately classifies inputs as phishing or legitimate. It reduces user risk, improves cybersecurity, and overcomes the limitations of traditional rule-based systems. With future enhancements, the system can be expanded into a real-time security solution suitable for widespread deployment in modern digital environments.

XI. FUTURE WORK

- Integration of deep learning models for improved accuracy
- Real-time phishing detection using browser extensions
- Multi-language phishing email detection
- API integration for live URL reputation checking
- Cloud-based deployment for large-scale usage
- Continuous learning models to adapt to new phishing attacks

Reference

Research Papers & Articles on Phishing Detection
1.Comparative analysis of ML algorithms
Naïve Bayes, SVM & Logistic Regression for phishing email detection. Comparative Analysis of ML Algorithms for Text-based Phishing Detection (IJRASET)
2.High-accuracy ML approach for phishing websites
Uses multiple classifiers including SVM, Random Forest, XGBoost. Machine-Learning-based Phishing Website Detection Method (ScienceDirect)
3.Phishing URL detection using ML
Feature extraction and classification using machine learning. Phishing URL Detection Using Machine Learning (IJRASET)
4.ML-based phishing detection system using Random Forest
URL feature analysis to distinguish between phishing and safe sites. Machine Learning-Based Phishing Detection System (IJISAE)
5.Heuristic ML approaches for phishing across email & web
Combines heuristics with machine learning for strong detection accuracy. Heuristic ML for Phishing Threats Across Platforms (Frontiers)
6.Systematic literature review on phishing detection techniques
Covers list-based, heuristic, ML and deep learning methods. Systematic Literature Review on Phishing Detection Techniques (ScienceDirect)
7.ML-based phishing URL analysis survey
Analysis of multiple classifiers and accuracy comparisons. Phishing Detection Using ML-based URL Analysis – Survey (IJERT)
8.Deep learning & NLP for phishing detection
Explores neural techniques including CNN & RNN for phishing detection. Phishing Email Detection Model Using Deep Learning (MDPI)
9.Transformer-based phishing detection research
Integrates semantic and URL structure analysis for advanced detection. Dual-Path Phishing Detection (arXiv)
10.Survey of state-of-the-art classifiers
Analyses Bayesian, non-Bayesian & deep learning detectors. Phishing Detection Techniques Survey (arXiv)