

Email Spam Detection Using Machine Learning

Chandana K J , Mr.Vinay Patel G L

P.G. Student, Department of Master of Computer Applications, BIET, Davangere-577004.

kjchandana77@gmail.com, Davangere , Karnataka, India.

Assistant Professor, Department of Master of Computer Applications, BIET, Davangere-577004.

Vinaypatel.gl@gmail.com, Davangere, Karnataka, India.

ABSTRACT

Phishing, spoofing, and business email compromise threaten people and businesses globally. Traditional rule-based spam filters cannot detect sophisticated social engineering fraud efforts. Recent machine learning advances allow intelligent detection systems to identify fake emails using textual patterns, metadata elements, and behavioural cues. This research proposes a machine learning-based email fraud detection methodology using text preparation, feature extraction, and ensemble classification. The suggested system classifies emails as real or fraudulent using natural language processing and supervised learning. Experimental results show that phishing email detection is more accurate and recall is higher than conventional filtering. Enterprise email security solutions can scale with the framework.

Keywords: *Email Fraud Detection, Phishing Detection, Machine Learning, Natural Language Processing, Cybersecurity, Classification*

I. INTRODUCTION

Email is a popular communication channel, making it a cybercriminal target. Phishing attacks, faked emails, and business email compromise attempts can cause financial loss and data breaches. Traditional email filters use predefined rules and blacklists, which are useless against developing attack techniques.

Recent machine learning advances have improved cybersecurity by enabling adaptive

and data-driven detection. Machine learning classifiers outperformed spam filtering in phishing email detection in 2023 and 2024 [1], [2]. Advanced feature extraction approaches using textual, header, and URL attributes [3].

In cybersecurity, ensemble learning and deep learning-based text modelling have shown strong generalisation [4]. Inspired by these advances, this paper presents a machine learning-based email fraud detection framework for strong and scalable email security.

II. RELATED WORK

The 2023–2026 research shows significant phishing and email fraud detection system advancements. The supervised machine learning system [1] used lexical and structural email features to detect phishing with excellent accuracy. For better fraud categorisation, [2] presented a hybrid methodology including natural language processing and metadata analysis.

Email content analysis uses deep learning models like recurrent neural networks and transformer-based architectures. Contextual embedding models increased phishing detection in 2024 [3]. Ensemble learning approaches with several classifiers were investigated in [4], improving adversarial resistance.

Real-time deployment and scalability are also researched. For enterprise email filtering, [5] developed lightweight categorisation models. In [6], Explainable AI methods for cyber

security applications improved automated fraud detection system transparency confidence.

These advances lay the groundwork for a powerful machine learning-based email fraud detection system.

III. METHODOLOGY

The proposed framework includes dataset prep, preprocessing, feature extraction, model training, evaluation, and deployment.

The dataset includes real and fraudulent email samples. Email subject, body text, sender address, URL links, header metadata, and indicators.

Remove stop words, tokenise, stem, and convert text to numbers using TFIDF and word embeddings during data preprocessing. Extracted URL features include domain age, suspicious keywords, and hyperlink frequency. Header analysis finds sender abnormalities.

Textual and structural metadata characteristics are used in feature engineering. The dataset includes training, validation, and test sets. The class imbalance is handled via oversampling or learning.

Logistic Regression, SVM, Random Forest, and Gradient Boosting are used. The best model is found by cross validating hyperparameter adjustment.

The system workflow is described as follows:

- Email Dataset Collection
- Text and Metadata Pre processing
- Feature Extraction and Encoding
- Model Training and Validation
- Fraud Classification
- Performance Evaluation

Accuracy, precision, recall, F1score, confusion matrix, and ROC Curve Area are evaluation metrics. Recall is prioritised to reduce fraud detection false negatives. Particular emphasis is placed on recall to minimize false negatives in fraud detection.

IV. RESULTS AND DISCUSSION



Figure : Form to sign up



Figure : Form to log in



Figure: A suspicious or phishing E-mail



Figure : E-mail detected as Fraud

Ensemble-based models like Random Forest and Gradient Boosting outperform linear classifiers in email fraud detection. The model detects phishing attempts with excellent precision and recall, minimising false alarms.

Suspicious URLs, uncommon sender domains, and certain keyword patterns improve classification performance, according to feature importance analysis.

Enterprise email servers can classify in real time with lightweight deployments. However, adversarially crafted phishing emails continue to challenge models, requiring constant adjustments.

The results show that machine learning improves email fraud detection.

V. CONCLUSION AND FUTURE WORK

This paper introduced a machine learning-based email fraud detection methodology using text processing and metadata analysis. Proposed system has good classification accuracy and robust detection.

Deep learning-based transformer models for contextual understanding, federated learning for privacy-preserving collaboration across organisations, real-time URL threat intelligence feeds, and adversarially robust training strategies are future goals.

VI. REFERENCES

- [1]Chen et al., “Machine Learning-Based Phishing Email Detection Using Textual and Structural Features,” IEEE Access, 2023.
- [2]M. Kumar et al., “Hybrid Email Fraud Detection Using NLP and Metadata Analysis,” IEEE Transactions on AI, 2024.
- [3]Lin Zhang et al., “Contextual Embedding Models for Phishing Detection,” IEEE Transactions on Information Forensics and Security, 2024.
- [4]Patel et al., “Ensemble Learning for Cybersecurity Email Classification,” IEEE Access, 2025.
- [5]H.Lee et al., “Scalable Machine Learning Models for Enterprise Email Security,” IEEE Internet of Things Journal, 2025.
- [6]A. Singh et al., “Explainable AI Techniques for Cyber Threat Detection,” IEEE Transactions on Neural Networks and Learning Systems, 2026.
- [7]T.Nguyen et al., “Robust Fraud Detection Systems Using Supervised Learning,” IEEE Access, 2023.
- [8]P.Wang et al., “Advanced Feature Engineering for Phishing Email Classification,” IEEE Transactions on AI, 2024.
- [9]K.Roy et al., “RealTime Email Threat Detection Using Optimised Classifiers,” IEEE Access, 2025.
- [10]J.Brown et al., “Adaptive Cybersecurity Systems Using Machine Learning,” IEEE Access, 2026.
- [11]Verma et al., “Deep Learning Approaches for Email Spam and Fraud Detection,” IEEE Access, 2024.
- [12]“PrivacyPreserving Machine Learning for Secure Email Systems,” IEEE Transactions on Information Forensics and Security, 2025.