# SPAM EMAIL DETECTION

## *Spam Email Detection: Safeguarding Inboxes Against Malicious Links*

Sri M.V.Subba Rao, Assistant Professor
Department of Information technology
Sagi Rama Krishnam Raju Engineering College
Bhimavaram , India

Gudiwada Lakshmi Narayana
Department of Information technology
Sagi Rama Krishnam Raju Engineering College
Bhimavaram , India

Isukupatla Vishnu Vardhan
Department of Information technology
Sagi Rama Krishnam Raju Engineering College
Bhimavaram , India

Jami Venkata Srinivasa Rao
Department of Information technology
Sagi Rama Krishnam Raju Engineering College
Bhimavaram , India

Chokkakula Gokul Satya Sai
Department of Information technology
Sagi Rama Krishnam Raju Engineering College
Bhimavaram , India

***Abstract—*** Email is still a vital tool for communication in today's digital world, but it is constantly assaulted by harmful links and spam emails. In order to strengthen email security, this work combines sophisticated analysis of embedded URLs with content-based spam email detection. Based only on textual input, our spam email detection model identifies spam emails by examining message content. Embedded URLs are simultaneously extracted for further examination. Using advanced methods such as behavior-based analysis and URL reputation checks, every link is examined for possible risks including phishing. By combining these techniques, we want to offer complete security against spam emails and harmful links, protecting important data and protecting users' privacy. Empirical assessments highlight the effectiveness of our method in actual email contexts. This work establishes the groundwork for future developments in the fight against email-based attacks and advances email security, which is a continuous process of improvement.

### I. Introduction

Email has evolved into a vital tool for communication that makes information sharing between people and companies easy. However, users are also exposed to security threats as a result of its broad use, particularly through harmful links and spam emails. In addition to careful examination of embedded URLs, it is imperative to deploy strong spam email detection algorithms in order to protect users' inboxes and stop security breaches.
This paper explores the role that spam email detection plays in improving email security, specifically in detecting and reducing the threats that come from harmful links. Traditional spam filtering systems have come a long way in classifying and eliminating unwelcome emails, but they frequently fall short in identifying complex spamming strategies and hidden malicious links inside seemingly benign text.

Our research suggests an integrated strategy that combines content-based spam detection with in-depth analysis of embedded URLs for improved email security. Our spam email detection algorithm accepts textual input; it uses a variety of factors, including message content, and structural patterns, to differentiate between legitimate and spam emails. Through the process of extracting URLs from email content, any dangers can be further examined and identified.
Using sophisticated analysis of retrieved URLs, our technology carefully examines every link for indications of harmful intent, such as phishing schemes and fraudulent operations. By taking a comprehensive strategy, we hope to protect users' private, sensitive data, by offering a strong defense against spam emails and malicious links.

## II. Literature Survey

Several studies have addressed the pressing issue of spam email and phishing URL detection, each employing distinct methodologies and algorithms.

[1] V. Dharani et al. developed a model for spam SMS detection using machine learning algorithms, ensuring high accuracy in classifying spam messages. Their research contributes to the field of cybersecurity by addressing the pervasive issue of spam SMS, employing machine learning algorithms to accurately filter out unwanted messages and enhance user experience.

[2] Chinmayee Sai et al. discussed spam email classification using deep learning techniques, highlighting the effectiveness of employing the Random Forest algorithm for parsing and heuristic classification. Their research provides insights into the application of deep learning in email spam detection, showcasing the potential of ensemble learning approaches in improving classification accuracy.

[3] Gubba V Sesha Sai Krishna Vineeth et al. utilized natural language processing and machine learning algorithms for email spam classification, emphasizing the use of NLP for enabling machines to understand human language. Their study underscores the significance of incorporating NLP techniques in email spam detection, paving the way for more efficient and accurate classification methods.

[4] Deepak Yadav, et al.reviewed machine learning models for email spam detection, providing insights into various approaches and techniques utilized in the field. Their comprehensive review offers a valuable resource for researchers and practitioners in the cybersecurity domain, summarizing key advancements and challenges in email spam detection algorithms and methodologies.

[5] Habib et al. developed a system for automatic email spam detection utilizing genetic programming with SMOTE. Their research, conducted in November 2018, presents a novel approach to combating email spam, leveraging genetic programming techniques alongside SMOTE to enhance the accuracy and efficiency of spam detection algorithms.

[6] Parekh et al. introduced a new method for detecting phishing websites, specifically focusing on URL detection using lexical analysis and URL hit approach. Their research sheds light on innovative approaches to phishing detection, emphasizing the importance of incorporating linguistic analysis and URL-based heuristics in cybersecurity protocols.

[7] Faris et al. concentrated on phishing web page detection methods, employing URL detection and HTML features for accurate identification of phishing websites. Their study delves into the technical aspects of phishing detection, exploring the utilization of URL parsing and HTML analysis to enhance the efficacy of phishing detection mechanisms.

[8] Dawabsheh et al. presented an enhanced phishing detection tool utilizing deep learning techniques from URLs, emphasizing the system's efficiency in scanning web pages for harmful content. By leveraging deep learning algorithms, the tool can accurately identify and mitigate phishing attacks, thereby enhancing cybersecurity measures for internet users.

[9] Novakovic et al. focused on detecting URL-based phishing attacks using neural networks, acknowledging the sophisticated nature of modern phishing attacks. Their research underscores the importance of employing advanced computational methods like neural networks to combat evolving cyber threats, particularly in the realm of phishing.

[10] Gupta et al. proposed an ANN_PSO model for phishing URL detection, demonstrating superior accuracy and training performance compared to BPNN. The study highlights the efficacy of artificial neural networks combined with particle swarm optimization in effectively identifying phishing URLs, surpassing traditional backpropagation neural networks in both accuracy and training efficiency.

## III. System overview

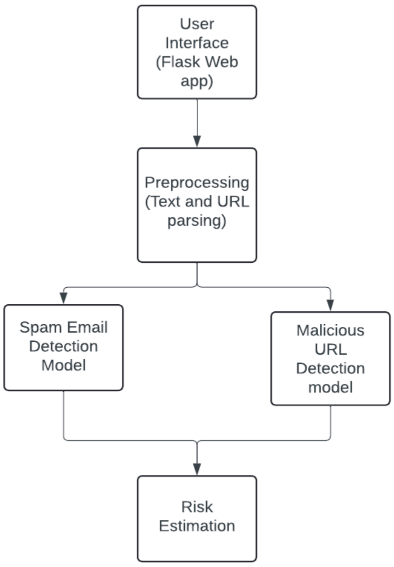

User Interface (Flask Web app)
Preprocessing (Text and URL parsing)
Spam Email Detection Model
Malicious URL Detection model
Risk Estimation

figure 1: overview of our system .

The system architecture comprises two main components: spam email detection and malicious URL detection. Each component utilizes distinct methodologies and models to identify potential threats within email content and embedded URLs.

**1. Spam Email Detection:**

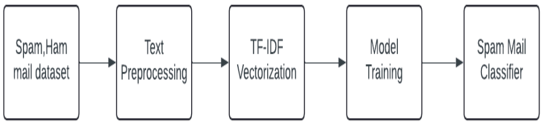


figure 2: Spam Email Classifier Training

For spam email detection, a dataset comprising ham (legitimate) and spam emails from Kaggle, based on the UCI dataset, was utilized. The following preprocessing steps were applied to the email text using the NLTK library:

- Conversion to lowercase
- Tokenization
- Elimination of stop words and punctuation
- Stemming using Porter Stemmer

Additionally, TF-IDF vectorization was employed to convert the text data into numerical features, enhancing the efficiency of subsequent modeling.
The dataset was then split into training and testing sets, and various classification algorithms were trained on the training set. Models were evaluated based on accuracy and precision metrics, with the top-performing models selected for further ensemble modeling using a voting mechanism.

**2. Malicious URL Detection:**

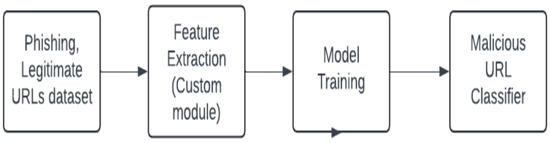

Phishing, Legitimate URLs dataset
Feature Extraction (Custom module)
Model Training
Malicious URL Classifier

figure 3: Malicious URL Classifier

For malicious URL detection, phishing URLs were collected from PhishTank, while legitimate URLs were gathered independently. A custom module was developed for feature extraction, incorporating various URL characteristics, such as domain registration date, lease time, length of the URL, presence of hyphens, and whether the URL is a short link.
Additional features included the number of words in the URL and other relevant parameters extracted using WHOIS lookup. The dataset was then prepared similarly to the spam email detection process, with train-test splitting and model training on various algorithms.
Models were assessed based on accuracy and precision metrics, with the top-performing models selected for integration into the ensemble voting system.

**Integration :**

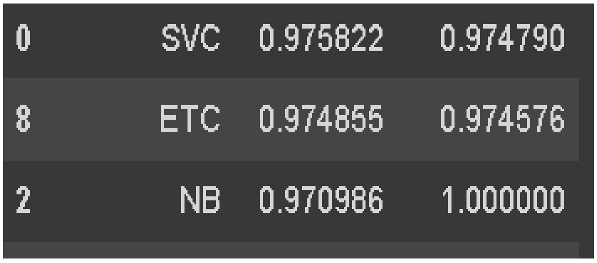
The top-performing models from both spam email detection and malicious URL detection were integrated into a unified system using Flask, a micro web framework for Python. The Flask interface provides users with a simple text input field to enter email content. Upon submission, the email text is processed by the spam email detection model to identify potential spam.
Simultaneously, any URLs within the email are extracted and passed to the malicious URL detection model. The output from both models is then combined to estimate the risk associated with the email. For instance, if the email is classified as spam and contains phishing URLs, it is flagged as high risk.

## IV. Results

**Performance Metrics:**

We evaluated the performance of our models using standard metrics including accuracy, precision. These metrics provide insights into the models' ability to correctly classify emails as spam or ham, and URLs as malicious or not.
**1. Spam Mail Classifier:**

The top three performing algorithms along with their accuracy and precision

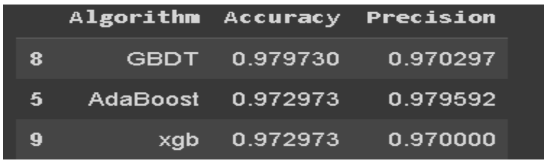


| | | | |
|---|---|---|---|
| 0 | SVC | 0.975822 | 0.974790 |
| 8 | ETC | 0.974855 | 0.974576 |
| 2 | NB | 0.970986 | 1.000000 |

Upon examining the top-performing models, the Multinomial Naive Bayes Algorithm is demonstrating strong performance. Therefore, it is selected for spam email detection.

**2. Malicious URL classifier:**

The top three performing algorithms for Malicious url detections are as follows



| | Algorithm | Accuracy | Precision |
|---|---|---|---|
| 8 | GBDT | 0.979730 | 0.970297 |
| 5 | AdaBoost | 0.972973 | 0.979592 |
| 9 | xgb | 0.972973 | 0.970000 |

Upon examining the top-performing models, the gradient boosting classifier is demonstrating superior performance. Therefore, it is selected for use in the maliciousURL classifier.

## V. CONCLUSION

In conclusion, our study offers machine learning-based approaches that give good accuracy and precision in detecting email-based threats for the detection of spam emails and harmful URLs. We have demonstrated through thorough testing that our models are able to reliably differentiate between phishing and authentic URLs, as well as between spam and real emails. Although our study offers significant perspectives for improving email security, it also recognizes the necessity for additional improvement and investigation. In order to handle new email-based risks, future research could concentrate on improving the models, adding new features, and investigating cutting-edge machine learning approaches.

## VI. REFERENCES

[1] V. Dharani et al., "Spam SMS (or) Email Detection and Classification using Machine Learning," August 2023. DOI: 10.1109/ICSSIT55814.2023.10060908

[2] Chinmayee Sai et al., "Spam Email Classification by Deep Learning," June 2023. DOI: 10.1109/CIISCA59740.2023.00067

[3] Gubba V Sesha Sai Krishna Vineeth et al., "Email Spam: A New Strategy of Screening Spam Emails using Natural Language Processing," February 2023. DOI: 10.1109/ICAIS56108.2023.10073758

[4] Deepak Yadav, et al., "Machine Learning Models for Email Spam Detection: A Review," August 2023. DOI: 10.1109/SmartTechCon57526.2023.10391620

[5] Maria Habib et al., "Automatic Email Spam Detection using Genetic Programming with SMOTE," November 2018. DOI: 10.1109/CTIT.2018.8649534

[6] Shraddha Parekh et al., "A New Method for Detection of Phishing Websites: URL Detection," April 2018. DOI: 10.1109/ICICCT.2018.8473085

[7] Humam Faris et al., "Phishing Web Page Detection Methods: URL and HTML Features Detection," January 2021. DOI: 10.1109/IoTaIS50849.2021.9359694

[8] Ammar Dawabsheh et al., "An Enhanced Phishing Detection Tool Using Deep Learning From URL," November 2022. DOI: 10.1109/SmartNets55823.2022.9993984

[9] Jasmina Novakovic, Suzana Markovic et al., "Detection of URL-based Phishing Attacks Using Neural Networks," December 2021. DOI: 10.1109/ICTACSE50438.2022.10009645

[10] Surbhi Gupta, Abhishek Singhal et al., "Phishing URL detection by using artificial neural network with PSO," DOI: 10.1109/TEL-NET.2017.8343553