Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 03 Issue: 12 | Dec-2025
ISSN (O) 3107-6696

Autonomous Intelligent Detection and Continuous Protection System

Fathima Nida Zarnain[1], Ms Kavya H V[2]

[1] P.G. Student, Department of Master of Computer Applications, PES Institute of Technology and Management College, Shivamogga, India
[2] Assistant Professor, Department of Master of Computer Applications, PES Institute of Technology and Management College, Shivamogga, India

---***---

Abstract - Phishing schemes and junk emails represent a serious risk to internet users by deceiving them into disclosing confidential information. Current detection systems rely on blacklists and fixed rule-based filtering which often fail to detect newly developed malicious websites and misleading email content. This paper presents a machine learning-based intelligent system that can identify spam in emails and URLs. Preprocessing and TF-IDF vectorization are used in the process to extract features from supplied text and URLs. The inputs are classified as authentic or fraudulent using algorithms such as Random Forest and Logistic Regression. The goal of a Streamlit interface is to give users a simple interesting and easy-to-use experience. According to experimental results the recommended approach is more effective than traditional detection systems at revealing hidden phishing patterns. The developed model provides fast accurate and reliable forecasts for cybersecurity applications in real time.

KEYWORDS: Machine learning TF-IDF Streamlit email spam detection phishing detection and URL classification.

I. INTRODUCTION

Phishing and spam attacks have increased rapidly as a result of the expansion of internet services. In order to impersonate reputable organizations and obtain login credentials bank account information or other information cybercriminals frequently craft false emails and web links. Conventional detection techniques such as blacklist comparison or keyword filtering are ineffective against modern phishing strategies which are ever-evolving and employ lexical changes obfuscation and hidden links. As a result a more sophisticated system is needed that can identify dangerous content and automatically identify patterns in real data. This study suggests a unified system based on machine learning to identify malicious URLs and fraudulent email communications. The system utilises preprocessing methods to eliminate irrelevant characters, identify key textual components, and transform them into numerical features through TF-IDF vectorisation. Machine learning models are developed using extensive datasets of URLs and emails to identify distinguishing characteristics. A streamlined Streamlit interface allows for straightforward access to the system for immediate assessment of email content or URL links. The integration of preprocessing, feature extraction, and supervised learning guarantees enhanced detection precision.

The paper is organised as follows: Section II describes the literature survey and related work. The suggested systems flow and methodology are described in Section III. In Section IV experimental results are discussed. Lastly the paper is concluded in Section V.

II. LITERATURE SURVEY

Different machine learning and deep learning techniques for identifying phishing threats in web links and email exchanges have been studied by researchers. Machine learning solutions that look at lexical structures and domain patterns are used because systems that rely on rules and blacklists are unable to detect newly created phishing URLs. Email spam detection has advanced from simple keyword filtering to complex NLP techniques and TF-IDF feature extraction. Recent studies show that ML and DL models markedly exceed traditional methods in identifying harmful content.The concept of machine learning–based URL detection has been widely studied. Zou and Liu [1] proposed a lightweight ML-based system for real-time malicious URL detection using structural and lexical features. Gupta et al. [2] used character-level tokenization with Random Forest and SVM, showing improved accuracy for obfuscated URLs. Tandel and Bhatt [3] introduced LSTM architectures for phishing email classification, highlighting the benefits of capturing sequential text patterns. Shah and Patel [4] analyzed NLP preprocessing with classical ML models for email spam detection, demonstrating strong results with Logistic Regression. Kumar and Singh [5] proposed an ensemble learning approach for email filtering. Aswale and Hingmire [6] explored hybrid lexical and host-based features for malicious URL identification. Adebowale et al. [7] demonstrated that feature engineering combined with Random Forest produces robust phishing detection.

The combined limitations identified in these works include reliance on large datasets, difficulty in detecting zero-day attacks, and the need for efficient real-time deployment. These gaps motivate the proposed system.

III. METHODOLOGY

The suggested system carries out spam detection for URLs and emails in several stages. The preparation of inputs is part of the first step. Prefixes encoded characters and unnecessary symbols are removed in URLs. Regular expressions are used to remove hyperlinks numbers punctuation and unwanted elements from email content. After cleaning TF-IDF vectorization is used to convert the inputs into a numerical representation. Better classification results result from the TF-IDF models ability to capture terms that are unique and frequently occur.

Machine learning models are trained using the vectorized data in the second stage. Random Forest is used to classify URLs due to its ability to handle lexical and structural variations. For the purpose of identifying spam emails Random Forest or Logistic Regression are used and they achieve exceptional accuracy on high-dimensional text features. The trained models are stored as pkl files and integrated into an interface powered by Streamlit. The system prepares and vectorizes the input retrieves the stored model and predicts whether the content is genuine or fraudulent when a user inputs a URL or email text. Visual color signals are then used to present the outcome.

IV. EXPERIMENTAL RESULTS

Two datasets were used to test the system: an email dataset with samples of genuine and spam emails and a URL dataset with legitimate and phishing URLs. The models demonstrated consistent performance with consistent detection accuracy after preprocessing and TF-IDF vectorization. The Random Forest classifier showed a strong capacity to learn features associated with lexical patterns and was very successful in classifying URLs. Likewise, the Logistic Regression model applied for email detection showed effective differentiation between spam and genuine emails.

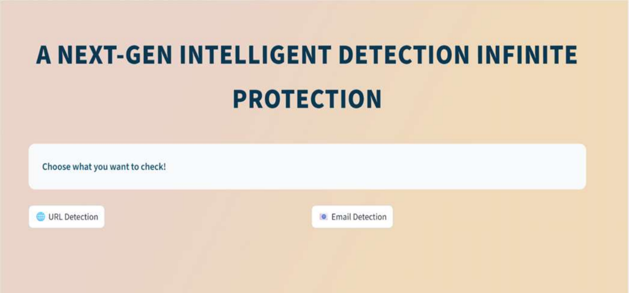

A NEXT-GEN INTELLIGENT DETECTION INFINITE PROTECTION
Choose what you want to check!
URL Detection
Email Detection

Fig 1 Home page for the detection of real and fake URLs and emails

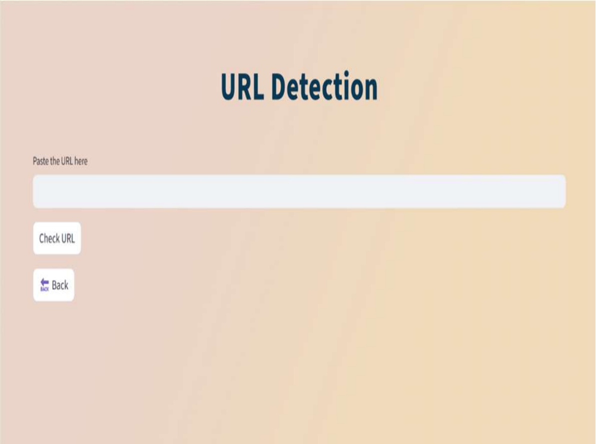


Fig 2 (a) URL detection page

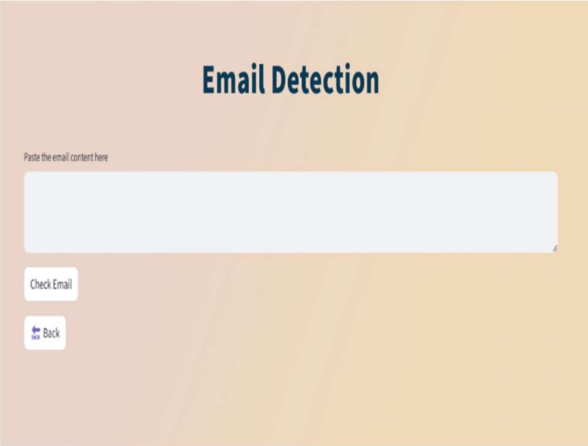
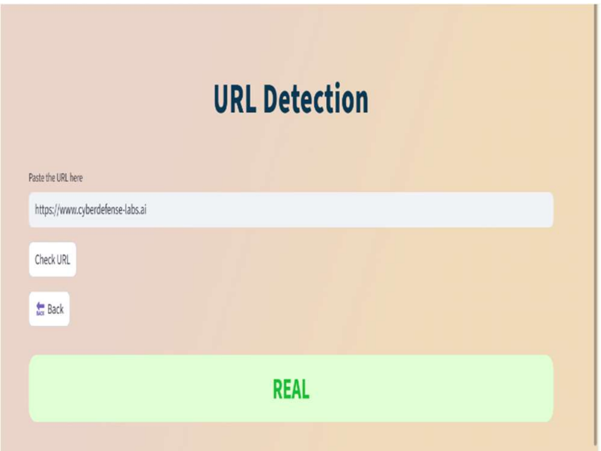


Fig 2 (b) email detection page



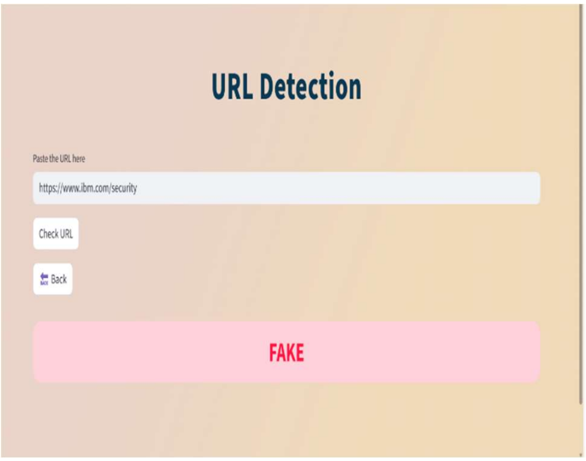
URL Detection

Paste the URL here

https://www.cyberdefense-labs.ai

REAL

Fig 3 (a) detection of real URL



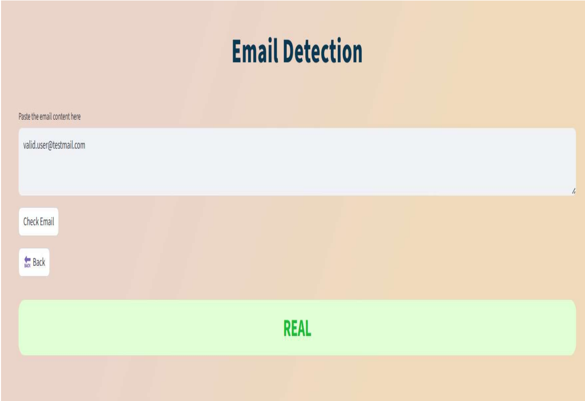
URL Detection

Paste the URL here

https://www.ibm.com/security

FAKE

Fig 3 (b) detection of fake URL



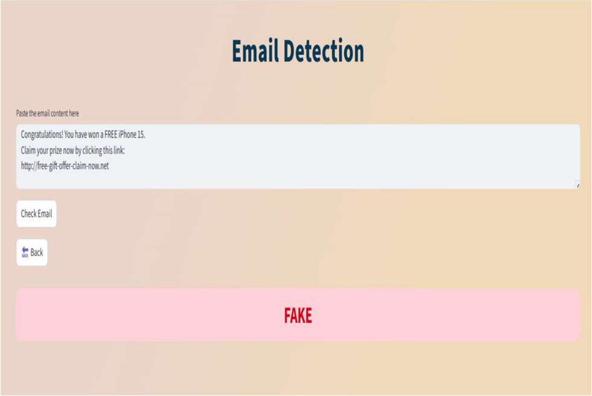
Email Detection

Paste the email content here

valid.user@testmail.com

REAL

Fig 4 (a) detection of real email



Email Detection

Paste the email content here

Congratulations! You have won a FREE iPhone 15.
Claim your prize now by clicking this link:
http://free-gift-offer-claim-now.net

FAKE

Fig 4 (b) detection of fake email

While testing in the Streamlit interface, the system accurately classified both recognized and unfamiliar URLs and email texts. Predictions held true for a variety of inputs and the interface responded in a matter of seconds. To assist users the results were displayed with clear labels and color-coded feedback. The results of the experiment show that the recommended approach works well for quickly spotting dangerous URLs and phishing emails.

V. CONCLUSION

A machine learning-based system for detecting spam emails and URLs has been released. The system classifies user-submitted URLs and email content using preprocessing TF-IDF vectorization and supervised learning techniques. Instantaneous prediction and simple interaction are made possible by the Streamlit interface. Experimental findings show that the system proficiently identifies phishing URLs and counterfeit emails with great precision. The suggested method demonstrates that ML-driven solutions surpass conventional rule-based systems, providing a dependable and scalable strategy for cybersecurity applications.

REFERENCES

[1] L. Zou and H. Liu, “Real-time malicious URL detection using lightweight machine learning models,” *IEEE Access*, vol. 8, pp. 145233–145243, 2020.

[2] H. Gupta, R. Banerjee, and S. Nandi, “Suspicious URL detection using supervised machine learning with character-level features,” *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3892–3903, 2020.

[3] Tandel and J. Bhatt, “Phishing email classification using LSTM-based deep learning models,” *Proc. IEEE ICISDS*, pp. 201–208, 2021.

[4] A. Shah and M. Patel, “Email spam detection using NLP preprocessing and supervised machine learning algorithms,” *IJACSA*, vol. 11, no. 7, pp. 334–341, 2021.

[5] P. Kumar and A. Singh, “Ensemble machine learning methods for improved email spam detection,” *Proc. ICMLC*, pp. 411–418, 2020.

[6] S. R. Aswale and P. Hingmire, “Hybrid lexical and host-based feature fusion for enhanced malicious URL detection,” *Proc. IEEE CAST*, pp. 98–104, 2019.

[7] A. Adebowale, S. Shukla, and R. Yadav, “Machine-learning based detection of phishing websites using lexical and URL feature analysis,” *IJCA*, vol. 182, no. 45, pp. 12–20, 2020.

[8] Sidharth, S. (2023). AI-Driven Anomaly Detection for Advanced Threat Detection. Volume No.4, Issue No.1 - Journal of Science Technology and Research (JSTAR) pp.266-272.

[9] Hussain, H., Kainat, M., & Ali, T. (2025). Leveraging AI and Machine Learning to Detect and Prevent Cyber Security Threats. Dialogue Social Science Review (DSSR), 3(1), 881-895.