INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 10, October 2025, pp : 1471-1473
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

PHISHGUARD-A RULE BASED EMAIL THREAT DETECTION MODEL

Abinaya S[1]

[1]B.Tech, Artificial Intelligence And Machine Learning, Sri Shakthi Institute Of Engineering And Technology, Coimbatore, Tamilnadu, India.

DOI: https://www.doi.org/10.58257/IJPREMS44411

ABSTRACT

Email phishing remains a major cyber threat, exploiting user trust to steal sensitive information such as credentials and financial data. This paper presents a rule-based phishing email detection system focused on individuals, designed to identify suspicious Gmail messages in real time using heuristic and domain-specific rules. The system analyzes email headers, body content, embedded URLs, and attachments to assign a phishing risk score. When the score surpasses a predefined threshold, immediate alerts are sent via WhatsApp using the Twilio API, ensuring users are promptly informed and can take protective action. The model offers transparency, low computational overhead, and is readily adaptable compared to data-driven approaches. Experimental evaluation demonstrates high detection accuracy and low false positives, forming a foundation for future integration with machine learning-based hybrid systems.

Keywords: Phishing Detection, Email Security, Rule-Based System, Heuristic Analysis, Real-Time Alerts, Whatsapp Notification.

1. INTRODUCTION

Email is widely used for communication but is increasingly targeted by phishing attacks designed to steal sensitive information such as passwords and financial data. In response to this evolving threat, the proposed Rule-Based Phishing Email Detection System analyzes incoming Gmail messages using heuristic and domain-specific rules. The system evaluates headers, content, URLs, and attachments to compute a phishing risk score. When the score exceeds a set threshold, alerts are sent to users via WhatsApp. This approach delivers transparent, fast decisions and provides a practical, lightweight defense against phishing, while enabling easy integration with future machine learning-based detection for broader email platforms.

2. METHODOLOGY

The proposed system follows an automated process to identify and alert users about suspicious emails:

2.1 Email Extraction:

The system connects to the user's Gmail inbox via the IMAP protocol and extracts email components, including headers, subjects, and bodies, for analysis.

2.2 Feature Extraction and Preprocessing:

Unnecessary symbols and encoded characters are removed. The detector extracts features like sender domain, URLs, and keywords

2.3 Heuristic Rule Evaluation:

A set of custom rules is used to detect warning signs, such as urgency words, suspicious links, mismatched domains, and URL shorteners. Each indicator increases the phishing score

2.4 Phishing Score Calculation:

All rule indicators are combined into a cumulative phishing risk score. The score is compared with a fixed threshold value; if exceeded, the email is flagged as phishing.

2.5 Alert Generation:

If the phishing score surpasses the threshold, a WhatsApp alert is sent to the user through the Twilio API.

2.6 Logging and Extensibility:

Every analysis instance is logged for transparency and future refinement. The modular design allows for easy ML integration

3. MODELING AND ANALYSIS

The system is structured in three layers: Email Processing, Detection, and Notification. Email Processing handles IMAP access and message extraction. The Detection layer applies rules and computes phishing scores. The Notification layer sends alerts via WhatsApp if phishing is detected. This architecture enables real-time, accurate detection with transparent processes and easy scalability.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 10, October 2025, pp : 1471-1473
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

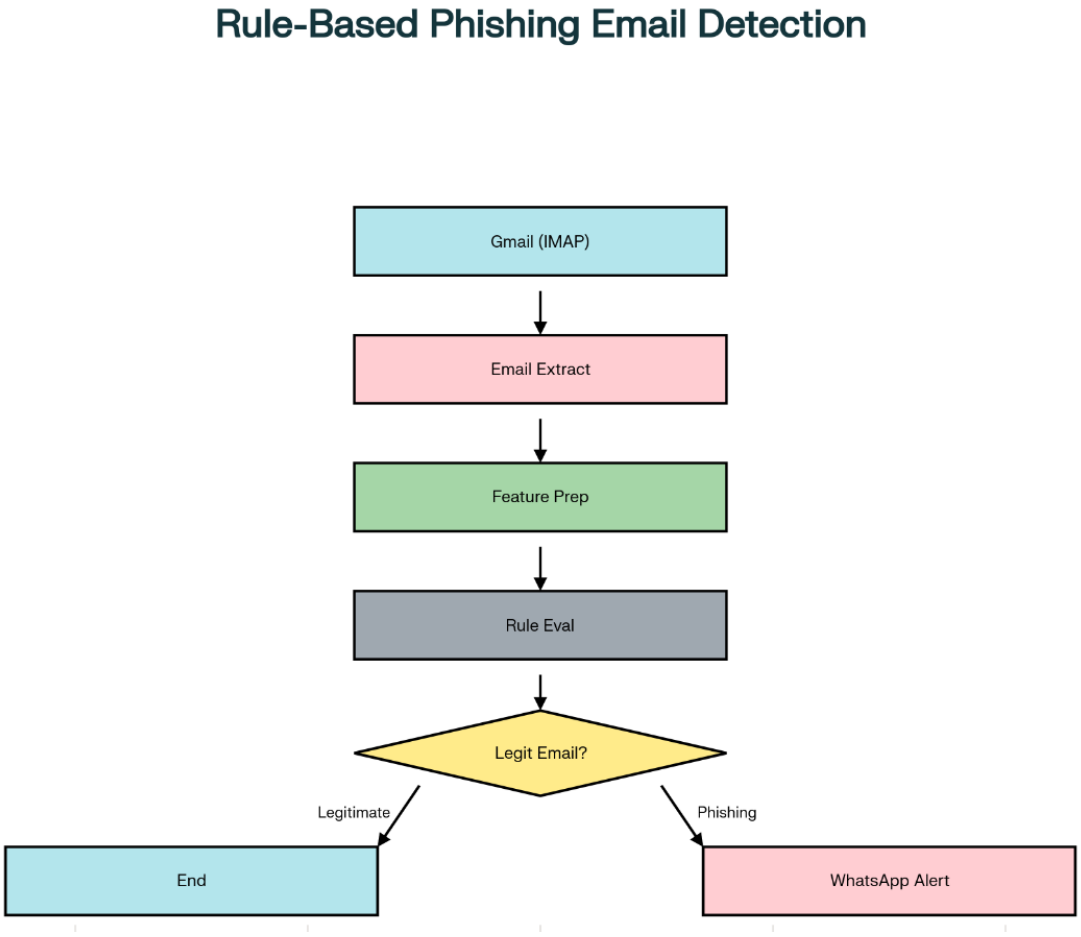

Figure 1: Block diagram of the PhishGuard system

4. RESULTS AND DISCUSSION

The system was evaluated with both legitimate and phishing emails. As shown in Figure 2, the terminal output logs detection workflow—only suspicious emails trigger warnings. Figure 3 shows a WhatsApp alert notification via Twilio, summarizing the sender, subject, and a snippet of the phishing email. The results confirm that the system reliably identifies phishing attacks and delivers instantaneous user alerts, supporting effective defense.

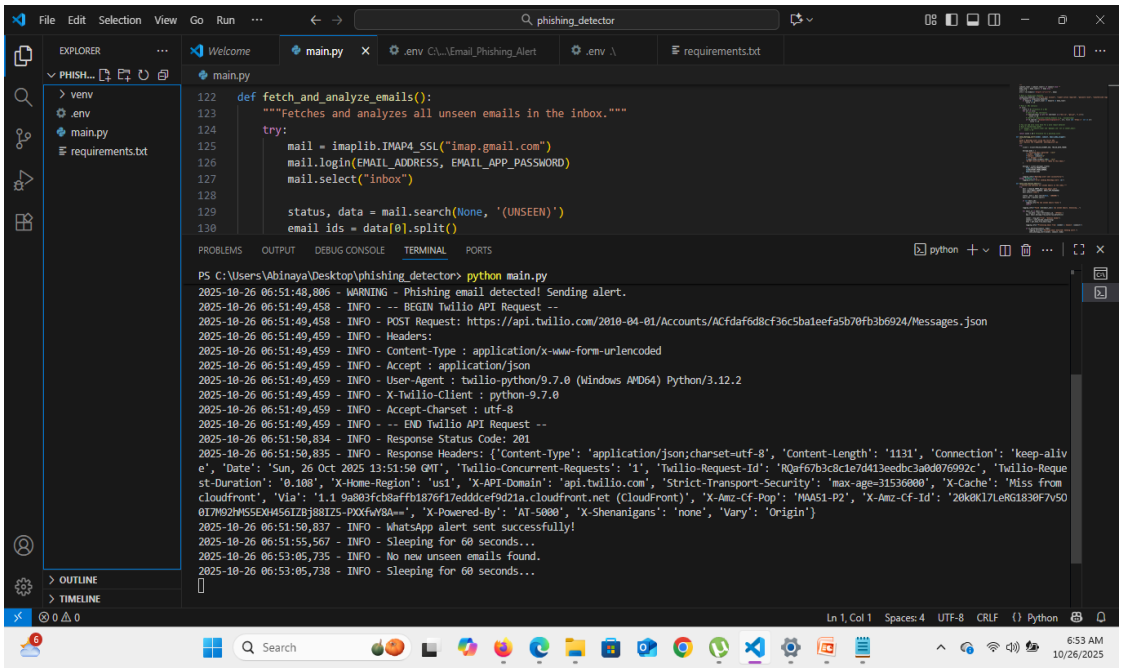

Figure 2: Terminal output showing phishing detection.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 10, October 2025, pp : 1471-1473
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

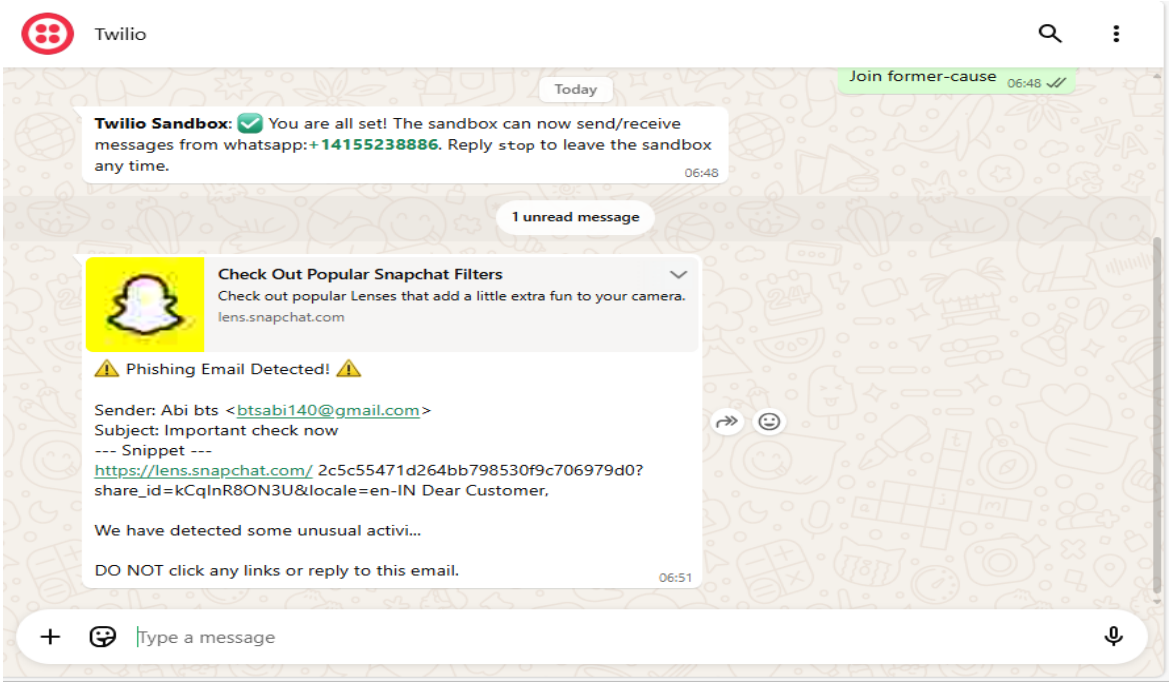

Figure 3: WhatsApp alert for a detected phishing email.

5. CONCLUSION

This work presents a rule-based real-time phishing email detection system for Gmail, integrating WhatsApp alerts via Twilio. The approach is transparent, efficient, and easily expandable, serving as a strong foundation for future integration with machine learning and support for Outlook or Yahoo mail.

6. REFERENCES

[1] S. Basnet and S. Mukkamala, "Rule-Based Phishing Attack Detection," Proceedings of the 19th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI), 2015, pp. 133–138

[2] Q. Li, J. Larsen, and P. H. Blöbaum, "Detecting Phishing Emails Using Rule-Based Heuristics and Text Analysis," Journal of Information Security and Applications, Vol. 57, 2021, pp. 102690.

[3] R. Bhatia, G. Singh, and P. Kumar, "Phishing Email Detection and Classification Using Machine Learning and Heuristic Analysis," IEEE Access, Vol. 10, 2022, pp. 34567 –34576.

[4] A. Sahay and M. Nautiyal, "Statistical and Machine Learning based Hybrid Approach for Phishing Websites Detection," Computers & Security, vol. 89, 2020, pp. 101666.

[5] K. T. Nguyen and T. T. Nguyen, "Deep Learning Approaches for Phishing URLs Detection," IEEE Transactions on Information Forensics and Security, vol. 15, 2020, pp. 1250-1264.

[6] S. K. Dwivedi, P. K. Singh, and N. K. Goyal, "A Survey on Phishing Attacks Detection Using Machine Learning," International Journal of Computer Science and Information Security (IJCSIS), vol. 18, no. 3, 2020.