International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 01 | Jan - 2025 SJIF Rating: 8.448 ISSN: 2582-3930

Anomaly Detection and Prevention in SMTP

Dr. K Malarvizhi[1], Nitish R G[2], Gayathri M[3],Agalya R[4] and Sowmithra R[5]
1-5Coimbatore Institute of Technology, Coimbatore, India
Email: malarvizhi@cit.edu.in, {rgnitish@gmail.com,
rajuagalya2004@gmail.com,gayathrimadhappan@gmail.com,sowmithrar19@gmail.com}

***Abstract*— Emails are a vital part of communication in organizations, but they are increasingly at risk of threats like data breaches and cyberattacks. Protecting sensitive information shared through emails is essential for maintaining data security and complying with regulations. However, manually checking emails for anomalies or confidential information can be tedious and impractical, especially in large-scale setups.To address this issue, we propose a system that detects and classifies email anomalies in real time. The system uses advanced machine learning algorithms to analyze email content and sending patterns, effectively identifying unusual activities. By leveraging a pre-trained dataset like the Enron email dataset, it compares email features to detect anomalies. Additionally, it integrates with an SMTP server using Python libraries, allowing it to monitor outgoing emails and flag any suspicious behavior in email-sending patterns.This system provides real-time oversight, ensuring that threats are quickly identified and managed. With a simple and intuitive interface, users can easily monitor and address flagged emails, enabling proactive security measures. In the end, this solution strengthens email security, ensures compliance with data protection rules, and creates a more secure and trustworthy communication environment.**

***Index Terms*— Mail Security, Machine Learning , Anomaly Detection , Data Protection**

1.INTRODUCTION

In today's digital world, securing communication is essential to protect sensitive information and maintain the integrity of organizations. Emails, being one of the most commonly used tools for communication, are often targeted by threats like phishing, data breaches, and unauthorized sharing of confidential data. To tackle these challenges, this project introduces an email monitoring system that focuses on real-time detection and prevention of potential risks.

The system combines SMTP server monitoring with anomaly detection algorithms to enhance email security. By integrating with an SMTP server through Python libraries like smtplib, it can observe outgoing emails in real time, analyzing patterns such as the frequency, timing, and recipients of emails. This helps identify unusual behaviors that might indicate issues like spam, phishing, or data leaks. At the same time, the system evaluates email content using machine learning algorithms, allowing it to spot sensitive data or abnormal communication patterns.

To achieve this, the system uses algorithms such as Naive Bayes and Isolation Forest, which specialize in classifying emails and identifying anomalies. It can detect irregularities in individual emails (single-email anomaly detection) and analyze larger datasets to uncover broader trends (multiple-email anomaly detection). This dual approach provides a comprehensive solution for identifying both specific threats and larger-scale risks.

For testing purposes, the system incorporates MailHog, a mock SMTP server that captures emails in a safe environment. This tool allows developers to test the system's performance without sending actual emails, making it easier to identify and resolve any potential issues before deployment. By using this controlled setup, the system ensures reliability and effectiveness.

This email monitoring solution not only strengthens organizational security but also helps maintain compliance with data protection regulations. By providing real-time alerts for suspicious activity, it enables quick action to address risks, creating a safer and more trustworthy communication environment.

2.LITERATURE SURVEY

Data Leakage Prevention in Email Communication

Gateway-level deployment has been explored to prevent data leakage in email communication by analyzing outgoing emails using pattern-matching algorithms. While effective for structured data, these methods face challenges in handling unstructured data and high email volumes, necessitating adaptive solutions. Techniques such as TF-IDF and Natural Language Processing (NLP) have also been applied to classify sensitive email content, offering high accuracy but struggling with high false-positive rates and the need for labeled datasets.

Data Leakage in AI Models

Advanced AI models exhibit risks of data leakage due to memorization patterns, identified through techniques like sequence repetition analysis and cross-entropy loss. Challenges include encryption issues, false positives, and scaling difficulties, highlighting the need for robust mechanisms to address these vulnerabilities.

Anomalous Behavior Detection

An Isolation Forest model has been employed to detect anomalies in business processes by analyzing deviations in system logs. Despite its efficacy, scalability remains a challenge, and careful threshold calibration is required for optimal performance. Similarly, SMTP sniffing leverages packet analysis and anomaly detection to monitor email traffic, though issues with encrypted communication and scalability persist.

Anomaly Detection in SMTP Traffic

Techniques like the Leaky Integrate-and-Fire (LIF) model have been used to detect irregular patterns in SMTP traffic, enhancing data security. However, these approaches show limited flexibility and effectiveness in handling sophisticated attack patterns, underscoring the need for dynamic adaptation.

Credential Leak Detection Using SMTP Honeypots

SMTP honeypots track unauthorized access and credential theft using tools such as Conpot and Wireshark. While effective for specific leak types, their reliance on predefined setups limits their applicability in dynamic environments.

Cloud Computing for Data Leakage Detection

Cloud-based approaches employing fake object insertion and pattern-matching algorithms improve scalability and detection accuracy. However, they face limitations in identifying unstructured leaks and maintaining performance with heavy data loads.

3.SYSTEM ARCHITECTURE

The system architecture is designed to detect and handle sensitive data in messages effectively. The process starts when a user sends an email. The system classifies the content, separating it into sensitive and non-sensitive categories. Sensitive data is further analyzed for potential data leakage and anomalies. If any anomalies or data leakage are detected, the system generates an alert to notify the relevant authorities, as well as the sender and receiver. If no issues are found, the email is delivered to its intended recipient, completing the process. This architecture ensures the secure management of sensitive data in communication systems.

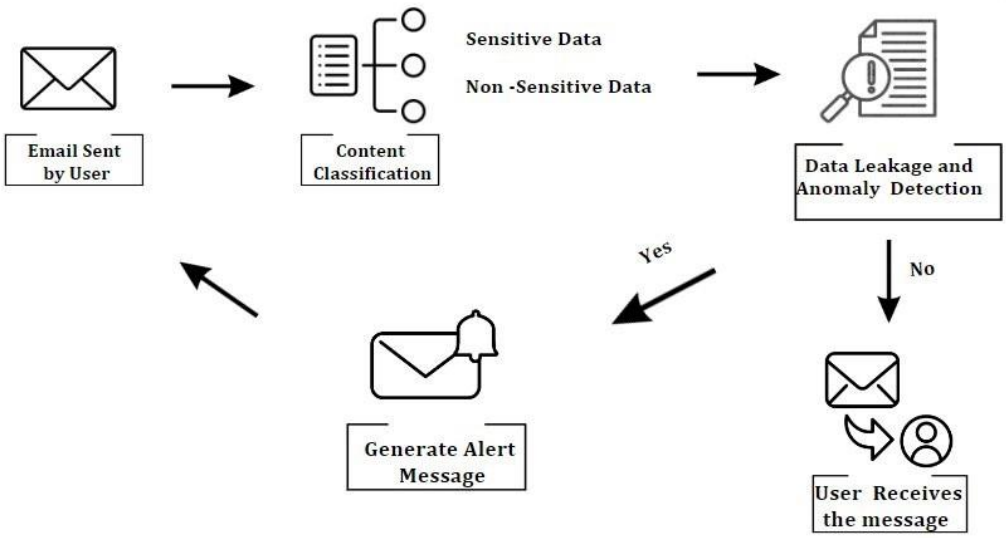

FIG.1. System Architecture

Here are the Modules used to implement the above model :

SMTP Server Integration :

This module facilitates the connection and real-time monitoring of SMTP servers for outgoing email traffic. Emails are sent securely using encryption protocols like TLS, with authentication through OAuth2 or standard username/password. Metadata such as sender, recipient, and timestamps are extracted for further processing.

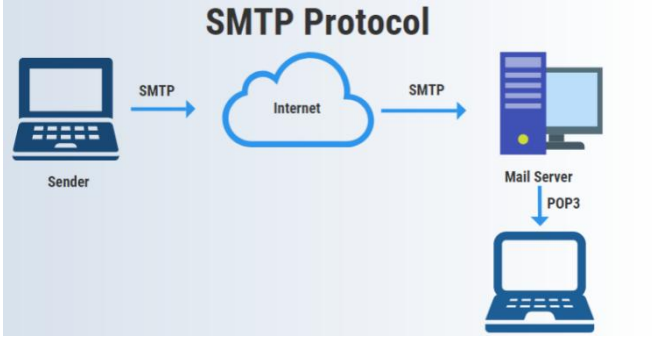

FIG.2.SMTP Protocol

Email Preprocessing :

Raw email data is parsed to extract key components (subject, body, sender, recipient, etc.). Text preprocessing techniques like stop-word removal, tokenization, and stemming are applied for uniformity. Features such as email frequency, recipient domains, and keywords are extracted for anomaly detection. Structured data is saved in .pkl files for efficient retrieval.

Anomaly Detection Engine :

The engine employs TF-IDF for anomaly detection by prioritizing significant keywords. It identifies anomalies in single emails and patterns across multiple emails through keyword trends and behavior-based detection. This ensures precise and scalable content analysis.

$$\text{TF-IDF}(t, d, D) = \text{TF}(t, d) \times \text{IDF}(t, D)$$

FIG.3.TF-IDF Score

Machine Learning Integration :

Three algorithms are utilized for anomaly detection:

- **One-Class SVM:** Identifies outliers by learning a decision boundary around normal data points.

$$\begin{cases} \min\limits_{\gamma} \dfrac{1}{2} \sum\limits_{i,j=1}^{m} \gamma_i \gamma_j K(\mathbf{x}_i, \mathbf{X}) \\ \text{s.t.} \quad 0 \le \gamma_i \le \dfrac{1}{m\nu}, \sum\limits_{i=1}^{m} \gamma_i = 1 \end{cases}$$

FIG.4.One Class SVM

- **Local Outlier Factor (LOF):** Flags anomalies based on density deviations relative to neighbors.

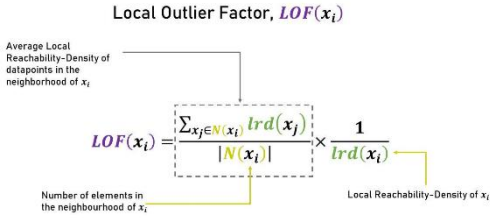

FIG.5.Local Outlier Factor

- **Isolation Forest:** Detects anomalies by recursively isolating rare and distinct data points.

$$s(x,m) = 2^{\frac{-E(h(x))}{c(m)}}$$

FIG.6.Isolation Forest

Models are evaluated using metrics like accuracy, F1 score, and confusion matrices.

Alert and Reporting :

This module triggers alerts and generates reports for anomalies in email content. It identifies salary discrepancies, activates anomaly mechanisms, and sends alert emails without disclosing sensitive content. Real-time notifications are provided via pop-ups. Logged activities enable long-term analysis and reporting.

4.RESULTS AND DISCUSSION

In our research, we trained our models using a massive dataset , from the Enron Corporation, encompassing approximately 600,000 messages . This dataset was compiled by the Federal Energy Regulatory Commission (FERC) during its investigation into Enron's activities. It includes data from about 150 users, organized into folders, and contains a total of about 0.5 million messages. The Enron Email Dataset has become a valuable resource for our research

VISUALIZATION OF ANOMALY DETECTION

The t-SNE plot shows POI (yellow) and Non-POI (purple) clustering, with some overlap indicating challenges in separating anomalies from normal data. This visualization aids in evaluating feature separability for anomaly detection.

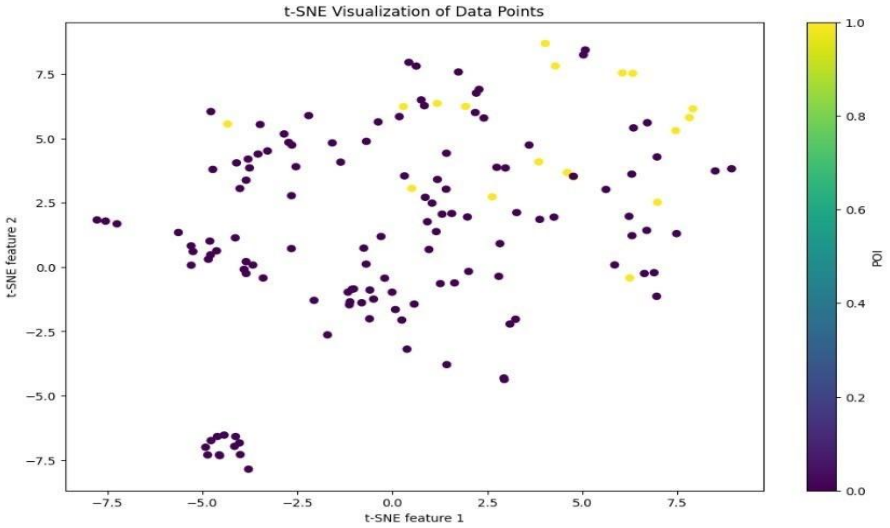

FIG.7.Visualisation of Anomaly Detection

PAIRPLOT VISUALIZATION FOR FEATURE RELATIONSHIPS IN ANOMALY DETECTION

This pairplot provides a comprehensive visualization of feature relationships within the dataset, highlighting the distributions and pairwise correlations between variables. Each plot compares two features, with diagonal elements showing feature distributions as histograms or density plots. Points are color-coded to represent different classes, such as anomalies (orange) and normal points (blue). This visualization is instrumental in identifying patterns, outliers, and clusters that may aid in anomaly detection and classification.

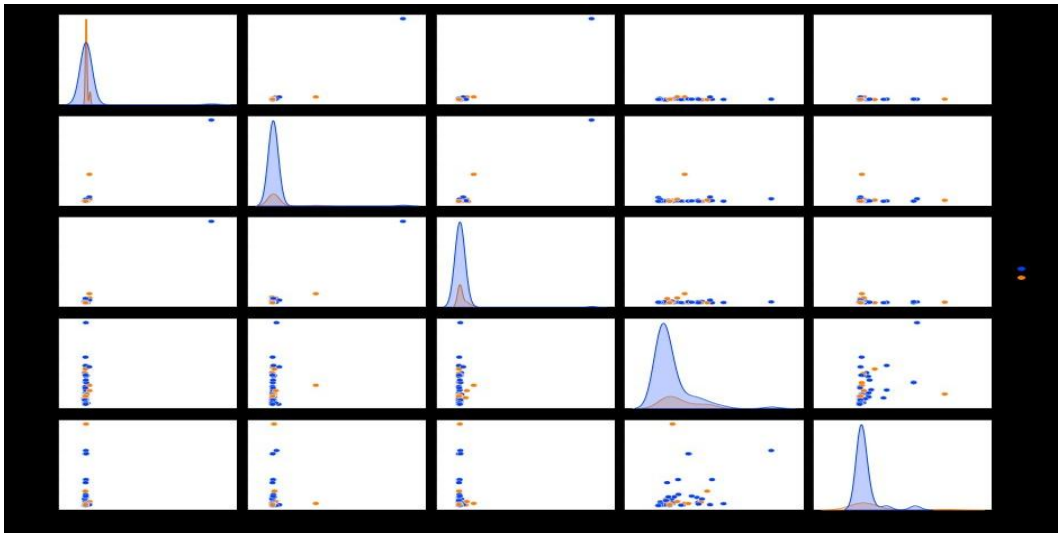

FIG.8. Pairplot Visualization for Feature Relationships in Anomaly Detection

COMPARISON WITH THE OTHER ALGORITHMS

S. No.	Method	Accuracy
1	One Class SVM	72%
2	Local Outlier Factor	74%
3	Isolation Forest	94%

FIG.9.Accuracy comparison of Algorithms

CONCLUSION

The study of anomaly detection in SMTP traffic has shown significant potential for identifying and mitigating security threats in email communication systems. Techniques such as packet sniffing, pattern recognition, and anomaly-based models have demonstrated their effectiveness in detecting irregularities in email traffic, such as spam, phishing, and data leaks. While methods like the Isolation Forest, LIF model, and SMTP honeypots offer promising results, challenges such as scalability, encryption handling, and false-positive rates remain critical barriers to widespread implementation. These findings emphasize the need for more adaptive, efficient, and context-aware detection frameworks to address evolving cybersecurity threats effectively.

SCOPE OF FUTURE WORK

To enhance scalability, it is essential to develop more resource-efficient anomaly detection algorithms capable of handling high traffic volumes in large-scale environments without compromising performance. This can be achieved by incorporating advanced decryption techniques and secure enclave computing, which would allow for the analysis of encrypted

SMTP traffic while ensuring data privacy. Additionally, employing AI-driven approaches, such as deep learning and reinforcement learning, can improve accuracy and reduce false-positive rates in anomaly detection. By integrating behavioral analysis and contextual information, anomaly detection systems can become more adaptive to dynamic and sophisticated attack patterns. Designing systems with real-time anomaly detection and response capabilities is crucial to mitigate threats as they occur. Furthermore, adopting hybrid models that combine multiple detection methodologies—such as rule-based, anomaly-based, and signature-based approaches—can help leverage the strengths of each method, providing a more comprehensive threat detection framework. Finally, integrating global threat intelligence feeds allows for the proactive identification of emerging SMTP-based attack vectors, enabling the detection mechanisms to be adapted and strengthened in response to new threats.

REFERENCES

1. K. Kaur, I. Gupta, and A. K. Singh, "E-Mail Protection via Gateway for Data Leakage Prevention," *Proc. IEEE Conf.*, 2021.

2. S. Alneyadi, E. Sithirasenan, and V. Muthukkumarasamy, "Discovery of Potential Data Leaks in Email Communications," *Proc. IEEE Conf.*, 2020.

3. S. Duan, M. Khona, A. Iyer, and R. Schaeffer, "Assessing Data Leakage and Memorization Patterns in Frontier AI Models," *Springer AI J.*, vol. 8, pp. 121–140, 2024.

4. N. Fang, X. Fang, and K. Lu, "Anomalous Behavior Detection Based on the Isolation Forest Model," *Int. J. Comput. Syst.*, vol. 10, no. 3, pp. 220–234, 2022.

5. S. N. Holambe, U. B. Shinde, and A. U. Bhosale, "Data Leakage Detection Using Cloud Computing," *Cloud Comput. J.*, vol. 9, pp. 104–114, 2021.

6. M. Aiello, D. Avanzini, D. Chiarella, and G. Papaleo, "SMTP Sniffing for Intrusion Detection Purposes," *J. Netw. Secur.*, vol. 14, no. 2, pp. 114–127, 2020.

7. H. Luo, B. Fang, and X. Yun, "Anomaly Detection in SMTP Traffic," *Int. Conf. Cyber Secur.*, vol. 7, pp. 94–108, 2019.

8. K. Trnovcová and D. Dancs, "Detecting Credential Leaks Using SMTP Honeypots," *Springer Cyber Secur. J.*, vol. 12, pp. 310–320, 2020