

Mitigating Cybercrime Risks through Advanced Email Sender Detection and Flood Attack Prevention

Anitha Rao¹, Madhumita R², Monika S M³, Rianna Thangamma I G⁴ and Shreeya Dinesh⁵

¹⁻⁵GSSS Institute of Engineering and Technology for Women, Mysuru, India.

Email: anitharao@gsss.edu.in, madhugowda0304, vaishnavimona2004, riannathangammaig, shreeyadinesh2004}@gmail.com

Abstract— Email continues to be a critical channel exploited by cybercriminals for threats such as spoofing, phishing, and flood-based attacks. Conventional static filtering methods often fall short in addressing these evolving risks. This paper introduces a robust and intelligent email security framework that incorporates AES-based message encryption, SHA-256 digital signatures for sender verification, IP-based validation, and mechanisms to detect and prevent email flooding. To assess its reliability, an attacker simulation module is included, which tests the system's response to tampering attempts. Developed using Java Networking and a Swing-based graphical interface, the system ensures secure, real-time communication between clients and servers. Its proactive approach to threat detection makes it well-suited for both organizational and individual use cases. **Keywords:** Email Security, Cybercrime, AES Encryption, SHA-256, IP Verification, Flood Attack Detection, Java Networking, Swing UI

Index Terms— Email Security, Spoofing Detection, Phishing Prevention, AES Encryption, SHA-256 Digital Signature, IP Verification, Flood Attack Detection, Swing UI.

I. INTRODUCTION

Cyberattacks leveraging email have significantly increased in both frequency and sophistication. Threats such as email spoofing, phishing scams, and flood-based attacks present serious risks to data privacy and system reliability. Conventional filtering methods and static rule-based systems are often ineffective against these advanced intrusion techniques.

To mitigate these concerns, this research presents an intelligent, multi-layered email security solution that combines real-time sender authentication, data encryption, and dynamic threat detection to enhance communication safety and system resilience.

A. Motivation

Conventional email filtering mechanisms frequently depend on keyword-based analysis or machine learning classifiers, which may not effectively authenticate the sender or prevent identity spoofing. The proposed system overcomes these shortcomings by integrating encryption techniques, IP address validation, and digital signature verification. This approach enables the proactive identification of suspicious activity, thereby enhancing both the security and usability of the email communication system.

B. Problem Statement

Email spoofing, phishing, and flood attacks continue to exploit gaps in conventional filtering mechanisms, often resulting in severe consequences such as unauthorized data access, identity compromise, and disruption of email services. These challenges underscore the necessity for a robust, real-time security framework that combines sender authentication with intelligent flood detection to safeguard digital communication channels.

C. Objectives

- Secure Communication: Encrypt emails using AES and sign them with SHA-256.
- Sender Verification: Match IP addresses and block impersonators.
- Flood Attack Detection: Identify and mitigate bulk message attempts.
- Client-Server Model: Implement using Java for real-time protection and usability.

II. LITERATURE SURVEY

Multiple scholarly works have analysed techniques to email security using various machine learning, authentication, and filtering techniques. Despite ongoing advancements, several current systems focus exclusively on classification methods, neglecting critical components like encryption, sender authentication, and live anomaly detection. This section highlights key contributions and limitations from recent literature relevant to spam detection, phishing authentication, and prevention, and email.

Many existing email security systems focus primarily on content filtering, neglecting sender verification. This often leaves them vulnerable to spoofing, phishing, message and flood-based integrity attacks. In this research, the outlined framework tackles these challenges by integrating AES encryption, SHA-256 signatures, and IP-based validation. It ensures secure email communication through real-time verification and proactive threat detection.

Agung Althaaf Emha Damanik et al. [1] proposed an LSTM-based spam email detection system that classifies emails using inbox inspection, pre-processing, and deep learning. The system demonstrates improved accuracy and F1-scores over traditional models. However, it focuses solely on spam classification without addressing sender authentication or content encryption, limiting its defence against spoofing and phishing attacks.

Sanjeev Shukla et al. [2] introduced a machine learning technique to detect email bombing attacks using time gap analysis. Their model identifies abnormal surges in email traffic to mitigate denial-of-service scenarios. While effective for volume-based threats, it lacks integration with IP tracking or digital signature verification, making it vulnerable to targeted spoofing.

Najwa Altwaijry et al. [3] performed a comparative study on phishing detection, employing deep learning models such as adaptive boosting, ANN, and random forest. The models demonstrate high classification accuracy, but the system depends heavily on historical data. It does not incorporate sender authentication or support dynamic real-time verification.

Samaila Kasimu Ahmad et al. [4] used hyperparameter-tuned random forest models for phishing detection. Their approach improves accuracy through feature selection, but it remains ineffective against zero-day phishing attacks due to its dependency on known features. The model does not address email integrity or provide encryption capabilities.

J. Mythili et al. [5] developed a Temporal Naive Bayes classifier that incorporates email arrival times and keyword patterns to enhance spam detection. Though it adapts to timing-based attacks, it lacks encryption and sender validation, leaving gaps in overall security.

Wosah Peace Nmachi [6] proposed a framework to secure email access points and prevent impersonation by improving settings control. While it addresses unauthorized forwarding and login security, it lacks provisions for verifying message content, detecting flood-based attacks, or ensuring encrypted communication.

Nethni Hirusha Wanigasingha et al. [7] applied leveraging evolutionary methods to refine feature selection for classifying spam emails. This improves model precision, but like other ML-only approaches, it lacks contextual threat validation, encryption, and sender IP tracking.

Abhinav Kachole et al. [8] explored employing supervised learning algorithms for phishing detection in emails through content analysis. Though effective in classification, the model cannot handle spoofed sender identities or detect content tampering.

Sahote Tejinder Singh et al. [9] examined the use of machine learning and deep learning approaches implemented in Python for spam detection. While their study focuses on improving classification accuracy, it does not incorporate real-time verification, encryption mechanisms, or sender authentication.

Shuji Sakuraba, Minami Yoda, Yuichi Sei, Yasuyuki Tahara [10] also proposed a sender authentication-based spam filtering system that improves legitimate mail detection. While it introduces sender verification via allow-list mechanisms, it lacks encryption and cannot detect tampered messages or simulate man-in-the-middle attacks.

III. DESIGN AND IMPLEMENTATION

The proposed system adopts a modular client- server design communication, encryption mechanisms, and an interactive graphical user interface. The server component, developed in Java, manages email transmission, authentication, and threat simulation processes, while the client interface—built using Java Swing—facilitates user operations such as registration, login, email composition, and message verification. During email composition, the system encrypts the message content using the Advanced Encryption Standard (AES) and generates a corresponding SHA-256 digital signature to ensure message integrity. Concurrently, the sender's IP address is captured and cross- checked against the IP address manually provided by the user. If the addresses align, the communication is accepted and delivered; otherwise, the system blocks the sender and adds them to a restricted list. On the recipient's side, incoming emails undergo signature verification to confirm authenticity and detect any unauthorized alterations. If tampering is detected, the system labels the email and alerts the recipient. To further assess the system's reliability, an attacker simulation module is integrated. This module intentionally modifies the message during transit, allowing the system identify the anomaly through signature mismatch and generate an appropriate alert. All communication between the client and server takes place over secure Java sockets, enabling real-time processing and validation. The centralized architecture supports efficient email management, while immediate GUI- based notifications enhance user awareness. This layered implementation ensures robust email security by combining encryption, sender verification, and proactive threat detection.

A. Hardware Components

- Hard Disk
- RAM
- Processor

B. Software Components

- Operating System: WINDOWS 10 and above
- Programming Language: Java
- NetBeans or Eclipse
- Database: MySQL
- Tools: JDK, IDE

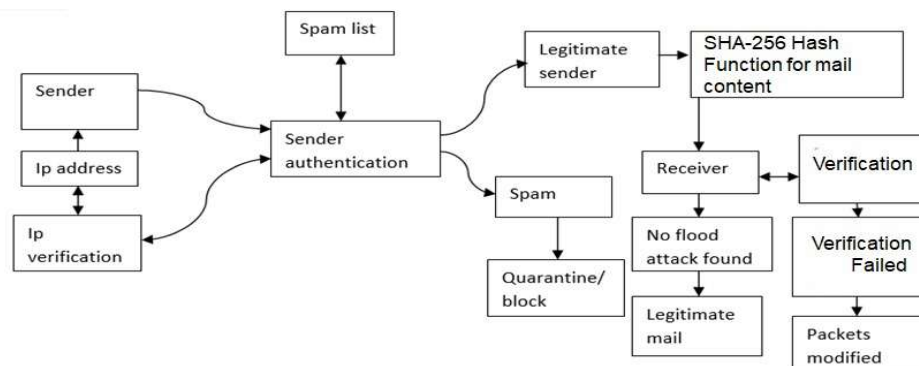


Fig.1 Data Flow Diagram

IV. EXPERIMENTAL SETUP

A. Methodology

User Authentication:

Users initiate interaction with the system by registering through a secure interface, providing unique credentials. The implemented authentication protocol restricts usage to users who have been properly verified and authorized, thereby maintaining system integrity and preventing unauthorized usage.

Email Composition and Encryption:

Authenticated users compose emails through a Java Swing-based graphical user interface. Before transmission, each message is encrypted using the Advanced Encryption Standard (AES) to ensure confidentiality. Additionally, a SHA-256 digital signature is generated for each email to support integrity verification upon receipt.

IP-Based Sender Verification

When an email is sent, the system records the sender's IP address and cross-verifies it against the IP entered by the user. A match allows the message to be delivered to the intended recipient, whereas a mismatch marks the sender as potentially malicious and results in the email being blocked to safeguard against spoofing or impersonation attempts.

Email Reception and Signature Validation

Upon receiving an email, the system regenerates a SHA-256 digital signature from the received content and verifies it against the original signature attached by the sender. A match confirms message integrity, while a mismatch indicates potential tampering, prompting the system to alert the recipient.

Email Reception and Signature Validation

Upon receiving an email, the system regenerates a SHA-256 digital signature from the received content and compares it with the original signature attached by the sender. A match confirms message integrity, while a mismatch indicates potential tampering, prompting the system to alert the recipient.

Flood Attack Simulation Module

To evaluate the robustness of the system, a simulated attacker module is incorporated. This module intercepts and modifies email content during transmission, and flag unauthorized modifications indicative of a flood or spoofing attack.

Blacklisting and Access Control

Users who fail IP validation or exhibit suspicious behaviour are added to a blacklist. Once blacklisted, these users are denied further access to the system, ensuring continued protection against repeated spoofing attempts and unauthorized access.

SYSTEM ARCHITECTURE

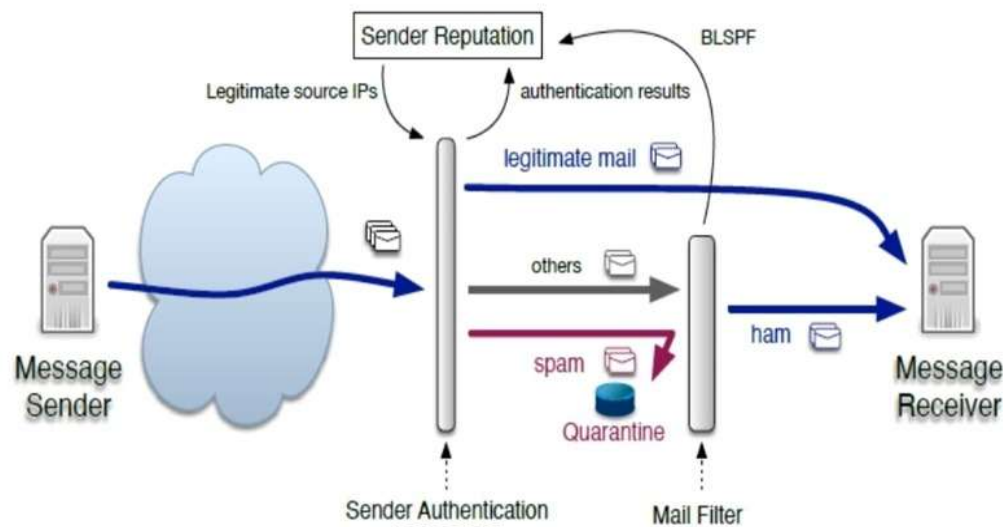


Fig. 2 System Architecture

V. RESULTS

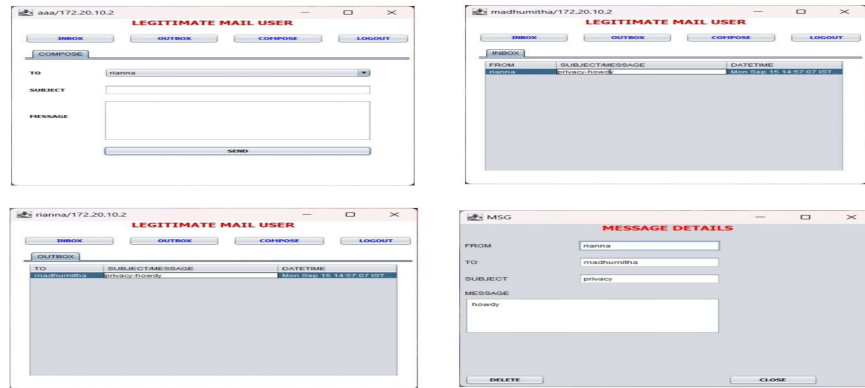


Fig.3 Demonstration of Email Threat Défense Model



Fig. 4 System Performance Metrics

The Legitimate Mail Sender Verification and Flood Attack Detection System provides a secure and intelligent email platform with the following outcomes:

A. Secure Email Transmission

- All outgoing emails are encrypted with AES for confidentiality.
- A SHA-256 digital signature is generated for each email, ensuring integrity and authenticity.
- Any unauthorized modification in transit is immediately detectable.

B. Sender Legitimacy Verification

- The sender's IP address is captured and cross-checked against the registered IP stored during user registration.
- If the IP does not match, the system blocks the sender and quarantines the message, effectively preventing spoofing.

C. Flood Attack Detection

- The system monitors email flow in real time.
- Multiple incoming emails from suspicious or unverified sources within a short interval are flagged as flood attacks, and the messages are blocked before reaching the recipient.

D. Attack Simulation and Detection

- Using the attacker module, we tested interception and tampering scenarios.
- The system consistently detected SHA-256 signature mismatches, proving its effectiveness against man-in-the-middle and message modification attacks.

E. Quarantine and Alerts

- All flagged or suspicious messages are diverted to a quarantine zone instead of being deleted silently.
- Users are notified with clear alerts about spoofing attempts, tampered content, or possible attacks.

VI. CONCLUSION

The developed system presents a comprehensive and resilient approach to email security by integrating encryption, sender authentication, and real-time verification. It effectively addresses common cyber threats such as spoofing, phishing, and flood attacks. Looking ahead, the system can be enhanced by integrating with cloud-based email platforms to support large-scale deployment and seamless access. Additionally, a companion mobile application could provide real-time alerts and remote monitoring capabilities. Incorporating AI-driven anomaly detection based on user behaviour may further strengthen the system's ability to detect sophisticated threats. Features such as voice command recognition or biometric authentication can also be introduced to improve accessibility and user convenience.

FUTURE SCOPE

The proposed email security system offers a strong foundation for enhancing secure digital communication. That said, there is significant potential for future development and expansion. The system can be integrated with cloud-based email services to allow seamless access and scalability across enterprise environments. A dedicated mobile application can be introduced to provide users with real-time alerts, remote access, and enhanced control over email activity. In addition, utilizing AI and ML-based methods can enable the system to learn user behaviour patterns and detect anomalies more effectively, thereby improving its ability to respond to emerging threats. Support for voice-based commands and biometric authentication, such as fingerprint or facial recognition, could also enhance both usability and security. These advancements would make the system more adaptive, user-friendly, and suitable for deployment across diverse operational settings, including educational institutions, businesses, and government agencies.

REFERENCES

- [1] Agung Althaaf Emha Damanik, Hilal H. Nuha, Niken Dwi Wahyu Cahyani, Setyorini, Mod Arfian Bin Ismail, "Email Spam Detection using Long Short-Term Memory (LSTM) Network Method", IEEE Xplore, 2024. <https://ieeexplore.ieee.org/document/10836586/authors>
- [2] Sanjeev Shukla, Manoj Misra, Gaurav Varshney, "Email Bombing Attack Detection and Mitigation using Machine Learning", ResearchGate, 2024. https://www.researchgate.net/publication/381403562_Email_bombing_attack_detection_and_mitigation_using_machine_learning
- [3] Najwa Altwaijry, Reem Alotaibi, Isa Al-Turaiki, Fatimah Alakeel, "Advancing Phishing Email Detection: A Comparative Study of Deep Learning Models", MDPI, 2024. <https://www.mdpi.com/1424-8220/24/7/2077>
- [4] Samaila Kasimu Ahmad, Babagana Dapshima, Yasmin Essa, "Detection of Phishing Attacks using Machine Learning Techniques", ResearchGate, 2024. https://www.researchgate.net/publication/382149371_DETECTION_OF_PHISHING_ATTACKS_USING_MACHINE_LEARNING_TECHNIQUES
- [5] J Mythili, B Deebeshkumar, T Eshwaramoorthy, J N Ajay, "Enhancing Email Spam Detection with Temporal Naive Bayes Classifier", IEEE Xplore, 2024. <https://ieeexplore.ieee.org/document/10550229/authors>
- [6] Nethni Hirusha Wanigasingha, T.G.I. Fernando, "Optimizing Feature Selection in Spam Email Detection using Co-Evolutionary Algorithms", IEEE Xplore, 2024. <https://ieeexplore.ieee.org/document/10844981/authors>
- [7] Abhinav Kachole, Aniket Nagpure, Atharva Wagh, Prof. T. H. Patil, "Email Platform: Spam Detection", IJRASET, 2024. <https://www.ijraset.com/research-paper/email-platform-spam-detection#introduction>
- [8] Sahote Tejinder Singh, Surinder Pal Singh, Madhuri Dinesh Gabhane, Chaitanya Mahamuni, "Study of Machine Learning and Deep Learning Algorithms for the Detection of Email Spam based on Python Implementation", IEEE Xplore, 2023. https://www.researchgate.net/publication/371713771_Study_of_Machine_Learning_and_Deep_Learning_Algorithms_for_the_Detection_of_Email_Spam_based_on_Python_Implementation
- [9] Wosah Peace Nmachi, "A Framework for Securing Email Entrances and Mitigating Phishing Impersonation Attacks", ResearchGate, 2023. https://www.researchgate.net/publication/376384426_A_Framework_for_Securing_Email_Entrances_and_Mitigating_Phishing_Impersonation_Attacks
- [10] Shuji Sakuraba, Minami Yoda, Yuichi Sei, Yasuyuki Tahara, "Improvement of Legitimate Mail Server Detection Method using Sender Authentication", ResearchGate, 2021. https://www.researchgate.net/publication/353837275_Improvement_of_Legitimate_Mail_Server_Detection_Method_using_Sender_Authentication