International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT25111674

Legitimate Mail Sender Verification and Flood Attack Detection Using Java Networking and Swing UI

Sinchana K R*[1], Prof Dr. H P Mohan Kumar[2]

[1]Department of Masters of Computer Application, PES College of Engineering, Karnataka, India

[2]Department of Computer Science and Engineering, PES College of Engineering, Karnataka, India

ARTICLEINFO

Article History:

Accepted : 01 July 2025

Published: 04 August 2025

Publication Issue

Volume 11, Issue 4

July-August-2025

Page Number

322-326

ABSTRACT

With the growing prevalence of cyber threats, securing email communication is essential. This paper presents a Legitimate Mail Sender Verification and Flood Attack Detection System developed using Java Networking and Swing UI. The system comprises client and server modules, enabling user registration, authentication, and secure email exchange. To ensure sender legitimacy, email bodies are encrypted using AES, and MD5 hashes are used for signature verification.

The server records the sender's IP address and prompts users to validate it. A mismatch results in sender blocking. On the receiver's end, signature validation confirms message integrity. Any inconsistency flags the message as a flood attack. Additionally, a simulated attacker module allows testing by modifying messages mid-transit, aiding in real-time detection.

This approach integrates encryption, digital signature validation, and IP tracking to protect against spoofing, tampering, and denial-of-service threats in email systems.

Introduction

With the increasing reliance on email, cybersecurity threats such as email spoofing, phishing, and flood attacks have also risen significantly. Malicious actors often exploit vulnerabilities in email systems to impersonate legitimate users, alter message content, or launch mass email-based attacks, leading to data breaches, financial losses, and compromised communications. To counter these threats, this project introduces a Legitimate Mail Sender Verification and Flood Attack Detection System using Java Networking and Swing UI, designed to enhance email security through sender verification, encryption, and integrity checks.

The system is structured into two main components: the user module and the server module. The user module enables individuals to register, log in, compose, send, and receive emails through using GUI built using Java Swing. To ensure confidentiality, the email body content is encrypted using the Advanced

Encryption Standard (AES) before transmission, and an MD5-based digital signature is generated to verify its integrity. Once an email is sent, the server module immediately tracks the sender's IP address and prompts the user to manually verify it. If the provided IP matches the server-tracked IP, the sender is considered legitimate, and the email is delivered securely to the recipient. However, if a mismatch occurs, the sender is blocked and added to a restricted list, preventing unauthorized access to the system.

Upon receiving an email, the recipient can perform a content integrity verification by regenerating the signature and comparing it with the original signature generated at the sender's end. If both signatures match, the email is confirmed as legitimate and unaltered. However, if the signatures differ, the system identifies it as a flood attack or tampered cntent, alerting the recipient of possible fraudulent activity. Additionally, the system includes a dummy attacker module to simulate cyber threats. When enabled, this module allows an attacker to intercept, modify, and forward emails to the recipient, demonstrating how the system effectively detects unauthorized changes using digital signature verification.

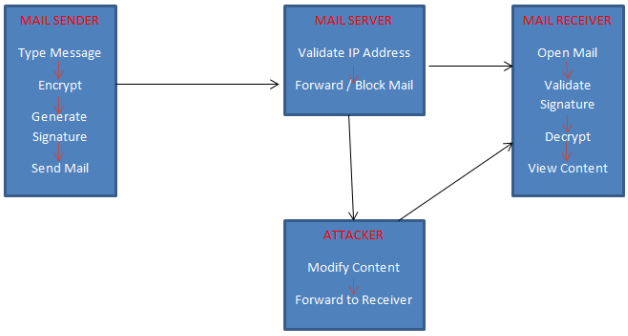

Figure 1. ARCHITECTURE

LITERATURE STUDY

Karim[1] (2019) presented a thorough review in IEEE Access on intelligent techniques for spam email filtering. Their work covers a wide range of machine learning and deep learning models, comparing accuracy, datasets, and detection strategies. The survey also discusses existing challenges such as high false positives and model adaptability to evolving spam patterns.

[2] The Spamhaus Project is a global initiative that provides real-time threat data, especially regarding spam-related IP addresses and domains. This information is commonly used by email service providers to block known spam sources and prevent delivery of malicious messages.

[3] DNSWL (DNS Whitelist) offers a public whitelist service of trusted senders to help reduce incorrect spam classification. By integrating this list, email systems can recognize legitimate servers and avoid marking them as spam.

[4] S. Kitterman done the work Sender Policy Framework (SPF), as outlined in RFC 7208 (2014), provides a way for domain owners to specify which IP addresses are allowed to send mail on their behalf. This authentication mechanism helps receivers detect and block unauthorized sources attempting to impersonate legitimate senders.

[5] D. Crocker The DomainKeys Identified Mail (DKIM) standard (RFC 6376) introduces a method for email signing using cryptographic keys. It ensures that the contents of an email remain unaltered and that the sender's domain can be verified through a public DNS record

[6] DMARC (Domain-based Message Authentication, Reporting, and Conformance), described in RFC 7489, builds on SPF and DKIM by providing a policy framework. It enables domain administrators to instruct receiving servers on how to handle authentication failures and to report such incidents

[7] In a 2021 study, Sakuraba et al. proposed a model to build sender reputations by leveraging SPF, DKIM, and DMARC authentication data. Their approach enhances trustworthiness scores of senders and strengthens filtering mechanisms against spoofed emails.

[9] Konno et al. (2019) introduced a clustering method using DMARC feedback to identify legitimate forwarding email servers. Their X-means clustering

algorithm groups servers based on behavioral similarity, aiding in distinguishing trusted servers from malicious ones in email infrastructures.

[10] Schanzenbach et al. (2021) investigated the effectiveness of SPF, DKIM, and DMARC protocols through large-scale testing and found significant gaps in policy enforcement, highlighting vulnerabilities in current email sender validation practices 101010.

PROPOSED SYSTEM

To address the challenges of email spoofing, phishing, and flood attacks, this project proposes a Legitimate Mail Sender Verification and Flood Attack Detection System using Java Networking and Swing UI. The system is designed to ensure secure email communication by incorporating encryption, digital signatures, IP-based sender verification, and attack detection mechanisms. Unlike traditional email services that primarily rely on basic authentication, this system provides multi-layered security to prevent unauthorized access, tampering, and fraudulent email activities.

The proposed system consists of two main modules: the user module and the server module. The user module allows individuals to register, log in, compose emails, select recipients, and send messages through an intuitive graphical user interface (GUI) built with Java Swing. To ensure confidentiality and data integrity, the system encrypts the email body content using the Advanced before transmission. This encryption Encryption Standard (AES) and generates a digital signature using the MD5 hashing algorithm prevents unauthorized users from reading the content, while the digital signature ensures that the email remains unaltered during transit.

The server module plays a crucial role in verifying the legitimacy of the sender. When a user sends an email, the server tracks the sender's IP address and prompts them to enter their current IP for verification. If the provided IP matches the tracked IP, the sender is confirmed as legitimate, and the email is forwarded to the recipient. However, if there is an IP mismatch, the user is blocked and added to a restricted list, preventing unauthorized access and impersonation attacks.

Upon receiving an email, the recipient can verify its integrity by clicking the "Verify" button. This action triggers the system to regenerate the digital signature for the received content and compare it with the original signature generated at the sender's end. If both signatures match, the email is confirmed as legitimate and unaltered. However, if the signatures differ, the system detects it as a flood attack or tampered content, alerting the recipient of potential email fraud.

Additionally, the system includes a dummy attacker module to simulate cybr threats and test the system's security features. If enabled by the server, this module intercepts emails before they reach the intended recipient, allowing an attacker to modify the content and resend it. When the recipient verifies the email, the system detects the altered content through signature mismatch and flags it as an attack attempt, demonstrating the effectiveness of the security measures in place.

By integrating encryption, sender authentication, IP tracking, and digital signatures, the proposed system ensures secure and reliable email communication. It effectively prevents email spoofing, unauthorized content modification, and fraudulent attacks, enhancing overall cybersecurity and providing a trustworthy platform for email exchange.

ASE

In this project, the AES (Advanced Encryption Standard) algorithm is used to securely encrypt the email content before transmission. AES is a symmetric key encryption method, meaning the same key is used for both encryption and decryption. It works on fixed-size blocks of 128 bits and supports key sizes of 128, 192, or 256 bits.

AES performs multiple rounds of transformations, including substitution, shifting rows, mixing columns, and adding round keys, to convert plaintext into unreadable ciphertext. In this system, AES with CBC

(Cipher Block Chaining) mode and PKCS5Padding is used to ensure both security and proper data block alignment.

By using AES encryption, the confidentiality of the email body is preserved, ensuring that only authorized users can read the message after verifying the sender.

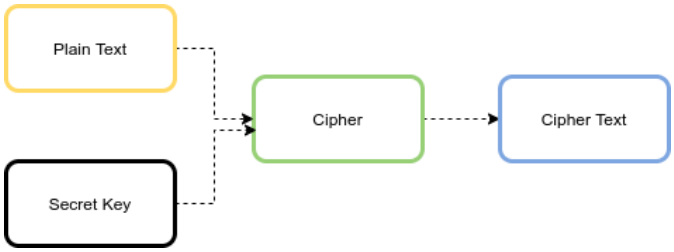

Figure 2. ASE Verification Method

MD5

In this project, the MD5 algorithm is used to generate a unique digital signature (hash) of the encrypted email content. MD5 is a widely used cryptographic hash function that takes an input message and produces a 128-bit (16-byte) hash value, commonly represented as a 32-character hexadecimal number.

The main purpose of using MD5 in this system is to ensure data integrity. After encrypting the email with AES, an MD5 hash of the ciphertext is created. This hash can later be used to verify whether the email content has been altered during transmission. If even a small change occurs in the message, the MD5 hash will change significantly, indicating potential tampering.

Though MD5 is not suitable for secure encryption due to known vulnerabilities, it is still effective for simple integrity verification in trusted environments like this one.

Result Analysis

The implementation of the Legitimate Mail Sender Verification System successfully achieved the goal of securing email communication and verifying the authenticity of the sender. The system allows users to compose, encrypt, and send emails using the AES (Advanced Encryption Standard) encryption technique. Additionally, an MD5 hash is generated for each encrypted message to ensure its integrity.

The system also verifies the sender's IP address before processing the email. If the entered IP address does not match the actual IP, the system prevents the email from being sent, thereby blocking unauthorized senders. This ensures that only legitimate users are allowed to transmit messages through the server.

Overall, the project demonstrates how a combination of encryption (AES), hashing (MD5), and IP verification can be effectively used to provide a secure and reliable email system, protecting against spoofing and unauthorized access.

CONCLUSION

This "Legitimate Mail Sender Verification and Flood Attack Detection System" successfully addresses critical vulnerabilities in modern email communication by integrating a multi-layered security approach. By implementing AES encryption for message confidentiality and MD5 digital signatures for content integrity, the system ensures that emails remain secure and untampered during transit. The novel IP-based sender verification mechanism significantly enhances authenticity checks, effectively preventing impersonation and blocking unauthorized senders. Furthermore, the real-time detection of modified content through signature mismatch, even with the simulated attacker module, demonstrates the system's robustness against flood attacks and malicious alterations. This project effectively establishes a more trustworthy and secure email environment, safeguarding users from prevalent cyber threats like spoofing and data manipulation.

All paragraphs must be indented. All paragraphs must be justified, i.e. both left justified and right-justified.

References

[1]. A. Karim, S. Azam, B. Shanmugam, K. Kannoorpatti. and M. Alazab: “A comprehensive survey for intelligent spam

email detection," IEEE Access, Vol. 7, pp. 168261-168295, 2019.

[2]. The Spamhaus Project: https://www.spamhaus.org/

[3]. DNS Whitelist - Protect against false positives: https://www.dnswl.org/

[4]. S. Kitterman: "Sender policy framework(SPF) for authorizing use of domains in email, version 1," RFC7208, 2014.

[5]. D. Crocker, T. Hansen, M. Kucherawy: "DomainKeys identified mail (DKIM) signature," STD 76, RFC6376, 2011.

[6]. M. Kucherawy and E. Zwicky: "Domain-based message authentication, reporting, and conformance (DMARC)," RFC7489, 2015.

[7]. S. Sakuraba, M. Yoda, Y. Sei, Y. Tahara and A. Ohsuga, "Sender reputation construction method using sender authentication technologies," IPSJ Journal, Vol.62, No.5, pp. 11731183, 2021.

[8]. S. Sakuraba: "Messaging technology," IIJ Internet Infrastructure Review (IIR), Vol. 47, pp.4-9, 2020, https://www.iij.ad.jp/en/dev/iir/pdf/iir vol47 EN.pdf

[9]. K. Konno, N. Kitagawa, S. Sakuraba, and N. Yamai: "Legitimate email forwarding server detection method by X-means clustering utilizing DMARC reports," Eleventh Internation Conference on Evolving Internet (INTERNET 2019), pp

[10]. M. Schanzenbach, P. Winter, and K. Borgolte: "Measuring email sender validation in the wild,"

[11]. Proceedings of the 17th International Conference on emerging Networking EXperiments and Technologies (CoNEXT 2021), ACM, pp. 318–332, 2021.