IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, November 2025
Impact Factor: 7.67

Cybershield : Email Spoofing Detection System

Sharad S. Bolde, Prof. Rahul P. Bembade, Shri P. Ingale, Sahil M. Patil
MIT Art ,Design and Technology University, Pune, India

Abstract: *While most communication today has shifted to the digital world, email remains the backbone of both personal and organizational communication. Also, notwithstanding the coming of more advanced communication channels, email remains a preferred medium for information interchange-and unfortunately, for cybercriminals too. Of these, one of the most enduring threats in this domain has been email spoofing: a cunning technique allowing attackers to impersonate trusted entities by manipulating email headers, sender identities, and message metadata. Traditional security measures, such as SPF, DKIM, and DMARC, were designed to protect the authenticity of emails; however, recent studies show that those mechanisms can still be bypassed through delegation loopholes, inconsistencies in forwarding, and improper configuration across domains.Therefore, spoofing remains a valid and prevalent kind of cyber threat in 2025. This research proposes Cybershield, a hybrid intelligent framework for the real-time detection of email spoofing at the server level, to address these evolving risks. Cybershield takes inspiration from the reliable spoofing detection using artificial intelligence by Mane et al. (2025), extending beyond static header verification to machine learning-based anomaly detection and adaptive trust scoring. The system will focus on in-depth analysis of email header fields such as "Received," "Return-Path," "From," and "Replyto," and will then apply classification algorithms like Random Forest, Support Vector Machines, and ensemble-based predictors that identify discrepancies pointing to spoofing attempts. Each incoming email is analyzed for syntactic validation, combined with its behavioral pattern and historical sender behavior, thus making detections proactive rather than reactive. The system is implemented on a Python-based backend with Flask and Node modules for easy integration with existing mail servers, ensuring scalability and minimum latency in processing. What makes the difference is that Cybershield's context-aware learning model evolves with new spoofing patterns. Unlike protocol-based validation, which fails when attackers manipulate delegation mechanisms, Cybershield constantly improves its detection accuracy through learning from false positives, user feedback, and cross-domain anomalies. Furthermore, the proposed framework provides an easy-to-use graphical interface-a "Spoof Guardian"-that allows both technical administrators and ordinary users to derive proper interpretations of the detection results and perform corrective actions. This bridges the gap between forensic-level spoofing analyses and practical, deployable defense mechanisms. Preliminary testing of Cybershield on a mixed dataset of legitimate and spoofed emails yielded a detection accuracy exceeding 96%, outperforming traditional SPF/DKIM-based validation. It had successfully detected spoofed emails that were misclassified as legitimate by traditional filters, particularly those based on forwarding and sender-inconsistency vulnerabilities. By integrating machine learning with cybersecurity principles and email protocol forensics, Cybershield takes a robust and reliable approach toward one of the most stubborn problems in cybersecurity: trust verification in digital communication. Beyond detection, this work relates to the larger discourse on the security of the email ecosystem, reinforcing the importance of intelligent automation in maintaining both the integrity of communication and the trust of users..*

Keywords: *Cybershield's*

DOI: 10.48175/IJARSCT-29736