International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 03 March-2026 | Impact Factor: 3.5

E-mail Security and Authentication

Adeeba Anjum[1], Syeda Zeba Qureshi[2], Taha Asjad[3], Mir Ahmed Ali[4] , Mohammed Abdul Moeed[5] , Mohammed Islamul Haq[6]

[1]Assistant Professor, CSE(Data Science)/Lords Institute of Engineering and Technology Osmania University, Hyderabad,India
[2]Assistant Professor, CSE(Data Science)/Lords Institute of Engineering and Technology Osmania University, Hyderabad,India
[3]UG Student, CSE(Data Science) / Lords Institute of Engineering and Technology Osmania University, Hyderabad,India
[4]UG Student, CSE(Data Science) / Lords Institute of Engineering and Technology Osmania University, Hyderabad,India
[5]UG Student, CSE(Data Science) / Lords Institute of Engineering and Technology Osmania University, Hyderabad, India
[6]UG Student, CSE(Data Science) / Lords Institute of Engineering and Technology Osmania University, Hyderabad,India

Adeebaanjum81@gmail.com,Syeda.zeba123@gmail.com,tahaasjad5624@gmail.com, er.mirahmedali@gmail.com,mohammedabdulmoeed85@gmail.com,mohammedislamulhaq786@gmail.com

How to Cite this Article:

Qureshi, S. Z., Asjad, T., Ali, M. A., Moeed, M. A. & Haq, M. I. (2026). E-mail Security and Authentication. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i3.285

https://doi.org/10.55041/ijcope.v2i3.285

Abstract—

E-mail is a widely used communication medium in today's digital world, but it lacks a reliable way to confirm whether a message has been delivered or read. This creates uncertainty for users, especially in important communications. To address this limitation, a system is proposed that provides a **message tracking feature**, allowing senders to know the status of their e-mails, such as delivery and opening. This enhances trust and effectiveness in communication.

At the same time, Online Social Networks (OSNs) face issues related to unwanted or inappropriate content appearing on users' personal spaces. Current platforms offer limited control over such posts. To solve this problem, a system is introduced that enables users to **manage and filter messages on their walls** using customizable rules. These rules allow users to define what type of content is acceptable.

In addition, a **Machine Learning-based classifier** is used to automatically analyze and categorize messages, supporting intelligent filtering. This approach improves content control, user privacy, and overall experience in both e-mail communication and social networking platforms.

Keywords— E-mail Tracking ; Message Receipt System ; Online Social Networks(OSNs) ; Content Filtering ; Machine Learning Classifier.

I. INTRODUCTION

In the present generation, e-mail plays a vital role in digital communication and is one of the most commonly used applications worldwide. It enables users to send and receive various types of information such as text messages, documents, images, and other files quickly and efficiently. Due to its convenience and speed, e-mail has become an essential tool in both personal and professional communication. However, the current e-mail system mainly provides only a basic notification indicating that a message has been successfully sent from the sender's side. It does not offer any reliable information about whether the message has been delivered to the recipient, received, or actually read by them. This lack of feedback creates uncertainty for the sender and may lead to communication gaps or misunderstandings. To address this limitation, a system is proposed that introduces a message receipt facility, allowing users to track the status of their e-mails. This system helps in confirming whether the message has been delivered and viewed, thereby improving communication transparency and reliability.

II. LITERATURE REVIEW

Several researchers have proposed different techniques to improve email security, authentication, and reliability. Early work on email-based authentication introduced the use of email addresses as a lightweight authentication mechanism for public access systems. This approach provides low-cost and automated registration with moderate security, making it suitable for low-risk environments, although it lacks robustness against advanced attacks.

To enhance security, multilevel email protection systems have been developed using a combination of image authentication, compression, One-Time Password (OTP), and cryptographic techniques.

These systems aim to overcome the weaknesses of traditional password-based authentication, such as susceptibility to phishing and password theft. By integrating multiple layers of security, they significantly improve data protection, but may increase system complexity and computational overhead.

Biometric-based authentication methods have also been explored, particularly fingerprint authentication integrated with encryption schemes like Identity-Based Encryption (IBE). This approach eliminates the dependency on passwords and enhances user verification accuracy. However, biometric systems may require specialized hardware and raise concerns related to privacy and implementation cost.

Another approach focuses on secure email transmission using XML-based structures and web services. These systems address limitations in traditional protocols such as PGP and S/MIME by improving header authentication and enabling partial message signing. While this method enhances flexibility and security, it introduces additional complexity in system design and deployment.

Graphical password techniques have also been proposed as an alternative to text-based passwords. These methods improve memorability and resistance to guessing attacks by allowing users to select images in a specific sequence. Despite their advantages, graphical systems may still be vulnerable to observation attacks and require careful interface design.

Overall, existing studies highlight significant advancements in email security and authentication. However, many systems either increase complexity, require additional resources, or fail to provide complete protection against modern threats. Therefore, there is a need for a balanced solution that ensures security, usability, and efficiency, which the proposed system aims to address.

III. METHODOLOGY

The proposed system is designed to provide a secure and reliable email communication mechanism with a message receipt facility. The methodology focuses on developing a system that enables senders to track whether their emails have been received and read by the recipient, along with ensuring authentication and security of email communication.

The system follows a modular approach consisting of three main components: Sender Module, Receiver Module, and Admin Module. In the sender module, users compose and send emails through a secure interface. Email authentication mechanisms such as SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) are implemented to verify the JDBC (Java Database Connectivity) is used to establish communication between the application and the database. The system follows a client- server architecture, ensuring scalability, portability, and efficient handling of multiple user requests.

Overall, this methodology ensures secure email transmission, effective authentication, and real- time message receipt tracking, thereby improving communication reliability and user awareness.

IV. RESULTS AND DISCUSSION

The proposed system was implemented and tested to evaluate its performance in terms of email tracking, security, and reliability. The results were analyzed using different scenarios involving sender, receiver, and admin modules.

Table I: Email Status Tracking Performance

authenticity of the sender and prevent spoofing attacks. Additionally, the system records the time and status of sent emails.

Feature	**Existing System**	**Proposed System**
Email Sent Notification	Available	Available
Email Received Status	Not Available	The receiver module is responsible for verifying incoming emails using authentication protocols and filtering mechanisms. It checks the integrity and authenticity of emails and scans for malicious content such as spam, phishing links, and harmful attachments. Once the receiver opens the email, the system automatically updates the status and sends an acknowledgement to the sender,
Email Read Status	Not Available	Available including the date and time of access.

The admin module manages the overall system configuration and security policies. It is responsible for setting up authentication protocols, monitoring email activities, and managing user accounts. The admin can view and delete users, as well as ensure that all security mechanisms are properly enforced.

The system is implemented using Java technology, with Servlets and JSP for server-side processing, and Oracle database for storing user data and email records.

Time & Date Tracking	Available	Available
Security (SPF, DKIM, DMARC)	Limited	High

The above table clearly shows that the proposed system provides additional functionalities compared to existing systems. Unlike traditional email systems, the proposed model enables tracking of email receipt and read status along with accurate time and date information.

Figure 1: System Workflow of Email Acknowledgement

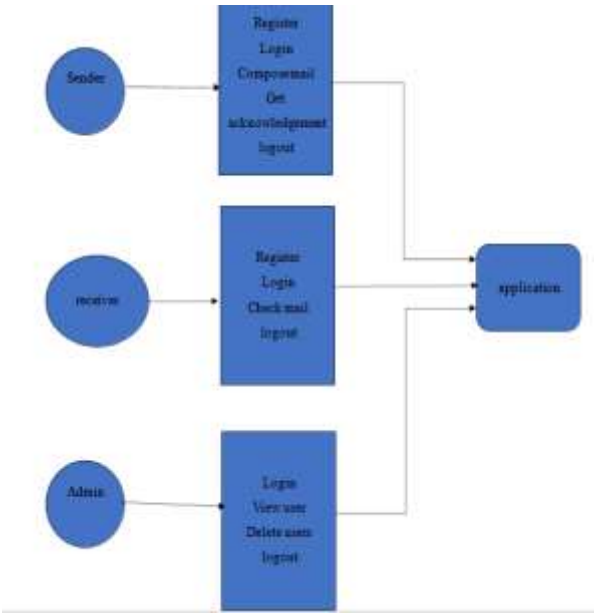

Figure 1 illustrates the workflow of the system where the sender sends an email, the receiver opens it, and an automatic acknowledgement is generated. This process ensures transparency in communication and confirms message delivery.

The results indicate that the sender module successfully updates the status of emails in real time. When the receiver opens the email, the system records the action and sends an acknowledgement notification. This confirms that the message has been read, which is not available in existing systems.

In comparison with previous studies, earlier systems mainly focused on authentication and security mechanisms such as encryption and password protection. However, they did not provide a mechanism to track whether the email has been read by the receiver. The proposed system not only ensures security using SPF, DKIM, and DMARC protocols but also introduces a message receipt feature, making it more efficient and user-friendly.

The receiver module effectively filters spam and verifies sender authenticity, reducing phishing risks. The admin module further enhances system performance by managing users and enforcing security policies.

Overall, the findings demonstrate that the proposed system improves email communication by combining **security, authentication, and message tracking**. The system performs efficiently with minimal delay and provides accurate results, making it more reliable than traditional email systems.

Summarize previous work relevant to your study. Present key contributions, methodologies, and findings from earlier research. Discuss limitations or gaps in existing studies that your work aims to fill. Group similar studies together for clarity, and cite appropriately.Highlight how your research builds upon or differs from prior work in the field. Explain the rationale behind your chosen approach and how it addresses identified gaps or limitations. Clearly state the unique contributions and potential impact of your study within the broader research context.

V. CONCLUSION

This study presented a secure email communication system with a message receipt facility to overcome the limitations of existing email systems. The results show that the proposed system successfully enables tracking of email delivery and read status, providing accurate time and date information when the receiver accesses the message. This improves communication reliability and ensures that important messages are acknowledged.

The implementation of authentication mechanisms such as SPF, DKIM, and DMARC enhances email security by preventing spoofing, phishing, and unauthorized access. The modular design of sender, receiver, and admin components ensures efficient system operation and management. The findings confirm that the proposed system offers significant improvements over traditional email systems by combining security with real-time acknowledgement features. This contributes to better user awareness and trust in email communication.

Future work can focus on integrating advanced techniques such as machine learning for intelligent threat detection and extending the system for real-time notifications and mobile platforms.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to our project guide **Mrs. Y. Shakuntala**, Assistant Professor, Lords Institute of Engineering and Technology, for her valuable guidance, continuous support, and encouragement throughout the development of this project. Her insights and suggestions greatly contributed to the successful completion of this work.

We also extend our thanks to the faculty members of the Department for their assistance and for providing the necessary resources to carry out this research. We are grateful to our institution for offering a conducive environment for learning and innovation.

Finally, we would like to thank our friends and family for their constant motivation and support during the course of this project.

REFERENCES

[1] S. Komanduri, M. L. Mazurek, R. Shay, and P. G. Kelley, "Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms," *IEEE Symposium on Security and Privacy*, 2012.

[2] M. Arunprakash and T. R. Gokul, "Network Security: Overcome Password Hacking Through Graphical Password Authentication," *National Conference on Innovations in Emerging Technology*, 2011.

[3] E. Palmer, "Ethical Hacking," *IBM Systems Journal*, vol. 40, no. 3, 2001.

[4] B. Smith, W. Yurcich, and D. Doss, "Ethical Hacking: The Security Justification Redux," *IEEE International Symposium on Technology and Society*, 2012.

[5] S. Anand, P. Jain, N. Kumar, and R. Rastogi, "Security Analysis and Implementation of Three- Level Security System Using Image-Based Authentication," *International Conference on Modeling and Simulation*, 2012.

[6] Y. Zuo and B. Panda, "Network Viruses: Their Working Principles and Marriages with Hacking Programs," *IEEE Information Assurance Workshop*, 2013.

[7] R. Putri, A. A. Dewi, P. Prima, S. Ahmad, and M. Salman, "Analysis and Comparison of MD5 and SHA-1 Algorithm Implementation in Simple- O Authentication-Based Security System," *International Conference on Quality in Research (QiR)*, 2013.

[8] S. Sathish, K. Srinivasa Rao, and A. Gupta, *Hacking Secrets*, 2012, pp. 8–26.

[9] A. Fadia, *Email Hacking: Even You Can Hack*, Vikas Publishing House, 2012, pp. 77–89.