International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 03 | March - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Survey Paper: Email Alert and Monitoring System Using a Web App

Rashida C K[1], Reshma S[2], S Amritha[3],Shreya D Nair[4],Silja Varghese[5]

Student[1],student[2],student[3],student[4],Assistant Professor[5]
of Computer Science Engineering Department,
Nehru College Of Engineering and Research Centre(NCERC),Thrissur,India

---

Abstract - Email correspondence is still a vital part of online communication, but it is becoming more and more susceptible to dangerous links, phishing scams, and spam. This study reviews the body of research on cybersecurity, automated response systems, and email alert systems. We compare several methods with our system, which incorporates an automatic answering bot and a dangerous link detection model, by examining previous studies on SMS/email notifications, spoof detection, and machine learning-based email classification. The study presents our system as an effective, real-time solution for email security and automation while highlighting the advantages and disadvantages of current approaches.

***Key Words*:** *survey, email, phishing, notification, alert*

1.INTRODUCTION

Traditional email monitoring solutions are not keeping up with the growing sophistication of cyber threats. Notification systems, intelligent filtering, and link verification models are just a few of the advancements brought about by the increasing need for automated email answers and security measures. Our suggested solution includes a hazardous link detection model that checks incoming messages for malicious URLs and an automated answering bot that reacts to emails according to predetermined instructions. In order to identify areas for improvement and possible difficulties, this study compares our system with earlier studies on automated email monitoring and security.

2. LITERATURE SURVEY AND COMPARISON

Notification systems that notify users when new emails or messages arrive have been the subject of numerous studies. In an effort to increase accessibility and guarantee that crucial messages are not missed, research has suggested email-based and SMS-based alert systems to notify users about emails they have received. In multi-story buildings where consumers are unable to physically check their mailboxes, some studies address the integration of alerting systems with centralized mail services[8],[2]. Although these methods offer rudimentary notification features, they lack content analysis for security issues and automated responses. Our technology, on the other hand, improves user interaction with incoming emails by integrating an automated reply function, going beyond basic warnings.

Automated email answers, especially those that let users choose precise criteria for getting messages, have also been the subject of studies. The usage of notification-based workflows, which guarantee users receive updates in response to predetermined triggers like modifications in data sources, has been studied [4],[10]. Although these systems do a good job of delivering structured notifications, they lack machine learning models and security checks to identify potentially dangerous content. Our solution improves on this strategy by alerting users, automatically replying, and scanning email content for possible dangers.

The issue of phishing and email spoofing has been thoroughly researched, and several techniques have been put out to identify fraudulent emails. Rule-based methods, like association rule mining, have been used in research to find patterns that point to shady emails. In order to detect deceit, these methods examine email features including word frequency and linguistic trends [11]. In a different study, spoofing assaults are actively monitored and controlled, with suspicious emails being identified and blocked before they are seen by consumers [9].Although these approaches offer fundamental security, they mostly rely on static rule-based detection, which might not be sufficient to counteract phishing attempts that are constantly developing. By adding a machine learning-based dangerous link detection model, our system outperforms current methods and enables dynamic and adaptive threat identification.

Recent developments have looked into integrating email alerts with messaging apps like WhatsApp in order to increase accessibility and provide real-time notifications. In order to guarantee that users receive important email notifications without having to manually check their inboxes, these research address connecting email systems with messaging platforms using automation tools [1],[3], [5],[6]. Although this connection improves ease, it doesn't automate responses or solve security issues. By concentrating on identifying and addressing email-based dangers instead than merely sending out notifications, our approach puts security first.

2.1. THE ROLE OF ARTIFICIAL INTELLIGENCE IN EMAIL SECURITY

Email filtering techniques based on rules are becoming insufficient due to the growing complexity of cyber threats. Email security is greatly improved by AI-driven technologies, especially machine learning (ML) and natural language processing (NLP). While unsupervised models identify novel phishing techniques by detecting abnormalities in incoming emails, supervised learning models may categorize malicious emails based on historical data. By comprehending the contextual meaning of communications, deep learning models have also been investigated to enhance email classification.
By adding a dangerous link detection model that dynamically examines incoming URLs for possible dangers, our system leverages AI. AI-based detection continuously adjusts to changing cyberthreats, in contrast to static blacklists that need frequent manual updates. By increasing the detection rate of dangerous links and phishing emails, this method lowers the possibility of security breaches.

2.2. CHALLENGES IN AUTOMATED EMAIL RESPONSE SYSTEMS

Although automation increases productivity, there are a number of difficulties when incorporating automatic response bots into email systems. Context awareness is important because pre-written responses might not always be suitable for complex discussions. A balance between human interaction and AI-driven automation is necessary because an over-reliance on automation can result in mistakes in sensitive or professional email discussions.
Another issue is security; by sending phony emails intended to trick bots into answering with private data, attackers can take advantage of automated systems. Maintaining security requires making sure the bot screens out questionable communications and adheres to stringent response guidelines.
In order to overcome these difficulties, our approach allows rule-based automatic responses rather than entirely AI-driven dialogues, guaranteeing regulated interactions.
Our harmful link identification technology also serves as a security layer, keeping the bot away from bad information. Contextual awareness powered by AI may improve automated response accuracy in the future while preserving security.

2.3. MACHINE LEARNING FOR HARMFUL LINK DETECTION

Machine learning-based detection systems are now crucial due to the rise in phishing and malware threats. AI-powered models have the ability to dynamically evaluate URLs based on a variety of criteria, such as redirection behavior, page content, and domain reputation, in contrast to static blacklists. This section looks at various methods for identifying hazardous links, including supervised learning for classification, heuristic-based methods for anomaly detection, and Natural Language Processing (NLP) for text analysis. There is also discussion of difficulties such adversarial attacks, false positives, and the requirement for ongoing model training.

2.4. FUTURE TRENDS IN EMAIL SECURITY AND AUTOMATION

Adaptive threat detection, AI-driven automation, and smooth connection with other communication platforms are key components of email security in the future. New technologies like quantum-resistant encryption, federated learning for decentralized security, and blockchain-based email authentication are becoming more popular. These patterns are examined in this section along with their potential integration into next email monitoring systems. Furthermore, developments in real-time URL analysis for better phishing detection and natural language processing (NLP) for more intelligent automated responses are covered.

5. DISCUSSION AND CHALLENGES

Email automation and security have advanced, yet a number of issues still exist. Since trustworthy URLs might occasionally be marked as dangerous, false positives in link detection are still a problem. Since fully automated responses might not always be suitable for sensitive communications, it's also crucial to strike a balance between automation and user control. Scalability is another problem because it takes effective resource management to handle high email traffic volumes while preserving fast reaction times and precise threat detection.

6. CONCLUSION AND FUTURE DIRECTIONS

This study compares our automated email system, which incorporates automatic answers and dangerous link identification, with other email monitoring, alert, and security solutions already in use. Our strategy blends automation and security, providing a more reliable defense against contemporary email threats than conventional notification systems or rule-based spam filters.
Future developments could include real-time phishing analysis through web scraping and behavioral modeling, improved AI-driven email responses using Natural Language Processing (NLP) for more context-aware automated replies, and multi-platform integration to extend security alerts across messaging apps like Signal and Telegram. Email communication will become safer and more effective as a result of these developments, which will also enhance email security and user experience.

REFERENCES

1. Abinaya, V., & Shobika, J. (2023).Email alerts on WhatsApp.EPRAInternationalJournalofResearch&Development(IJRD),8(5). https://eprajournals.com/IJSR/article/10537
2. Paluri, S. C. V., & Nag, S. K. (2022). Development of email notification system based on user criteria. International Research Journal of Engineering and Technology, 9(7), 2393-2396. https://www.irjet.net/archives/V9/i7/IRJET-V9I7439.pdf
3. Shishodia, M., Pal, S., & Shyamsundar. (2022). Email Alerts on Whatsapp. International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), 2(2), 112 . doi: 10.48175/568
4. Bazinette, Vincent & Cohen, Norman & Ebling, Maria & Hunt, Guerney & Lei, Hui & Purakayastha, Apratim & Stewart, Gregory & Wong , Danny.(2001)An intelligent Luke & Yeh, notificationsystem.RCComputerScience.22089. https://www.researchate.net/publication/228970929_An_intelligent_notification_syste m
5. Sakshi.K, Darshan.I, Maroof M, Sushant.J, & Kute, M.K. (2023). Email alerts on WhatsApp. EPRA International Journal of Research and Development(IJRD),8(5). https://doi.org/10.36713/epra2016
6. Lalitha, N., Neelima, N., Sravya, S., & Kumar, G. P. (2021). Email alerts on WhatsApp. Journal of Emerging Technologies and Innovative Research,8(7).Retrievedfrom https://www.jetir.org/papers/JETIR2107092.pdf
7. Rector, K., & Hailpern, J. M. (2014). MinEMail: SMS alert system for managing critical emails. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 783-792). ACM. https://doi.org/10.1145/2556288.2557182
8. Nanwin, D. N., & Williams, D. O. (2018). Development of an automated SMS alert mailing system. RIK International Journal of Science and Technology Research, 8(3), 110-115.Retrievedfrom https://www.researchgate.net
9. T. P. Fowdur and L. Veerasoo, "An email application with active spoof monitoring and control," 2016 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2016, pp. 1-6, doi: 10.1109/ICCCI.2016.7480002.
10. S. K. a. Subramaniam, S. H. b. Husin, Y. b. Yusop and A. H. b. Hamidon, "Real time mailbox alert system via SMS or email," 2007 Asia-Pacific Conference on Applied Electromagnetics, Melaka, Malaysia, 2007, pp. 1-4, doi: 10.1109/APACE.2007.4603963.
11. S. Appavu, Muthu Pandian and R. Rajaram, "Association Rule Mining for Suspicious Email Detection: A Data Mining Approach," 2007 IEEE Intelligence and Security Informatics, New Brunswick, NJ, USA, 2007, pp. 316-323, doi: 10.1109/ISI.2007.379491.
12. "EmailEye: An Email Alert System Using a WebApp" Rashida C K, Reshma S, S Amritha, Shreya D Nair, Silja Varghese Computer Science Engineering, Nehru College Of Engineering and Research Centre.