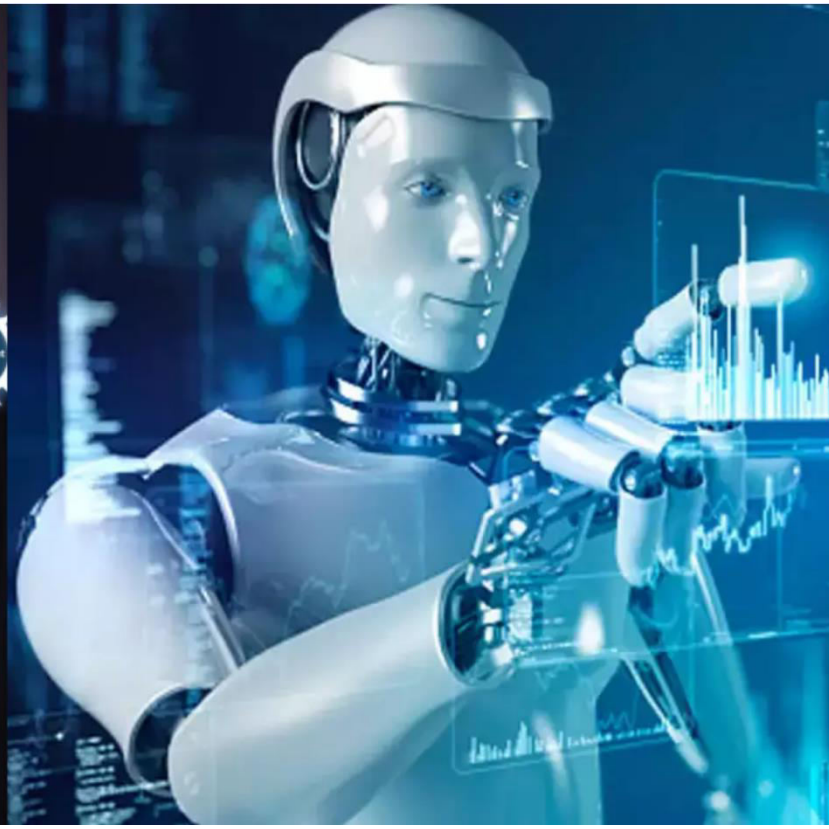
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Special Issue 1, January 2026

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

International Conference on Emerging Technologies and Pharmaceutical Research (ICETPR 2026)

17–18 January 2026

Indala College of Engineering, Polytechnic & Pharmacy, Kalyan, MH, India

|Volume 15, Special Issue 1, January 2026|

Temporary Mail Blocking System

Pranav Vishal Shinde[1], Dhaval Dilip Sarode[2], Siddesh Sandeep Sonvane[3], Latesh Chaudhary[4]

UG Student, Dept. of Information Technology, Indala College of Engineering, Kalyan, Maharashtra, India[1,2,3,4]

ABSTRACT: Email has become an essential communication platform for both personal and professional activities. However, the rapid growth of digital communication has also resulted in excessive unwanted emails such as promotional messages, spam, and disposable or temporary emails. These emails clutter inboxes, reduce productivity, and introduce potential security threats. Existing email filtering systems mainly focus on permanent blocking and conventional spam detection techniques, which fail to provide flexible, time-based control over incoming messages.

This review paper presents a detailed study of a Temporary Mail Blocking System, which allows users to temporarily restrict emails from specific senders, domains, or disposable email services for a defined time period. The system combines artificial intelligent email classification with High-Performance Computing (HPC) techniques to achieve fast and scalable processing. Various existing approaches such as rule-based filtering, blacklist-based detection, spam classification, and parallel computing frameworks are analyzed. The paper highlights the limitations of current systems and identifies research gaps that justify the need for an adaptive, high-speed, and user-centric temporary email blocking solution

KEYWORDS: Temporary Mail Blocking, Email Filtering Systems, Disposable Email Detection, Artificial Intelligence High-Performance Computing, Spam Management, Adaptive Email Control, Email Security

I. INTRODUCTION

Email is one of the most widely used communication tools in the modern digital era. It is extensively utilized for official communication, online registrations, marketing, and personal messaging. Despite its advantages, users face serious challenges due to the increasing volume of unwanted emails, including advertisements, newsletters, spam, and messages generated using temporary or disposable email addresses.

Traditional email filtering mechanisms are primarily designed for permanent blocking of spam emails. While these systems are effective to some extent, they do not provide users with flexibility for temporary control. In real-life scenarios, users may wish to block certain emails only for a limited duration, such as during examinations, work deadlines, or vacations. Existing platforms require manual rule creation and deletion, which is inefficient and inconvenient.

Another major concern is the misuse of disposable email addresses, which are commonly used to bypass authentication systems, create fake accounts, and distribute spam. Although Artificial Intelligence techniques have improved spam detection accuracy, their application in temporary and adaptive email blocking remains limited. Additionally, most systems are not optimized for real-time processing of large volumes of emails.

This review paper studies existing research related to email filtering, AI-Based classification, disposable email detection, and HPC-based optimization. The objective is to analyze current techniques, identify their drawbacks, and emphasize the importance of an intelligent Temporary Mail Blocking System.

II. SYSTEM MODEL

The proposed system model for the Temporary Mail Blocking System is designed to intelligently detect, classify, and temporarily restrict unwanted or disposable email messages using a combination of AI techniques and High-Performance Computing (HPC) principles. The system follows a modular and structured workflow to ensure high accuracy, scalability, and efficient processing of large volumes of email data in real time.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

International Conference on Emerging Technologies and Pharmaceutical Research (ICETPR 2026)

17–18 January 2026

Indala College of Engineering, Polytechnic & Pharmacy, Kalyan, MH, India

|Volume 15, Special Issue 1, January 2026|

The system accepts heterogeneous email-related inputs such as sender email addresses, domain information, email headers, content metadata, user-defined preferences, and historical interaction logs. These inputs may originate from multiple sources including mail servers, registration forms, or application-level email gateways. Since raw email data may contain redundancy, noise, and inconsistent formatting, an initial preprocessing module is employed.

The data preprocessing module performs email format validation, duplicate removal, normalization of textual data, and extraction of relevant metadata such as domain names and timestamps. Disposable or suspicious domains are preliminarily checked against known domain repositories. The cleaned and standardized data is then forwarded to the feature extraction stage.

In the feature engineering module, meaningful attributes are derived from the preprocessed data, including domain length, character entropy, frequency of numeric or special characters, sender reputation score, email arrival patterns, and user interaction history. These features effectively represent behavioral and structural characteristics of legitimate and temporary email addresses.

The core analytical component consists of Artificial intelligent email classification. In addition, adaptive learning mechanisms analyze user behavior to predict temporary blocking requirements. To achieve high-speed processing, HPC techniques such as multithreading and parallel execution are applied, enabling simultaneous analysis of multiple emails.

Model performance is evaluated using standard classification metrics such as accuracy, precision, recall, F1-score, and false positive rate. Based on the classification results and user-defined time constraints, emails identified as temporary or unwanted are blocked for a specified duration. Once the blocking period expires, the emails are automatically allowed without requiring manual intervention.

The final output of the system provides a filtered inbox with reduced clutter, temporary block logs, and performance summaries. This enables users and administrators to manage email flow efficiently while maintaining flexibility, security, and productivity.

III. EFFICIENT COMMUNICATION

Efficient communication refers to the optimized flow of data and control information between different components of the Temporary Mail Blocking System to ensure timely, accurate, and scalable email processing. Since the system handles large volumes of heterogeneous email data in real time, efficient communication mechanisms are essential to reduce computational overhead, minimize latency, and maintain high throughput.

At the data acquisition stage, incoming emails, sender metadata, domain information, and user preference data are collected from multiple sources such as mail servers, application gateways, and registration systems. These inputs are transmitted to a centralized processing unit using standardized data formats to ensure consistency and compatibility across system modules. Batch-based data transfer techniques are employed to reduce redundant communication and improve overall system efficiency.

During the preprocessing and feature extraction stages, only relevant and refined information—such as validated email domains, extracted metadata, and computed feature vectors—is forwarded to the Artificial Intelligence module. This selective communication strategy reduces data dimensionality and prevents unnecessary transfer of raw email content, thereby enhancing processing speed and protecting user privacy. Intermediate results, including cleaned data and extracted features, are stored locally to avoid repeated computation and excessive inter-module communication.

The Artificial Intelligence module communicates compact classification outputs, such as prediction labels (temporary or legitimate), confidence scores, and blocking duration indicators, instead of transmitting full datasets. This lightweight exchange minimizes communication overhead while preserving all critical information required for decision-making. Performance metrics such as accuracy, precision, recall, and false positive rates are computed efficiently and shared with the control module to enable rapid evaluation and system tuning.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

International Conference on Emerging Technologies and Pharmaceutical Research (ICETPR 2026)

17–18 January 2026

Indala College of Engineering, Polytechnic & Pharmacy, Kalyan, MH, India

|Volume 15, Special Issue 1, January 2026|

IV. SECURITY

Security is a critical requirement in the Temporary Mail Blocking System, as email platforms are frequent targets of spam attacks, fraudulent registrations, phishing attempts, and misuse of disposable or temporary email addresses. The system is designed to ensure secure handling of email data while preventing malicious activities that exploit temporary email services.

The primary security objective of the system is to detect, classify, and restrict malicious or disposable email usage without affecting legitimate users. Since email data may originate from untrusted or external sources, the system continuously monitors incoming emails and registration requests to identify suspicious patterns. This process is performed without requiring any changes to existing email infrastructure, making the system compatible with standard mail servers and applications.

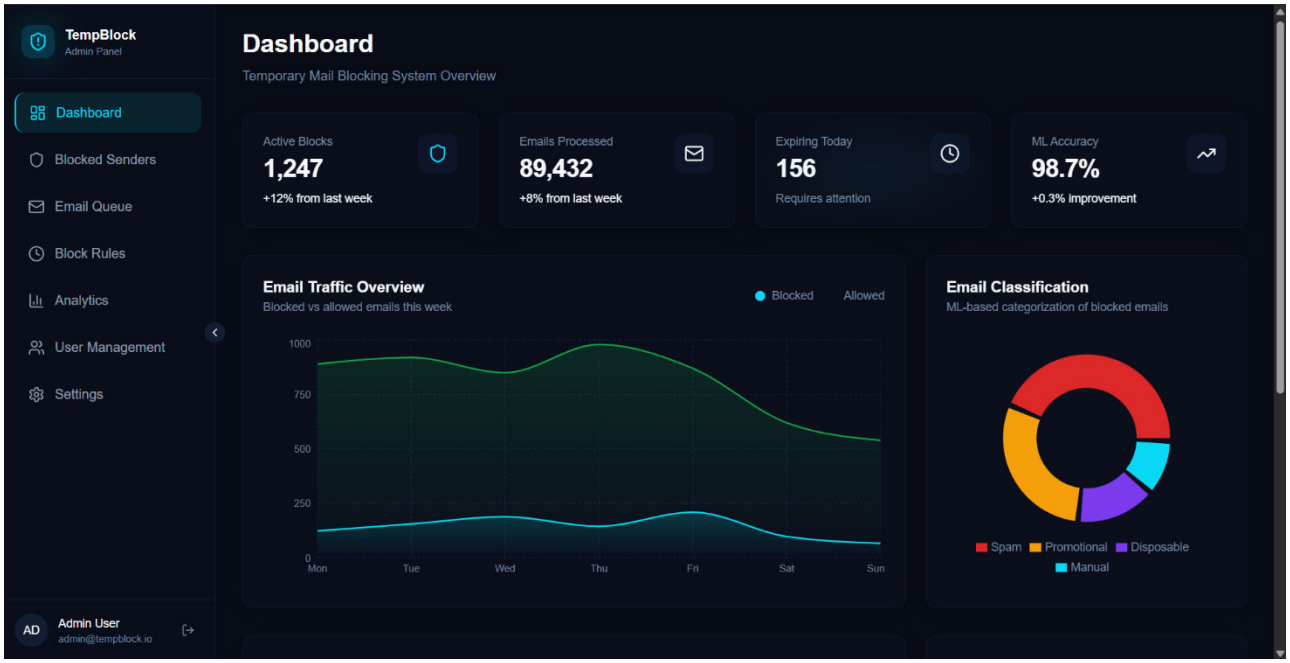
A. Email Detection and Classification Security

The system employs Artificial Intelligence–based detection to identify temporary or suspicious email addresses. Features such as domain reputation, character entropy, frequency of usage, and historical behavior are analyzed to distinguish legitimate users from malicious ones. This intelligent classification helps prevent attackers from bypassing security mechanisms using disposable emails.

B. Cooperative and Adaptive Detection

To improve reliability, the system supports adaptive learning using shared knowledge from previously detected temporary domains and user interaction patterns. Locally collected detection results are aggregated to construct a trusted decision environment. However, this collaborative information exchange may introduce vulnerabilities if false data is injected.

V. RESULTS



ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

International Conference on Emerging Technologies and Pharmaceutical Research (ICETPR 2026)

17–18 January 2026

Indala College of Engineering, Polytechnic & Pharmacy, Kalyan, MH, India

|Volume 15, Special Issue 1, January 2026|

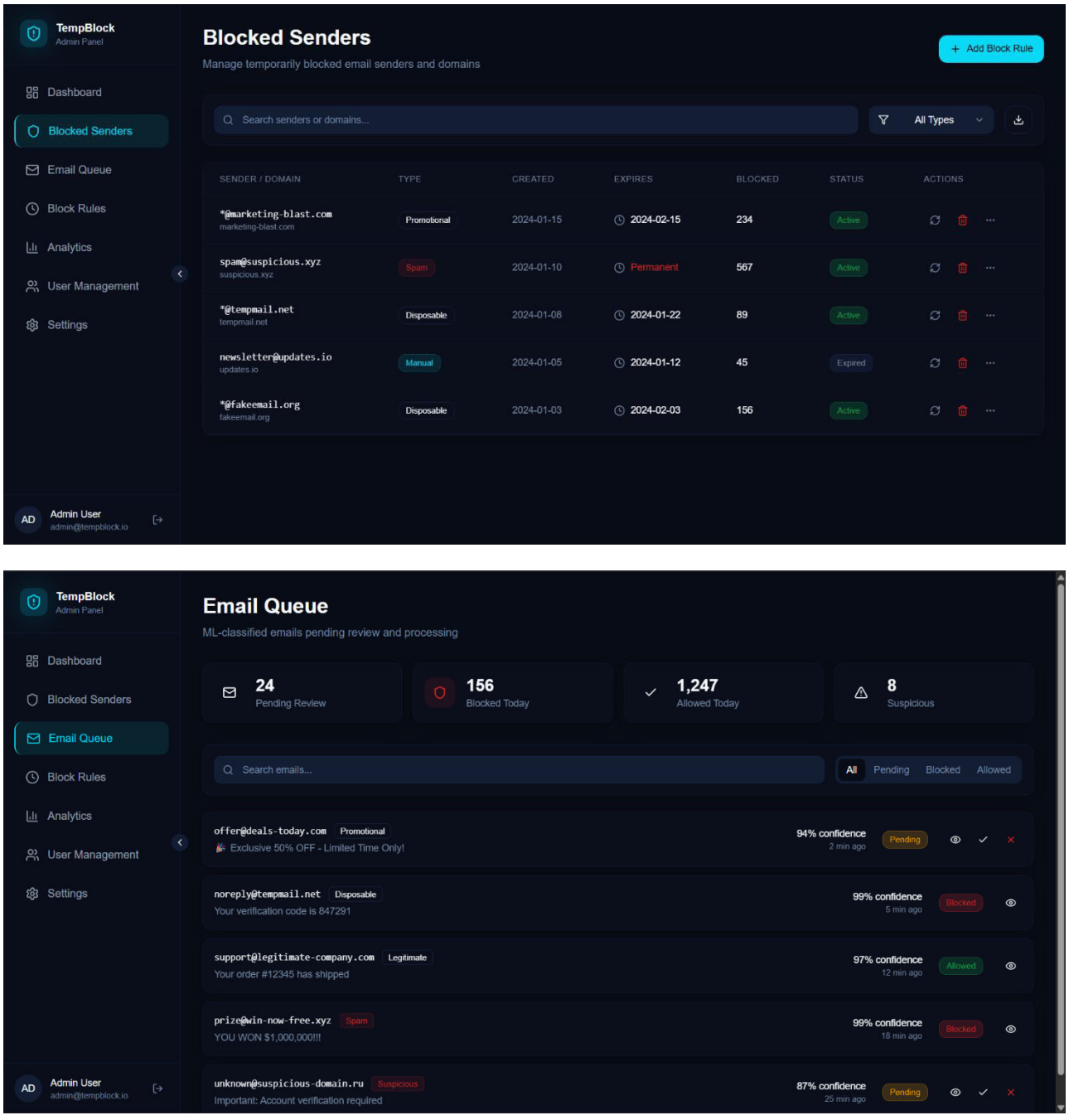


FIG 6.1 RESULTS OF THE PROJECT

VI. CONCLUSION

This review paper examined existing techniques for email filtering, spam detection, and disposable email identification. While Artificial Intelligence has significantly enhanced classification accuracy, current systems lack support for temporary email control and efficient large-scale processing. The absence of High-Performance Computing further limits real-time performance.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

International Conference on Emerging Technologies and Pharmaceutical Research (ICETPR 2026)

17–18 January 2026

Indala College of Engineering, Polytechnic & Pharmacy, Kalyan, MH, India

|Volume 15, Special Issue 1, January 2026|

The study concludes that a Temporary Mail Blocking System integrating HPC can effectively address these challenges. Such a system offers flexible, intelligent, and scalable email management, reduces inbox clutter, and enhances productivity and security. Future work may focus on real-time deployment, cloud-based integration, and advanced user behavior modeling.

REFERENCES

1. GeeksforGeeks, "Parallel Processing in C++ Using OpenMP," 2024. Available: https://www.geeksforgeeks.org/parallel-processing-in-cpp-using-openmp/
2. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, Cambridge, 2016.
3. J. Han, M. Kamber, and J. Pei, *Data Mining: Concepts and Techniques*, 3rd ed., Morgan Kaufmann, 2011.
4. S. Saini and J. Kaur, "Detection of Disposable and Temporary Email Addresses Using Machine Learning," *International Journal of Computer Applications*, vol. 175, no. 35, pp. 22–26, 2020.
5. V. Sharma and R. S. Thakur, "Parallel Implementation of Machine Learning Algorithms Using High-Performance Computing," *IEEE Access*, vol. 8, pp. 148720–148734, 2020.
6. Alomari and B. B. Gupta, "A Machine Learning-Based Framework for Email Spam Detection," *Journal of Network and Computer Applications*, Elsevier, 2021.
7. T. Fawcett, "An Introduction to ROC Analysis," *Pattern Recognition Letters*, vol. 27, no. 8, pp. 861–874, 2006.
8. OpenMP Architecture Review Board, *OpenMP Application Programming Interface*, Version 5.2, 2023.
9. Message Passing Interface (MPI) Forum, *MPI: A Message-Passing Interface Standard*, Version 4.1, 2023.
10. S. Rajasekaran and P. Ghosh, *High Performance Computing: Paradigm and Infrastructure*, CRC Press, 2018.
11. W. Tang and J. Dongarra, *Introduction to Parallel Computing Using C++ and MPI*, Cambridge University Press, 2019.
12. Y. Freund and R. E. Schapire, "A Decision-Theoretic Generalization of Online Learning and an Application to Boosting," *Journal of Computer and System Sciences*, vol. 55, no. 1, pp. 119–139, 1997.
13. Cloudflare Inc., "Blocking Disposable and Temporary Email Addresses Using Domain Intelligence," Cloudflare Blog, 2024.
14. GitHub Repository, "Disposable and Temporary Email Domain Lists," 2024. Available: https://github.com/disposable-email-domains

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details