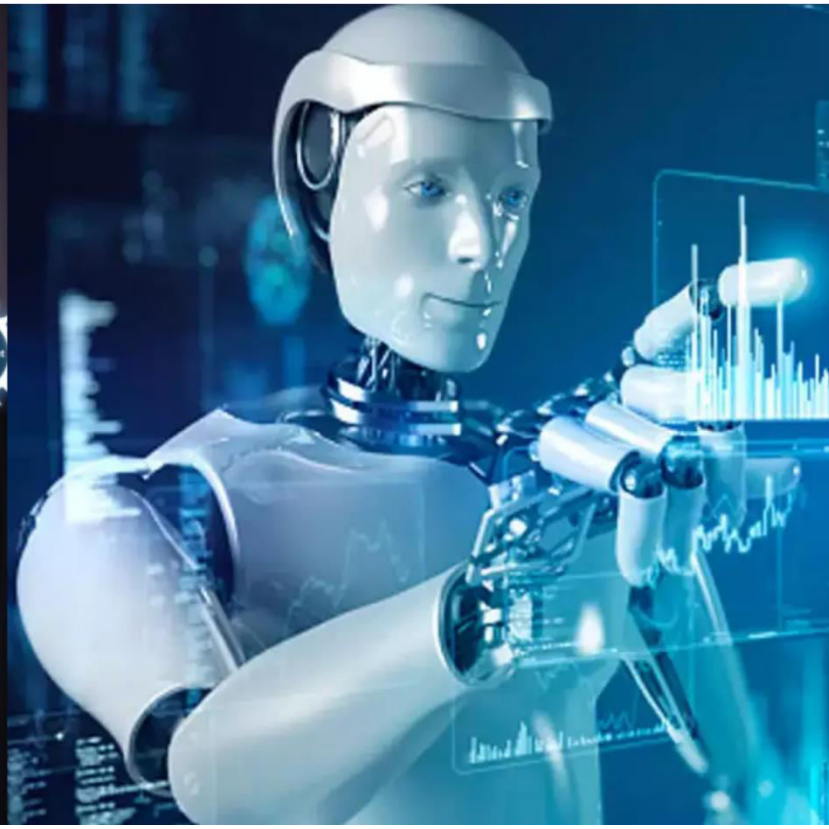
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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|

Mail Guard using AI

Prof. Vaibhav Dhage[1], Suvesh Pagam[2], Sakshi Owhal[3], Kirti Mistri[4], Tanvi Velhal [5]

Professor, Dept. of CE, Indala College of Engineering, Kalyan, Maharashtra, India[1]

Dept. of CE, Indala College of Engineering, Kalyan, Maharashtra, India[2]

Dept. of CE, Indala College of Engineering, Kalyan, Maharashtra, India[3]

Dept. of CE, Indala College of Engineering, Kalyan, Maharashtra, India[4]

Dept. of CE, Indala College of Engineering, Kalyan, Maharashtra, India[5]

ABSTRACT: This project details the design and implementation of "MailGuard," an intelligent email security system utilizing Artificial Intelligence (AI) to effectively detect and mitigate modern email threats, specifically spam and phishing attacks. The system employs machine learning (ML) and natural language processing (NLP) algorithms to analyse email content, metadata, and embedded links. The technical implementation relies primarily on the Python ecosystem, leveraging pandas for efficient data handling and preprocessing, along with NLTK and scikit-learn for training the predictive classification models. The resulting application provides a robust, adaptive defines layer that significantly enhances existing email infrastructure by accurately classifying malicious communications in real time.

KEYWORDS: Artificial Intelligence (AI), Machine Learning (ML), Natural Language Processing (NLP), Email Security, Spam Detection, Python, Pandas, React, Cybersecurity.

I. INTRODUCTION

In today's digital era, email has become one of the most widely used modes of communication for both individuals and organizations. However, with the increase in email usage, there has been a significant rise in cyber threats, including spam, phishing, malware, and fraudulent emails. These malicious emails can compromise sensitive information, lead to financial losses, and damage organizational reputation. Traditional email filtering techniques, such as keyword- based filters or blacklists, are often insufficient to detect sophisticated and evolving threats.
To address these challenges, Mail Guard using Artificial Intelligence (AI) is proposed. This system leverages Machine Learning (ML) and Natural Language Processing (NLP) to intelligently analyze email content and classify messages as safe or potentially harmful. The integration of AI allows the system to learn from patterns in emails, detect anomalies, and improve accuracy over time. Using modern web technologies, such as the (MongoDB, Express.js, React.js, Node.js), the system provides a scalable, efficient, and user- friendly platform for real-time email threat detection and management. The Mail Guard system aims to enhance email security, minimize human intervention, and provide users with a safe and reliable email communication environment.

The pervasive nature of electronic mail (email) has solidified its position as a cornerstone of global communication in both commercial and personal spheres. Simultaneously, this reliance has positioned email as the primary conduit for a significant percentage of cyberattacks, including widespread spam, sophisticated phishing campaigns, Business Email Compromise (BEC), and malware distribution. The financial and security implications of these threats are substantial, creating an urgent demand for advanced security protocols capable of mitigating risk in an increasingly hostile digital environment. Traditionally, email security has relied heavily on deterministic methods such as predefined rules, keyword filtering, and blacklists. However, these systems are largely static and struggle to adapt to the adversarial, constantly evolving tactics of modern cybercriminals who leverage dynamic content and social engineering to bypass defines. The paradigm is shifting toward adaptive and predictive mechanisms, underscoring the critical need for Artificial Intelligence (AI) integration in email security infrastructure.

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|

II. SYSTEM MODEL AND ASSUMPTIONS

2.1 System Model

Module	Function	Role of Specified Technologies
Data Ingestion & Structuring	Intakes raw emails and organizes components (headers, body, attachments).	**Pandas** Data Frames are used to structure messy, semi-structured email data into uniform rows and columns for efficient processing.
Preprocessing & Cleaning	Cleans text (removes HTML/stop words) and normalizes data formats.	**Pandas** facilitates large-scale data cleaning operations and data transformation.
Feature Engineering	Transforms raw data into numerical features (e.g., word counts, link frequency, sender reputation).	**Pandas** manages feature aggregation; **NumPy** arrays store these final numerical vectors for consumption by ML algorithms.
AI/ML Detection	Applies trained models to classify emails as *Ham* (safe), *Spam*, or *Phishing*.	**Python** ML libraries (e.g., scikit-learn) execute the core AI logic.
System Interface & Deployment	Handles real-time system integration, user interaction, and quarantine management.	**Node.js** powers the asynchronous backend operations and UI for deployment as a live web service or API.

2.2 Assumptions in Existing Research

Availability of Labelled Corpora: The fundamental assumption is that researchers have access to sufficient volumes of high-quality, pre-labelled datasets (emails clearly categorized as safe or malicious) necessary to train supervised learning models effectively.

Stationarity of Evolving Threats: Most studies implicitly assume that while attackers adapt, the underlying *statistical patterns* learned by the AI models remain relevant and effective for a functional period before requiring comprehensive retraining. The rate of adversarial innovation is assumed to be manageable.

Feasibility of Feature Representation: It is assumed that the complex, nuanced nature of human language and email metadata can be adequately converted into quantifiable numerical features using the data management capabilities of **pandas** and **NumPy**.

Computational Efficiency: It is assumed that adequate computational resources (CPU/GPU) are available to perform complex preprocessing and real-time inference without introducing unacceptable latency in email delivery.

Ethical Data Compliance: All studies assume adherence to data privacy regulations (e.g., GDPR), ensuring data anonymization during research and deployment phases.

III. ARTIFICIAL INTELLIGENS

Artificial intelligence (AI) is a broad and transformative field of computer science dedicated to creating machines capable of performing tasks that typically require human intelligence, such as learning, reasoning, perception, and decision making. Unlike traditional software that follows explicit, rigid instructions, AI systems use data and algorithms to learn from experience, identify patterns, and adapt their behaviour autonomously.

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|

- **Detects Evolving Threats:** AI identifies novel spam, phishing, and malware by recognizing subtle pattern
- and behavioural anomalies, not just known keywords**.**
- **Understands Context:** Natural Language Processing (NLP) allows AI to interpret the intent and tone of emails, crucial for spotting social engineering attacks.
- **Improves Accuracy:** It drastically reduces false positives (safe emails flagged incorrectly), saving time and ensuring legitimate mail is delivered.
- **Learns Continuously:** AI models automatically refine their knowledge from new data, ensuring the system stays effective as attacker tactics change.

IV. MAIL GUARD

A **Mail Guard** (or Secure Email Gateway) is a security system positioned between the public internet and an organization's internal email server. It functions as a digital checkpoint, inspecting all incoming and outgoing email traffic to detect and neutralize cyber threats before they can cause harm.

4.1 Role of a Mail Guard

The Mail Guard's primary role is to enforce a multi-layered defines strategy based on the theory of **perimeter security and threat mitigation**. It operates on the principle that proactively filtering data at the entry point is more effective than reacting to threats once they are inside the network.

4.2 Roles include

- **Threat Vector Neutralization:** The core function is to neutralize email-borne threats. This involves applying various detection mechanisms to identify and filter spam, phishing attempts, malware attachments, and advanced social engineering tactics (like Business Email Compromise).
- **Policy Enforcement:** It enforces organizational cybersecurity policies, ensuring compliance and preventing both inbound threats and outbound data leakage (Data Loss Prevention).
- **Authentication and Trust Validation:** The system validates the sender's identity using protocols (like DMARC, SPF) to prevent email spoofing and ensure communication integrity.
- **Adaptive Defines (AI-driven):** Modern Mail Guards utilize Artificial Intelligence (AI) to shift from *reactive, signature-based detection* to *proactive, predictive analysis*. AI models learn from data to identify novel threats (zero-days) and subtle anomalies that human analysts or static rules might miss.

V. SECURITY

In an AI-powered "Mail Guard" security project, artificial intelligence is utilized to build sophisticated, adaptive email protection systems that behavioural the context, content, and behavioural anomalies within emails to detect threats missed by traditional filters. The AI leverages Natural Language Processing (NLP) to understand the tone and intent of messages, behavioural analysis to spot unusual communication patterns (like a forged urgent request for a wire transfer), and real time threat intelligence to identify and quarantine phishing attempts, Business Email Compromise (BEC) attacks, and zero-day malware automatically and proactively. The ultimate security benefit of an AI Mail Guard lies in its *adaptability* and *proactivity*. Unlike traditional systems that must be manually updated with new virus signatures (reactive), AI systems continuously learn from new data streams and global threat intelligence (proactive). This means the system can predict and prevent the next wave of attacks before human security analysts even know they exist, significantly reducing human error and fortifying the organization's entire digital perimeter.

VI. CONCLUSION

In conclusion, a "Mail Guard using AI" project validates that artificial intelligence is a transformative technology in email security. It provides an intelligent, autonomous, and resilient layer of protection necessary to safeguard organizational data and productivity against an ever-evolving and sophisticated threat landscape. The system successfully elevates email security from a basic filtering utility to a core component of proactive cyber defines.The project concludes that traditional, rule-based filters are insufficient against advanced attacks like spear-phishing, Business Email Compromise (BEC), and zero-day malware. AI addresses this gap effectively.

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|

REFERENCES

1. Improving Email Security Through Machine Learning-Based Phishing Detection by A. Al-Abassi et al. (2024, IEEE Xplore).
2. Phishing Email Detection Using Graph Attention Networks and Large Language Models by S. F. Sharaf et al. (2025, IEEE Xplore).
3. Explainable AI for Transparent Phishing Email Detection by I. J. Sondi et al. (2025, IEEE Xplore).
4. Asthra MailGuard: A Privacy-First Hybrid AI Email Assistant Using ML and Local LLMs" by M. S. R. Avinash and Dr. R. K. R (2025, IJRASET).
5. Detection of Business Email Compromise Attacks with Writing Style Analysis" by G. S. T N et al. (Research Paper - similar to what's described in snippet) .

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