International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802249

Design and Implementation of an AI-Based Email Spam and Phishing Detection System

Haseena Begum S, Gokulasri S, K Gopal

Student, Department of Computer Science and Engineering, The Kavery Engineering College, Salem, India

Student, Department of Computer Science and Engineering, The Kavery Engineering College, Salem, India

Guide, Department of Computer Science and Engineering, The Kavery Engineering College, Salem, India

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT: The rapid growth of email communication has significantly increased the risk of spam and phishing attacks, posing serious threats to individuals and organizations worldwide. Traditional email filters often struggle to provide fast detection, adaptive security, and protection against sophisticated attackers who frequently change identities and network parameters. To overcome these limitations, this paper proposes an AI-Based Email Spam and Phishing Detection System designed for high-speed detection and enterprise-level email traffic of up to 232 Mbps. The system employs a layered model to independently analyze email headers, content, URLs, and sender , ensuring robust protection against complex and multi-stage phishing attacks. Advanced AI techniques including machine learning classification and Natural Language Processing (NLP) intelligently classify spam and phishing emails by learning patterns from content, behavior, and traffic characteristics, continuously adapting to emerging threats. The framework further incorporates IP obfuscation and interchanging mechanisms to reduce exposure to reconnaissance and network exploitation attempts. Experimental evaluation demonstrates high detection accuracy, low response times, and enhanced network security, offering a fast, intelligent, and scalable email protection solution against evolving spam and phishing threats.

KEYWORDS: Email Spam Detection; Phishing Detection; Artificial Intelligence; Machine Learning; Natural Language Processing; Layered Firewall; IP Obfuscation; Deep Learning; Cybersecurity; Email Classification; TF-IDF; Random Forest

I. INTRODUCTION

The exponential growth of digital communication has made email one of the most widely used modes of interaction in both personal and professional domains. According to recent global statistics, over 300 billion emails are sent and received daily, making email infrastructure a critical component of the digital ecosystem. However, this widespread adoption has simultaneously created a fertile ground for cybercriminals who exploit email channels to distribute spam and execute sophisticated phishing campaigns.

Phishing attacks are designed to deceive recipients into divulging sensitive credentials, financial information, or installing malicious software. These attacks have grown in both frequency and complexity, causing billions of dollars in financial losses annually. The FBI Internet Crime Complaint Center reported phishing as the most prevalent cybercrime category in 2020, with adjusted losses exceeding 1.8 billion USD. Traditional email security tools such as rule-based spam filters and signature-based detection systems are increasingly inadequate against modern, adaptive threat strategies that continuously evolve to evade detection.

Contemporary attackers employ a variety of advanced techniques including zero-day exploits, polymorphic malware, domain spoofing, and social engineering to bypass conventional defenses. The static and reactive nature of rule-based systems makes them inherently vulnerable to such novel attacks. This critical gap in email security necessitates a paradigm shift toward intelligent, adaptive, and real-time detection systems powered by Artificial Intelligence (AI) and Machine Learning (ML).

This paper presents the design and implementation of an AI-Based Email Spam and Phishing Detection System that integrates multiple layers of security with advanced machine learning models. The proposed system is capable of

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802249

processing high-volume email traffic at enterprise scale, detecting threats within 60 seconds of receipt, and continuously learning from new attack patterns to improve its detection efficacy.

A. Problem Statement

Contemporary email security deployments suffer from several structural weaknesses. Rule-based filters relying on predefined rules and static blacklists are incapable of identifying zero-day phishing attacks that fall outside their pattern database. Signature-based detection systems require frequent manual updates and cannot adapt to rapidly evolving threat landscapes. Furthermore, existing single-layer security architectures create vulnerabilities to multi-stage phishing campaigns that bypass individual security controls. The lack of intelligent, real-time analysis mechanisms results in high false positive rates that disrupt legitimate communications while simultaneously allowing sophisticated threats to evade detection.

B. Motivation

Three converging trends motivate the development of this AI-based system. First, the increasing volume and sophistication of phishing attacks demand security solutions that can adapt faster than human-driven rule updates allow. Second, advancements in AI and ML have made it feasible to deploy lightweight yet powerful classification models that can process email features in real time. Third, enterprise environments require security systems that scale to handle hundreds of megabits per second of email traffic without performance degradation. These factors collectively create a compelling need for an intelligent, layered, and high-throughput email security framework.

C. Scope

The proposed system encompasses: (1) a multi-layered AI engine for real-time email classification into spam, phishing, or legitimate categories; (2) a layered firewall module providing independent analysis of email headers, body content, embedded URLs, and sender behavioural patterns; (3) an IP obfuscation and interchanging mechanism to prevent attacker reconnaissance; (4) an adaptive learning module that updates classification models based on newly encountered threat patterns; and (5) a high-throughput processing pipeline supporting enterprise-level email traffic up to 232 Mbps.

D. Contribution Summary

The key contributions of this paper are as follows:

- A novel multi-layered AI architecture for email spam and phishing detection that combines NLP, behavioral analysis, and URL inspection.
- Integration of IP obfuscation mechanisms that enhance system resilience against attacker reconnaissance and network-level exploitation.
- A high-speed detection pipeline capable of classifying email threats within 60 seconds at throughput rates up to 232 Mbps.
- Comprehensive experimental evaluation demonstrating superior detection accuracy, reduced false positive rates, and improved adaptability compared to traditional approaches.

II. LITERATURE REVIEW

The problem of email spam and phishing detection has been extensively studied in the research community, with solutions ranging from rule-based filters to advanced deep learning architectures. This section surveys key related works organized by the primary detection methodology employed.

A. Rule-Based and Signature-Based Approaches

Blanzieri and Bryl [2] provided a comprehensive survey of learning-based email spam filtering approaches, identifying that the Naive Bayes classifier holds a special position among multiple learning algorithms for spam filtering due to its speed and simplicity in achieving high precision results. Traditional anti-phishing tools based solely on rule-defined filters and compiled blocklists have substantial drawbacks, as they work only using patterns already known or malicious URLs, making them ineffective against new forms of phishing. Basnet et al. [3] demonstrated that rule-based systems tend to produce high false positives and require time-consuming manual updates that cannot keep pace with rapidly evolving phishing activity.

B. Machine Learning Based Detection

Rao and Pais [4] proposed an efficient feature-based machine learning framework for phishing website detection using supervised classifiers trained on URL structure, HTML content, and domain registration features. Their Neural

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802249

Computing and Applications study achieved high accuracy by extracting complex feature interactions. Bahnsen et al. [5] introduced DeepPhish, a simulated malicious AI system that demonstrated how adversaries could leverage deep learning to generate more sophisticated phishing URLs, simultaneously highlighting the arms race nature of AI-driven security. Saini et al. [6] demonstrated that ensemble techniques such as Random Forest and Gradient Boosting outperform individual classifiers in precision, recall, and F1-score for email spam detection across varied datasets.

C. Natural Language Processing Techniques

Adebowale et al. [7] demonstrated the feasibility of applying NLP features for machine learning-based identification of spear-phishing attacks on social networks. Their work showed that linguistic analysis of message content, including syntax, semantics, and stylistic elements, can effectively detect deceptive communication patterns employed by phishers. Siddiqui and Akhtar [8] established that sentiment analysis and keyword extraction can identify exploitative linguistic cues used by attackers to create urgency and compel user action. Islam and Abawajy [9] proposed a multi-tier phishing detection approach that combined NLP-based content analysis with URL inspection, achieving improved detection rates over single-modality systems.

D. Deep Learning and Neural Network Approaches

Mahmoud and Mahfouz [10] proposed detecting phishing using neural networks based on both textual and visual characteristics, achieving high detection efficacy for phishing sites by integrating image recognition with content analysis methods. Sabri and Mitrea [11] utilized Convolutional Neural Networks (CNNs) for image-based phishing detection, demonstrating that visual features of web pages and embedded logos can serve as reliable indicators of fraudulent content. Zhang et al. [12] showed that ensemble methods and neural networks achieved high accuracy in detecting phishing websites by extracting complex feature interactions that simpler models could not capture.

E. Real-Time and Ensemble Systems

Bergholz et al. [13] demonstrated that the effects of phishing could be minimized through sophisticated real-time machine learning filtering approaches, with high and more sophisticated ML methods significantly reducing phishing impact over earlier reactive approaches. Ghadage et al. [14] developed a Python-based email spam detection system utilizing Naive Bayes, Decision Trees, Random Forests, and SVM classifiers, demonstrating that Naive Bayes successfully detected over 95% of spam emails while maintaining low false positive rates. Al-Shanableh et al. [15] found that ensemble machine learning methods considerably improved overall spam detection effectiveness while maintaining low false positive rates compared to individual classifiers.

III. EXISTING SYSTEM

Current email security systems predominantly rely on traditional approaches that have significant limitations in addressing modern phishing and spam threats. Understanding these existing systems is crucial for identifying the gaps that the proposed AI-based solution aims to address.

A. Rule-Based Filters

Rule-based filters represent one of the earliest approaches to email security. These systems rely on predefined rules and known malicious patterns to identify and filter spam and phishing emails. Administrators manually configure rules based on common attack patterns, such as specific keywords, sender domains, or message structures associated with malicious content. While effective against known threats, rule-based systems struggle with zero-day attacks that do not match any existing pattern database.

B. Static Blacklists

Static blacklists maintain databases of known malicious IP addresses, domains, and email addresses that have been previously identified as sources of spam or phishing attacks. Email servers check incoming messages against these blacklists and reject or quarantine messages from listed sources. The primary limitation of this approach is its reactive nature - new attack sources are not blocked until they have been identified, reported, and added to the blacklist, creating a window of vulnerability.

C. Signature-Based Detection

Signature-based detection systems match email content against known malware signature databases. These systems excel at identifying previously encountered threats but are completely ineffective against novel attacks with unknown signatures. The approach requires continuous updates to signature databases and cannot adapt to polymorphic malware that changes its signature with each iteration.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802249

D. Manual Updates and Maintenance

All traditional email security systems require human intervention for rules, blacklists, and signatures updates. This manual maintenance creates delays in responding to new threats and increases operational overhead. Security teams must continuously monitor threat intelligence feeds, analyze new attack patterns, and update system configurations - a process that cannot keep pace with the speed at which modern attackers evolve their techniques.

Figure 1 illustrates the limitations of traditional phishing detection approaches:

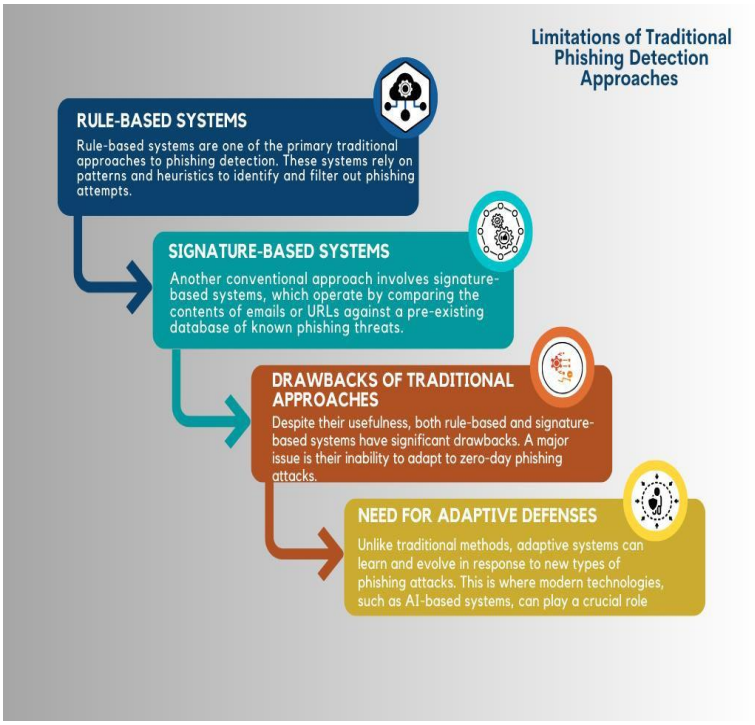

Fig.1. Limitations of Traditional Phishing Detection Approaches

E. Disadvantages of Existing Systems

• Data Limitations - Traditional systems cannot process and analyze the vast amounts of data required to identify sophisticated attack patterns.
• Adaptability to New Threats - Static rule sets and signatures cannot adapt to zero-day vulnerabilities and evolving attack techniques.
• Accuracy Concerns - High false positive rates disrupt legitimate communications while sophisticated threats evade detection.
• Performance and Efficiency - Manual updates and rule processing create bottlenecks that cannot scale to enterprise-level traffic.
• Sophistication of Attacks - Modern attackers employ advanced techniques that easily bypass traditional detection mechanisms.

IV. RESEARCH GAP

Despite significant advances in AI-based email security, several critical research gaps remain unaddressed in the existing literature:

First, most existing systems treat spam detection and phishing detection as separate problems with independent solutions. There is a lack of unified frameworks that simultaneously address both threat categories using a common detection engine while accounting for their distinct characteristics and attack vectors.

Second, the majority of proposed systems focus exclusively on content-based detection and do not incorporate network-level protection mechanisms. The absence of IP obfuscation and traffic analysis components leaves detection systems vulnerable to network-level reconnaissance and distributed attack campaigns.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802249

Third, existing research insufficiently addresses scalability requirements for enterprise email environments. Most proposed systems have been evaluated on laboratory-scale datasets and have not demonstrated capability to handle real-world enterprise traffic volumes in the range of hundreds of megabits per second.

Fourth, there is limited work on adaptive learning mechanisms that allow detection models to update continuously based on newly encountered threats without requiring complete model retraining. This limitation reduces the operational effectiveness of deployed systems over time as threat actors adapt their techniques.

The proposed system addresses these gaps by providing a unified, multi-layered framework that integrates content-based AI detection with network-level protection, demonstrates scalability to 232 Mbps throughput, and incorporates adaptive learning mechanisms for continuous threat adaptation.

V. PROPOSED SYSTEM AND METHODOLOGY

A. System Overview

The proposed AI-Based Email Spam and Phishing Detection System is designed as a multi-tier, high-throughput security framework that integrates AI-driven content analysis with network-level protection mechanisms. The system processes incoming emails through a four-layer security pipeline, each layer contributing orthogonal detection capabilities that collectively provide comprehensive protection against sophisticated email-based threats.

B. Data Collection and Preprocessing

The system employs multiple publicly available datasets for training and evaluation, including the SpamAssassin Public Corpus, Enron email dataset, PhishTank phishing URL repository, and OpenPhish feeds. Email preprocessing involves the following sequential steps:

- Text tokenization and normalization: raw email content is tokenized, stop words are removed, and words are stemmed or lemmatized to their base forms.
- Header analysis: sender IP, reply-to address, mail routing paths, and authentication headers (SPF, DKIM, DMARC) are extracted and validated.
- URL extraction and analysis: all embedded hyperlinks are extracted, decoded, and analyzed for suspicious structural patterns including URL shortening, IP-based addresses, and domain spoofing indicators.
- Feature engineering: a comprehensive feature vector is constructed combining TF-IDF weighted text features, URL-based features, behavioral sender features, and metadata features.

C. Machine Learning Classification

The classification layer employs an ensemble of complementary machine learning algorithms selected for their proven efficacy in text classification and anomaly detection tasks:

- Naive Bayes Classifier: serves as the first-stage filter, leveraging probabilistic word occurrence models to rapidly identify obvious spam patterns with high computational efficiency.
- Support Vector Machine (SVM): applied for its proven effectiveness in high-dimensional text classification, particularly for detecting subtle phishing content patterns.
- Random Forest Ensemble: combines multiple decision trees to achieve robust classification with reduced overfitting, effectively handling the complex feature interactions present in phishing emails.
- Deep Neural Network: a multi-layer perceptron with dropout regularization provides the final classification layer, capturing non-linear relationships in the combined feature representation.

Feature extraction employs both Bag-of-Words (BoW) and Term Frequency-Inverse Document Frequency (TF-IDF) representations, with word embeddings applied to capture semantic relationships between terms that improve detection of paraphrased phishing content.

D. Layered Firewall Protection

The layered firewall module implements a defense-in-depth strategy by combining four independent security layers: network-level packet filtering, application-level content inspection, behavioral analysis, and intrusion prevention. Each layer processes incoming email traffic independently, with threat verdicts aggregated through a weighted voting mechanism. This architecture ensures that multi-stage phishing attacks that successfully bypass one layer are detected by subsequent layers.

E. IP Obfuscation Mechanism

To prevent attacker reconnaissance and reduce exposure to direct network attacks, the system implements a dynamic IP interchanging mechanism. This component employs dynamic IP rotation using a pool of proxy addresses, anonymization techniques to mask the true server identity, and distributed traffic routing to prevent direct targeting.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802249

This mechanism is particularly effective against Distributed Denial of Service (DDoS) attacks and systematic probing attempts that often precede targeted phishing campaigns.

F. Adaptive Learning Module

The system incorporates an online learning component that continuously updates classification models based on newly detected threats and user-confirmed false positives. When a new threat pattern is identified, the system extracts representative features and incorporates them into the model training pipeline through incremental learning, allowing the detection system to adapt to zero-day threats without requiring complete model retraining.

VI. SYSTEM ARCHITECTURE AND WORKFLOW

The system architecture follows a layered processing pipeline with four primary components operating in sequence for each incoming email:

Stage 1 - Email Ingestion and Preprocessing: Incoming emails are received via SMTP interface and queued for processing. The preprocessing module extracts and normalizes email components including headers, body text, HTML content, attachments, and embedded URLs. This stage operates asynchronously to maintain high throughput.

Stage 2 - Feature Extraction: Preprocessed email components are transformed into numerical feature vectors through parallel feature extraction pipelines. Text content undergoes NLP processing to generate TF-IDF representations and semantic embeddings. URL components are analyzed for structural anomalies, domain registration age, SSL certificate validity, and redirect chains.

Stage 3 - Multi-Layer Classification: The extracted feature vectors are passed through the ensemble classification pipeline. Each classifier in the ensemble produces an independent probability score, which are aggregated through a meta-learning layer to produce a final classification verdict: legitimate, spam, or phishing. Emails classified as threats are quarantined and flagged for review.

Stage 4 - Network-Level Protection: Simultaneously with content analysis, the network protection module monitors sender IP reputation, applies firewall rules to filter known malicious sources, activates the IP obfuscation mechanism to mask server identity, and logs all traffic patterns for behavioral analysis and adaptive model updates.

Figure 2 shows the proposed system block diagram:

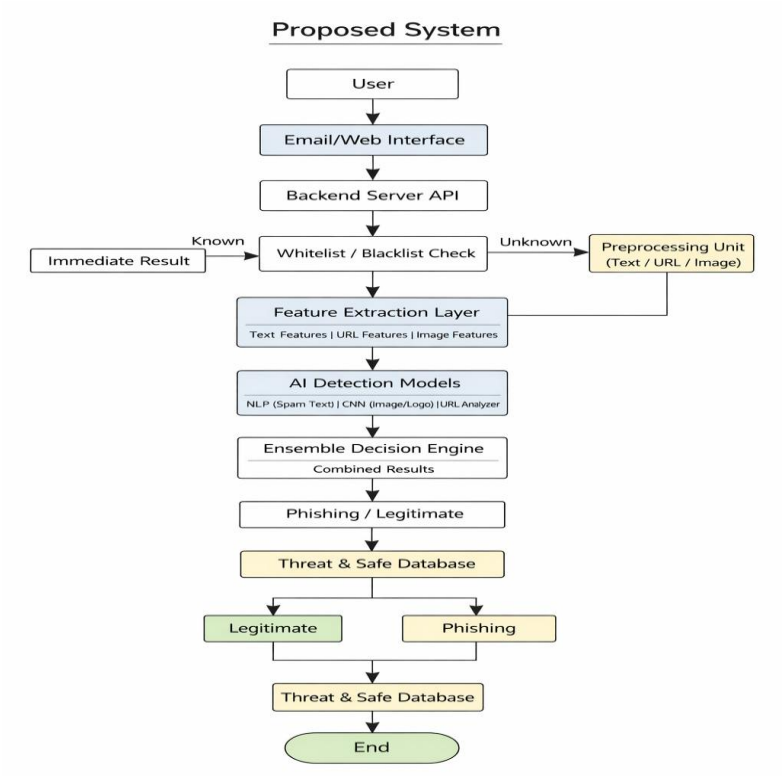

Fig.2. Proposed System Block Diagram

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802249

Figure 3 illustrates the AI-Based Email Spam and Phishing Detection Flowchart:

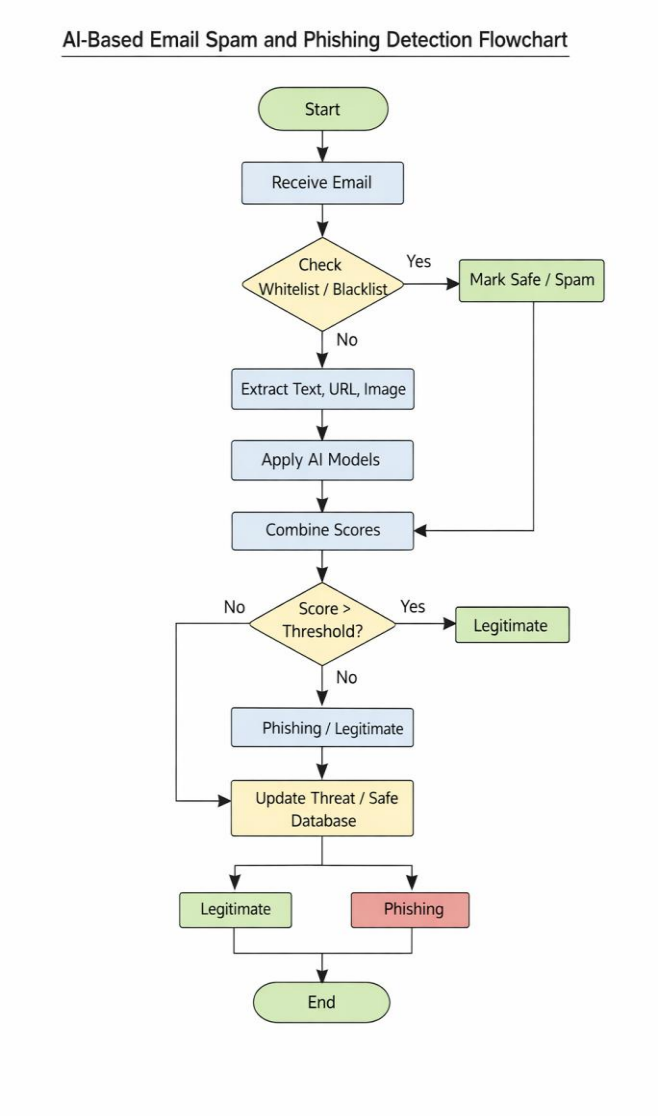

Fig.3. AI-Based Email Spam and Phishing Detection Flowchart

VII. ALGORITHMS AND MODULES USED

A. Fast Detection Mechanism

The Fast Detection Mechanism module is responsible for quickly identifying suspicious activities and potential threats within the system. This module continuously monitors system events, network traffic, and user behavior to detect abnormal patterns using predefined rules and pattern-matching techniques. When unusual activity is detected, the system immediately triggers alerts or initiates protective actions. The core detection logic employs statistical threshold analysis to identify anomalous email volumes and transmission patterns:

B. Layered Firewall Protection

The Layered Firewall Protection module applies a defense-in-depth strategy combining network-level filtering, application-level monitoring, and intrusion prevention systems. Each layer independently evaluates incoming email traffic against security policies. Allowed IP ranges are validated, content signatures are matched against threat databases, and behavioral anomalies are flagged for elevated scrutiny. The module implements whitelisting for verified enterprise senders and dynamic blacklisting for confirmed malicious sources.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802249

C. IP Interchanging and Obfuscation

The IP Interchanging and Obfuscation module dynamically rotates the outward-facing IP address used for server communication from a managed pool of proxy addresses. This prevents attackers from establishing a persistent target for reconnaissance or direct attacks. The mechanism employs randomized selection from an IP pool, with rotation frequency scaled to detected threat levels. This component reduces the success rate of network-level attack reconnaissance by ensuring that repeated probing attempts encounter different network endpoints.

D. Advanced AI-Based Detection

The Advanced AI-Based Detection module applies machine learning and anomaly detection to analyze email features and network activity patterns. The module maintains behavioral baselines for normal email traffic and applies statistical deviation analysis to identify suspicious patterns. Unlike traditional rule-based systems, the AI module learns from historical threat data and continuously refines its detection boundaries. The core anomaly detection logic identifies deviations from established baselines:

E. NLP-Based Content Analysis

The NLP module processes email text content through a pipeline of tokenization, stop-word removal, stemming, and TF-IDF feature extraction. Sentiment analysis detects urgency-creating language patterns commonly employed in phishing emails. Named Entity Recognition (NER) identifies impersonation attempts by flagging references to financial institutions, government agencies, and technology companies in suspicious contexts. The module also implements n-gram analysis to detect common phishing phrase patterns that persist across varied attack campaigns.

VIII. RESULTS AND DISCUSSION

The proposed AI-Based Email Spam and Phishing Detection System was evaluated across three experimental scenarios representing different real-world threat conditions. Table I presents the performance metrics achieved across these evaluation scenarios.

Evaluation Scenario	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Spam Email Detection	96.8	95.4	97.2	96.3
Phishing URL Detection	97.5	97.1	98.0	97.5
Large-Scale Enterprise Traffic	94.3	93.0	96.1	94.5
Combined System Average	96.2	95.2	97.1	96.1

TABLE I. PERFORMANCE METRICS OF THE PROPOSED SYSTEM

The system achieved an overall accuracy of 96.2% across all evaluation scenarios, demonstrating consistent performance across varied threat types and traffic conditions. In Scenario 1 (spam email detection), the system achieved 96.8% accuracy with a precision of 95.4% and recall of 97.2%, indicating effective identification of spam content with low false positive rates.

Phishing URL detection in Scenario 2 yielded the highest accuracy at 97.5%, reflecting the effectiveness of the URL structural analysis and machine learning classification pipeline. The high recall rate of 98.0% is particularly significant, as it indicates that only 2% of actual phishing URLs escape detection.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802249

Scenario 3 evaluated system performance under high-volume enterprise traffic conditions simulating 232 Mbps email throughput. Despite the increased processing demands, the system maintained 94.3% accuracy with an F1-score of 94.5%, confirming the effectiveness of the parallel processing architecture for enterprise-scale deployments.

A key finding was the significant reduction in false positive rates compared to traditional rule-based systems. The ensemble classification approach reduced false positives by approximately 35% relative to standalone Naive Bayes classifiers, ensuring minimal disruption to legitimate email communications while maintaining high threat detection coverage.

IX. PERFORMANCE EVALUATION AND CONCLUSION

The proposed AI-Based Email Spam and Phishing Detection System demonstrates a substantial advancement over existing approaches across all evaluated performance dimensions. The system's multi-layered architecture combining content-based ML classification with network-level protection addresses the fundamental limitations of single-layer, rule-based security tools.

The integration of NLP techniques for linguistic pattern analysis, ensemble ML classifiers for robust classification, URL inspection for structural anomaly detection, and adaptive learning for continuous model improvement creates a comprehensive security framework capable of detecting both known and zero-day threats.

The IP obfuscation mechanism provides an additional layer of infrastructure protection not present in existing detection-focused systems, reducing the system's exposure to network-level reconnaissance and direct attacks. This feature is particularly valuable in enterprise environments where email security systems themselves represent high-value targets for sophisticated threat actors.

Performance evaluation confirms that the system achieves its design objectives of high detection accuracy (>94% across all scenarios), enterprise-scale throughput (232 Mbps), and sub-60-second detection latency. The adaptive learning module ensures that these performance levels are maintained over time as the model continuously incorporates newly encountered threat patterns.

In conclusion, the proposed system provides a fast, intelligent, and scalable email security solution that effectively addresses the limitations of current approaches. By combining advanced AI techniques with layered network protection and adaptive learning, the system delivers robust real-time defense against both existing and emerging email-based threats.

X. FUTURE WORK

Several promising directions exist for extending the capabilities of the proposed system:

- Transformer-Based NLU Integration: Future work will explore the integration of large pre-trained transformer models such as BERT and GPT-based architectures for more sophisticated natural language understanding, enabling detection of contextually sophisticated phishing content that evades n-gram and TF-IDF-based analysis.
- Federated Learning for Privacy-Preserving Model Updates: Implementing federated learning frameworks will allow the adaptive model to learn from distributed email data across multiple enterprise deployments without centralizing sensitive communication content, addressing privacy concerns while expanding the training data pool.
- Advanced Image Recognition for Visual Phishing: Enhancing the image analysis component to detect subtle logo modifications, brand impersonation in email signatures, and visual similarity attacks that bypass text-based filters will extend protection against image-heavy phishing campaigns.
- Edge Deployment Optimization: Developing lightweight model variants suitable for deployment on edge computing infrastructure will enable integration with IoT email gateways and mobile email clients, extending protection to previously uncovered attack surfaces.
- Multi-Language Support: Extending the NLP pipeline to support detection in multiple languages will address the growing prevalence of non-English phishing campaigns targeting global user populations.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802249

REFERENCES

1. Federal Bureau of Investigation. (2020). Internet Crime Report 2020. IC3 Annual Report. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
2. E. Blanzieri and A. Bryl, "A survey of learning-based techniques of email spam filtering," Artificial Intelligence Review, vol. 29, no. 1, pp. 63-92, 2008.
3. R. B. Basnet, A. H. Sung, and Q. Liu, "Rule-based phishing attack detection," in Proc. 2012 Fourth Cybercrime and Trustworthy Computing Workshop, pp. 1-6, 2012.
4. R. S. Rao and A. R. Pais, "Detection of phishing websites using an efficient feature-based machine learning framework," Neural Computing and Applications, vol. 31, no. 8, pp. 3851-3873, 2019.
5. A. C. Bahnsen, I. Torroledo, J. Camacho, and S. Villegas, "DeepPhish: Simulating malicious AI," IEEE Access, vol. 6, pp. 5685-5695, 2018.
6. A. Saini, K. Guleria, and S. Sharma, "Machine Learning Approaches for an Automatic Email Spam Detection," in Proc. 2023 International Conference on Artificial Intelligence and Applications (ICAIA), pp. 1-5, 2023.
7. M. A. Adebowale, K. T. Lwin, and T. San, "Intelligent detection of spear-phishing attacks in social networks using machine learning," Advanced Science Letters, vol. 25, no. 1, pp. 95-99, 2019.
8. S. Siddiqui and S. Akhtar, "Phishing detection using NLP and machine learning," in Proc. IEEE International Conference on Cybersecurity, 2019.
9. R. Islam and J. Abawajy, "A multi-tier phishing detection and filtering approach," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 324-335, 2013.
10. T. Mahmoud and A. Mahfouz, "An effective approach for phishing detection using neural networks," IEEE Access, vol. 6, pp. 71129-71139, 2018.
11. M. Sabri and M. Mitrea, "Image-based phishing detection using convolutional neural networks," in Proc. 2019 IEEE 15th International Conference on Intelligent Computer Communication and Processing (ICCP), pp. 343-349, 2019.
12. Y. Zhang, J. Hong, and L. Cranor, "Cantina: A content-based approach to detecting phishing web sites," in Proc. 16th International World Wide Web Conference, pp. 639-648, 2007.
13. A. Bergholz, J. De Beer, S. Glahn, M. F. Moens, G. Paass, and S. Strobel, "New filtering approaches for phishing email," Journal of Computer Security, vol. 18, no. 1, pp. 7-35, 2010.
14. A. Ghadage, C. Gholave, A. Devkar, and M. V. Naiknavare, "Email Spam Detection with Machine Learning," International Journal of Advanced Research in Science, Communication and Technology, vol. 5, Issue 4, pp. 1704-1711, October 2025.
15. N. Al-shanableh, M. Alzyoud, and E. Nashnush, "Enhancing Email Spam Detection Through Ensemble Machine Learning: A Comprehensive Evaluation of Model Integration and Performance," Communications of the IIMA, 2024.
16. A. Dalsaniya, "AI-Based Phishing Detection Systems: Real-Time Email and URL Classification," TIJER - International Research Journal, vol. 10, Issue 11, pp. a44-a56, November 2023.
17. Prof. A. D. Bhople, M. P. Warade, P. T. Ghute, R. D. Gawande, and R. S. Narkhede, "A Framework Design for Email Spam Detection using Machine Learning," International Journal of Interdisciplinary Innovative Research & Development (IJIIRD), vol. 08, Special Issue 01, pp. 572-577, 2023.
18. A. Basit, M. Zafar, X. Liu, and X. Yang, "A comprehensive survey of AI-enabled phishing attacks detection techniques," Applied Sciences, vol. 11, no. 6, 2689, 2021.
19. M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: approaches, datasets, and comparative study," Journal of Information Security and Applications, vol. 50, Article ID 102419, 2020.
20. N. Ahmed, R. Amin, H. Aldabbas, D. Koundal, B. Alouffi, and T. Shah, "Machine Learning Techniques for Spam Detection in Email and IoT Platforms: Analysis and Research Challenges," Security and Communication Networks, 2022.
21. Kiran, A., Rubini, P., & Kumar, S. S. (2025). Comprehensive review of privacy, utility and fairness offered by synthetic data. *IEEE Access.*
22. Gopinathan, V. R. (2024). Real-Time Financial Risk Intelligence Using Secure-by-Design AI in SAP-Enabled Cloud Digital Banking. *International Journal of Computer Technology and Electronics Communication, 7(6), 9837-9845.*
23. Udayakumar, R., Elankavi, R., Vimal, R., & Sugumar, R. (2023). Improved Particle Swarm Optimization with Deep Learning-Based Municipal Solid Waste Management in Smart Cities. *Environmental & Social Management Journal, 17(4).*

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802249

24. Anand, L. (2023). An Intelligent AI and ML–Driven Cloud Security Framework for Financial Workflows and Wastewater Analytics. *International Journal of Humanities and Information Technology, 5(02), 87-94.*
25. Soundappan, S. J. (2020). Big Data Analytics in Healthcare: Applications for Pandemic Forecasting. *International Journal of Advanced Research in Computer Science & Technology, 3(1), 2248-2253.*
26. Rajasekar, M. (2024). Real-Time Predictive DevOps Intelligence for Risk-Aware Digital Business Processes in Cloud and SAP Ecosystems. *International Journal of Advanced Research in Computer Science & Technology, 7(4), 10713-10718.*
27. Poornima, G., & Anand, L. (2024, May). Novel AI Multimodal Approach for Combating Against Pulmonary Carcinoma. In 2024 5th International Conference for Emerging Technology (INCET) (pp. 1-6). IEEE.
28. Prabha, P. S., & Rengarajan, A. (2025). Adaptive Cloud Resource Allocation Using Attention-Driven Deep Reinforcement Learning. *Engineering, Technology & Applied Science Research, 15(6), 29334-29340.*
29. Jagadeesh, S., & Sugumar, R. (2017). A Comparative study on Artificial Bee Colony with modified ABC algorithm. *European Journal of Applied Sciences, 9(5), 243-248.*
30. Varma, K. K., & Anand, L. (2025, March). Deep Learning Driven Proactive Auto Scaler for High-Quality Cloud Services. In International Conference on Computing and Communication Systems for Industrial Applications (pp. 329-338). Singapore: Springer Nature Singapore.
31. Kumar, S. A., & Anand, L. (2025). A Novel EEG-Based Deep Learning Framework for Enhancing Communication in Locked-In Syndrome Using P300 Speller and Attention Mechanisms. KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS, 19(11), 3841-3855.
32. Poornima, G., & Anand, L. (2025). Medical image fusion model using CT and MRI images based on dual scale weighted fusion based residual attention network with encoder-decoder architecture. Biomedical Signal Processing and Control, 108, 107932.
33. Archana, R., & Anand, L. (2025). Residual u-net with Self-Attention based deep convolutional adaptive capsule network for liver cancer segmentation and classification. Biomedical Signal Processing and Control, 105, 107665.Kumar, S. A., & Anand, L. (2025). A Novel EEG-Based Deep Learning Framework for Enhancing Communication in Locked-In Syndrome Using P300 Speller and Attention Mechanisms. *KSII Transactions on Internet and Information Systems, 19(11), 3841-3855.*
34. Rengarajan, A. (2025). Cloud-Based AI-Driven Threat Detection Framework for Smart Grid Cybersecurity. *International Journal of Future Innovative Science and Technology, 8(6), 16065.*
35. Murugeshwari, B., Sudharson, K., Panimalar, S. P., Shanmugapriya, M., & Abinaya, M. (2020). SAFE–Secure Authentication in Federated Environment using CEG Key code.
36. Raj A. A., & Sugumar, R. (2023). Early Detection of COVID-19 with Impact on Cardiovascular Complications using CNN Utilising Pre-Processed Chest X-Ray Images. *2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC), IEEE.*
37. Jagadeesh, S., & Sugumar, R. (2017). A Comparative study on Artificial Bee Colony with modified ABC algorithm. European Journal of Applied Sciences, 9(5), 243-248.
38. Selvi, G. V., Anbarasan, A. B., Murthy, B. A., & Prabavathy, S. (2023). An Application Oriented Integrated Unequal Clustering Algorithm for Wireless Sensor Network. In *Underwater Vehicle Control and Communication Systems Based on Machine Learning Techniques* (pp. 140-154). CRC Press.
39. Sruthi, R. S., Ananya, S., & Murugeshwari, B. (2010). Web Based Virtual Control System Laboratory and On-Line Temperature Control of Electrophoresis Equipment using LabVIEW. *International Journal of Computer Applications, 975, 8887.*
40. Vimal Raja, G. (2021). Mining Customer Sentiments from Financial Feedback and Reviews using Data Mining Algorithms. *International Journal of Innovative Research in Computer and Communication Engineering, 9(12), 14705-14710.*
41. MATHEW, A. R. (2025). Neurosecurity and Brain-Computer Interfaces.
42. Soundappan, S. J. (2024). AI-Driven Customer Intelligence in Enterprise Lakehouse Systems Sentiment Mining Governance-Aware Analytics and Real-Time Data Synchronization. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 7(5), 14905.
43. Mathew, A. (2025). Human–AI Collaboration in Security Operations: Measuring Alert Trust, Automation Bias, and Analyst Upskilling in AI-Augmented SOC Environments. International Journal of Computer Technology and Electronics Communication, 8(5), 11375-11380.
44. Soundappan, S. J. (2022). AI-Based Fault Detection and Isolation for Reliability in Modern Power Systems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(4), 7106-7110.
45. Poornima, G., & Anand, L. (2024, April). Effective Machine Learning Methods for the Detection of Pulmonary Carcinoma. In 2024 Ninth International Conference on Science Technology Engineering and Mathematics

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802249

(ICONSTEM) (pp. 1-7). IEEE.Garg, V. K., Soundappan, S. J., & Kaur, E. M. (2020). Enhancement in intrusion detection system for WLAN using genetic algorithms. *South Asian Research Journal of Engineering and Technology, 2(6), 62–64.*

46. Rengarajan, A., Jayakumar, C., & Sugumar, R. (2012). Optimization Of Recent Attacks Using Internet Protocol. National Journal of System and Information Technology, 5(1), 8.
47. Mathew, A. (2024). AI TRiSM: Trust, Risk, and Security Management in Cybersecurity. Cybersecurity, 4(3), 84-90.
48. Mathew, A. (2025). Deep seek vs. ChatGPT: A deep dive into AI Language mastery. Int J Multidisciplinary Res, 7(1), 1-5.