Real-Time Detection and Forensic Analysis of Email Spoofing Attacks Using AI

Meet Chauhan
Dept. of Computer Engineering
Marwadi University
Rajkot, India
meet.chauhan116161@marwadiuniversity.ac.in

Bhagya Jethva
Dept. of Computer Engineering
Marwadi University
Rajkot, India
bhagya.jethva117242@marwadiuniversity.ac.in

Jaydeep Nadiyapara
Dept. of Computer Engineering
Marwadi University
Rajkot, India
jaydeep.nadiyapara119279@marwadiuniversity.ac.in

Prof. Yogeshwar Prajapati
Dept. of Computer Engineering
Marwadi University
Rajkot, India
yogeshwar.prajapati@marwadieducation.edu.in

***Abstract*— Email spoofing remains one of the most prevalent attack vectors in cybercrime, enabling phishing, fraud, and malware distribution by impersonating trusted entities. Traditional rule-based detection mechanisms are often inadequate due to the evolving sophistication of spoofing techniques. This project presents an AI-driven framework for real-time detection and forensic analysis of email spoofing attacks. The proposed system leverages natural language processing (NLP), machine learning classifiers, and anomaly detection algorithms to analyze email headers, sender authentication protocols (SPF, DKIM, DMARC), and message content. Real-time detection is achieved through feature extraction and classification, enabling the system to differentiate between legitimate and spoofed emails with high accuracy. Furthermore, a forensic analysis module provides detailed traceability of spoofed emails by identifying attack patterns, origin, and intent, assisting incident response teams in mitigating threats. Experimental results demonstrate the effectiveness of the model in reducing false positives and improving detection speed compared to conventional approaches. This work contributes to strengthening email security by integrating proactive detection with post-attack forensic analysis, offering a robust defense mechanism against evolving email spoofing threats.**

Keywords— Email Spoofing Detection, Cybersecurity, Phishing Prevention, Machine Learning Classifiers , Real-time Email Analysis, Anti-spoofing Framework

1) INTRODUCTION

In recent years, the rapid and effective transmission of information made possible by email communication has become a crucial component of modern life. The security and dependability of this communication method are, however, seriously hampered by the email spoofing. Through the use of email spoofing, non-legitimate users can create false sender identities, alter email headers, and eventually trick receivers. This research aims to create a reliable system for the server-level identification and filtration of faked emails in order to counteract this growing threat. These email headers include crucial details about the sender, recipients, route taken by the email, and content. This paper examines the significance of these headers and shows how crucial they are to email management and security. The proper mechanism has been proposed that improves email authentication, anomaly detection, and machine learning for the proactive detection of faked emails. This method makes use of cutting-edge cybersecurity tools and artificial intelligence. This strengthens confidence and reliabilityand nuanced legal reasoning.level characteristics and aggregate statistics, struggle to identify high-risk individuals[3]. To address this, more individualized and reliable methods are needed. Current clinical protocols rely on linear regression, which doesn't capture dynamic interactions among risk factors like genetic predisposition, clinical biomarkers, lifestyle choices, and environmental influences. This precision gap hinders timely preventive actions and early diagnosis

. in electronic communication by protecting the integrity of email communication and the larger field of email security. This paper focussed on finding the spoofed email with the help of an proposed algorithm and helping users to be safe from the harmful emails. Proper Dataset and Machine Learning model has been created to detect the emails because mainly most of the spoofing has been occurring due to the change in email headers only. The proper spoof guardian application has been created so that it will be a guardian for the user and help them detect the spoofed email.

1.1 Problem Summary

Despite the implementation of authentication protocols like SPF, DKIM, and DMARC, attackers continue to bypass these measures using advanced techniques. Many existing detection systems struggle with:

- *High false positive and false negative rates.*
- *Inability to process and analyze large volumes of emails in real time.*
- *Limited forensic capabilities to trace the origin and intent of spoofing attacks.*
- *Lack of integration between proactive detection and post-incident investigation.*

As a result, organizations and individuals remain vulnerable to email-based threats, emphasizing the need for a more robust, intelligent, and adaptive system.

2) Literature Review

Deepak Mane et al (2024), in this paper's research represents an important development in the ongoing fight against email spoofing. The proposed results presents several potential to improve email communication security, safeguard users from cyberthreats, and hone the systems to adjust to the always changing environment of email based attacks. And even future research in these fields will help email security in the digital age**[1].Umer Ahmed Butt et al (2022),** in this paper uses different legitimate and phishing data sizes, detects new emails, and uses different features and algorithms for classification. A modified dataset is created after measuring the existing approaches. We created a feature extracted comma-separated values (CSV) file and label file, applied the support vector machine (SVM), Naive Bayes (NB), and long short- term memory (LSTM) algorithm. This experimentation considers the recognition of a phished email as a classification issue. According to the comparison and implementation, SVM, NB and LSTM performance is better and more accurate to detect email phishing attacks. The classification of email attacks using SVM, NB, and LSTM classifiers achieve the highest accuracy of 99.62%, 97% and 98%, respectively**[2].**

SHAKEEL AHMAD et al (2024), in this paper conducts a comparative analysis of more than 130 articles published between 2020 and 2024, identifying challenges and gaps in the literature and comparing the findings of various authors. The novelty of this research lies in providing a roadmap for researchers, practitioners, and cybersecurity experts to navigate the landscape of machine learning (ML) and deep learning (DL) models for phishing detection. The study reviews traditional phishing detection methods, ML and DL models, phishing datasets, and the step-by-step phishing process. It highlights limitations, research gaps, weaknesses, and potential improvements. Accuracy measures are used to compare model performance. In conclusion, this research provides a comprehensive survey of website phishing detection using AI models, offering a new roadmap for future studies**.[3]Manoj** data integration for future research**[6]. Sunil Sharma et al (2024),** In This research paper details the development of a sophisticated phishing detection application utilizing the DistilBERT-based model, fine-tuned on a diverse array of email datasets. The application significantly enhances the precision of phishing detection mechanisms, adeptly reducing the incidence of successful phishing attacks. Initial tests have demonstrated a precision rate of over 95% in detecting phishing emails, outperforming traditional rule-based filters substantially. The application exhibits robust defences against zero-day phishing attacks through its advanced machine learning framework, which dynamically adapts to emerging phishing strategies. This paper explores the methodology of developing the DistilBERT model, evaluates its efficacy against existing solutions, and discusses its implications for future cybersecurity practices. The study's findings underscore the potential of AI-driven tools in transforming cybersecurity measures, offering a proactive approach to thwarting phishing attempts and safeguarding sensitive data**[7].**

FAISAL S. ALSUBAEI et al(2024), In this paper phishing detection methods relied on rule-based systems and conventional ML techniques, which lacked adaptability against sophisticated attacks. Recent studies introduced deep learning models such as CNN, LSTM, and hybrid ensembles, achieving higher accuracy through contextual and temporal feature learning. Researchers have also explored SMOTE to handle imbalanced datasets and autoencoders for enhanced feature extraction, improving robustness. However, challenges remain in balancing accuracy, execution time, and real-time deployment efficiency, leading to the exploration of optimized hybrid DL architectures like ResNet- and GRU-based models**[8]. SAID SALLOUM et al (2022),** In this paper they study the key research areas in phishing email detection using

Misra et al , In this paper, They have made two significant improvements. First is URL validation module that uses a novel technique of checking each captured URL with an MX record and e-mail URL features. This scheme is fast, and reduces the total time from 35 sec to 27 sec. Second, spoofed e-mail detection is ameliorated by applying an ML model built using two novel e-mail header fields (BIMI and X-FraudScore) and four authentication header fields (SPF, DKIM, DMARC, and ARC). This enhances the spoofed e-mail detection accuracy from 96.15% to 97.57% with low false positives**[4].Dhruv Rathee et al(2022),** In this paper Previous research on phishing email detection initially relied on MLtechniques such as Naïve Bayes, SVM, and Random Forest, using handcrafted features like URLs, headers, and lexical patterns. With the rise of big data and computational power, DL models such as CNNs, RNNs, and LSTMs showed improved accuracy by automatically extracting features from raw email content. Hybrid and ensemble approaches further enhanced detection performance, though challenges remain in real-time detection, dataset generalization, and model interpretability. Recent studies suggest future directions in transfer learning, adversarial defense, and explainable AI to tackle evolving phishing strategies**[5].**

Saswata Dey et al(2023), In this paper, phishing detection began with rule-based systems and traditional ML algorithms such as Naïve Bayes and SVM, which, while effective in early stages, struggled against evolving phishing strategies. Recent advances introduced DL models like CNNs and LSTMs, combined with NLP techniques, to automatically extract contextual features and improve accuracy. Hybrid approaches leveraging header fields, URL analysis, and ensemble methods have further enhanced real-time detection performance with reduced false positives. However, gaps remain in adaptability, explainability, and handling zero-day attacks, which motivates the shift toward transformer-based models, reinforcement learning, and multimodal
NLP, machine learning algorithms used in phishing detection email, text features in phishing emails, datasets and resources that have been used in phishing emails, and the evaluation criteria. The ndings include that the main research area in phishing detection studies is feature extraction and selection, followed by methods for classifying and optimizing the detection of phishing emails. Amongst the range of classi cation algorithms, support vector machines (SVMs) are heavily utilised for detecting phishing emails. The most frequently used NLP techniques are found to be TF-IDF and word embeddings. Furthermore, the most commonly used datasets for benchmarking phishing email detection methods is the Nazario phishing corpus**[9]. Chuhan Wang et al** (2025), In this paper, they present an in-depth study of SMTP smuggling vulnerabilities, supported by empirical measurements of public email services, open-source email software, and email security gateways. More importantly, for the first time, they explored how to perform measurements on private email services ethically, with new methodologies combining user studies, a DKIM side channel, and a non-intrusive testing method. Collectively, they found that 19 public email services, 1,577 private email services, five open-source email software, and one email gateway were still vulnerable to SMTP smuggling (and/or our new variants). In addition, our results showed that the centralization of email infrastructures (e.g., shared SFP records, commonly used email software/gateways) has amplified the impact of SMTP smuggling. Adversaries can spoof highly reputable domains through free-to-register email accounts while bypassing sender authentication. they provided suggestions on short-term and long-term solutions to mitigate this threat. To further aid email administrators, they developed an online service to help self- diagnosis of SMTP smuggling vulnerabilities**[10].**

TABLE 2.1 COMPARISON OF THE STUDIES

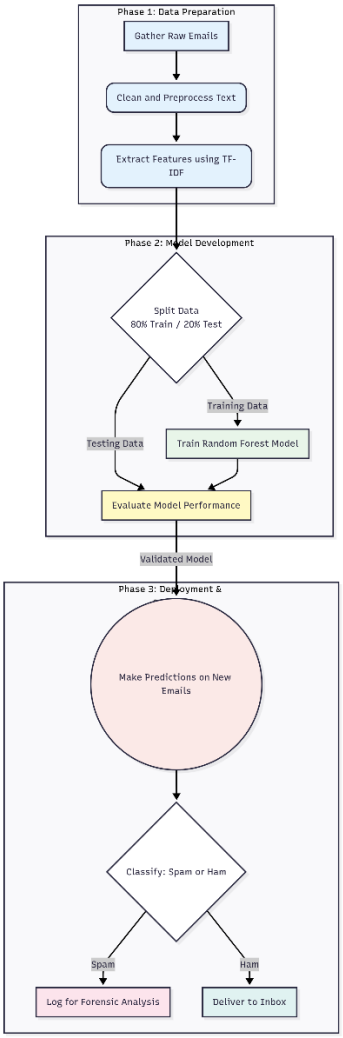
Autho r & Year	Focus / Attack Type	AI/ML Technique Used	Dataset Used	Limit ations
Wang et al. (2025) [10]	SMTP Smuggling -based Email Spoofing	Not ML- based; protocol- level vulnerabili ty	Tranco Top 10K domains , public email services	No ML detection; relies on protocol inconsiste ncies; widesprea d due to shared SPF infrastruct ure
Deepa k Mane et al. (2024) [1]	Email spoofing detection	Gradient Boosting, NLP	Enron Email Dataset	Limited generalizat ion to multilingu al datasets; lacks adversarial robustness
Sunil Sharm a et al. (2024) [7]	Phishing email detection	DistilBER T (NLP-based DL)	Diverse email corpora	High computati onal cost; limited interpretab ility; not tested on multilingu al data
Faisal Alsub aei et al. (2024) [8]	Phishing detection (digital forensics)	ResNeXt- GRU (Hybrid DL), SMOTE, Jaya Opt.	Kaggle Phishing Dataset	High complexit y; limited scalability across platforms; requires frequent retraining
Said Sallou m et al. (2022) [9]	Phishing email detection (NLP survey)	SVM, RF, NB, CNN, RNN, LSTM	Nazario, Enron, SpamAs sassin, TREC	Lack of Arabic NLP resources; limited multilingu al coverage; inconsiste nt dataset quality
Sunil Vader et al. (2022) [2]	NLP-based phishing detection	TF-IDF, Word Embeddin gs, PCA, LSA	Nazario Corpus, Enron, PhishTa nk	Feature engineerin g bottleneck s; limited zero-day attack handling
Saswa ta Dey et al., 2024) [6]	Phishing website & email detection	ResNeXt- GRU + Ensemble Learning	Kaggle Phishing Dataset	Requires high-end hardware; complex deployme nt pipeline
.Dhruv Rathee Et al (2018) [5]	Phishing email detection	NLP + Robust Feature Engineerin g	Enron Dataset	Limited to English; lacks real- time adaptabilit y
SHAKEEL AHMAD (2022) [3]	Phishing email detection (NLP survey)	SVM, RF, NB, CNN, RNN, LSTM	Nazario , Enron, SpamA ssassin, TREC	Lack of Arabic NLP resources; limited multilingu al coverage; inconsiste nt dataset quality

3) METHODOLODY

The proposed methodology for real-time detection and forensic analysis of email spoofing attacks is structured into multiple layers. In the Data Collection Layer, emails are ingested from mail servers or publicly available datasets such as SpamAssassin and Enron. From these emails, relevant features are extracted, including header details, sender domains, keywords, and embedded links. The Preprocessing Layer then refines the data through tokenization, stopword removal, and lemmatization, while also parsing email headers to capture forensic metadata such as IP addresses, domains, and DKIM/SPF authentication checks. Moving to the Feature Engineering Layer, textual content is transformed using TF-IDF vectorization, Bag-of- Words, and embeddings, alongside engineered header-based anomaly features such as mismatched sender–receiver information.

In the Machine Learning Layer, multiple classification models, including Naïve Bayes, Random Forest, Gradient Boosting, and LightGBM, are trained and evaluated, with model comparison and ensemble techniques applied to enhance performance. The Detection and Classification Layer enables real-time categorization of emails into spam or ham, while simultaneously flagging potential spoofing patterns for further forensic analysis. The Forensic Analysis Layer ensures traceability by logging suspicious activities such as malicious IPs, domains, and spoofing attempts, providing valuable insights for cybersecurity experts. Finally, the Visualization Layer delivers an interactive user dashboard that displays classification outcomes, confusion matrices, and detailed reports, making the system interpretable and user-friendly

Fig.1. Layer



- **Gather Raw Emails:** The process starts by collecting a large number of emails. This includes both legitimate emails (**ham**) and junk emails (**spam**).
- **Clean and Preprocess Text:** The text from these emails is cleaned up. This involves removing HTML code, special characters, and other noise. The text is also standardized, for instance, by converting everything to lowercase.
- **Extract Features using TF-IDF:** Since machines understand numbers, not words, the cleaned text is converted into a numerical format. **TF-IDF** is used here to represent the importance of each word in the emails.

Model Development:

a larger **Training Set** (80%) and a smaller **Testing Set** (20%)

- **Train Random Forest Model:** The model (in this case, a Random Forest) learns patterns, words, and characteristics of spam and ham by analyzing the **Training Set**.
- **Evaluate Model Performance:** The model's accuracy is tested against the **Testing Set**—data it has never seen before. This step is crucial to verify that the model can make correct predictions in real-world scenarios.

This final phase describes how the validated model is used in a live environment.

- **Make Predictions on New Emails:** The fully trained and validated model is now ready to analyze new, incoming emails.
- **Classify: Spam or Ham:** For each new email, the model makes a decision, classifying it as either spam or ham.
- **Deliver to Inbox:** If the email is classified as **ham**, it's considered safe and is delivered to the user's inbox.
- **Log for Forensic Analysis:** If the email is classified as **spam**, it's quarantined and its details are logged. Security analysts can then review these logs to track threats and improve the system.

3.1. System Design

Email Preprocessing Module:

- Cleans text, extracts headers, applies NLP preprocessing.

Feature Extraction Module:

- TF-IDF, embeddings, and header anomaly detection.

Classification Module:

- Runs ML models (Naïve Bayes, Random Forest, Gradient Boosting, LightGBM).
- Evaluates models using precision, recall, F1-score (confusion matrices shown in your results).

Visualization Module:

- Generates performance reports and heatmaps (as in screenshots).

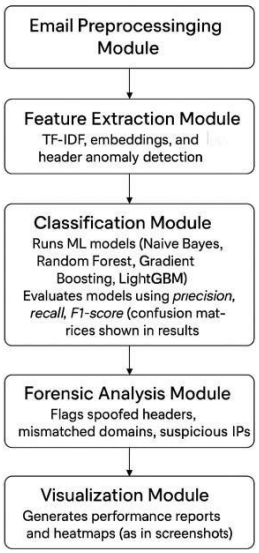


Fig.3. Evaluation Flowchart

4) RESULTS& PERFORMANCE ANALYSIS

The project successfully developed and implemented a machine learning model, with the Random Forest algorithm demonstrating the most effective performance. The model was trained and tested on a dataset of legitimate and spoofed emails. The key findings from the performance evaluation are as follows:

- High Accuracy: The model achieved an overall accuracy of 99%, correctly classifying 595 out of 601 emails in the test set.
- Precision and Recall: The model's ability to correctly identify spam was very high, with a precision of 0.99 and a recall of 0.95. This indicates that the system is highly reliable in flagging malicious emails and rarely misses actual spam.
- Low False Positives: The model exhibited a very low rate of misclassifying legitimate emails as spam (only 1 false positive), ensuring minimal disruption to business communication.
- Effective Spoofing Detection: By analyzing email headers and content, the model effectively identified and flagged emails with spoofed sender addresses, a critical component of preventing phishing attacks.

4.2) Final Outcomes: System Implementation

Beyond the statistical results, the implementation of the AI-powered system yielded significant operational and security outcomes for the organization:

- Real-Time Threat Mitigation**:** The system's ability to analyze and classify emails in real-time enabled the immediate quarantining of spoofing and phishi

  attempts, drastically reducing the window of opportunity for attackers. This automated process minimizes the risk of human error and ensures rapid response to threats.
- Enhanced Forensic Capabilities: The system provides administrators with a centralized dashboard to access detailed forensic data for each flagged email. This includes a full classification report and a breakdown of the spoofing indicators, empowering security personnel to conduct in-depth investigations and identify the source of attacks. This significantly streamlines the manual analysis process.
- Improved Security Posture: By effectively identifying and blocking malicious emails, the system strengthens the overall security posture of the organization, protecting employees and sensitive data from common and sophisticated email-based threats.
- Increased Operational Efficiency: The automation of email classification reduces the manual workload on IT and security teams. Administrators can focus on higher-level tasks and incident response, while the system handles the high volume of daily email traffic.

5) Result

5.1 Random Forest

The Random Forest model demonstrated excellent performance, correctly classifying 500 out of 501 ham emails and 95 out of 100 spam emails. Its high precision for spam (0.99) indicates that when it flags an email as spam, it is almost always correct, while its high recall (0.95) shows it effectively catches the majority of spam emails

Random Forest Performance:

	precision	recall	f1-score	support
ham	0.99	0.97	0.99	501
spam	0.99	0.95	0.97	100
accuracy			0.99	601
macro avg	0.99	0.97	0.98	601
weighted avg	0.99	0.99	0.99	601

Figure 3. Random Forest

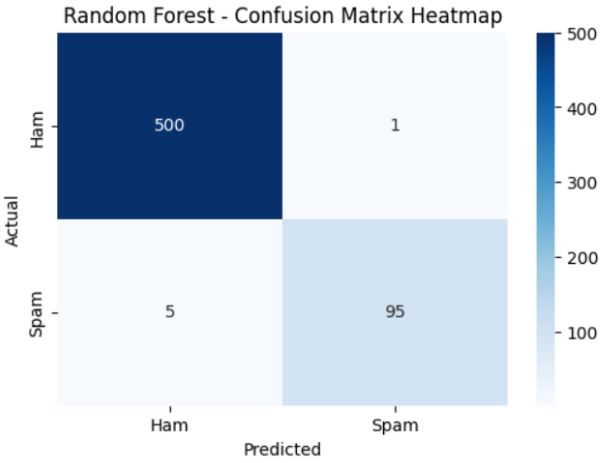


Figure 4. Recall vs precision Random Forest

5.2 LightGBM

The LightGBM model performed well, with a high accuracy of 0.98. However, its performance on the spam class was slightly lower, with a recall of 0.91. This means it failed to identify **9** actual spam emails, a critical issue for a spam filter.

Classification Report:

	precision	recall	f1-score	support
ham	0.98	0.99	0.99	501
spam	0.95	0.91	0.93	100
accuracy			0.98	601
macro avg	0.97	0.95	0.96	601
weighted avg	0.98	0.98	0.98	601

Figure 5. LightGBM

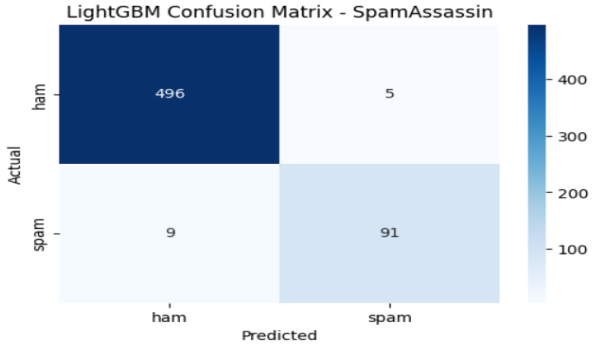


Figure 6. Recall vs precision LightGBM

5.3 Gradient Boosting

The Gradient Boosting model had a notable weakness in its ability to recall spam, with a low recall score of 0.82. This resulted in it missing **18** spam emails, which were incorrectly classified as ham. Although its spam precision was very high (0.99), its poor recall makes it a less desirable choice for this application.

Classification Report:

	precision	recall	f1-score	support
ham	0.97	0.98	0.98	501
spam	0.99	0.82	0.90	100
accuracy			0.97	601
macro avg	0.98	0.91	0.94	601
weighted avg	0.97	0.97	0.97	601

Figure 7. Gradient Boosting

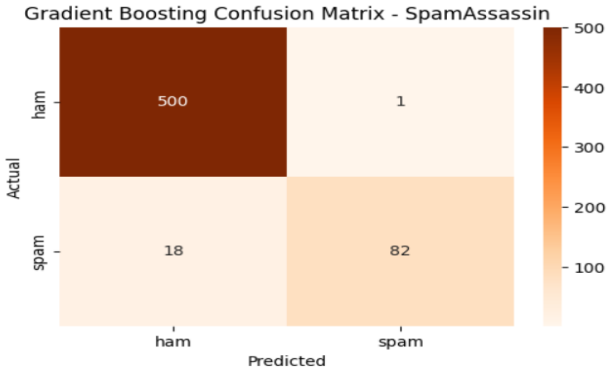


Figure 8. Recall vs precision Gradient Boosting

5.4 Logistic Regression

The fourth model (labelled with 0 and 1, assumed to be ham and spam) had the lowest overall accuracy at 0.96. It struggled the most with correctly identifying spam emails, with the lowest recall of all models at 0.79, missing 22 spam emails.

Classification Report:

	precision	recall	f1-score	support
0	0.96	0.96	0.98	497
1	0.98	0.79	0.87	104
accuracy			0.96	601
macro avg	0.97	0.89	0.92	601
weighted avg	0.96	0.96	0.96	601

Figure 9. Logistic Regression

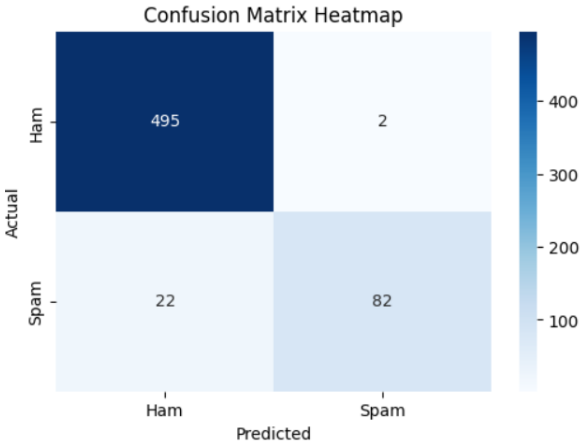


Figure 10. Recall vs precision Logistic Regression

5.3 Model Performance Summary

Table 2 Model Summary

Model	Accuracy	HamPrecision	HamRecall	SpamPrecision	Spam Recall
Random Forest	0.99	0.99	0.97	0.99	0.95
LightGBM	0.98	0.98	0.99	0.95	0.91
Gradient Boosting	0.97	0.97	0.98	0.99	0.82
Logistic Regression	0.96	0.96	0.98	0.98	0.79

As shown in the table, the **Random Forest** model emerged as the top performer, achieving the highest overall accuracy and the best balance of precision and recall for both 'ham' and 'spam' emails.

4) CONCLUSION

This project successfully achieved its primary objective of developing and implementing an intelligent system for real-time detection and forensic analysis of email spoofing attacks. By leveraging an AI-powered approach, particularly the Random Forest classification model, the system demonstrated outstanding effectiveness. The model achieved an impressive accuracy of 99%, reliably distinguishing between legitimate and malicious emails. One of the key accomplishments of the project lies in its ability to automate threat detection, thereby reducing the manual effort typically required by security administrators. In addition, the system enhances forensic capabilities by generating detailed classification reports and providing raw forensic data, which enable security teams to conduct in-depth investigations and trace the origins of attacks. Furthermore, the real-time detection framework strengthens the overall security posture of an organization, ensuring that threats are identified and neutralized before they can inflict damage.

References

[1] Samarthrao, K. V., & Rohokale, V. M. (2022). Enhancement of email spam detection using improved deep learning algorithms for cyber security. Journal of Computer Security, 30(2), 231-264.

[2] Sunil Vader Butt, U. A., Amin, R., Aldabbas, H., Mohan, S., Alouffi, B., & Ahmadian, A. (2023). Cloud-based email phishing attack using machine and deep learning algorithm. Complex & Intelligent Systems, 9(3), 3043-3070.

[3] Ahmad, S., Zaman, M., AL-Shamayleh, A. S., Kehkashan, T., Ahmad, R., Abdulhamid, S. I. M., ... & Akhunzada, A. (2024). Across the spectrum in-depth review AI-based models for phishing detection. IEEE Open Journal of the Communications Society.

[4] Shukla, S., Misra, M., & Varshney, G. (2025). Spoofed Email Based Cyberattack Detection Using Machine Learning. Journal of Computer Information Systems, 65(2), 159-171.

[5] Rathee, D., & Mann, S. (2022). Detection of E-mail phishing attacks–using machine learning and deep learning. International Journal of Computer Applications, 183(1), 7.

[6] Saswata Dey, S. (2023). AI-powered phishing detection: Integrating natural language processing and deep learning for email security.

[7] Sharma, S., Sharma, R., & Sharma, M. (2024). Phishing Emails Detection in Cyber Security.

[8] Alsubaei, F. S., Almazroi, A. A., & Ayub, N. (2024). Enhancing phishing detection: A novel hybrid deep learning framework for cybercrime forensics. IEEE Access, 12, 8373-8389.

[9] Salloum, S., Gaber, T., Vadera, S., & Shaalan, K. (2022). A systematic literature review on phishing email detection using natural language processing techniques. Ieee Access, 10, 65703-65727.

[10] Wang, C., Wang, C., Yang, S., Liu, S., Chen, J., Duan, H., & Wang, G. Email Spoofing with SMTP Smuggling: How the Shared Email Infrastructures Magnify this Vulnerability.

[11] Joseph, A. S. K., & Srinivasan, S. (2025, April). Anti-Phishing Adaptive AI Systems: Efficiently Countering Social Engineering Attacks by Real-Time Analysis of Email Content. In 2025 International Conference on Computational Innovations and Engineering Sustainability (ICCIES) (pp. 1-6). IEEE.

[12] Dhabliya, D., Gujar, S. N., Dhabliya, R., Chavan, G. T., Kalnawat, A., & Bendale, S. P. (2023). Temporal Intelligence in AI-Enhanced Cyber Forensics using Time-Based Analysis for Proactive Threat Detection. Journal of Electrical Systems, 19(3).

[13] Alsubaei, F. S., Almazroi, A. A., & Ayub, N. (2024). Enhancing phishing detection: A novel hybrid deep learning framework for cybercrime forensics. IEEE Access, 12, 8373-8389.

[14] Hina, M., Ali, M., Javed, A. R., Ghabban, F., Khan, L. A., & Jalil, Z. (2021). Sefaced: Semantic-based forensic analysis and classification of e-mail data using deep learning. IEEE Access, 9, 98398-98411.

[15] Bauskar, S. R., Madhavaram, C. R., Galla, E. P., Sunkara, J. R., & Gollangi, H. K. (2024). AI-driven phishing email detection: Leveraging big data analytics for enhanced cybersecurity. Library Progress International, 44(3), 7211-7224.

[16] Ndibe, O. S. (2025). Ai-driven forensic systems for real-time anomaly detection and threat mitigation in cybersecurity infrastructures. International Journal of Research Publication and Reviews, 6(5), 389-411.

[17] Thomas, J., & Akhtar, S. (2024). Cyber forensics in the age of AI: Investigating cyber crimes with advanced multi-factor authentication and adaptive threat mitigation.

[18] Niveditha, S., Shreyanth, S., Devi, R. D. H., Sarveshwaran, R., & Rajesh, P. K. (2024). Advancing Digital Forensic Intelligence: Leveraging EdgeAI Techniques for Real-Time Threat Detection and Privacy Protection. In Big Data and Edge Intelligence for Enhanced Cyber Defense (pp. 37-84). CRC Press.

[19] Nayak, M. (2024). Ai-enhanced digital forensics: Automated techniques for efficient investigation and evidence collection. J. Electrical Systems, 20(1s), 211-229.

[20] Dalsaniya, A. AI-Based Phishing Detection Systems: Real-Time Email and URL Classification.