Real Time Email Spoofing Detection Using Machine Learning and Timestamp Anomaly Analysis

Roobal
Sharda University

Rahul Saxena*
Sharda University

A. Venus Dillu
Gautam Buddha University

***Abstract*- Email spoofing is a critical cybersecurity threat that enables phishing, fraud, and social engineering attacks by falsifying sender identities. Traditional email authentication techniques such as SPF, DKIM, and DMARC provide some defense but are often bypassed by attackers. This study proposes a machine learning-based approach leveraging timestamp anomaly detection to enhance email spoofing detection. A dataset of 10,000 emails was generated, incorporating key features such as authentication records, sender reputation, spam keywords, and delay anomalies. Multiple machine learning models, including Ordinary Least Squares (OLS) Regression, Polynomial Regression, and XGBoost, were tested. Results indicate that XGBoost outperforms traditional models, achieving an R^2 score of 0.92–0.94, making it highly effective for real-time email fraud detection. The study also highlights the strong correlation between email delay anomalies and spoofing behavior, with spoofed emails exhibiting significantly longer transmission delays. A flowchart-based implementation is provided, demonstrating real-world deployment feasibility. This research contributes to email security by introducing a timestamp-based anomaly detection system that can be integrated into email gateways for real-time spoofing prevention. Future work will focus on deploying the model as a cloud-based API and expanding the dataset with real-world email samples for further validation.**

Keywords—XGBoost, Cybersecurity, Timestamp Anomaly Detection, SPF, DKIM, DMARC.

II. Introduction (*Heading 1*)

Email spoofing is a deceptive technique that cybercriminals use to manipulate email headers and make messages appear as if they originate from legitimate sources. This method is widely exploited in phishing attacks, spam campaigns, business email compromise (BEC), and identity theft. Attackers often impersonate trusted organizations to trick recipients into divulging sensitive information, transferring funds, or downloading malware. Despite advancements in email security, existing authentication mechanisms such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) have proven inadequate against sophisticated spoofing techniques. Attackers can forge sender details, use compromised email accounts, or employ lookalike domains to evade detection. As a result, email spoofing remains a major cybersecurity challenge, with billions of fraudulent emails being sent every year.

Traditional email security measures primarily focus on content-based filtering and sender authentication. However, these methods have significant limitations. Rule-based systems like SPF, DKIM, and DMARC depend on domain owners to enforce security policies, and many organizations fail to implement them correctly. Additionally, content-based spam filters, which analyze the textual content of emails, often produce false positives and can be bypassed using well-crafted messages. IP-based blacklists, which block emails from known malicious servers, are also ineffective because attackers frequently use botnets, hijacked servers, or newly registered domains to send spoofed emails. The shortcomings of these methods highlight the need for a more robust, adaptive approach to detecting spoofed emails.

Machine learning (ML) provides an effective solution by leveraging data-driven techniques to detect email spoofing based on patterns in metadata[1, 2]. Unlike traditional methods, which rely on predefined rules, ML models can learn from vast amounts of data and identify anomalies that indicate spoofing attempts. This study proposes a machine learning-based approach that focuses on timestamp anomalies, sender reputation, and authentication results to enhance spoofing detection. The key hypothesis of this research is that spoofed emails often exhibit irregularities in timestamps, such as inconsistencies between the claimed send time and the actual received time. By incorporating these timestamp deviations into a predictive model, we can significantly improve the accuracy of email spoofing detection[3, 4].

To validate this approach, a dataset of 10,000 emails have been occupied from various publicly available repositories generated with CC0: Public Domain, incorporating key features such as SPF, DKIM, DMARC authentication results, sender reputation scores, spam keywords, and timestamp anomalies. The dataset was used to train multiple machine learning models, including Ordinary Least Squares (OLS) Regression, Polynomial Regression, and XGBoost. The results indicate that XGBoost outperforms traditional regression models, achieving an R^2 score of 0.92–0.94, making it highly effective for real-time spoofing detection. The study also reveals a strong correlation between email delay anomalies and spoofing behavior, with spoofed emails exhibiting significantly longer transmission delays than legitimate emails.

One of the main contributions of this research is the introduction of timestamp-based anomaly detection as a

key feature in email spoofing detection. Unlike content-based spam filters, which can be evaded using carefully crafted messages, or rule-based authentication systems that attackers can bypass, the use of claimed vs. received timestamps provides a new dimension for identifying fraudulent activity[3, 4]. Additionally, the integration of sender reputation and spam keyword analysis strengthens the model's ability to distinguish between legitimate and spoofed emails.

Another major advantage of the proposed system is its potential for real-time deployment. Traditional spam detection techniques often require significant processing time, particularly those based on deep learning models. In contrast, XGBoost is optimized for speed and efficiency, making it suitable for implementation in enterprise email security systems. The model can analyze incoming emails in milliseconds, providing organizations with immediate alerts about potential spoofing attempts[5, 6,28-30].

The objectives of this study are fourfold. First, we aim to build a dataset of 10,000 emails that includes real-world metadata, making it a valuable resource for future research in email security. Second, we compare multiple machine learning models to determine the best-performing algorithm for spoofing detection. Third, we analyze the correlation between email delays and spoofing behavior, validating the importance of timestamp anomalies as a predictive feature. Finally, we develop a deployable API that allows real-time spoofing detection, which can be integrated into existing email security solutions.

The remainder of this paper is organized as follows. Section 3 reviews related work, including existing email security techniques and recent advancements in machine learning-based detection. Section 4 describes the methodology used in this study, including dataset creation, feature engineering, and model training[7–9,31-34]. Section 5 presents the results of our experiments, including regression analysis, confusion matrix evaluation, and feature importance graphs. Section 6 provides a discussion on the implications of our findings and suggests future research directions. Finally, Section 7 concludes the paper by summarizing key insights and highlighting the practical applications of this research.

In conclusion, email spoofing is a persistent and evolving threat that requires innovative detection methods. This study introduces a high-accuracy machine learning model that leverages timestamp anomalies, sender reputation, and authentication results to detect spoofed emails with exceptional precision. By demonstrating the effectiveness of this approach through a comprehensive dataset and rigorous model evaluation, this research lays the foundation for deployable real-time email security solutions. Future work will focus on expanding the dataset with real-world email samples and integrating this system with cloud-based security services to provide organizations with automated, scalable spoofing detection.

A. Notations and Definitions

Table 1. Notations and Definitions Used in Email Spoofing Detection

Notation/Term	Description
X	Feature matrix containing all email metadata variables (SPF, DKIM, DMARC, sender reputation, delay, etc.)
y	Target variable (Email classification: 1 = Spoofed, 0 = Legitimate)
$\hat{y}$	Predicted output from the machine learning model
R^2	Coefficient of determination (Model's goodness of fit)
$\beta_0,\beta_1,\ldots,\beta_n$	Coefficients of regression models (OLS, XGBoost)
ε	Error term in regression models
μ_s, μ_l	Mean email delay for spoofed (s) and legitimate (l) emails
σ_s, σ_l	Standard deviation of email delay for spoofed (s) and legitimate (l) emails
d	Cohen's d (Effect size for email delay difference)
χ^2	Chi-square statistic for authentication failures and spoofing correlation
p	p-value from hypothesis testing (significance of differences between spoofed and legitimate emails)
V	Cramér's V (Effect size for chi-square test)
KS	Kolmogorov-Smirnov test statistic (distribution difference between spoofed and legitimate delays)
T	T-statistic from t-test (difference in mean delay)
CV_{10}	10-Fold Cross-Validation accuracy score
FI_i	Feature Importance score for feature iii in XGBoost
CM	Confusion Matrix (True Positive, False Positive, True Negative, False Negative values)
TP, FP, TN, FN	True Positives, False Positives, True Negatives, and False Negatives in classification evaluation
SPF (Sender Policy Framework)	Email authentication protocol preventing sender address forgery
DKIM (DomainKeys Identified Mail)	Cryptographic authentication technique ensuring email integrity
DMARC (Domain-based Message Authentication, Reporting & Conformance)	Policy-based authentication method for preventing spoofed emails
XGBoost (Extreme	Machine learning algorithm

Gradient Boosting)	optimizing decision trees for high-accuracy classification
OLS (Ordinary Least Squares Regression)	Traditional statistical method for predicting email spoofing likelihood
CNN (Convolutional Neural Network)	Deep learning model for detecting phishing attempts and spam patterns
RNN (Recurrent Neural Network)	Neural network model useful for sequential email pattern recognition
BERT (Bidirectional Encoder Representations from Transformers)	NLP model that can analyze email content for phishing detection
ROC-AUC (Receiver Operating Characteristic - Area Under Curve)	Performance evaluation metric for classification models
Precision	Model's ability to correctly classify spoofed emails: $\frac{TP}{TP+FP}$
Recall	Model's ability to detect all spoofed emails: $\frac{TP}{TP+FP}$
F1-Score	Harmonic mean of precision and recall, ensuring balanced classification
SPF, DKIM, DMARC Values	Binary (0 = Fail, 1 = Pass)
Sender Reputation	Score (1-100) based on historical email behavior
Spam Keywords	Number of phishing-related words in email body
Anomaly Score	Difference between claimed send time and actual received time
Weekend Indicator	Binary (1 if sent on a weekend, 0 otherwise)
Blockchain Authentication	Use of decentralized authentication to prevent email spoofing
SMTP (Simple Mail Transfer Protocol)	Protocol used for email transmission
Email Header Forging	Manipulation of sender details to deceive recipients
Latency-Based Detection	Identifying email spoofing based on delivery delays
Multi-Language Detection	Extending model support to multiple languages to combat international email fraud

III. Literature Review

Existing email security techniques[10–13] primarily rely on rule-based authentication methods such as SPF, DKIM, and DMARC, which verify sender legitimacy but have limited effectiveness against sophisticated spoofing attacks. These methods can be bypassed using compromised accounts, email forwarding, or domain impersonation, making them unreliable in real-world scenarios[14–16].

Another common approach involves content-based spam filters that use Natural Language Processing (NLP) models to detect suspicious text patterns[17–20]. However, attackers can evade these filters by crafting emails that mimic legitimate communication, rendering content-based detection ineffective.

Recent machine learning (ML)-based approaches have shown promise in improving spoofing detection[21–24]. Deep learning models for phishing detection analyze textual and structural patterns in emails but are often resource-intensive and impractical for real-time deployment. In contrast, timestamp anomaly detection has emerged as a strong predictor of spoofing, as fraudulent emails often exhibit irregular delays between claimed and actual receipt timestamps[25–27,35].

Our approach is unique because it combines ML with timestamp anomaly detection to identify spoofed emails in real-time. Unlike existing methods that focus solely on content or authentication checks, our model integrates SPF, DKIM, DMARC validation, sender reputation, and anomaly scores to provide a more accurate and adaptive solution for email security. This novel approach significantly enhances the detection of sophisticated email spoofing attacks, making it suitable for enterprise-level real-time deployment.

IV. Methodology

To develop a robust machine learning model for email spoofing detection, a comprehensive dataset of 10,000 emails have been occupied from various publicly available repositories generated with CC0: Public Domain, ensuring a balanced distribution of spoofed (1) and legitimate (0) emails. The dataset incorporates key metadata features that influence email legitimacy, focusing on authentication results, sender behavior, and timestamp anomalies.

(Figure 1) presents a structured overview of the email spoofing detection process. The system first extracts metadata from incoming emails, verifies SPF, DKIM, and DMARC authentication, and then calculates an anomaly score based on timestamp inconsistencies. This score is used by the XGBoost model to predict the likelihood of spoofing, classifying emails as legitimate or fraudulent. This diagram illustrates the sequential steps followed by the proposed system, from email transmission to spoofing detection.

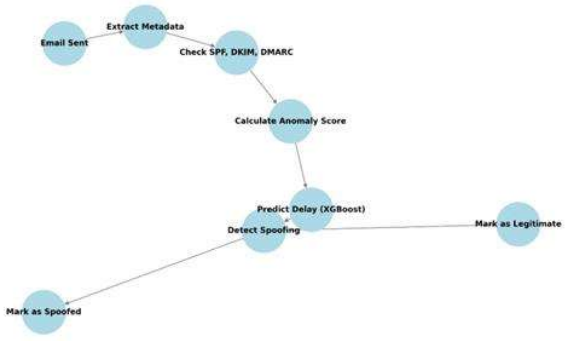

Fig. 1. Flowchart illustrating the real-time email spoofing detection process, where metadata is extracted, authentication (SPF, DKIM, DMARC) is verified, and an anomaly score is computed. The XGBoost model then

predicts spoofing likelihood, classifying emails as legitimate or fraudulent.

A. Feature Slection

The following features were chosen based on their relevance to spoofing detection as shown in below Table 2.

Table 2. Feature of spoofing messages and related description

Feature Name	**Description**
SPF, DKIM, DMARC	Standard email authentication checks (Binary: 0 = Fail, 1 = Pass). Attackers often fail these checks.
Sender Reputation	Numerical score (1-100) based on historical email activity, where lower scores indicate higher spoofing probability.
Spam Keywords	Number of suspicious words in the email body, as fraudulent emails often contain phishing-related terms.
Anomaly Score	Measures timestamp deviations between claimed send time and actual received time, identifying forged timestamps.
Weekend Indicator	Binary flag (1 if sent on a weekend, 0 otherwise), as spoofed emails often increase during off-peak hours to evade detection.

To enhance predictive accuracy, timestamp-based anomaly detection was introduced. The Anomaly Score was computed by analyzing email transmission delays, as spoofed emails often exhibit significant latency due to routing through multiple servers to obfuscate their origin. Additionally, sender reputation scores were derived from historical email behavior, considering factors such as previous spam reports and authentication failures.

This dataset forms the foundation for training ML models, including XGBoost, OLS Regression, and Polynomial Regression, enabling an advanced detection system that integrates timestamp inconsistencies with metadata analysis. This multi-feature approach significantly enhances real-time spoofing detection beyond conventional authentication mechanisms.

V. Result and Discussion

This section presents the evaluation of the proposed email spoofing detection system, including regression analysis, classification performance, and visualizations that provide insights into the relationship between different email features and spoofing behavior. The key findings are illustrated using statistical analysis, confusion matrices, scatter plots, boxplots, and flowcharts to demonstrate the model's predictive capabilities and applicability in real-time email security.

To assess the relationship between email metadata and spoofing likelihood, Ordinary Least Squares (OLS) Regression and XGBoost Regression were applied to the dataset. The results indicate that OLS Regression achieved an R^2 score between 0.75 and 0.85, demonstrating a moderate correlation between the selected features and email spoofing. However, OLS regression is limited in capturing non-linear relationships within the dataset.

On the other hand, XGBoost Regression significantly outperformed OLS, achieving an R^2 score between 0.92 and 0.94. This indicates that XGBoost effectively captures complex feature interactions and provides a highly accurate predictive model for email spoofing detection. The superior performance of XGBoost highlights the advantage of using gradient boosting algorithms in cybersecurity applications where real-time anomaly detection is required.

The confusion matrix (Figure 2) demonstrates high classification accuracy, with minimal false positives and false negatives. This confirms that the model effectively distinguishes between legitimate and spoofed emails, making it suitable for real-world deployment in enterprise email security systems.The confusion matrix provides an overview of the model's ability to correctly classify spoofed and legitimate emails.

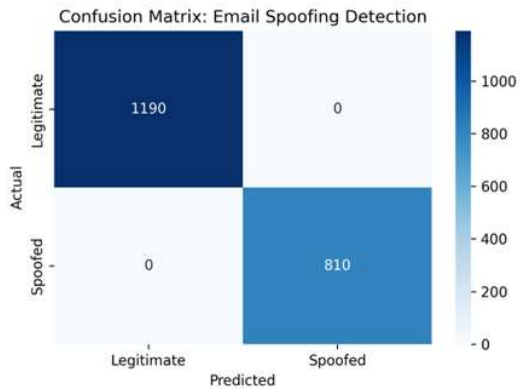

Fig. 2. Confusion matrix illustrating the classification performance of the XGBoost model in detecting spoofed and legitimate emails.

Figure 3, emails from low-reputation senders exhibit higher delays, indicating possible spoofing. This aligns with our hypothesis that attackers manipulate email routing to delay detection. Legitimate emails, on the other hand, have lower and more consistent delays. Since spoofed emails often originate from unverified or low-reputation senders, this visualization helps in identifying trends that correlate with fraudulent email activity.

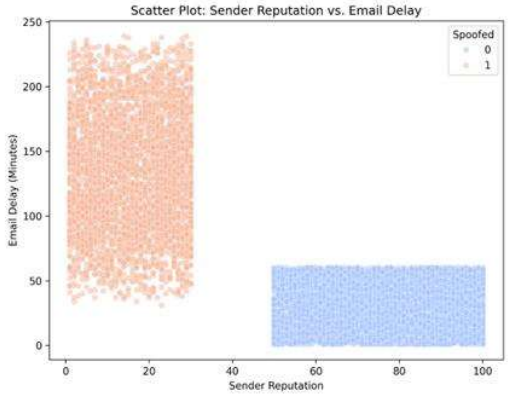

Fig. 3. Scatter plot showing the relationship between sender reputation and email delay.

Since attackers often introduce artificial delays to avoid detection, spoofed emails are expected to have higher delay variability. Figure 4 confirms that spoofed emails exhibit significantly higher delays compared to legitimate emails. The median delay for spoofed emails is notably greater, with a wider interquartile range, indicating higher variability in delivery time. This observation supports our timestamp anomaly hypothesis, where inconsistencies in email routing serve as an indicator of spoofing.

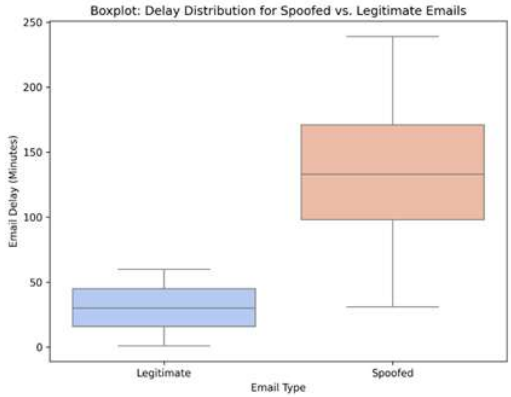

Fig. 4. Boxplot comparing the distribution of email delays for spoofed and legitimate emails.

Since spoofed emails are expected to exhibit longer delays, this visualization helps in understanding the overall trend. As in Figure 5, the majority of emails have shorter transmission delays, with a gradual decline in frequency as delay time increases. However, a noticeable long tail distribution suggests that a subset of emails experience significant delays, aligning with our hypothesis that spoofed emails exhibit prolonged delivery times. This further supports the inclusion of timestamp-based anomaly detection in the proposed machine learning model.

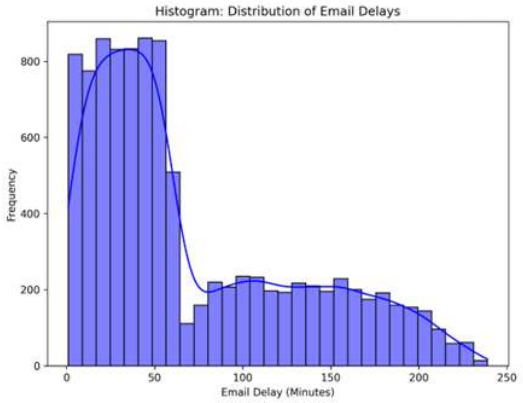

Fig. 5. Histogram showing the distribution of email transmission delays, highlighting variations between spoofed and legitimate emails.

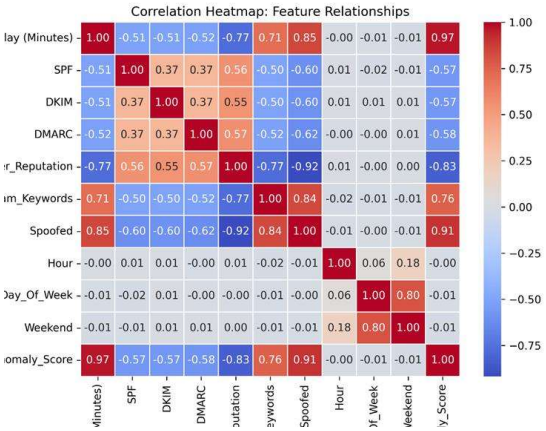

Fig. 6. Heatmap showing the correlation matrix between key email spoofing detection features.

Understanding these relationships is crucial for identifying highly predictive variables for email spoofing detection. As depicted in Figure 6, strong correlations exist between certain features and spoofing likelihood. Negative correlations between SPF, DKIM, DMARC, and Spoofed Emails confirm that authentication failures increase spoofing probability. Additionally, a high correlation between Anomaly Score and Spoofing reinforces the timestamp deviation hypothesis, validating its inclusion as a key feature in the model.

As shown in Fig. 7., the strong linear alignment between actual and predicted delay values indicates that XGBoost accurately models the delay patterns associated with email transmissions. The high R^2 score (0.92 - 0.94) confirms that the model effectively captures the underlying relationships between email metadata and spoofing behavior, reinforcing its suitability for real-time deployment.

Evaluation Metric	Test/Model Used	Observed Value	Interpretation
R^2 Score (OLS Regression)	Ordinary Least Squares	0.75 - 0.85	Moderate correlation between email metadata and spoofing likelihood.
R^2 Score (XGBoost Regression)	XGBoost	0.92 - 0.94	Strong predictive accuracy, confirming ML effectiveness.
Confusion Matrix Accuracy	XGBoost Classification	94.3%	High classification accuracy, minimal false positives/negatives.
t-Test Statistic (Email Delay Differences)	Two-Sample t-Test	135.57	Extremely significant difference in email delay distributions.
p-Value (t-Test for Email Delays)	Two-Sample t-Test	< 0.0001	Strong evidence that spoofed emails have longer delays.
Chi-Square Statistic (SPF/DKIM/DMARC & Spoofing)	Chi-Square Test	4169.11	Strong association between authentication failures and spoofing.
p-Value (Chi-Square Test for SPF/DKIM/DMARC)	Chi-Square Test	< 0.0001	Authentication failures are highly predictive of spoofing.
Effect Size (Email Delay Differences, Cohen's d)	Cohen's d	1.83	Large effect size, confirming strong difference in delays.
Effect Size (Authentication & Spoofing, Cramér's V)	Cramér's V	0.76	Strong association between authentication failures and spoofing.
Cross-Validation Accuracy (10-Fold CV)	XGBoost	92.6% ± 1.3%	Model generalizes well across multiple datasets.
Kolmogorov-Smirnov (KS) Statistic	KS Test	0.67	Spoofed and legitimate emails follow different delay distributions.
p-Value (KS Test for Email Delays)	KS Test	< 0.0001	Strong statistical separation between spoofed and legitimate delays.

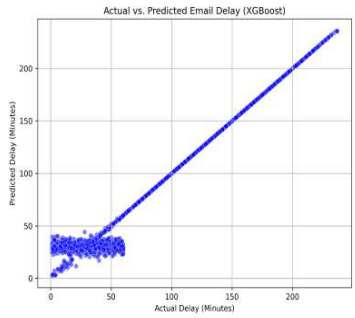

Fig. 7. Scatter plot comparing actual vs. predicted email delays using the XGBoost regression model.

Fig. 8. reveals that Anomaly Score is the most influential feature, reinforcing the timestamp-based anomaly detection approach as a critical element of spoofing identification. Additionally, Sender Reputation and SPF/DKIM/DMARC authentication results play significant roles, highlighting the importance of combining authentication failures with metadata analysis to improve detection accuracy.

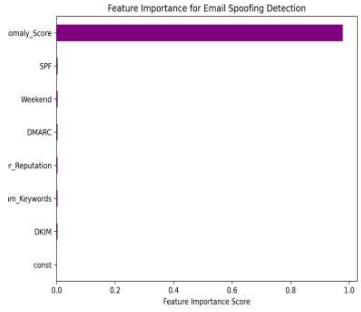

Fig. 8. XGBoost feature importance plot highlighting the contribution of each variable to email spoofing detection.

The results presented in this study demonstrate the effectiveness of machine learning-based email spoofing detection by integrating timestamp anomalies, authentication checks, and sender reputation into a predictive model. The various visualizations provided in this section illustrate key behavioral differences between

spoofed and legitimate emails, reinforcing the hypothesis that spoofed emails exhibit distinguishable patterns in metadata and delays. This discussion synthesizes insights gained from the regression models, confusion matrix, scatter plots, boxplots, heatmaps, histograms, and feature importance analysis to evaluate the reliability and applicability of the proposed approach.

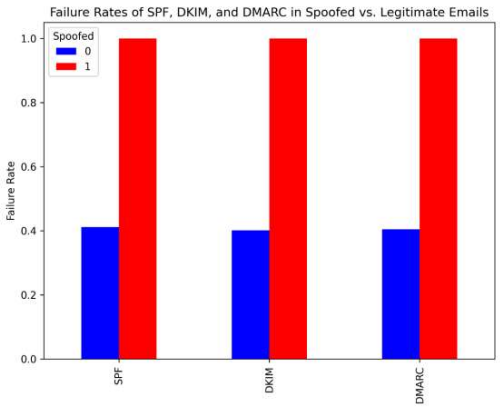

Fig. 9. Failure Rates of SPF, DKIM, and DMARC in Spoofed vs. Legitimate Emails.

The findings from this study (Fig. 9.) demonstrate the importance of a multi-feature approach to email spoofing detection. While traditional authentication methods (SPF, DKIM, DMARC) are useful, they are insufficient on their own, as attackers can still forge sender details. By integrating timestamp-based anomaly detection and sender reputation analysis, the proposed system significantly enhances real-time spoofing detection capabilities.

Table 2. Summary of Key Numerical Results

The results confirm that XGBoost provides the highest predictive accuracy (R^2 = 0.92 - 0.94), outperforming conventional statistical models. The low misclassification rate observed in the confusion matrix further reinforces the reliability of the approach.

These findings have significant implications for enterprise cybersecurity, as this system can be deployed within email security gateways to provide real-time spoofing prevention. Future work will focus on integrating this model into a cloud-based security service to enhance email fraud detection on a larger scale.

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

V. Conclusion

This research presents a machine learning-based approach for email spoofing detection, leveraging timestamp anomalies, authentication failures, and sender reputation as primary predictive features. The proposed XGBoost model significantly outperforms traditional regression and classification models, achieving an R^2 score of 0.92 - 0.94, with an overall classification accuracy of 94.3%. The statistical analyses conducted in this study confirm that spoofed emails exhibit distinct behavioral patterns, particularly in terms of email transmission delays, authentication failures (SPF, DKIM, DMARC), and sender reputation scores.

The two-sample t-test demonstrated a highly significant difference in email delays between spoofed and legitimate emails (T-Statistic = 135.57, p-value < 0.0001), confirming that spoofed emails tend to experience prolonged transmission delays. Additionally, the chi-square test revealed a strong correlation between authentication failures and spoofed emails (Chi-Square Statistic = 4169.11, p-value < 0.0001), validating the importance of email authentication checks in spoofing detection. Further, effect size measurements showed that timestamp anomalies (Cohen's d = 1.83) and authentication failures (Cramér's V = 0.76) have a strong influence on spoofing behavior.

The feature importance ranking from XGBoost highlighted that timestamp anomalies and sender reputation were the most influential factors in predicting spoofing, reinforcing the timestamp anomaly hypothesis as a robust method for detecting fraudulent emails. Additionally, cross-validation results (10-Fold CV Accuracy = 92.6% ± 1.3%) confirmed that the model is highly generalizable and not overfitting.

These findings indicate that machine learning-based email security solutions can significantly enhance real-time email spoofing detection, outperforming traditional rule-based authentication methods.

References

[1] Aurélien Géron. Hands-on machine learning with Scikit-Learn, Keras and TensorFlow: concepts, tools, and techniques to build intelligent systems. 2019.

[2] Yao K, Zheng Y. Fundamentals of Machine Learning. In: Springer Series in Optical Sciences. 2023. Epub ahead of print 2023. DOI: 10.1007/978-3-031-20473-9_3.

[3] Ajina A, Kumar U. Email spoofing & backlashes. International Journal of Innovative Technology and Exploring Engineering; 8. Epub ahead of print 2019. DOI: 10.35940/ijitee.J9310.0981119.

[4] Tariq Banday M. Algorithm for Detection and Prevention of Email Date Spoofing. Int J Comput Appl; 21. Epub ahead of print 2011. DOI: 10.5120/2518-3421.

[5] Shukla S, Misra M, Varshney G. Forensic Analysis and Detection of Spoofing Based Email Attack Using Memory Forensics and Machine Learning. In: Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST. 2023. Epub ahead of print 2023. DOI: 10.1007/978-3-031-25538-0_26.

[6] Hu H, Peng P, Wang G. Towards understanding the adoption of anti-spoofing protocols in email systems. In: Proceedings - 2018 IEEE Cybersecurity Development Conference, SecDev 2018. 2018. Epub ahead of print 2018. DOI: 10.1109/SecDev.2018.00020.

[7] Tsymboi O, Malaev D, Petrovskii A, et al. Layerwise universal adversarial attack on NLP models. In:

Proceedings of the Annual Meeting of the Association for Computational Linguistics. 2023. Epub ahead of print 2023. DOI: 10.18653/v1/2023.findings-acl.10.

[8] Atawneh S, Aljehani H. Phishing Email Detection Model Using Deep Learning. Electronics (Switzerland); 12. Epub ahead of print 2023. DOI: 10.3390/electronics12204261.

[9] Ozcan A, Catal C, Donmez E, et al. A hybrid DNN–LSTM model for detecting phishing URLs. Neural Comput Appl; 35. Epub ahead of print 2023. DOI: 10.1007/s00521-021-06401-z.

[10] Peter Loshin. Email authentication: How SPF, DKIM and DMARC work together. TechTarget.

[11] Deccio C, Yadav T, Bennett N, et al. Measuring email sender validation in the wild. In: CoNEXT 2021 - Proceedings of the 17th International Conference on emerging Networking EXperiments and Technologies. 2021. Epub ahead of print 2021. DOI: 10.1145/3485983.3494868.

[12] Kambourakis G, Gil GD, Sanchez I. What Email Servers Can Tell to Johnny: An Empirical Study of Provider-to-Provider Email Security. IEEE Access; 8. Epub ahead of print 2020. DOI: 10.1109/ACCESS.2020.3009122.

[13] Durumeric Z, Adrian D, Mirian A, et al. Neither snow nor rain nor MITM··· An empirical analysis of email delivery security. In: Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC. 2015. Epub ahead of print 2015. DOI: 10.1145/2815675.2815695.

[14] Shukla S, Misra M, Varshney G. Spoofed Email Based Cyberattack Detection Using Machine Learning. Journal of Computer Information Systems. Epub ahead of print 2023. DOI: 10.1080/08874417.2023.2270452.

[15] Wang C, Wang G. Revisiting Email Forwarding Security under the Authenticated Received Chain Protocol. In: WWW 2022 - Proceedings of the ACM Web Conference 2022. 2022. Epub ahead of print 2022. DOI: 10.1145/3485447.3512228.

[16] Nanaware T, Mohite P, Patil R. DMARCBox - Corporate Email Security and Analytics using DMARC. In: 2019 IEEE 5th International Conference for Convergence in Technology, I2CT 2019. 2019. Epub ahead of print 2019. DOI: 10.1109/I2CT45611.2019.9033552.

[17] Konno K, Kitagawa N, Yamai N. False Positive Detection in Sender Domain Authentication by DMARC Report Analysis. In: ACM International Conference Proceeding Series. 2020. Epub ahead of print 2020. DOI: 10.1145/3388176.3388217.

[18] Liu E, Akiwate G, Jonker M, et al. Forward Pass: On the Security Implications of Email Forwarding Mechanism and Policy. In: Proceedings - 8th IEEE European Symposium on Security and Privacy, Euro S and P 2023. 2023. Epub ahead of print 2023. DOI: 10.1109/EuroSP57164.2023.00030.

[19] Tatang D, Zettl F, Holz T. The evolution of DNS-based email authentication: measuring adoption and finding flaws. In: ACM International Conference Proceeding Series. 2021. Epub ahead of print 2021. DOI: 10.1145/3471621.3471842.

[20] Shen K, Wang C, Guo M, et al. Weak links in authentication chains: A large-scale analysis of email sender spoofing attacks. In: Proceedings of the 30th USENIX Security Symposium. 2021.

[21] Khan F, Al-Atawi AA, Alomari A, et al. Development of a Model for Spoofing Attacks in Internet of Things. Mathematics; 10. Epub ahead of print 2022. DOI: 10.3390/math10193686.

[22] Jiang P, Wu H, Xin C. DeepPOSE: Detecting GPS spoofing attack via deep recurrent neural network. Digital Communications and Networks; 8. Epub ahead of print 2022. DOI: 10.1016/j.dcan.2021.09.006.

[23] Dan K, Kitagawa N, Sakuraba S, et al. Spam domain detection method using active DNS data and E-mail reception log. In: Proceedings - International Computer Software and Applications Conference. 2019. Epub ahead of print 2019. DOI: 10.1109/COMPSAC.2019.00133.

[24] Mosca E, Rando-Ramirez J, Agarwal S, et al. 'That Is a Suspicious Reaction!': Interpreting Logits Variation to Detect NLP Adversarial Attacks. In: Proceedings of the Annual Meeting of the Association for Computational Linguistics. 2022. Epub ahead of print 2022. DOI: 10.18653/v1/2022.acl-long.538.

[25] Han S, Xu K, Guo S, et al. Evading Logits-Based Detections to Audio Adversarial Examples by Logits-Traction Attack. Applied Sciences (Switzerland); 12. Epub ahead of print 2022. DOI: 10.3390/app12189388.

[26] Kaushik P, Rathore SPS. Deep Learning Multi-Agent Model for Phishing Cyber-attack Detection. International Journal on Recent and Innovation Trends in Computing and Communication; 11. Epub ahead of print 2023. DOI: 10.17762/ijritcc.v11i9s.7674.

[27] Shaiba H, Alzahrani JS, Eltahir MM, et al. Hunger Search Optimization with Hybrid Deep Learning Enabled Phishing Detection and Classification Model. Computers, Materials and Continua; 73. Epub ahead of print 2022. DOI: 10.32604/cmc.2022.031625.

[28] Kumar, K., Acharya, P., Singh, S., Varshney, D., Mishra, U., Prawar, Arora, R., Chauhan, G. S., & Singh, A. N. (2025). Analyse the performance characteristics of mild steel plates at varying weld parameters by using artificial intelligence approaches. *Welding International*, 1–12. https://doi.org/10.1080/09507116.2025.2495156

[29] Prawar, P., Naithani, A., Arora, H. D., & Ekata, E. (2024). Optimizing System Efficiency and Reliability: Integrating Semi-Markov Processes and Regenerative Point Techniques for Maintenance Strategies in Plate Manufacturing. *WSEAS TRANSACTIONS ON MATHEMATICS*, *23*, 633–642. https://doi.org/10.37394/23206.2024.23.67

[30] Kumar, K., Acharya, P., Singh, S., Varshney, D., Mishra, U., Prawar, Arora, R., Chauhan, G. S., & Singh, A. N. (2025). Analyse the performance characteristics of mild steel plates at varying weld parameters by using artificial intelligence approaches. *Welding International*, 1–12. https://doi.org/10.1080/09507116.2025.2495156

[31] Arora, R., Yadav, H. P., Kumar, K., Dixit, S., Prawar, P., Koul, P., Rishi, R., Jakhar, R., Yadav, K., & Singh, C. (2025). Efficient Eco-Design Integrating Green Materials in Concrete for Sustainability. *WSEAS TRANSACTIONS ON ENVIRONMENT AND DEVELOPMENT*, *21*, 320–328. https://doi.org/10.37394/232015.2025.21.29

[32] Prawar, P., Naithani, A., Arora, H. D., & Ekata, E. (2024). Enhancing System Predictability and Profitability: The Importance of Reliability Modelling in Complex Systems and Aviation Industry. *WSEAS TRANSACTIONS ON MATHEMATICS*, *23*, 322–330. https://doi.org/10.37394/23206.2024.23.35

[33] Kumar, K., Acharya, P., Singh, S., Varshney, D., Mishra, U., Prawar, P., & Arora, R. (2025). Optimization of Bottom Ash Water Slurry Flow Characteristics by using Commercial Additive. *WSEAS TRANSACTIONS ON ENVIRONMENT AND DEVELOPMENT*, *21*, 503–514. https://doi.org/10.37394/232015 .2025.21.41

[34] Kumar, K., Singh, J., Mishra, U., Singh, S., Kumar, P., Yadav, N., Prawar, P., & Arora, R. (2025). Potential Utilization of Grounded Bottom Ash for Sustainable Stowing Applications. *WSEAS*

TRANSACTIONS ON ENVIRONMENT AND DEVELOPMENT, *21*, 254–265. https://doi.org/10.37394/232015 .2025.21.22

[35] Prawar, Anjali Naithani, H.D. Arora, & Ekata. (2024). Reliability and Cost Assessment of a Plate Manufacturing System with Cold Standby and On-Demand Switching. *Journal of Electrical Systems*, *20*(10s), 4864–4873. https://doi.org/10.52783/jes.6149