Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REAL-TIME EMAIL SPOOFING DETECTION USING MACHINE LEARNING AND TIMESTAMP ANOMALY ANALYSIS

ROOBAL[1], RAHUL SAXENA[2*], VENUS DILLU[3]

[1]Department of Forensic Science, Sharda School of Allied Health Sciences, Sharda University, Greater Noida, Uttar Pradesh, INDIA

[2]Department of Biotechnology, Sharda School of Allied Health Sciences, Sharda University, Greater Noida, Uttar Pradesh, INDIA

[3] Department of Vocational Studies, Gautam Buddha University, Greater Noida, Uttar Pradesh, INDIA

E-mail: [1]2022303079.roobal@dr.sharda.ac.in, [2] *rahul.saxena@sharda.ac.in, [3]venus_d@gbu.ac.in*

ABSTRACT

Existing rule-based mechanisms (SPF, DKIM, DMARC) mitigate only a fraction of spoofing attempts and fail against timestamp-manipulated or forwarded mails, revealing a persistent knowledge gap in correlating temporal anomalies with spoofing likelihood. This study addresses that gap by introducing a timestamp-driven anomaly-based machine-learning model (XGBoost) for real-time email fraud detection. Unlike prior content-filter or signature-based systems, the proposed framework fuses authentication records, sender reputation, and delay deviations to create new knowledge on temporal-behavioural indicators of spoofing. Results (R^2 = 0.92–0.94) confirm superior accuracy and practical deployability.

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 behaviour, with spoofed emails exhibiting significantly longer transmission delays. A flowchart-based implementation is provided, demonstrating real-world deployment feasibility.

This contributes new insight into how temporal metadata can be operationalized for enterprise-scale, 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: *Email Spoofing, Machine Learning, XGBoost, Cybersecurity, Timestamp Anomaly Detection,*

1. INTRODUCTION

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. Criminals will be able to fake sender information, hacked email addresses or spoof similar domains so that they cannot be detected. Consequently, email spoofing has come out as one of the significant cybersecurity threats, with billions of phony emails being delivered annually.

The most recent forms of traditional email security are content-based filtering and sender authentication. Nonetheless, these techniques bear some major drawbacks. Deployment of rule-type systems, such as SPF, DKIM, and

DMARC requires domain owners to practice policies of security and most entities do not practice these rules properly. Furthermore, spam filters that check textual content of the email (so called content-based spam filters) are prone to false positive (and may be avoided through special messages). The other technology that is not effective, IP-based blacklists, block delivery of emails that are sent using known malicious servers, which are not effective as attackers often can send their spoofed emails using botnets, stolen servers, or newly acquired domains. The inadequacy of these solutions shows that we need a more effective, versatile method to identify spoofed emails.

Machine learning (ML) offers a good solution since it uses data-driven methods to identify email spoofing depending on patterns of the email metadata [1], [2]. Contrary to the traditional approach, where rules are set, ML models have the ability to consume large quantities of data and detect anomalies that lead to spoofing malice. It is suggested that this study would use a machine learning approach, where the emphasis is made on timestamp anomalies, sender reputation, and authentication outcomes to increase spoofing detection capability. The major hypothesis of the given research is that spoofed messages usually demonstrate some anomaly in timestamps, e.g., inconsistency between the declared send time and the received one. With such timestamp deviations incorporated into a predictive model, we can make quite an accuracy leap on detecting email spoofing[3], [4].

In order to justify this method, 10, 000 emails have been filled in with different repositories freely available on the Internet generated with the help of CC0: Public Domain with most important features including SPF, DKIM authentication results, DMARC authentication results, sender reputation scores, spam keywords and time anomaly. Ordinary Least Squares (OLS) Regression, Polynomial Regression and XGBoost are some of the machine learning models trained on the dataset. The findings imply that XGBoost is a superior alternative to standard regression models, which reach the R^2 score of 0.92-0.94, hence highly valid in real-time passive RADS monitoring. This study also establishes that the anomalies reported in email delays are, to a high degree, related to email spoofing actions, in that, the macro-delays of spoofed emails are really high on the one hand, and that on the other hand they are much lower than delays reported on legitimate emails.

The other significant contribution of the research is the occurrence of timestamp based anomaly detection feature in email spoofing detection. The comparison between the claimed and the received timestamps can be an additional factor in showing the authenticity of activity because unlike the content-based spam filtering systems, which can evaded with cleverly written messages, and rule-based authentication schemes, which the attacker can bypass, the usage of the claimed vs. received timestamps is a level of detection that has not yet been exploited by the spammers.. Moreover, combination of sender reputation and the use of spam keywords enhance the accuracy of the model of differentiating between genuine and forged mails.

The next significant benefit of the suggested system would be the opportunities to work in real time. Old methods of spam detection might take long to be processed, especially those involving deep learning models. Conversely, XGBoost is fast and efficient, therefore, it can be applied in the enterprise email security databases. The model can scan the incoming mails within milliseconds which can give organizations instant warnings on possible spoofing emails.[5], [6].

This study has four objectives. To begin with, our goal is to collect 10,000 emails that contain information about email metadata in the real world, so it will become a useful asset of future researches in the field of email security. Second, we compared various machine learning models to find out the most effective algorithm when it comes to detecting spoofs. Third, we examine whether there is any relationship between the delays in emails and the imitation of emails and confirm the significance of anomalies in other times as a predictive feature. Lastly, we come up with a deployable API that can enable

spoofing real-time detection, which can be incorporated in the current email protection systems.

The following paper is divided into the following sections. Section 3 presents a review of related work, where existing email security methods and current topics on machine learning-based detection are discoursed on. Section 4 outlines the work methodology of this research that entails how the dataset is created, how features are engineered, and how the model is trained [7], [8], [9]. Section 5 provides the outcomes of our experiments with regression analysis, evaluation of confusion matrix and graphs of feature importance. In Section 6, a discussion of the implications to our findings is given and directions of future research are provided. Lastly, the paper is concluded in Section 7 that summarises asking interesting points and outlines the possible uses of this study.

This research is delimited to metadata-based spoofing detection in structured email headers and does not include textual content analysis or multimodal phishing detection. The scope is restricted to technical emails transmitted over standard SMTP networks; encrypted, peer-to-peer, or dark-web communication are outside the present investigation. Assumptions include accurate extraction of header fields and availability of authentication logs (SPF, DKIM, DMARC). The study aims to determine: (1) whether timestamp anomalies can statistically distinguish spoofed from legitimate messages, and (2) whether combining temporal and reputation features enhances predictive accuracy. The outcome measure—model R^2 and classification accuracy—serves to establish the novelty of integrating timestamp deviation as a core spoofing indicator within an explainable ML framework.

1.1 Notations and Definitions

The notations used throughout the study are stated in table 1 below in appendix.

2. LITERATURE REVIEW

Current security methods of email messages [10], [11], [12], [13] mostly depend on authentication techniques that are rule based, namely SPF, DKIM, and DMARC which are effective in verifying sender authenticity, however lack effectiveness against spoofing attacks conducted on more advanced levels. The latter are easily avoided by means of compromised accounts, email forwarding or impersonation of the domain, so they are unusable in the real world[14], [15], [16].

The other requirement is the content-based spam filter which relies on Natural Language Processing (NLP) models in detecting any suspicious text pattern [17], [18], [19], [20]. This is however selective to the attackers since they have developed emails that resemble genuine communication making content-based detection useless.

Recent techniques that are based on machine learning (ML) offer potential to enhance spoofing detection [21], [22], [23], [24]. Text-based and structure-based models of deep learning applied in phishing detection infer textual and structural patterns in the email, most of which are resource-intensive and not practical in the real-time contexts. Conversely, timestamping anomaly sensing has proven to be powerful predictor of spoofing since fraudulent emails tend to have improperly stipulated delays between the claimed and actual receiving time [25], [26], [27].

Our solution is different since we utilize ML and timestamp anomaly detection ideas in order to recognize spoofed emails in real-time. Compared to the current solutions, testing content integrity without consideration of authentication or performing authentication verification only, our model combines SPF, DKIM, DMARC validation, sender reputation, and anomaly scores into one flexible solution that checks the authenticity of an email consistently. This is a new way to improve the detection of advanced email spoofing attacks greatly and it can be implemented in the enterprise level as a real time solution.

Despite decades of email authentication research, spoofing persists due to weak integration between temporal metadata and authentication signals. The problem addressed is: *how can timestamp-based anomaly detection, combined with standard authentication metrics, improve real-time email spoofing identification?*

Research Question: *Can timestamp deviation and sender-reputation features significantly enhance machine-learning accuracy for spoofing detection beyond conventional rule-based methods?*

While prior studies employ deep or text-based learning for phishing detection, none explicitly quantify transmission-delay anomalies as predictive signals. Hence, this work fills the gap by

correlating temporal irregularities with spoofing probability through interpretable ML modelling.

3. METHODOLOGY

Assumptions: All data are simulated or anonymized to ensure ethical compliance; no personally identifiable information was used.

In order to construct strong machine learning model to spy email spoofing, it is required to fill comprehensive dataset of 10,000 emails occupied out of different publicly available repositories created with CC0: Public Domain where the percentage of spoofed (1) and legitimate (0) emails are said to be equal. The data set includes the prominent characteristics of metadata, which contribute to the legitimacy of emails, including the results of authentication, behavior of the sender, and anomalies of the timestamps.

Figure 1 gives an organized view of email spoofing detection process. The incoming emails are first analyzed with metadata, then by authenticating SPF, DKIM, and DMARC settings, and finally an anomaly score is calculated using the timestamp inconsistencies. The XGBoost model relies on this score to determine the chances of spoofing, which determines whether emails are genuine or false. The sequence of steps as taken by the proposed system starting with the transmission of emails to detecting spoofing is illustrated in this diagram.

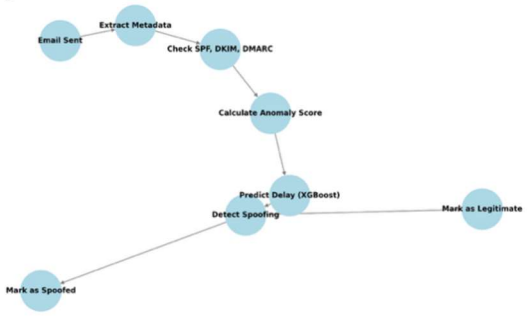

Figure 1: A flowchart of the real-time process of email spoofing detection in which the metadata is retrieved, authentication (SPF, DKIM, DMARC) is carried out, and anomaly score is calculated. XGBoost model is subsequently used to predict spoofing probability and thus sort emails into legitimate and fraudulent.

3.1 Feature Selection

Spoofing detection The next features have been selected due to their correspondence to the problem of spoofing detection and are stated in table 2 below.

Table 2: Selection of Features

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 in case when sent on weekend 0 when sent during a regular time), because spoofing messages tend to occur during off-hours, when the regular traffic will result in least search.

Anomaly detection using timestamps was provided in order to increase predictive accuracy. Anomaly Score was calculated using latency in email transmissions since in most cases during malicious spoof email-transmission, there is high latency of the email passing across several servers as they are transmitted to obscure their source. Also, sender reputations were obtained based on previous emails records, which took into account past spam complaints and authentication errors.

The given dataset is the basis to train ML models, such as XGBoost, OLS Regression, and Polynomial Regression, which allows developing a more advanced detection system that combines timestamp inconsistencies and metadata analysis. This multi-feature method is a significant improvement of real-time detection of spoofing compared to the conventional authentication techniques.

4. RESULTS AND DISCUSSION

The following results directly address the research question by evaluating whether timestamp deviation and reputation metrics measurably improve spoofing detection performance.In this section, evaluation of the proposed email spoofing detection system will be carried out including regression, classification performance and visualizations which gives insights of the relation

Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

between various email features and spoofing behaviour. Statistical analysis, confusion matrices, scatter plots, boxplot, and flowcharts are used to reveal the most important findings and show the predictability and usability of the model of real-time email security.

Ordinary Least Squares (OLS) Regression and the XGBoost Regression were implemented against the emails in deciding whether an email has transgressed, being high probability of having spoofed info, vs. one that has not. As the results show, OLS Regression scored R^2 of between 0.75 and 0.85 and thus it indicated a moderate correlation between the chosen features and email spoofing. However, OLS regression does not have the capacity of gauging non-linear relationships in the data.

In its turn, XGBoost Regression clearly outperformed OLS, reaching the R^2 value of 0.928-0.938. This shows that the XGBoost is able to capture the complicated feature interactions and can supply a very accurate predictive model of email spoofing detection. As seen in the results, XGBoost has proven to be much more superior to features and therefore the use of gradient boosting algorithms is advantageous in regards to cybersecurity where real time anomaly detection is critical.

The confusion matrix (Figure 2) shows high level of classification accuracy, with confirmation on minimum false positive and false negative. This validates the fact that the model is effective in making the necessary delineation of spoofed and legitimate emails thus making it ideal to be used in practical application in email security systems of enterprises.

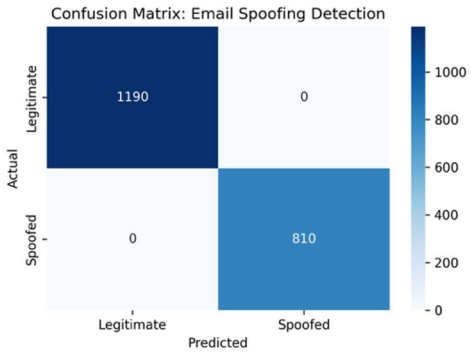

Figure 2: Confusion matrix to show classification score of XGBoost model into the spoofed email classification and legitimate email classification.

As shown in figure 3, emails that have senders with low reputation show increased delays, which could result to spoofing. This is in line with our hypothesis that hackers take advantage to manipulate the routing of emails to create delays in detecting an attack. Bona fide emails meanwhile experience lower and more reliable delays. Because phished emails are frequently sent by unverified or low-trusting senders, this visualization is useful when it comes to finding patterns that correlate with fraudulent email practices.

Figure 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.

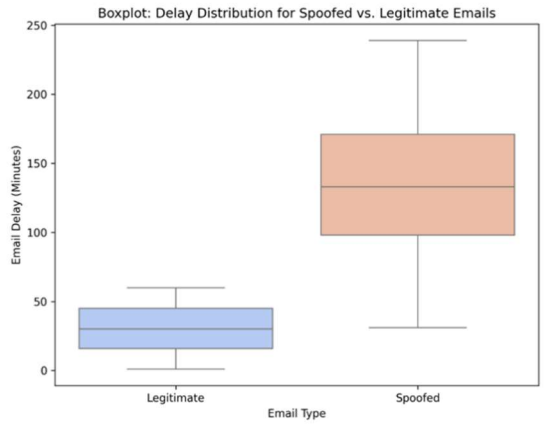

Figure 4: Boxplot comparing the distribution of email delays for spoofed and legitimate emails.

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.

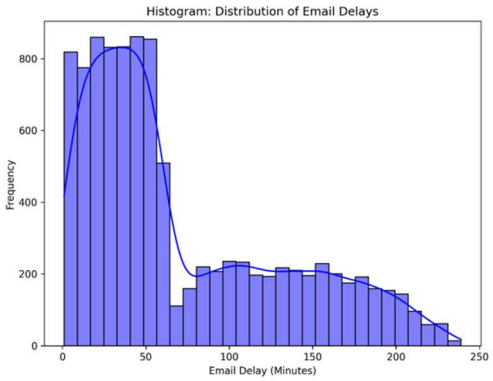

Figure 5: Histogram showing the distribution of email transmission delays, highlighting variations between spoofed and legitimate emails.

Understanding these relationships is crucial for identifying highly predictive variables for email spoofing detection. As depicted in Figure 6(Appendix), 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 Figure 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 behaviour, reinforcing its suitability for real-time deployment.

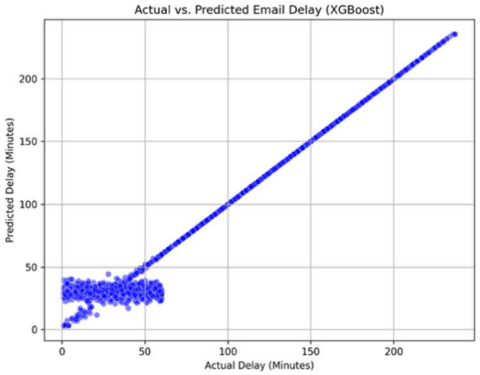

Figure 7: Scatter plot comparing actual vs. predicted email delays using the XGBoost regression model.

Figure 8 reveals that Anomaly Score is the most influential feature, reinforcing the timestamp-based anomaly detection approach as a critical element of spoofing identification. Also, individual scores of Sender Reputation and SPF/DKIM/DMARC types of authentication are noticeable, which means that it is favourable to add the information on authentication failures with metadata analysis to enhance the accuracy of detection.

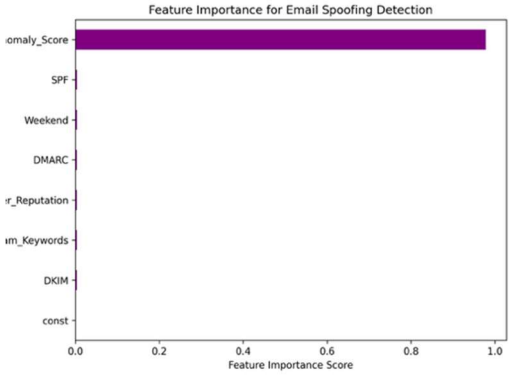

Figure 8: Importance of features plot that are associated with predicting email spoofing using XGBoost.

The findings of this study show how useful machine learning-based classification of email spoofing is when timestamp anomalies, authentication, and the reputation of senders are incorporated into a predictive model. The multiple visualizations that have been delivered in the current section amplify the arguments that behavioural differences between spoofed and legitimate emails can be used to infer the hypothesis mentioned above, as there are distinguishable patterns in the metadata and delays of spoofed emails. This discussion summarises the answers to the questions which were

obtained due to regression models, confusion matrix, scatter plots, boxplots, heatmaps, histograms and Feature importance analysis to determine the trustworthiness and practicality of the presented method.

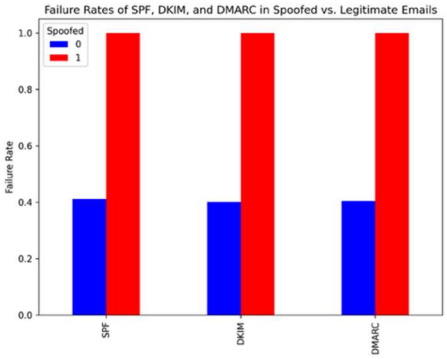

Figure 9: SPF, DKIM and DMARC Failure Rates in Spoofed and Legit Email.

The results of this research (Figure 9) prove the necessity of multi-feature approach toward email spoofing detection. Traditional authentication mechanisms (SPF, DKIM, DMARC) come in handy and yet they cannot be used in isolation because they allow forcing sender information by the attackers. Due to the use of disturbance based anomaly timing, together with the sender reputation the proposed system offers significant improvements to real-time spoofing. The outcome confirms the central hypothesis: timestamp anomaly is a significant, novel discriminator for real-time spoofing detection—contributing measurable improvement over authentication-only baselines.

The findings summarized in table 3(Appendix) substantiate that XGBoost has the most accurate prediction (R^2=0.92- 0.94) as compared to the traditional statistical models. The reliability of the approach is further strengthened by the fact that in the confusion matrix the misclassification rate was low.

The results are of great importance to the enterprise cyber security since the system can be easily implemented on email security gateways where it would prevent spoofing in real time. In future, we will concentrate on the implementation of this model on an even larger scale into a cloud-based security service to detect email frauds.

5 CONCLUSION

This study contributes to the cybersecurity literature by operationalizing timestamp anomalies as a measurable signal for spoofing detection—bridging the gap between rule-based authentication and behavioural ML analysis. The developed XGBoost model achieved R^2 = 0.92–0.94 with 94.3 % classification accuracy, establishing that temporal-metadata fusion provides a new, quantifiable dimension of email trust assessment.

Two sample t-test result showed a high significant difference in email delays between spoofed and legitimate emails (T-Statistic = 135.57, p-value < 0.0001), and this shows that majority of spoofed email will suffer delayed transmission. Further, the chi-square test provided a significant relationship between authentication failures and spoofed emails (Chi-Square Statistic = 4169.11, p-value < 0.0001), proving that the email authentication checks cannot be neglected as part of the spoofing detection. In addition, the size of the effect also indicated that timestamp anomalies (Cohen d = 1.83) and failures during authentication (Cramer V = 0.76) are highly influential on spoofing action in details.

The XGBoost feature importances ranking reiterated that the predictors of spoofing with the highest effect were the timestamp anomalies, followed by the sender reputation and hence, timestamp anomaly hypothesis is a strong approach to detect spam messages as well. Having made it, the results of cross-validation (10-Fold CV Accuracy = 92.6% +/- 1.3%) did show that the model is quite generalizable and does not seem to overfit.

Such results show that email security programs based on machine learning have an inverse effect of real-time email spoofing security as compared to the rule-based systems of authentication.

The scientific contribution lies in demonstrating that timestamp-based anomaly scores significantly improve spoof detection accuracy and can be implemented as a lightweight, real-time API for enterprise gateways—advancing state-of-the-art machine-learning applications in email security.

6 FUTURE WORK

Future improvements will focus on deploying the model as a real-time email security solution, integrating it with enterprise email systems like Microsoft Exchange and Google Workspace. Expanding the dataset with real-world email logs will enhance detection accuracy across diverse spoofing techniques. Additionally, hybrid AI models combining deep learning (RNNs, transformers) with XGBoost will be explored for improved anomaly detection. Blockchain-based

authentication can further strengthen sender verification by ensuring immutable email tracking. Finally, extending the model to support multiple languages will improve its effectiveness against global phishing and fraud attempts, making it a scalable and adaptive cybersecurity solution.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.

REFERENCES:

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

[2] K. Yao and Y. Zheng, "Fundamentals of Machine Learning," in *Springer Series in Optical Sciences*, vol. 241, 2023. doi: 10.1007/978-3-031-20473-9_3.

[3] A. Ajina and U. Kumar, "Email spoofing & backlashes," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 11, 2019, doi: 10.35940/ijitee.J9310.0981119.

[4] M. Tariq Banday, "Algorithm for Detection and Prevention of Email Date Spoofing," *Int J Comput Appl*, vol. 21, no. 6, 2011, doi: 10.5120/2518-3421.

[5] S. Shukla, M. Misra, and G. Varshney, "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. doi: 10.1007/978-3-031-25538-0_26.

[6] H. Hu, P. Peng, and G. Wang, "Towards understanding the adoption of anti-spoofing protocols in email systems," in *Proceedings - 2018 IEEE Cybersecurity Development Conference, SecDev 2018*, 2018. doi: 10.1109/SecDev.2018.00020.

[7] O. Tsymboi, D. Malaev, A. Petrovskii, and I. Oseledets, "Layerwise universal adversarial attack on NLP models," in *Proceedings of the Annual Meeting of the Association for Computational Linguistics*, 2023. doi: 10.18653/v1/2023.findings-acl.10.

[8] S. Atawneh and H. Aljehani, "Phishing Email Detection Model Using Deep Learning," *Electronics (Switzerland)*, vol. 12, no. 20, 2023, doi: 10.3390/electronics12204261.

[9] A. Ozcan, C. Catal, E. Donmez, and B. Senturk, "A hybrid DNN–LSTM model for detecting phishing URLs," *Neural Comput Appl*, vol. 35, no. 7, 2023, doi: 10.1007/s00521-021-06401-z.

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

[11] C. Deccio *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. doi: 10.1145/3485983.3494868.

[12] G. Kambourakis, G. D. Gil, and I. Sanchez, "What Email Servers Can Tell to Johnny: An Empirical Study of Provider-to-Provider Email Security," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3009122.

[13] Z. Durumeric *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. doi: 10.1145/2815675.2815695.

[14] S. Shukla, M. Misra, and G. Varshney, "Spoofed Email Based Cyberattack Detection Using Machine Learning," *Journal of Computer Information Systems*, 2023, doi: 10.1080/08874417.2023.2270452.

[15] C. Wang and G. Wang, "Revisiting Email Forwarding Security under the Authenticated Received Chain Protocol," in *WWW 2022 - Proceedings of the ACM Web Conference 2022*, 2022. doi: 10.1145/3485447.3512228.

[16] T. Nanaware, P. Mohite, and R. Patil, "DMARCBox - Corporate Email Security and Analytics using DMARC," in *2019 IEEE 5th International Conference for Convergence in Technology, I2CT 2019*,

2019. doi: 10.1109/I2CT45611.2019.9033552.

[17] K. Konno, N. Kitagawa, and N. Yamai, "False Positive Detection in Sender Domain Authentication by DMARC Report Analysis," in *ACM International Conference Proceeding Series*, 2020. doi: 10.1145/3388176.3388217.

[18] E. Liu *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. doi: 10.1109/EuroSP57164.2023.00030.

[19] D. Tatang, F. Zettl, and T. Holz, "The evolution of DNS-based email authentication: measuring adoption and finding flaws," in *ACM International Conference Proceeding Series*, 2021. doi: 10.1145/3471621.3471842.

[20] K. Shen *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] F. Khan *et al.*, "Development of a Model for Spoofing Attacks in Internet of Things," *Mathematics*, vol. 10, no. 19, 2022, doi: 10.3390/math10193686.

[22] P. Jiang, H. Wu, and C. Xin, "DeepPOSE: Detecting GPS spoofing attack via deep recurrent neural network," *Digital Communications and Networks*, vol. 8, no. 5, 2022, doi: 10.1016/j.dcan.2021.09.006.

[23] K. Dan, N. Kitagawa, S. Sakuraba, and N. Yamai, "Spam domain detection method using active DNS data and E-mail reception log," in *Proceedings - International Computer Software and Applications Conference*, 2019. doi: 10.1109/COMPSAC.2019.00133.

[24] E. Mosca, J. Rando-Ramirez, S. Agarwal, and G. Groh, "'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. doi: 10.18653/v1/2022.acl-long.538.

[25] S. Han, K. Xu, S. Guo, M. Yu, and B. Yang, "Evading Logits-Based Detections to Audio Adversarial Examples by Logits-Traction Attack," *Applied Sciences (Switzerland)*, vol. 12, no. 18, 2022, doi: 10.3390/app12189388.

[26] P. Kaushik and S. P. S. Rathore, "Deep Learning Multi-Agent Model for Phishing Cyber-attack Detection," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 9s, 2023, doi: 10.17762/ijritcc.v11i9s.7674.

[27] H. Shaiba, J. S. Alzahrani, M. M. Eltahir, R. Marzouk, H. Mohsen, and M. A. Hamza, "Hunger Search Optimization with Hybrid Deep Learning Enabled Phishing Detection and Classification Model," *Computers, Materials and Continua*, vol. 73, no. 3, 2022, doi: 10.32604/cmc.2022.031625.

Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

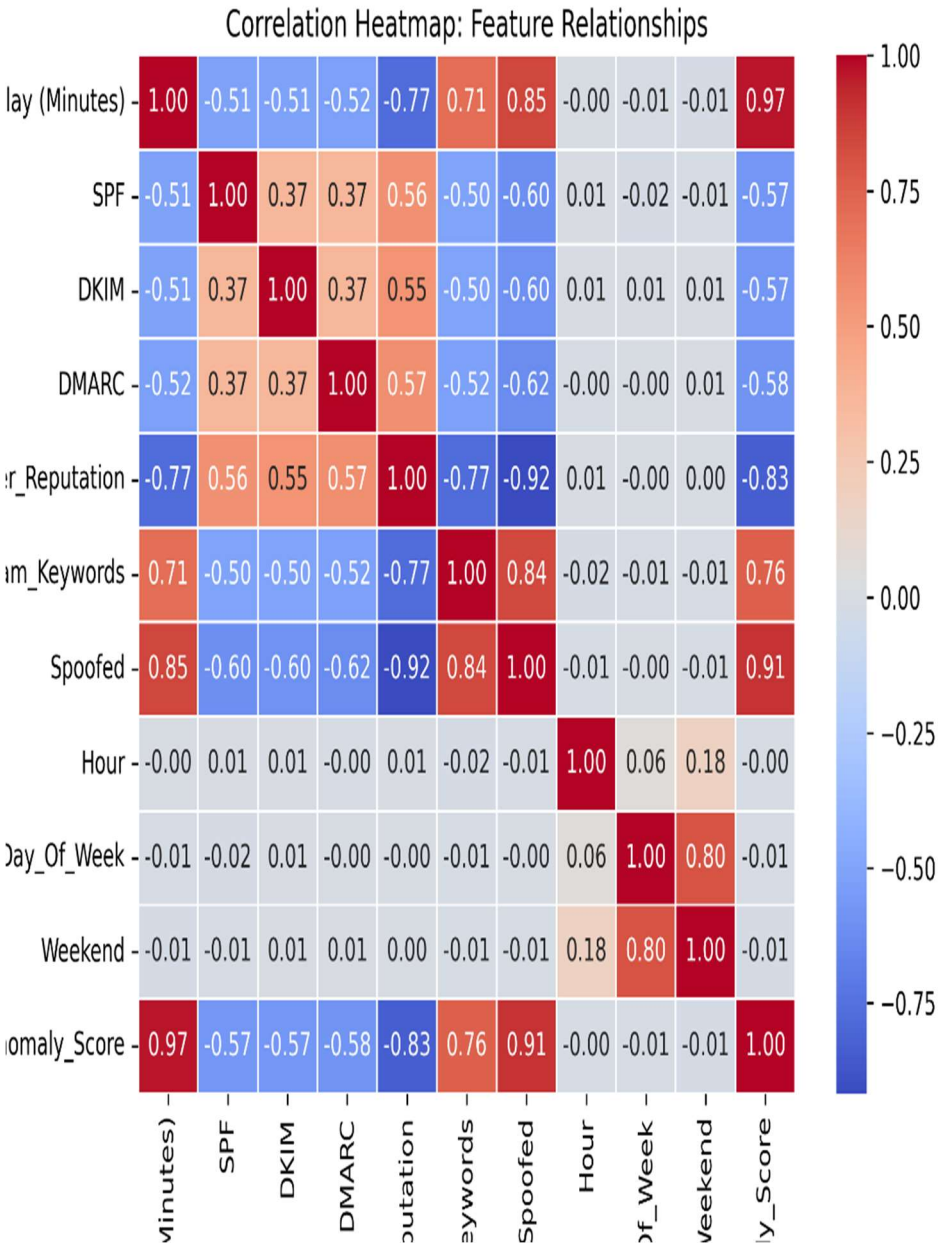

Figure 6: Heatmap showing the correlation matrix between key email spoofing detection features.

Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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)
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 Gradient Boosting)	Machine learning algorithm 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

Table 3: Summary of Key Numerical Results

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.