International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Monitor and Manage Email Spoofing Threats in Real-Time

Eslavath Charan[1], Kanchan Thapa[2], Minnekanti Sneha[3], Dr. S. Janardhana Rao[4]

[1,2,3,4]Department of CSE, IARE collage Hyderabad

Abstract:
The proposed system is detection of spoofing emails using a web application which take input as an email detail and gives the answer as an email is spoofed or legitimate. To identify the user is sending spoofed email or legitimate email mechanism of authentication which is based on DNS is used in this application which includes DMARC, DKIM and SPF. For the infection inspection user need to upload content of an email as well as header totally which is received. The risk score is calculated based on results of authentication with lookups of DNS such as DMARC, DKIM, SPF, TXT, MX, etc. The details of factors affecting the risk is studied in detail using visual verdict like high risk, medium risk, low risk. An interactive dashboard is prepared for demonstrating user management, history of risk recent users, risky users are color coded. Administrator has full access to either keep the user or delete the user from the database. To implement this application python software is used and the framework used is flask framework. In the back end sqlite database is used which provides lightweight model for storing the data. The dashboard prepared is web interface which is completely reactive and secure which even provides securities reports. This application identifies emails are spoofed or legitimate which help users to get rid of email authentication, phishing attacks.

Keywords: Email Spoofing , DNS authentication , Web Application , Flask Framework , Email Security, Visual verdict.

1. INTRODUCTION

One of the most common communication tools in everyday life and organizations is email, but it is also the most popular and, therefore, is an easy target of cyberattacks. Attackers commonly use threats like spam, spoofing, and phishing to mislead users into providing sensitive information or downloading harmful files and pose a severe security threat.

It has been demonstrated that spam and spoof emails do not only fill inboxes, but they also harbor phishing links and malware, and thus can be harmful to the user and institutions [1]. The email header analysis is also examined as a means of tracking spoofed email messages and gathering some reliable facts against the attackers [2]. Besides the forensic methods, scholars have suggested machine learning-based solutions in identifying spoofed emails. Feature extraction with the help of TF-IDF and classification with the help of Random Forest, along with authentication mechanisms like SPF and DMARC have been demonstrated to enhance accuracy in fake email detection [3]. Such hybrid solutions not only scan the content and source of emails but also provide a better shield than the conventional filtering technology.

Another increasing threat is Business Email Compromise (BEC) and spear-phishing attacks. These attacks are less frequently detected with the help of standard spam filters because they do not imply the use of malicious links or files. Researchers are thus resorting to more sophisticated ML models to learn behavioral and contextual characteristics of emails to enhance detection [4], [6]. Deep learning approaches have seen other recent applications in phishing detection. Research reveals that DL models are better able to handle new and advanced phishing methods than rule-based systems that are in place. Nevertheless, the ability of these models to keep up with ever-changing phishing techniques is the first research gap [5].
In this paper is to come up with a real time email spoofing detection and monitoring system that incorporates machine learning and authentication systems. Not only does our model analyze the content of emails, but it also verifies the sender domains so that it is more likely to detect. Findings are presented to users in a simple and safe interface which is effective and present in spoofed email spoofing and in real time.

2. LITERATURE SURVEY

Digital technology has simplified life but it has also posed more risks such as information security breach. Email spam is one of the biggest problems that overload the inboxes with spam. These are not only time wasters, but also they may have phishing, malware or hacking potential. Spam spreads fast as it is cheap and can be sent in bulk. In this research, the researcher aims at developing effective spam filters on university networks where the threat is too great. It places emphasis on Bayesian filters, which rely on statistical techniques to identify and block spam, with the help of pattern learning in email content. [1]
One of the most popular modes of communication among people all over the world is the email, which has security loopholes that are used to commit fraud and forgery by the criminals. Attackers may impersonate email address or send their messages anonymously to commit an illegal act. Email headers leave a comprehensive history of the path messages follow and therefore by examining them one can identify vital evidence such as the route, software and network information. Forensic analysis of email assists investigators in tracking forged emails and providing proof against cybercriminals. The paper identifies the need of forensic investigation, analysis tools, how to identify spoofed headers, and problems that investigators might encounter and how they can be resolved. [2]
Email is a highly popular method of communication today but also a primary source of cyberattacks. Email spoofing, in which the attackers impersonate an authoritative source, is a major threat. To address this, we developed a spoofing detection model based on machine learning and mail authentication tests. TF-IDF is used to identify patterns within the email contents and random forest is used to tell whether the email is fake or not. It also authenticates the domain of the sender by reference to SPF and DMARC records. Using Gmail API and OAuth 2.0, emails are safely checked and the findings are displayed in real time with just a simple Flask web application. In this manner, information about the content and the senders is resolved to enhance spoof detection. [3]
Business email compromise (BEC) is a type of phishing that is among the most threatening cyberattacks on businesses. The attacks are difficult to identify since most emails of BEC do not include evident malicious files or links. This renders the old spam filters and the old method of detection less useful. In this regard, researchers are investigating more sophisticated machine-learning based detection methods. In this paper, 38 of the most important studies out of 950 articles are reviewed in terms of their methods, strengths, and weaknesses. It describes characteristics, datasets, and ML algorithms to detect BEC, as well as points to open challenges and future research directions. [4]

Phishing email attacks are increasingly becoming sophisticated and such traditional means of defense as blacklists, whitelists, and rule-based approaches are not that efficient any more, particularly with spear-phishing and zero-day attacks. Researchers are currently moving to machine learning and deep learning in order to enhance detection. The research is a systematic literature review of 33 articles that were developed in accordance with PRISMA principles to investigate the process of phishing detection by deep learning techniques. It gives a taxonomy of these methods, their advantages and their limitations and gaps. The review also notes that modelling models to suit new phishing practices is also a central issue. Lastly, it provides future research directions to enhance detection of phishing attacks with the help of deep learning. [5]

Emails have found their way in the organization, and this has also rendered spear-phishing a formidable weapon that attackers can exploit to infiltrate the networks. In comparison with standard phishing, spear-phishing relies on personal or organizational information to appear authentic emails. Hacked email accounts are even used in many of the new attacks and they are more difficult to detect by the old security means. By using these emails, the victims are duped to open malicious links or infected files that may cause severe security violations. [6]

3. Proposed Method

Following are the steps of proposed method

Step 1: User Authentication
Step 2: Input an Email from user
Step 3: Analysis of Results
Step 4: Results Generation
Step 5: Visualization and Storage in database

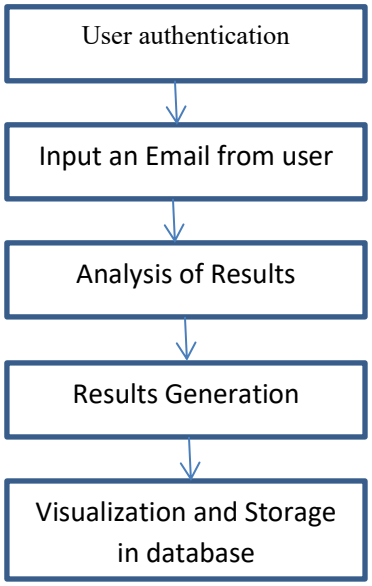

Fig.3.1 Block diagram for proposed method

Step 1: User Authentication

This system initiates the process of identity validation of the user. Each time a user tries to log in, he or she will have his/her credentials compared to the stored information in the database. The hashing of passwords is done to ensure security and only authorized users can access the email analysis dashboard. The extra privileges given to the user of the admin are to view all the stored analyses and control the user

accounts. This makes sure that emails are uploaded by authorized persons only, results are only viewed by authorized persons and sensitive features of the system used.

Step 2: Input an Email from User: The user is then allowed to enter an email to be analysed into two formats: by pasting the entire raw email header/contents into the input box, or by uploading a file (.eml or .txt). The system filters the addressed information of the sender, domain, and header of the content provided. This action is done to guarantee that the email contains sufficient metadata so that it can be subjected to SPF, DKIM, DMARC and DNS validation.

Step 3: Analysis of Results: After the email information was received, the system handles the header and triggers DNS queries to SPF, DKIM, DMARC, MX, and TXT records of the domain of the sender. SPF is checked to determine the authentication of the server of the sender. DKIM is examined in order to establish whether the email has a valid cryptographic signature. The policies of DMARC are reviewed to find out how the domain manages authentication failures. Other anomalies which are assessed by the system include the oddities of header fields, including the received, the return-path, and patterns of routing. According to these checks, weighted scores will be given to every missing or misconfigured authentication factor.

Step 4: Results Generation: Once the analysis is done, a system estimates a total risk score and comes up with an understandable decision like Low Risk, Medium Risk and High Risk. One of the outcomes is an elaborate account of what checks were passed, failed or looked suspicious. As an example, a lack of DKIM can raise the risk score whereas a strong SPF and DMARC set up can lower it. This step-by-step analysis enables the users to know precisely why an email is safe or spoofed.

Step 5: Visualization and Database Storage: The final findings would be presented in a visual form that is easy to comprehend with the help of color-coded badges green (safe), orange (suspicious), and red (spoofed). The dashboard displays charts and graphs showing the analysis of the last analyses and the trends within the risk levels. All the analysis results are also stored in the SQLite database with timestamps, domains, and verdicts according to the system. This enables users and administrators to view history, monitor repeat suspicious email systems, and keep security logs to use in future.

4. RESULTS

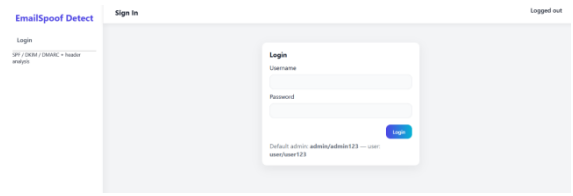

Fig 1: User login Page

User needs to login fist for email spoofing detection.

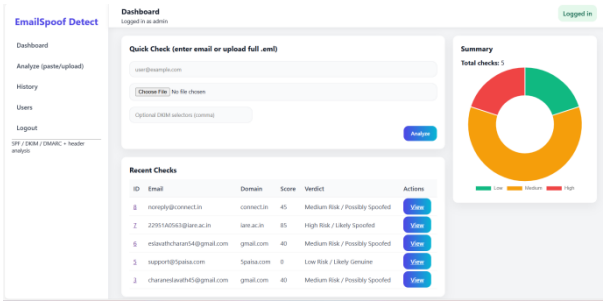

Fig 2: Dashboard

ANALYSIS AND RESULTS

This tool that analyzes emails (address or .eml) for spoofing using SPF/DKIM/DMARC, with a Quick Check input and a Recent Checks history table. It also includes a summary chart showing overall risk distribution (Low/Medium/High).

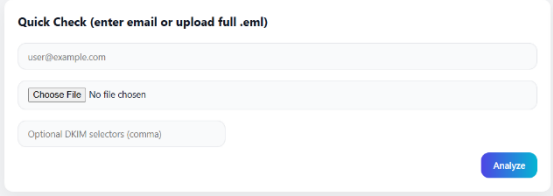

Fig 3: Email checking and analysing

User needs to enter email and can upload .eml or .txt files, which commonly contain full email metadata needed for spoofing analysis.

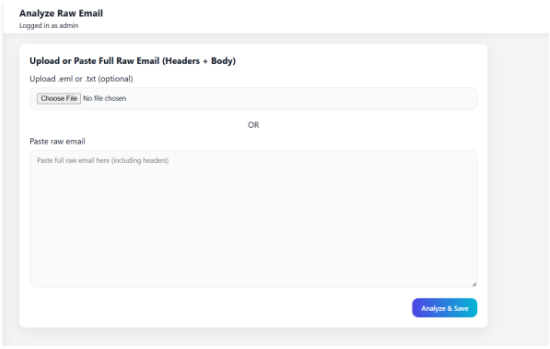

Fig. 4. Analyze Raw Email using complete mail file data

It also supports directly **pasting raw email text**, giving flexibility for manual investigations. The system likely checks **SPF (Sender Policy Framework)** to verify whether the sending IP is authorized for that domain.

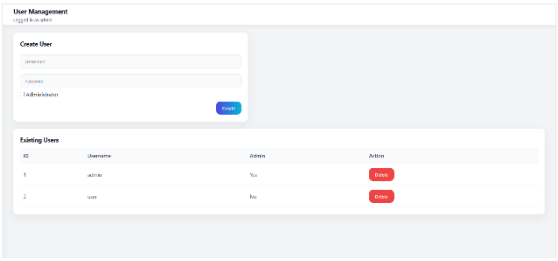

Fig5. User Management for admin

This involves controlling access to the system by adding, editing, or removing user accounts. It allows assigning roles or permissions to ensure secure and appropriate usage. The admin can also monitor user activity to maintain oversight and system integrity

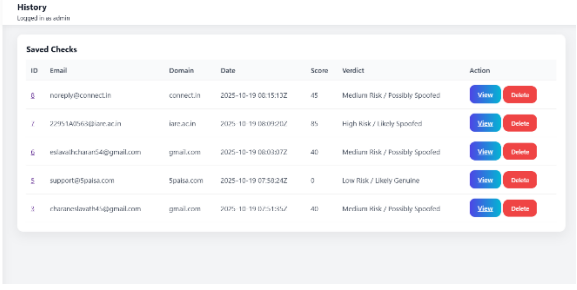

Fig.6: History check and its previous data history result check

History check allows you to view all previously analyzed email records, including their spoofing scores and DNS findings. It helps compare past vs. current results, showing whether authentication issues like SPF, DKIM, or DMARC have changed.

Score Range	Verdict	Meaning
0–29	Low Risk / Likely Genuine	Proper SPF, DKIM, DMARC, MX records. Email likely legitimate.
30–59	Medium Risk	Some issues in authentication records (e.g., softfail SPF, missing DKIM). Email could be spoofed.
60–100	High Risk / Likely Spoofed	Critical missing or unsafe records (e.g., no SPF, +all in SPF, missing DMARC). High chance of spoofing.

Fig: Verdict score based on the email that performance

The system assigns a score from 0 to 100, where a higher score indicates a greater likelihood of email spoofing.

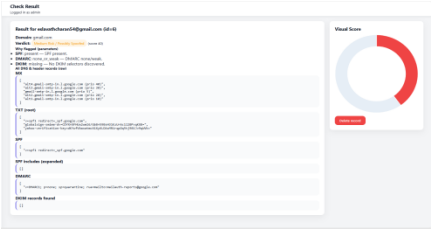

Fig 7: Parameters data and results

The domain analyzed is gmail.com, and the verdict shows Medium Risk / Possibly Spoofed with a score of 40. SPF is present, meaning Gmail publishes an SPF record, but the result still raises suspicion.The SPF record redirects to _spf.google.com, which is normal for Gmail.

5. Conclusion

Propose to work is successfully design using python software and relevant libraries. This dashboard is prepared using web application framework which is very famous called as flask framework. As an input user has to enter email header as well as email content to identify the user as legitimate or spoofed email. This application is very much efficient compared to the state of art techniques. Parameter and results of every step in the application is demonstrated in the result section which indicates that this application is more interactive and more reactive compared to the existing email spoofing algorithms or dashboards.

The future of this email spoofing detector system involves increasing the powers of the system to enable real-time email scanning, incorporation of machine learning based anomaly detector and including advanced features like automated notification of high-risk emails. The threat-intelligence APIs can also be added to the system and will be used to cross-link suspicious domains, phishing campaigns, and known malicious IPs. Subsequent iterations can also feature browser extensions or email client extensions, which automatically scan the dangers of spoofing inside of Gmail, Outlook or company mail. Also, pattern recognition based on AI to detect cases of header tampering, DKIM signature forgery and domain impersonation will be an added advantage in improving accuracy and will help organisations to create a more proactive cybersecurity environment.

REFERENCES

1. M. Sharabov, G. Tsochev, V. Gancheva, and A. Tasheva, “Filtering and Detection of Real-Time Spam Mail Based on a Bayesian Approach in University Networks,” *Electronics*, vol. 13, no. 2, art. 374, 2024. [Online]. Available: DOI link MDPI

2. S. Shukla, M. Misra, and G. Varshney, "Forensic Analysis and Detection of Spoofing-Based Email Attack Using Memory Forensics and Machine Learning," in *Proc. SecureComm 2022 (EAI Int. Conf. Security & Privacy in Communication Networks)*, Virtual Event, 2022, pp. –. Springer, 2023. DOI: 10.1007/978-3-031-25538-0_26 EUDL
3. S. Shukla, M. Misra, and G. Varshney, "Spoofed Email-Based Cyberattack Detection Using Machine Learning," *J. Computer Information Systems*, online, 20 Oct 2023. DOI: 10.1080/08874417.2023.2270452 Taylor & Francis Online
4. H. F. Atlam and O. Oluwatimilehin, "Business Email Compromise Phishing Detection Based on Machine Learning: A Systematic Literature Review," *Electronics*, vol. 12, no. 1, art. 42, 2023. DOI: 10.3390/electronics12010042 MDPI
5. "A Systematic Review of Deep Learning Techniques for Phishing Email Detection," *Electronics*, vol. 13, no. 19, art. 3823, 27 Sep 2024. DOI: 10.3390/electronics13193823 MDPI
6. P. L. Arya and S. Chamotra, "Multi-Layer Detection Framework for Spear-Phishing Attacks," in *Innovative Security Solutions for IT & Communications*, LNCS, 2021, pp. 38–56. DOI reference via SecureComm citation ACM Digital Library
7. "Identification of Spoofed Emails by applying Email Forensics and Memory Forensics," in *Proc. 10th Int. Conf. on Communication and Network Security*, 2020, pp. –. ACM. DOI: 10.1145/3442520.3442527 ACM Digital Library
8. A. Alyammahi et al., "A Comparative Analysis of Email Artifacts from Gmail, Yahoo Mail, and Live Mail for Email Forensics," in *Information Systems & Technological Advances*, 2024, pp. 383–398.
9. Yu B., Li P., Liu J., Zhou Z., Han Y., and Li Z., "Advanced Analysis of Email Sender Spoofing Attack and Related Security Problems," in *Proc. 2022 IEEE 9th Int. Conf. on Cyber Security and Cloud Computing / 8th Int. Conf. on Edge Computing and Scalable Cloud*, 2022, pp. 80–85. DOI: via IEEE citation ACM Digital Library
10. Holmes: An Efficient and Lightweight Semantic-Based Anomalous Email Detector, P. Wu and H. Guo, Apr 2021 (arXiv tech report). [Online]. Available: arXiv preprint arXiv
11. "Forward Pass: On the Security Implications of Email Forwarding Mechanism and Policy," E. Liu et al., Feb 2023 (arXiv preprint). [Online]. Available: arXiv preprint arXiv
12. D. Mane, G. Sharma, S. Shinde, A. Banubakode, S. Sangve, and M. A. Ansari, "Reliable Email Spoofing Detection using Enhanced Cybersecurity Approaches," *Advances in Nonlinear Variational Inequalities*, vol. 28, no. 3s, 2025. International Publishing Services
13. "Staying ahead of phishers: a review of recent advances and emerging methodologies in phishing detection," *Artificial Intelligence Review*, 2024; mentions review of ML/ensemble models for phishing detection. SpringerLink
14. "A hybrid deep learning technique for spoofing website URL detection in real-time applications," *J. Electrical Systems and Information Technology*, 2023. DOI link via journal. SpringerOpen
15. "A Systematic Review on Deep-Learning-Based Phishing Email Detection," *Electronics*, 2022 (MDPI). DOI: via MDPI. MDPI
16. Samarthrao & Rohokale, "Email spam detection model using evolutionary feature selection," part of [15] extended review describing LSTM & BERT models.
17. MDPIDewis & Viana, "Phish Responder: hybrid ML & NLP solution," quoted in [15], 99% accuracy claim. MDPI

18. Khan et al., fuzzy-logic metric comparing BERT and LSTM for phishing detection (within [15]). MDPI
19. Malhotra & Malik, BiLSTM classifier with 98.5% accuracy for spam/phishing detection (within [15]). MDPI
20. Korkmaz et al., TshPhish hybrid model with 98.37% accuracy (within [15])