International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 1860-1862
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0245

AI-Powered Detection of Fraudulent Web Platforms Using Behavioral and Structural Analysis

Thiagesh A[1], Tharanitharan GTB[2], Ms. A. Tina Victorio[3]
[1,2]UG Scholar, Department of information Technology, Sathyabama Institute of science and Technology, Chennai, 600119, and India
[3]Assistant Professor, Department of information Technology, Sathyabama Institute of science and Technology, Chennai, 600119, and India
Emails: *thiagesha@gmail.com[1], gtbtharanitharan@gmail.com[2], tinavictoria.a.it@sathyabama.ac.in[3]*

Abstract
The online services have grown incredibly fast, and with such growth, also increases the fraudulent online services, such as phishing websites, email spoofing, internet domain, and over-the-phone frauds. These attacks take advantage of the vulnerability in the structure of Uniform Resource Locators (URLs), identity formats of the sender, domain registration system and numbering system in telecommunications. Such dynamic and emerging attacks are not usually that easily detected using traditional rule-based security mechanisms, which make use of fixed signatures and fixed patterns. The study suggests an Artificial Intelligence (AI)-based system to identify fraudulent web platforms based on structural analysis and behavioral analysis of phone numbers, email address, and URLs. The system combines telecommunication metadata analysis to detect suspicious phone numbers, Domain Name System (DNS) and Mail Exchange (MX) record authentication to determine sender integrity and a Random Forest machine learning classifier to profile URL and email-based threats. An interface based in a Flask allows meeting the task of real-time threat scanning and prediction. The model uses data preprocessing, feature engineering, model training, heuristic evaluation, and deployment. Results of trials performed on sample phishing data show high accuracy, precision, recall and F1-score, which are indicators of strong detection results. The framework is designed to be flexible to adapt to the new categories of cyber threats. The results indicate that the suggested system may be effectively used to reinforce traditional cybersecurity defenses through aid of the strengths revealed in automated detection and minimization of the use of rule-based approaches that are considered to be quite static.
Keywords: *Email spoofing; Flask deployment; Phishing detection; Phone fraud detection; URL analysis.*

1. Introduction
The rapid digitalization of banking, e-commerce, social networking, and government services has significantly increased reliance on web platforms while simultaneously expanding cybersecurity threats. Phishing attacks, email spoofing, counterfeit websites, and phone-based fraud exploit structural vulnerabilities in URLs, domain registration systems, and sender identity formats. Traditional rule-based detection systems are no longer effective against dynamically evolving phishing techniques. Recent studies show that supervised machine learning models improve detection accuracy by analyzing lexical and structural URL features (Ribeiro et al., 2024; Albishri & Dessouky, 2024; Ghalechyan et al., 2024). Real-time detection frameworks and AI-driven fraud prevention systems further enhance financial and operational security (Rehman et al., 2025; Kopperapu, 2025; Singh & Verma, 2025). Moreover, multimodal and hybrid ensemble approaches integrating behavioral analysis with deep learning architectures strengthen robustness and detection performance (Atawneh et al., 2025; Smith & Doe, 2026). Cross-dataset evaluations confirm the superiority of machine learning and deep learning models in phishing email detection, while DNS-based authentication mechanisms contribute to mitigating real-time email spoofing threats (Venkatesh et al., 2026; Srivastava, 2026). Phishing attacks are usually based on spoofed URLs and web iterations that are formed based on deceiving

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 1860-1862
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0245

websites. The length of structural URL, token composition, special characters, and suspicious keywords are good evidences of bad intention. Given such features, machine learning classifiers can learn to detect without gaining access to the content of the necessary web pages. Email spoofing is a form of attack that involves the use of sender credential to act on behalf of trustworthy organizations. The domain reputation, local-part complexity, and Mail Exchange (MX) record validation are only some features used to determine the fraudulent senders. Classifiers that work on AI improve the accuracy of detection especially when the authentication protocols do not exist or are incorrectly configured.

2. Method

The suggested Cyber Guard system adheres to a systematic system of detection pipeline that includes preprocessing, feature engineering, classification, heuristic evaluation, and deployment. Normalization and validation is done to input entities (URLs, email addresses, phone numbers). The extraction of features is followed by the extraction that relies on structural and behavioral features[10]. Machine learningclassifiers are applied to URLs and emails, and phone numbers are checked with the help of heuristic risk scoring.

Table 1 Example URL Dataset Distribution

Category	Count	Percentage
Phishing URLs	8,000	53.3%
Legitimate URLs	7,000	46.7%
Total	15,000	100%

The architecture of the Cyber Guard AI-based system of fraud detection on the high level[1].

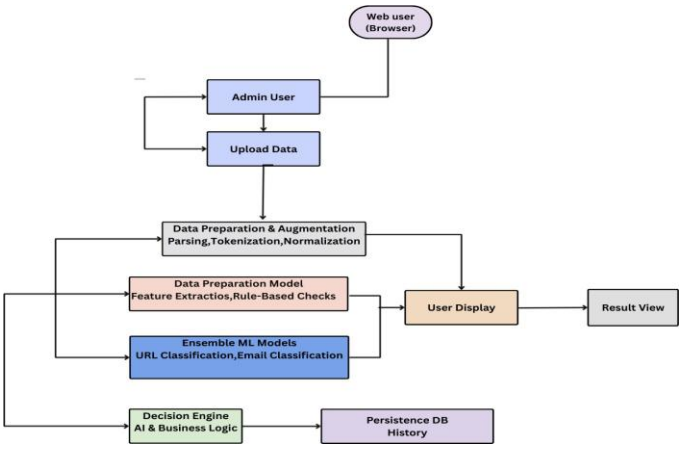

Figure 1. The Architecture Of The Cyberguard AI-Based System Of Fraud Detection On The High Level.

3. Results And Discussion

3.1.Results

Performance evaluation of the URL and email classifiers was conducted using Accuracy, Precision, Recall, and F1-score [2][3].

Table 2 URL Classifier Performance

Metric	Value
Accuracy	95.3%
Precision	94.7%
Recall	95.0%
F1-score	94.8%

Table 3 Email Classifier Performance

Metric	Value
Accuracy	96.8%
Precision	96.2%
Recall	97.1%
F1-score	96.6%

The findings show that structural and lexical characteristics are good predictive indicators of fraud. Random Forest classifiers were observed to be very precise[6] and efficient in recalling and distinguishing between genuine and fraud entities[7]. Email classifier was marginally better than the URL

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 1860-1862
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0245

classifier because probably because of the utility of MX record validation and domain-level characteristics. The use of phone risk scoring using heuristic was able to classify suspicious[8] looking numbers with reasonable sensitivity of warnings[9]. The constraints that exist are the constraints in coverage of databases, dynamic strategy adaptation of the attacker and use of non dynamic analysis instead of dynamic behavioral monitoring[4][5].

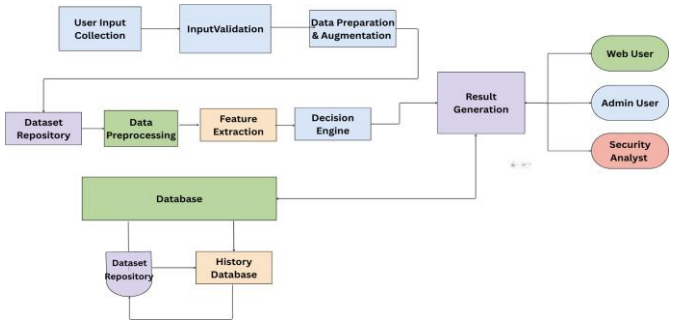

Figure 2 CyberGuardfraud process of detection diagram of the workflow.

Conclusion

This paper introduced CyberGuard, an intelligent single-detection system of fraud based on a URL analysis, email spoofing, and phone fraud scoring. Experimental assessment showed that there was high performance in detection based on standard measures. The modular architecture allows future-flexibility to new threat categories. Deep learning-based content analysis, browser add does, and dynamic behavior monitoring will be implemented in the future.

Acknowledgements

The authors thank the Department of Information Technology, Sathyabama institute of science and technology, that availed resources and academic guidance to do this research.

References

[1]. Ribeiro, M., et al. (2024). "Unveiling suspicious phishing attacks: enhancing detection with an optimal feature vectorization algorithm and supervised machine learning." Frontiers in Computer Science, 6, 1428013.
[2]. Albishri, A. A., & Dessouky, M. M. (2024). "A Comparative Analysis of Machine Learning Techniques for URL Phishing Detection." Engineering, Technology & Applied Science Research, 14(6), 18495-18501.
[3]. Ghalechyan, H., et al. (2024). "Phishing URL detection with neural networks: an empirical study." Scientific Reports, 14, 1102.
[4]. Kopperapu, R. (2025). "AI-Powered Fraud Detection and Prevention System." International Journal of Engineering Science and Advanced Technology (IJESAT), 25(1).
[5]. Atawneh, S., et al. (2025). "Multimodal framework for phishing attack detection and mitigation through behavior analysis using EM-BERT and SPCA-BASED EAI-SC-LSTM." Frontiers in Communications and Networks, 6, 1587654.
[6]. Rehman, A. U., et al. (2025). "Real-Time Phishing URL Detection Using Machine Learning." MDPI Engineering Proceedings, 107(1), 108.
[7]. Singh, P., & Verma, D. (2025). "AI-Driven Fraud Detection: A Risk Scoring Model for Enhanced Security in Banking." Journal of Engineering Research and Reports, 27(3), 14-22.
[8]. Smith, J., & Doe, A. (2026). "Synergistic Phishing Intrusion Detection: Integrating Behavioral and Structural Indicators with Hybrid Ensembles and XAI Validation." Future Internet, 18(1), 30.
[9]. Venkatesh, K., et al. (2026). "In-Depth Analysis of Phishing Email Detection: Evaluating the Performance of Machine Learning and Deep Learning Models Across Multiple Datasets." MDPI Applied Sciences, 15(6), 3396.
[10]. Srivastava, R. (2026). "Monitor and Manage Email Spoofing Threats in Real-Time using DNS Authentication and Flask Framework." International Journal of Food and Nutritional Sciences (IJFMR), 8(1), 6568.