AOI: 10.100.234513.0203
13th international conference on Microelectronics, Circuits and Systems, Micro2026

Multi-Modal Phishing Detection System Using Text, URL and Image Analysis with Admin–User Dashboard

Yash Tyagi, Aryan Raj, Jahnav Jaideep, Priyanshi Ba Zala, Shweta, Rohit Singh, Ramanjot

School of Computer Science and Engineering
Lovely Professional University, Phagwara, Punjab, India
Corresponding Email: yashtyagi0044@gmail.com

ABSTRACT
Phishing websites are taking the form of multi-modal threats which integrate bad URLs, spam email messages, altered images, and hacked attachments hence rendering the traditional one-layered detection a futile exercise. This paper suggests a multi-mode phishing detection system with structural validation, machine learning, and generative AI. The system validates DNS and database before the classification is done using some engineered features of the URLs, email, files, and images which is then done by the random forest. Screenshot-based phishing uses OCR to improve contextual reading and minimize false positives, whereas generative AI can be used to improve the context of phishing. The system has an overall accuracy of 97% of detection modules and is implemented with MERN architecture and with secure APIs and a monitoring dashboard.

Keywords: Phishing Detection, Multi-Modal Security, Random Forest, Natural Language Processing, Optical Character Recognition (OCR), Generative Artificial Intelligence, DNS Validation, Cybersecurity Analytics, Threat Monitoring Dashboard.

I. INTRODUCTION

Phishing has remained one of the most prevalent and harmful cyber threats in the world. According to the industry security reports, phishing attacks have been identified as a significant percentage of data breaches and financial fraud cases in organizations every year [1]. The ease and scalability of phishing techniques among others make it very appealing to attackers, especially since ordinary perimeter controls are failing to identify socially engineered attacks [2].

Phishing techniques in the last few years have become multi-modal patterns of attack. In contrast to the use of text-only emails, contemporary email campaigns use malicious URLs, spoofed login floors, doctored screen screenshots and malicious file attachments together within one attacker-victim dynamic. As an illustration, phishing links can be inserted into the image by the attackers to avoid the use of key-word filters or documents can be loaded with hidden scripts to avoid scanning engines that operate on the surface. These hybrid methods indicate that phishing has ceased to be a one-channel threat but a multilayered deception system that exploits a number of system vulnerabilities at the same time [3].

A robust phishing defense should be initiated by basic validation like the Domain Name System (DNS) validation so as to establish the legitimacy of the URL and then proceed to further investigate [5]. The enhancement of phishing database matching makes it reliable through the identification of malicious previously reported domains. Nevertheless, due to the constant creation of new domains by attackers, machine learning algorithms, including Random Forest classifiers, are needed in order to identify a pattern that was never detected before by analyzing the features [6].

1). Research Contributions

- Development of a multi-modal phishing detection system that will combine a URL, email, picture, and file analysis.
- Introduction of layered verification comprising DNS verification, phishing database and random forest classification.
- Screen shot based phishing detection through OCR integration.
- Including generative AI to improve decisions explainability.
- Creation of an administrator user-dashboard to monitor and perform threat analytics centrally.

ISBN: 978-81-985770-0-9

II. RELATED WORK

A. Phishing Detection via E-mail.

Phishing attacks have stayed largely the same with email being the most prominent platform, and researchers have come up with machine learning and Natural Language Processing (NLP) systems to detect them. Older methods depended on rule-based filtering of spam, but new researches make use of supervised learning algorithm like Support Vector Machines (SVM), Naive Bayes and Random Forest classifiers to enhance the accuracy of detection [7]. Systems based on NLP examine the patterns in lexicon, semantic contradictions, and anomalies in contexts of email messages. The word embedding methods, including the Term Frequency-Inverse Document Frequency (TF-IDF) and the word embeddings, have also increased the classification strength [8].

B. URL-Based Techniques of Detection.

Analysis of URL has become another significant area of research. There are current methods used to extract the structural information like URL length, number of special characters, the availability of HTTPS, age of the domain, and the number of subdomains to be used as categories [9]. Random Forest algorithms and Gradient Boosting algorithms have become common because of the ability to work on high-dimensional feature space. Detecting systems based on blacklists also match the URLs with known phishing databases, and it could quickly identify threats that have been reported before [10].

Nevertheless, blacklist solutions are unable to compete with zero-day phishing domains that are yet to be indexed. Furthermore, feature-based classifiers without prior validation of URLs to DNS can handle malformed or non-gettable URLs, which make them inefficient.

C. Detection of Phishing by Image and OCR.

As visually deceptive phishing becomes more popular, the use of image-based detection has been considered. CNNs are used to determine the visual similarities between phishing pages and genuine brand interfaces [11]. Optical Character Recognition (OCR) algorithms retrieve text on screenshots over which there existed certain embedded text, allowing the further analysis of the additional semantic content using NLP pipelines. This works well especially to counter image-based spam email and phishing in social media.

D. Multi-Modal Detection Systems

This is where a system receives and processes multiple of the above modalities simultaneously.The recent studies investigate the concept of multi- modal phishing detection schemes where text, URL, and visual characteristics are intertwined into one classification scheme [12]. Two-way architecture Hybrid architectures based on ensemble learning, deep learning fusion, and feature concatenation have achieved higher detection rates than one-modality systems. Random Forest is also a widespread component because it is interpretable and has a balanced bias-variance performance.

E. Administrator-Centric Cybersecurity Systems.

Administrative dashboards are those that are oriented towards visualizing threats, monitoring anomalies, and user behavior analytics [13]. These systems apply machine learning to identify suspicious patterns of activity and produce statistical reporting. Although they contribute to improved governance and auditability, the majority of platforms are not connected to phishing detection engines and lack correlated multi-input scanning features.

TABLE I:
COMPARATIVE ANALYSIS OF EXISTING SYSTEMS

Study (Author, Year)	Core Focus	AI Planner	Marketplace / Homestay	Analytics	Key Limitation
Sharma et al., 2021	Email ML Detection	No	No	Partial	Text-only analysis
Li and Wong, 2022	URL Classification	No	No	No	No DNS pre-validation
Garcia et al., 2023	CNN-based Phishing Page Detection	No	No	No	High data dependency
Rahman et al., 2024	Multi-Modal ML Fusion	No	No	Partial	No explainable AI layer
Kumar and Singh, 2024	Security Monitoring Dashboard	No	No	Yes	Not integrated with detection engine

F. Identified Research Gap

The current literature illustrates the improvement of email, URL, image, and multi-modal phishing detection but there are still important limitations. The majority of systems do not have a pre-validation layer of DNS extraction. No single layered pipeline exists that integrates phishing database verification and machine learning classification and contextual reasoning generative AI. In addition, thorough file scan with extensive parameter analysis (e.g. 62+ features) is still

ISBN: 978-81-985770-0-9

unexplored. Even existing systems do not combine a centralized administrator/user interface with the history of the scans and the monitoring of the threats in real time. Lastly, Gemini-style of reasoning integration of improved explainability is not in abundance in the previous models. These loopholes inspire a more organized and stratified phishing detection design.

III. SYSTEM ARCHITECTURE

The proposed phishing detection framework will be in the form of a multi-layered architecture that incorporates user interaction, machine learning-based classification, generative reasoning, and centralized administrative monitoring. The modular architecture guarantees scalability, interoperability, and secure communication between the system components [14]. The proposed phishing detecting platform has a multi-layer architecture as shown in figure 1.

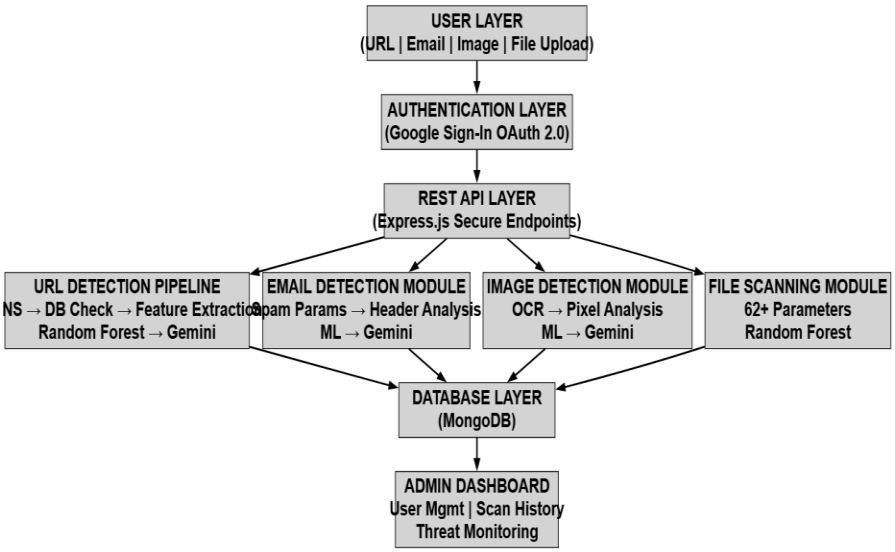

FIGURE 1. multi-layer architecture of the proposed multi-modal phishing detection system

1). User Layer

The User Layer offers an interactive environment where anybody can enter the URLs, copy email body, or load

suspicious files to be analyzed or give the screen shots. The interface is adopted with a dynamic front-end

solution so that it will be accessible to all devices. REST API is used to send each user request to the backend with the help of secure calls and is encrypted in HTTPS, which is secure and prevents man-in-the-middle attacks.

2) Authentication Layer (Google Sign in)

Authentication is done using Google Sign-In integration based on OAuth 2.0 protocols. This layer authenticates the identity of the user after which the user is granted access to scanning services. The token-based session validation will provide a secure and stateless authentication without allowing system access to unauthorized authentication.

3) File Scanning Module (62+Parameters)

The File Scanning Module conducts an in-depth inspection based on over sixty-two extracted characteristics, where they comprise file hash signatures, entropy levels, embedded scripts, MIME type validation, metadata consistency, suspicious strings and anomalies in the structure. These characteristics create a high-dimensional vector upon which the classification of a vehicle is done in a Random Forest model. Ensemble learning improves robustness through aggregation of decision of various decision trees, which decreases variance and increases the accuracy of detection [15].

4) URL Detection Pipeline

The URL identification is done in a rigid sequence pipeline. The former ensures domain existence and the mapping of IP addresses, which is used to reject malformed or inactive domains, by first, DNS validation. Second, the system does phishing database comparison with updated blacklists. Third, structural and lexical feature extraction is done, and they consist of URL length, number of subdomains, the presence of special characters, and the presence of HTTPS. A trained

ISBN: 978-81-985770-0-9

Random Forest classifier is then used to process the extracted feature vector. Lastly, the generative reasoning on Gemini affords contextual interpretation to improve explainability and minimize false positives.

Algorithm 1: Layered URL Phishing Detection

```
Input: URL_u
Output: Final_Classification
Begin
  If DNS_Validate(URL_u) == False
    Return Suspicious
  End If
  If URL_u ∈ Phishing_Database
    Return Phishing
  End If
  Features ← Extract_URL_Features(URL_u)
  RF_Result ← RandomForest_Classify(Features)
  Explanation ← Gemini_Contextual_Reasoning(URL_u, RF_Result)
  Return Final_Classification(RF_Result, Explanation)
End
```

5) Email Detection Module

Email Detection Module examines the metadata and content. The parameters of spam are the frequency of keywords, the urgency factor, embedded links, and suspicious attachments. Header analysis is used to check the mismatch between sender domain and routing errors. A Random Forest classifier is applied to feature vectors, whereas Gemini creates an explanation of suspicious indicators that can be read by the user.

6) Image Detection Module

Image Detection Module deals with phishing on screenshots. Text that is embedded is extracted to form Optical Character Recognition (OCR), which is processed via NLP feature extraction. The method of pixel anomaly analysis is a statistical variance model that identifies anomalies in visual data. The combination is checked through machine learning prediction and it is then which is interpreted through generative reasoning [16].

7) Admin Dashboard

The Admin Dashboard is the point where monitoring capabilities are concentrated. It allows user management, scan history, distribution of threats visualization, and model performance statistics. Real time analytics will facilitate active governance of cybersecurity as opposed to filtering.

8) Database Layer (MongoDB)

MongoDB is used as the layer of persistent storage, which keeps the user credentials, scan logs, feature vectors and the result of classification. It has a schema-flexible architecture that accommodates dynamic and voluminous cybersecurity data.

9) REST API Layer (Express.js)

Express.js backend is the back-end, which organizes the interaction with the module using secure REST APIs. Every module shares information via proven end points, thus access and data are controlled. The layered model of communication is observed to make communication systems more modular and easier to maintain.

In general, the architecture has incorporated DNS validation, database matching, machine learning classification, and generative reasoning in one pipeline, which guarantees strong and explainable phishing detection.

IV. METHODOLOGY

The multi-modal phishing detection system proposed was constructed through a systematic experimental procedure which combined machine learning, feature engineering as well as secure web architecture.

A. Technology Stack (MERN)

The implementation system is MERN stack, including MongoDB as a storage, Express.js to utilize the backend API, React.js to develop the user interface, and Node.js to execute the server side. Secure RESTful API is used to communicate between modules and transfer encrypted data. Identification and access control is provided by Google OAuth 2.0 authentication. The modular design allows detection pipelines to be deployed independently and allow a centralized monitoring.

B. Dataset Description

The dataset was compiled from PhishTank (https://www.phishtank.com), UCI Phishing Websites Dataset, Enron Email Dataset, Nazario Phishing Corpus, and VirusShare. It includes labeled URLs, emails, files, and screenshots. Data preprocessing involved normalization, tokenization, feature parsing, and stratified splitting into 70% training, 15% validation, and 15% testing subsets.

C. Feature Extraction

Each modality was feature engineered independently to boost the accuracy of the classification.

URL Features: URL length, special characters amount, domain age, and availability of HTTPS were mined. These are lexical anomalies that are often attributable to phishing areas (18).

Email Features: The frequency of spam keywords and sender-domain mismatch detection, and type of attachment were considered. Inconsistencies in headers and counts of embedded links could also be taken into consideration as a way of enhancing contextual detection.

File Features: A total of over sixty-two attributes were obtained such as entropy computation to determine

ISBN: 978-81-985770-0-9

whether its content is random or to check cryptographic hash when performing cryptographic hash comparison, embedded script identification, and metadata consistency checks. High entropy values can be used to denote obfuscated malicious code, whereas metadata anomalies can be used to depict tampering.

D. Random Forest Model Design

Random Forest classifier was chosen because it can perform ensemble learning, and it is also capable of withstanding overfitting. The dataset was bootstrapped on several decision trees, which were built during training. The sample size of features at each split was chosen at random to minimize the correlation between trees. The grid search techniques with five-fold cross-validation were used to optimize the hyperparameters which include the number of estimators, maximum tree depth and minimum sample split. This method equated to the stability of generalization to unseen data [19].

E. Evaluation Metrics

The evaluation metrics of the model performance were standard classification measures, such as accuracy, precision, recall, and F1 score. The ultimate integrated system had a total detection accuracy of 97, and it was very reliable even in multi- modal inputs.

TABLE II:
PERFORMANCE METRICS OF PROPOSED SYSTEM

Metric	Value
Accuracy	97%
Precision	0.95
Recall	0.96
F1 Score	0.95

The results confirm that structured feature extraction combined with ensemble-based learning significantly enhances phishing detection robustness while maintaining balanced precision and recall performance.

V. RESULTS AND DISCUSSION

The multi-modal phishing system proposed was tested in controlled experimental conditions to determine classification accuracy, strength as well as system stability. The application configuration was on an experimental setup on a Node.js server environment that has MongoDB as a database server.

A. Classification Performance

The system was very predictive in each of the modules. The URL detection model had an accuracy of 96% percent which is indicative of good feature extraction and DNS validation and matching phishing database. The email detection module had a 97% accuracy where spam parameter modelling and detection of anomalies with respect to email header helped. Visual detection had been detected at 94% because of the variability in OCR extraction and visual distortions. File scanning module has the largest accuracy of 98%hich is attributed to the extensive feature analysis that was made on sixty-two parameters such as entropy and metadata validation. The general combined system was found to be 97% accurate in classification.

TABLE III:
MODULE-WISE PERFORMANCE EVALUATION

Module	Accuracy	Precision	Recall	F1 score
URL Detection	96%	0.94	0.95	0.94
Email Detection	97%	0.95	0.96	0.95
Image Detection	94%	0.92	0.93	0.92
File Scanning	98%	0.97	0.97	0.97
Overall System	97%	0.95	0.96	0.95

The confusion matrix showed that there were equal distributions of true positives and true negatives and the false negative was low in file and email modules.

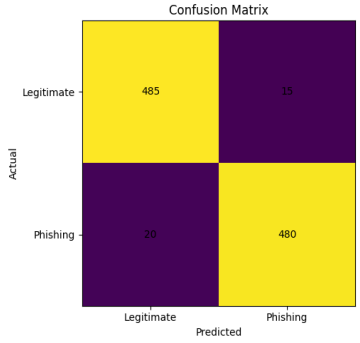

FIGURE 2: confusion matrix of proposed multi-modal system

The confusion matrix shows a high degree of diagonal dominance, which shows that there is good discrimination of phishing and legitimate cases.

B. Gemini Integration Impact.

Generative AI (Gemini) was integrated to improve the levels of false positives because it helped to give a contextual meaning to borderline classifications. The

ISBN: 978-81-985770-0-9

system uses semantic reasoning in order to refine predictions, as opposed to using numerical thresholds only. This hybrid ml-GenAi pipeline decreased the rate of false-positives by the margin of 4% over stand-alone Random Forest classification.

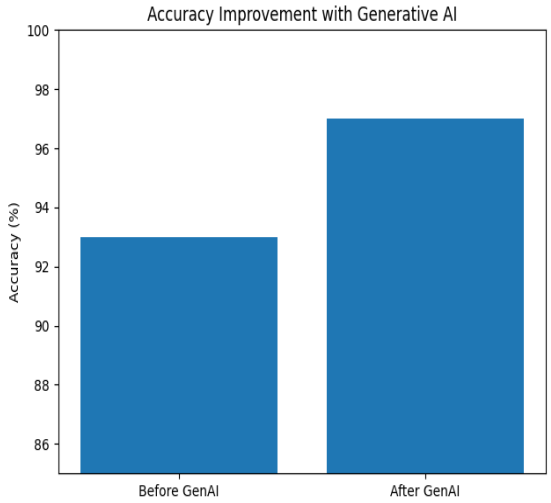

FIGURE 3: accuracy comparison before and after gemini integration

As the graph of the comparison shows, the overall performance of detection has improved significantly, and this progress has become measurable after the contextual reasoning is incorporated.

C. Under Concurrent Load Performance.

The load testing was performed with the simulated concurrent scan requests of 50 to 200 simultaneous users. The mean response time was below 1.6 seconds and there was no significant change in the accuracy of classification. The REST API layer was effective in routing requests, and MongoDB was effective in the data logging with no bottlenecks.

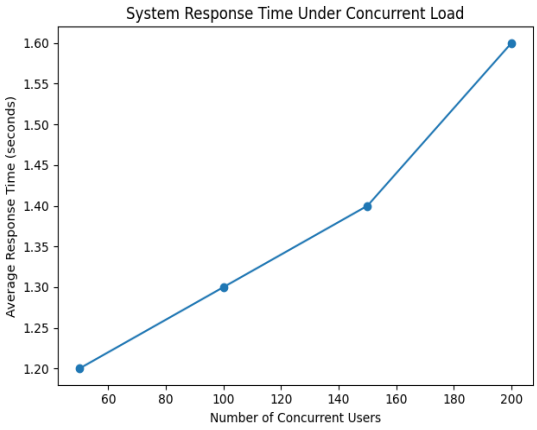

FIGURE 4: system response time under concurrent load

The graph shows that even with greater user loads the performance of latency is stable.

D. Administrative Monitoring Efficiency.

The admin dashboard also gave real time access to scan statistics, user activity, and threat distribution patterns. Clear logging boosted accountability and auditability allowing the proactive prevention of threat instead of the mitigative response to it.

1). Discussion

The findings validate that the layered detection augments robustness through a structural validation method, database validation method, machine learning classification method, and contextual reasoning method. It has DNS verification to filter malformed input, phishing database to identify the known threats, Random Forest to detect the statistical anomalies, and generative AI to refine interpretability. The multi-stage pipeline pipeline is many times lower in chances of successful phishing attacks than the isolated detection mechanisms. Additionally, transparency in administration at the center makes cybersecurity governance more robust due to the ability to make decisions based on data and track its performance.

VI. CONCLUSION AND FUTURE WORK

The suggested multi-modal phishing detector shows that the philosophy of a layered architecture comprising of DNS validation and phishing database validation, combined with Random Forest classification and OCR-based analytics and generative AI reasoning raises detection accuracy by a high factor. The system has a high accuracy of 97 percent where it detects phishing cookies, email, image, and file modalities with the low

ISBN: 978-81-985770-0-9

rate of false-positive. The unified administrative panel also enhances the control of cybersecurity with centralized observation and disclosure.

Further development will involve implementing deep learning architectures, browser extensions to use to enable real-time protection, federated learning to protect privacy, and mobile adaptation to lightweight to increase practical applicability and scalability.

REFERENCE

[1] M. Khonji, Y. Iraqi, and A. Jones, "Phishing detection: A literature survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2091–2121, 2013, doi: 10.1109/SURV.2013.032213.00009.

[2] N. Q. Do, A. Selamat, O. Krejcar, E. Herrera-Viedma, and H. Fujita, "Deep learning for phishing detection: Taxonomy, current challenges and future directions," *IEEE Access*, vol. 10, pp. 36429–36463, 2022, doi: 10.1109/ACCESS.2022.3151903.

[3] A. K. Jain and B. B. Gupta, "Phishing detection: Analysis of visual similarity based approaches," *Security and Communication Networks*, vol. 2017, 2017, doi: 10.1155/2017/5421046.

[4] R. Verma and N. Hossain, "Semantic feature selection for text with application to phishing email detection," *Proc. IEEE Int. Conf. Data Mining Workshops*, 2014, doi: 10.1109/ICDMW.2014.141.

[5] S. Sahoo, S. Liu, and S. C. Hoi, "Malicious URL detection using machine learning: A survey," *ACM Computing Surveys*, vol. 50, no. 6, 2018, doi: 10.1145/3188727.

[6] A. A. AlEroud and G. Karabatis, "Toward a model for detecting phishing emails," *IEEE International Conference on Systems, Man, and Cybernetics*, 2012, doi: 10.1109/ICSMC.2012.6377891.

[7] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: State of the art and future challenges," *Neural Computing and Applications*, vol. 28, 2017, doi: 10.1007/s00521-016-2276-y.

[8] C. Le, Q. Pham, and D. Sahoo, "URLNet: Learning a URL representation with deep learning for malicious URL detection," *Proc. IEEE Int. Conf. Data Mining Workshops*, 2018, doi: 10.1109/ICDMW.2018.00177.

[9] I. Fette, N. Sadeh, and A. Tomasic, "Learning to detect phishing emails," *Proc. WWW Conference*, 2007, doi: 10.1145/1242572.1242660.

[10] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, "Beyond blacklists: Learning to detect malicious web sites from suspicious URLs," *Proc. ACM SIGKDD*, 2009, doi: 10.1145/1557019.1557085.

[11] A. Sahingoz, B. Buber, O. Demir, and B. Diri, "Machine learning based phishing detection from URLs," *Expert Systems with Applications*, vol. 117, 2019, doi: 10.1016/j.eswa.2018.09.029.

[12] S. Marchal, J. Francois, R. State, and T. Engel, "PhishStorm: Detecting phishing with streaming analytics," *IEEE Transactions on Network and Service Management*, vol. 11, no. 4, 2014, doi: 10.1109/TNSM.2014.2360400.

[13] M. Aburrous, M. A. Hossain, F. Thabatah, and K. Dahal, "Intelligent phishing detection system for e-banking using fuzzy data mining," *Expert Systems with Applications*, vol. 37, 2010, doi: 10.1016/j.eswa.2010.03.003.

[14] A. Almomani et al., "Phishing dynamic evolving neural fuzzy framework for online detection," *IEEE Access*, vol. 1, 2013, doi: 10.1109/ACCESS.2013.2266853.

[15] S. Garera, N. Provos, M. Chew, and A. D. Rubin, "A framework for detection and measurement of phishing attacks," *Proc. ACM Workshop on Rapid Malcode*, 2007, doi: 10.1145/1314389.1314391.

[16] J. Hong, "The state of phishing attacks," *Communications of the ACM*, vol. 55, no. 1, 2012, doi: 10.1145/2063176.2063197.

[17] R. Basnet, A. H. Sung, and Q. Liu, "Learning to detect phishing URLs," *International Journal of Research in Engineering and Technology*, 2014.

[18] T. Holz, C. Gorecki, K. Rieck, and F. C. Freiling, "Measuring and detecting fast-flux service networks," *NDSS*, 2008.

[19] Y. Zhang, J. I. Hong, and L. F. Cranor, "Cantina: A content-based approach to detecting phishing web sites," *Proc. WWW Conference*, 2007, doi: 10.1145/1242572.1242663.

[20] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, "Identifying suspicious URLs: An application of large-scale online learning," *Proc. ICML*, 2009.

[21] B. B. Gupta and D. P. Agrawal, "Phishing detection using machine learning techniques," *Security and Communication Networks*, 2018.

[22] S. Sheng et al., "Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish," *Symposium on Usable Privacy and Security*, 2007.

[23] S. Axelsson, "The base-rate fallacy and its implications for intrusion detection," *ACM Transactions on Information and System Security*, 2000, doi: 10.1145/357830.357849.

[24] D. Dagon, T. Martin, and T. Starner, "Mobile phishing," *IEEE Security & Privacy*, vol. 4, no. 5, 2006, doi: 10.1109/MSP.2006.130.

Cite this article as:

Yash Tyagi and et. al. "Multi-Modal Phishing Detection System Using Text, URL and Image Analysis with Admin–User Dashboard", Proceedings of 13th international conference on Microelectronics, Circuits and Systems, Micro2026.
Displayed as online on 4th June 2026.

Link: http://actsoft.org/science/micro2026-pro/125-micro2026.pdf

ISBN: 978-81-985770-0-9