International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802166

AI-Powered Phishing Detection: Securing Web Navigation with Machine Learning

Dr. N. Devakirubai, Abishek R, Jayamani M, Balakrishnan R

HOD, Department of Artificial Intelligence and Data Science, R P Sarathy Institute of Technology, Salem, India

Department of Artificial Intelligence and Data Science, R P Sarathy Institute of Technology, Salem, India

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT: Phishing attacks are one of the most serious cybersecurity threats, where attackers create fraudulent websites to steal sensitive information such as login credentials, banking details, and personal data. Traditional protection methods like blacklists and antivirus tools are often ineffective because phishing websites are continuously evolving. This research proposes an AI-powered phishing detection system using Machine Learning techniques to improve web security. The proposed system analyzes URLs and website characteristics to distinguish between legitimate and phishing websites. A dataset containing more than 6000 URLs is used for training and evaluation. The system extracts multiple important features from URLs and webpage data, including lexical features, security- related attributes such as HTTPS usage and domain age, host- based information, and website popularity indicators. These features are preprocessed and converted into numerical form to train machine learning models effectively. Among the evaluated algorithms, the Gradient Boosting Classifier provided the best performance. The model achieved a detection accuracy of approximately 97. The proposed approach improves online security by detecting malicious websites before users interact with them. Unlike traditional blacklist systems, the machine learning model can identify new phishing patterns. This system can be further extended into browser extensions or scalable web services for enhanced phishing protection and safer web navigation.

KEYWORDS: AI-powered phishing detection, machine learning for web security, phishing attack prevention, intelligent threat detection, URL classification using AI, real-time phishing detection, cybersecurity with machine learning

I. INTRODUCTION

The rapid growth of internet technologies and digital services has significantly increased exposure to cyber-security threats. Among these threats, phishing attacks have become one of the most common and dangerous forms of cybercrime. In phishing attacks, malicious actors create fraud- ulent websites that imitate legitimate platforms in order to steal sensitive information such as usernames, passwords, banking credentials, and personal data. As phishing techniques evolve, attackers use methods such as URL manipulation, domain spoofing, and social engineering to deceive users.

Traditional phishing detection approaches mainly rely on blacklist databases and signature-based antivirus tools. Al-though these methods can block previously identified ma- licious URLs, they are ineffective against newly generated or zero-day phishing websites. Maintaining large blacklist databases also requires continuous updates and monitoring, making it difficult to respond quickly to emerging threats.

To overcome these limitations, intelligent detection systems based on Machine Learning (ML) have gained significant attention. Machine learning models can analyze multiple char- acteristics of websites and identify patterns associated with phishing activities. Important indicators include lexical URL features, domain registration details, security attributes such as HTTPS usage, and host-based information such as DNS records and website popularity.

In this research, an AI-powered phishing detection system is proposed using machine learning techniques. The system extracts multiple features from URLs and webpage data and uses them to train a classification model. Among various algorithms evaluated, the Gradient Boosting Classifier demonstrated strong predictive performance in identifying phishing websites.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802166

The proposed model is trained and tested using a dataset containing more than 5000 labeled URLs categorized as legitimate and phishing websites. Experimental results show that the model achieves a detection accuracy of approximately 97 This approach enhances user security by detecting malicious websites proactively and reducing the risk of credential theft. By leveraging machine learning techniques, the system over- comes the limitations of traditional blacklist-based methods and provides a scalable and intelligent solution for safer web browsing.

II. LITERATURE SURVEY

Detecting Phishing Websites Using Large Language Mod- els (2025)
The work in **LLM2025** proposes a phishing detection framework that combines deep learning with feature-based classification. A Multi-Layer Perceptron (MLP) model was trained using lexical, domain-based, and webpage features extracted from phishing and legitimate websites. The model achieved an accuracy of 96.6

Machine Learning Based Phishing Detection (2024)
The study in **NovelML2024** introduces a machine learning approach that analyzes URL-based features such as URL length, subdomain count, domain age, and HTTPS usage. Several classifiers including Decision Tree, Random Forest, Support Vector Machine, and Logistic Regression were evalu- ated. Random Forest produced the best results with improved detection accuracy and lower false positive rates.

Explainable Phishing Detection Framework (2025)
In **Explainable2025**, the authors integrate Explainable Ar- tificial Intelligence (XAI) techniques such as SHAP to in- terpret phishing detection models. The approach improves
transparency and helps identify important features contributing to classification decisions while maintaining high prediction accuracy.

A. Phishing Website Detection Using ML Techniques (2024)
According to **MLTech2024**, several machine learning algo- rithms including Na¨ıve Bayes, Decision Tree, Random Forest, and Logistic Regression were tested on a large phishing dataset. The results show that ensemble models, particularly Random Forest, provide higher accuracy and robustness com- pared to individual classifiers.

Feature Selection Framework for Phishing Detection (2025)
The research in **FeatureSelect2025** proposes a feature selec- tion framework using SHAP and LIME techniques to identify the most influential attributes for phishing detection. The optimized feature set improved classification accuracy and reduced computational complexity.

Hybrid Machine Learning Model (2023)
The hybrid model proposed in **Hybrid2023** combines mul- tiple classifiers such as SVM, Random Forest, and Logistic Regression. By aggregating predictions from different models, the system improves robustness and achieves better perfor- mance than single classifiers.

Comparative Study of ML Algorithms (2025)
The comparative analysis in **Comparative2025** evaluates various classifiers including Decision Tree, KNN, Random Forest, Na¨ıve Bayes, and SVM for phishing detection. The results indicate that Random Forest consistently achieved the highest accuracy and stability.

Adversarial Attacks on Phishing Detection (2023)
The study in **Adversarial2023** investigates the impact of adversarial modifications on deep learning-based phishing detection models. Experimental results reveal that slight URL modifications can reduce detection accuracy, highlighting the need for robust model design.

Phishing Email Detection Using Machine Learning (2025)
The research in **Email2025** focuses on phishing email de- tection using machine learning techniques. The system extracts linguistic and behavioral features from email content and applies classifiers such as Logistic Regression and Random Forest. The Random Forest model achieved 98.5

Reliability of ML-Based Phishing Detection (2022)
The work in **Robustness2022** evaluates the reliability of machine learning-based phishing detection systems under

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802166

noisy and adversarial conditions. Ensemble classifiers demon- strated stable performance, emphasizing the importance of robustness evaluation before real-world deployment.

III. METHODOLOGY

System Overview

The proposed phishing website detection system is designed to identify malicious websites before users interact with them. Phishing attacks typically attempt to deceive users by imitating legitimate websites and stealing sensitive information such as login credentials, banking details, and personal data. To address this issue, the proposed system utilizes a machine learning based approach to analyze various characteristics of websites and classify them as either phishing or legitimate.

The system follows a structured machine learning pipeline consisting of several major stages including URL input col- lection, feature extraction, data preprocessing, model training, prediction, and result output. By analyzing multiple website attributes simultaneously, the system can detect malicious patterns that are commonly used in phishing attacks.

Input Stage: The detection process begins when a user
enters a website URL through the web-based interface of the system. The input URL is treated as the primary source of in- formation for analysis. Unlike traditional security approaches that rely on static blacklist databases, the proposed system performs intelligent analysis of the URL structure, domain information, and webpage behavior.

Once the URL is received, the system retrieves relevant webpage information such as HTML content, domain details, and security indicators. These elements provide essential data that can be used for further feature extraction and machine learning analysis.

Feature Extraction: Feature extraction plays a critical
role in the phishing detection process. Since machine learn- ing models cannot directly interpret raw URLs or webpage content, the system converts various structural and behavioral characteristics of websites into numerical features.

In the proposed system, a total of 30 discriminative features are extracted from the input URL and its corresponding web- page. These features capture important indicators of phishing behavior such as suspicious URL patterns, domain registra- tion characteristics, security attributes, and webpage content structure.

The extracted features are categorized into several groups including URL-based features, domain-based features, secu- rity features, and behavioral features. These features provide meaningful representations of website properties that help the machine learning model identify malicious patterns.

Machine Learning Model: After feature extraction, the
generated feature vector is passed to a trained machine learn- ing model for classification. In this project, the Gradient Boosting Classifier was selected as the primary classification algorithm due to its strong predictive performance and ability to handle complex feature interactions.

Gradient Boosting is an ensemble learning algorithm that builds multiple decision trees sequentially. Each tree attempts to correct the errors made by the previous trees, thereby improving overall prediction accuracy. This iterative learning process allows the model to capture complex relationships between features and classification labels.

The model was trained using a labeled dataset containing phishing and legitimate URLs. During training, the classifier

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802166

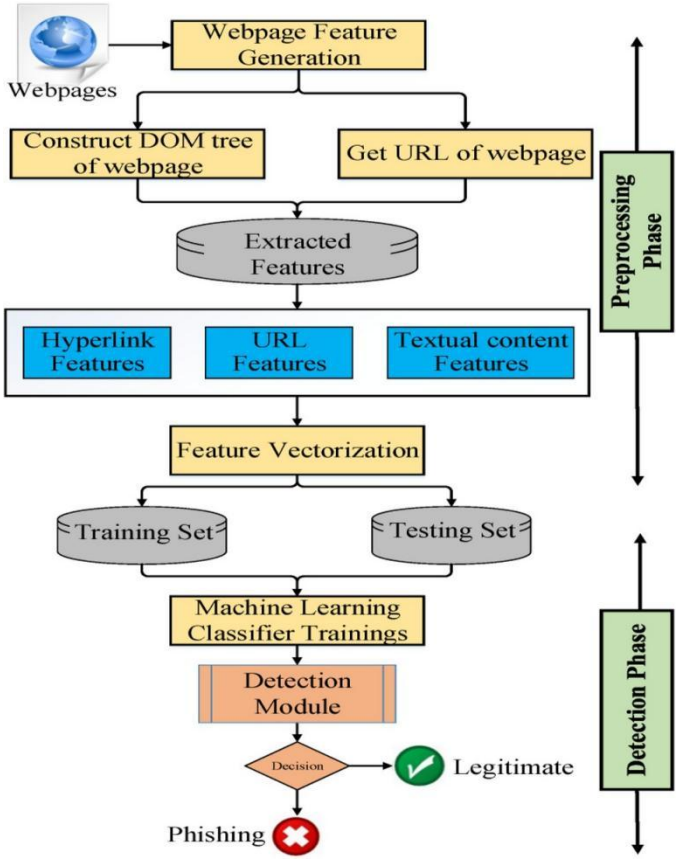

Fig.1. Architecture of the Proposed Phishing Detection System

learns the distinguishing characteristics of phishing websites based on the extracted feature patterns. Output Prediction: After the classification process is completed, the final prediction result is generated by the trained model. The system determines whether the input website is phishing or legitimate based on the predicted class label. The result is then displayed to the user through the web interface. If the system detects that the website is malicious, a warning message is displayed to alert the user. Otherwise, the website is classified as legitimate and the user is allowed to continue browsing safely. This proactive detection mechanism helps prevent users from interacting with fraudulent websites.

Dataset Collection

A well-structured dataset is essential for training an effective phishing detection model. In this research, a dataset containing more than 6000 URLs was collected and used for training and evaluation. The dataset includes both legitimate websites and phishing websites obtained from publicly available cybersecu- rity repositories and trusted online sources.

Each URL in the dataset is labeled as either legitimate or phishing, allowing the system to perform supervised machine learning classification. The dataset contains a diverse set of phishing patterns, enabling the model to learn various types of malicious website behaviors.

Before training the model, the dataset was carefully ana- lyzed and cleaned to ensure data quality. Duplicate URLs, inactive links, and corrupted records were removed during the preprocessing stage. Maintaining a clean dataset helps improve the accuracy and reliability of the machine learning model.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802166

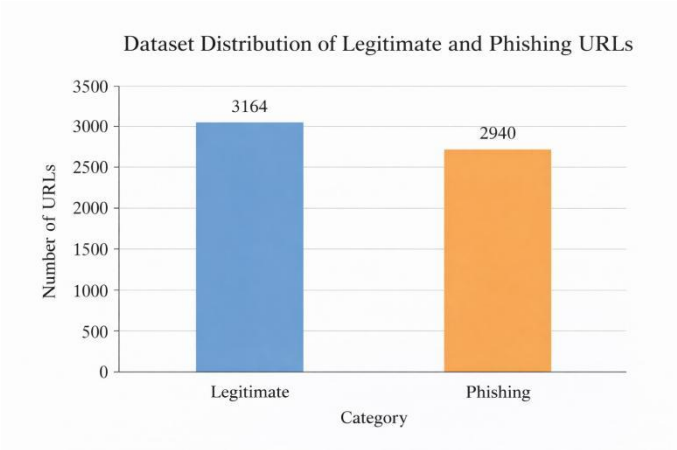

Fig.2. Dataset Distribution of Phishing and Legitimate URLs

Data Preprocessing

Data preprocessing is an important step in preparing the dataset for machine learning training. Raw datasets often contain incomplete records, inconsistent values, and duplicate entries that may negatively affect model performance.

During preprocessing, several data cleaning operations were performed. Duplicate URLs were removed to avoid bias in the training process. Missing values obtained from domain lookup or webpage analysis were handled using appropriate numerical encoding techniques.

The dataset labels were converted into numerical values where phishing websites were encoded as -1 and legitimate websites were encoded as 1. This transformation allows the machine learning algorithm to process classification labels effectively.

After preprocessing, the dataset was divided into two sub- sets: training data and testing data. Approximately 80

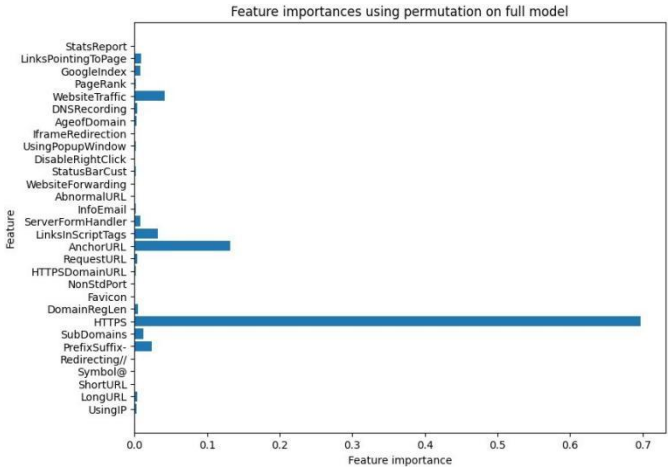

Fig.3. Data Preprocessing and Feature Extraction Workflow

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802166

Feature Extraction

Feature extraction converts raw website information into structured numerical attributes that can be processed by the machine learning model. In this project, a total of 30 features were extracted and categorized into four main groups.

URL-based features: These features analyze the struc- tural characteristics of the URL, such as URL length, presence of special symbols, number of subdomains, and shortened URLs.

Domain-based features: These features evaluate domain information including WHOIS records, domain age, reg- istration duration, and DNS records.

Security features: These features examine the security characteristics of the website, including HTTPS usage and SSL certificate availability.

Behavioral features: These features analyze webpage behavior such as iframe usage, popup windows, abnormal form actions, and redirection patterns.

These extracted features help the machine learning model identify suspicious patterns that are commonly associated with phishing attacks.

MACHINE LEARNING MODEL

The proposed phishing detection system uses a supervised machine learning approach to classify websites. After feature extraction and preprocessing, the structured feature vectors are passed to the Gradient Boosting Classifier for model training and prediction.

Model Selection

Gradient Boosting was selected because of its high predic- tion accuracy and ability to combine multiple weak learners into a strong predictive model. Unlike single decision tree classifiers, Gradient Boosting builds a sequence of trees where each tree learns from the mistakes of the previous tree.

This ensemble learning approach improves model stability, reduces overfitting, and enhances classification performance. The algorithm performs particularly well on structured datasets such as phishing detection datasets that contain multiple feature categories.

Training and Testing

To evaluate the effectiveness of the proposed system, the dataset was divided into training and testing subsets using an 80:20 ratio. The training dataset was used to train the Gradient Boosting model, allowing it to learn patterns from the extracted features.

The testing dataset was used to evaluate the prediction performance of the trained model on unseen data. Several classification metrics including Accuracy, Precision, Recall, and F1-score were used to measure the performance of the system.

Experimental results indicate that the proposed model achieves approximately 97

IV. SYSTEM IMPLEMENTATION

The phishing detection system was implemented using the Python programming language and deployed as a web-based application using the Flask framework. Python was chosen because of its extensive machine learning libraries and ease of integration with web technologies.

Several Python libraries were used during implementation, including Scikit-learn for machine learning algorithms, Pan- das and NumPy for data processing, and BeautifulSoup for webpage content analysis.

The trained Gradient Boosting model was saved as a serial- ized file named model.pkl. This file is loaded dynamically during application runtime to perform real-time predictions.

When a user submits a URL through the web interface, the Flask backend processes the request, extracts relevant features, and generates the feature vector. The feature vector is then passed to the trained model, which predicts whether the website is phishing or legitimate.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802166

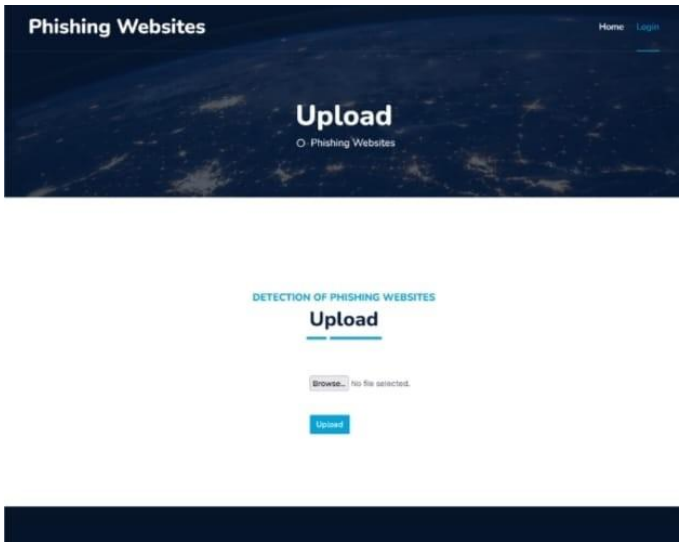

Fig.4. Web Interface for Phishing Website Detection

This implementation enables real-time phishing detection and provides an effective security mechanism for protecting users from malicious websites.

V. RESULTS

The performance of the proposed phishing detection system was evaluated using a dataset containing more than 6000 URLs consisting of both phishing and legitimate websites. Before training the machine learning model, the dataset was carefully preprocessed by removing duplicate records, handling missing values, and converting categorical attributes into numerical representations. The processed dataset was then divided into training and testing sets using an 80:20 ratio to evaluate the model performance on unseen data.

The Gradient Boosting Classifier was trained using the ex- tracted feature vectors representing structural, domain-based, security, and behavioral characteristics of websites. A total of 30 features were used to represent each website instance. These features provide important information about suspicious URL patterns, domain registration details, security indicators, and webpage behavior.

The dataset distribution shows that both phishing and le- gitimate URLs were fairly balanced, which helps improve the generalization capability of the machine learning model and prevents classification bias toward a specific class.
After the training phase, the model was evaluated using standard machine learning performance metrics including Ac-curacy, Precision, Recall, and F1-score. The experimental results indicate that the Gradient Boosting model achieved strong classification performance.

- Accuracy: 97
- Precision: 96
- Recall: 97
- F1-score: 96

The confusion matrix further illustrates the classification performance of the model by showing the relationship between predicted and actual class labels. The results show that the model successfully classifies most phishing and legitimate websites with only a small number of misclassifications.

In addition to model evaluation, the trained classifier was integrated into a Flask-based web application to perform real-time phishing detection. The system allows users to enter a website URL through a web interface. After receiving the input URL, the system automatically extracts the required features, converts them into a feature vector, and passes them to the trained machine learning model.

The model then predicts whether the website is phishing or legitimate and displays the prediction result to the user instantly. This real-time prediction mechanism helps users verify the safety of websites before interacting with them.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802166

Overall, the experimental results demonstrate that the pro- posed machine learning based phishing detection system achieves high prediction accuracy and reliable classification performance. The integration of machine learning with a web- based interface provides a practical and scalable solution for improving online security and protecting users from phishing attacks.

V. DISCUSSION AND SUMMARY

The main objective of this research was to design and implement an intelligent phishing website detection system using machine learning techniques. Phishing attacks continue to be one of the most significant cybersecurity threats, as attackers frequently create fraudulent websites that mimic legitimate platforms to steal sensitive user information such as login credentials, banking details, and personal data. The proposed system addresses this issue by analyzing various characteristics of websites and automatically classifying them as phishing or legitimate.

The developed system utilizes a feature-based machine learning approach in which multiple attributes of a website are examined before classification. In this study, a total of 30 discriminative features were extracted from the input URL and its associated webpage. These features include structural URL patterns, domain-based information, security indicators, and behavioral characteristics of the webpage. By combining multiple feature categories, the system can effectively cap- ture suspicious patterns commonly associated with phishing attacks.

The performance evaluation of the proposed system demon- strates the effectiveness of the Gradient Boosting Classifier in detecting phishing websites. The trained model achieved an overall classification accuracy of approximately 97
The experimental analysis also highlights the advantages of machine learning based detection compared with traditional blacklist-based security mechanisms. Conventional blacklist systems can only block websites that have already been reported as malicious. However, phishing attackers frequently generate new URLs and domains that are not present in existing blacklist databases. In contrast, the proposed machine learning model learns patterns from historical data and can identify previously unseen phishing websites by analyzing suspicious features. This capability significantly improves the adaptability and scalability of phishing detection systems.

Another important contribution of this research is the im- plementation of the detection model within a Flask-based web application. The web application provides a user-friendly interface where users can enter a website URL for analysis. Once the URL is submitted, the system performs automated feature extraction and passes the feature vector to the trained machine learning model. The model then predicts whether the website is phishing or legitimate and displays the result to the user in real time. This real-time prediction mechanism allows users to verify the safety of websites before interacting with them.

From a practical perspective, the developed system demon- strates the feasibility of integrating machine learning based phishing detection into real-world applications. The proposed framework can be used as a security tool for web browsers, e- commerce platforms, and online financial services to prevent credential theft and fraudulent activities. By detecting mali- cious websites before user interaction occurs, the system helps improve overall web security and enhances user confidence in online services.

Although the proposed model achieves strong performance, there are several opportunities for further improvement. Future work may include expanding the dataset with newly emerging phishing URLs, integrating advanced deep learning models for improved feature learning, and deploying the system as a browser extension or cloud-based security service. Continuous model training and dataset updates would allow the system to adapt to evolving phishing attack strategies and maintain high detection accuracy.

In summary, the results of this research demonstrate that machine learning techniques provide an effective and scalable solution for phishing website detection. The proposed system successfully combines feature extraction, machine learning classification, and web-based deployment to provide real-time protection against phishing attacks. The achieved accuracy and practical implementation confirm the potential of the system to contribute to safer web browsing environments.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802166

APPENDIX A

HAND CALCULATIONS (OR NAME YOUR TITLE FOR APPENDIX SUBTITLE)

List any extra evidence such as photos of the session, that may help you support your claims. You can include all hand calculations, extra graphs and plots, simulation results, etc.

VI. ACKNOWLEDGMENT

The authors would like to thank the Department of Ar- tificial Intelligence Data Science, R P Sarathy Institute of Technology, Salem, for providing the necessary resources and guidance to carry out this research work successfully.

REFERENCES

1. Puente, H. Gonza´lez-Jorge, J. Mart´ınez-Sa´nchez, and P. Arias, "Re- view of mobile mapping and surveying technologies," Measurement, vol. 46, no. 7, pp. 2127–2145, 2013.
2. S. S. Shafin, "An explainable feature selection framework for web phish- ing detection with machine learning," Data Science and Management, vol. 8, pp. 127–136, 2025.
3. I. Lee, C. Kiekintveld, and A. Piplai, "An investigation into the per- formances of state-of-the-art machine learning approaches for various cyber-attack detection," arXiv preprint, arXiv:2402.17045, 2024.
4. J. Lee, Z. Xin, M. Ng, P. Se, K. Sabharwal, G. Apruzzese, and D.
5. M. Divakaran, "Attacking logo-based phishing website detectors with adversarial perturbations," arXiv preprint, arXiv:2308.09392, 2023.
6. P. C. R. Chinta, C. S. Moore, L. M. Karaka, M. Sakuru, V. Bodepudi, and S. R. Moka, "Building an intelligent phishing email detection system using machine learning and feature engineering," European Journal of Applied Science, Engineering and Technology, vol. 3, no. 2, pp. 41–54, 2025.
7. J. A. Ochu, G. I. O. Almufuh, H. Musa, and S. E. Chaku, "Detecting phishing websites using large language model," Science World Journal, vol. 20, no. 2, pp. 692–697, 2025.
8. O. T. Agboola, "Development of a novel approach to phishing detection using machine learning," Journal of Science Technology and Education, vol. 12, no. 2, pp. 336–351, 2024.
9. C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746
10. C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2
11. C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9
12. S.Tamilselvi, R.Prakash, C.Nagarajan,"Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller" Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025
13. S.Tamilselvi, R.Prakash, C.Nagarajan," Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance" Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
14. S.Thirunavukkarasu, C. Nagarajan, 2024, "Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
15. Nagarajan, M.Madheswaran and D.Ramasubramanian- 'Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model'- Acta Electrotechnica et Informatica Journal , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.
16. C.Nagarajan and M.Madheswaran - 'DSP Based Fuzzy Controller for Series Parallel Resonant converter'- Springer, Frontiers of Electrical and Electronic Engineering, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.
17. C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
18. C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802166

Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007

19. Suganthi Mullainathan, Ramesh Natarajan, "An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques", Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
20. M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
21. T. Kekhashan, M. Abdelhaq, A. S. Al-Shumayleh, N. Huda, I. A. Yaseen,
22. I. A. Ahmed, and A. Akhunzada, "Explainable phishing website detection for secure and sustainable cyber infrastructure," Scientific Reports, vol. 15, p. 41751, 2025.
23. R. Alzaidah, A. Al-Shaikh, M. R. Al-Mousa, H. Khafajah, G. Samara,
24. M. Alyou, A. Al-Shanableh, and S. Almarneh, "Website phishing detection using machine learning techniques," Journal of Statistics Applications and Probability, vol. 13, no. 1, pp. 119–129, 2024.
25. A. Karim, M. Shabroz, K. Mustofa, S. B. Belhaouari, and S. R. K. Joga, "Phishing detection system through hybrid machine learning based on URL," IEEE Access, vol. 11, pp. 3605–3682, 2023.
26. A. Sabir, M. A. Babar, R. Gaire, and A. Abuadbba, "Reliability and robustness analysis of machine learning-based phishing URL detectors," arXiv preprint, arXiv:2005.08454, 2020.
27. Anbazhagan, K. (2025). Next-Generation Enterprise Cloud AI for Healthcare: Secure CNN Pipelines and Privacy Controls. *International Journal of Future Innovative Science and Technology (IJFIST), 8(6), 15980.*
28. Mathew, A. (2023). Learning Metaverse Powered by Artificial Intelligence. Recent Progress in Science and Technology Vol. 4, 4, 134-141.
29. Dhinakaran, D. (2022). Joe Prathap P. M, Selvaraj D, Arul Kumar D and Murugeshwari B," Mining Privacy-Preserving Association Rules based on Parallel Processing in Cloud Computing,". *International Journal of Engineering Trends and Technology, 70(3), 284-294.*
30. Garg, V. K., Soundappan, S. J., & Kaur, E. M. (2020). Enhancement in intrusion detection system for WLAN using genetic algorithms. *South Asian Research Journal of Engineering and Technology, 2(6), 62–64.*
31. Mathew, A., & Fofang, T. S. I. AI-Driven Fraud Detection: Leveraging Machine Learning for Scam Identification.