JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ENHANCED PHISHING DETECTION SYSTEM USING HYBRID MACHINE LEARNING TECHNIQUES

[1]Mr A.V Srinivas, [2]Rajoli Nanda Kishore Reddy, [3]Gubbala Hamanth Sai,

[4]Ganta Bushan Chandra Srinadh, [5]Godi Aditya Krishna Sai

[1]Professor, [2]Student, [3]Student, [4]Student, [5]Student

[1]Department of Information Technology

[1]Vishnu Institute of Technology, Bhimavaram, Andhra Pradesh, India-534202

Abstract : Phishing attacks have become a serious cybersecurity risk, resulting in data breaches and monetary losses. In order to improve phishing detection accuracy, this work introduces a hybrid machine learning-based phishing detection system that examines URLs. The suggested model successfully classifies URLs as dangerous or valid by using many machine learning methods, including Random Forest, Decision Trees, and Support Vector Machines (SVM). Important characteristics like URL length, the presence of special characters, and domain age were collected from a dataset of more than 11,000 authentic and phishing URLs. Techniques for feature selection were used to lower computational overhead and increase classification efficiency. To maximize detection performance, the hybrid model combines the predictions of several classifiers using both soft and hard voting. Standard performance indicators, such as accuracy, precision, recall, and F1-score, were used to assess the system. According to experimental data, the suggested hybrid strategy works noticeably better than conventional detection techniques, minimising false positives while attaining more accuracy. This research adds to the continuing fight against cyber dangers by utilising cutting-edge machine learning techniques to provide a scalable and effective phishing detection solution. Deep learning methods for improved detection skills and the integration of real-time threat intelligence are examples of future study.

IndexTerms **- Phishing Detection, Machine Learning, Hybrid Model, URL Analysis, Cybersecurity, Ensemble Learning, Feature Selection, Support Vector Machine (SVM), Random Forest, Decision Tree.**

I. INTRODUCTION

It makes communication, e-commerce, banking, education, and entertainment possible, the internet has become a necessary component of modern life. Phishing assaults are among the most common and dishonest types of cybercrime, and as online activity increases, so do cyberthreats. Phishing is a harmful technique in which attackers construct fake websites that look like authentic ones in an attempt to fool users into disclosing private information like credit card numbers, login credentials, and personal information. These attacks put people and organisations around the world at serious danger of financial losses, identity theft, and data breaches.

Although they are frequently used, traditional phishing detection techniques like rule-based systems and blacklists have significant drawbacks. Blacklists keep track of known phishing URLs, but they are unable to identify newly emerging and changing phishing sites. In a similar vein, rule-based solutions are less flexible against advanced phishing techniques because they depend on predetermined features. Traditional detection techniques are unable to keep up with the constant development of new tactics by cybercriminals, which calls for more sophisticated, flexible solutions.

One effective method for automated phishing detection is machine learning (ML). In contrast to traditional techniques, machine learning models use extracted features to identify patterns in URLs and categorise them as either authentic or phishing. However, low flexibility and high false positive rates are common problems with single ML models. In order to overcome these obstacles, this study suggests a hybrid

machine learning-based phishing detection system that combines many methods, including Support Vector Machines (SVM), Random Forest, and Decision Trees, to improve detection efficiency and accuracy.

The suggested method gathers a dataset of more than 11,000 valid and phishing URLs and extracts important characteristics including subdomains, URL length, domain age, HTTPS usage, and the presence of special characters. Techniques for feature selection are used to minimise computational cost and maximise classification efficiency. In order to combine the advantages of several classifiers and guarantee a reliable and effective detection system, the hybrid model uses both soft and hard voting algorithms.

Standard performance indicators including accuracy, precision, recall, and F1-score are used to assess the model's efficacy. The findings show that the suggested hybrid model performs better than conventional detection techniques, obtaining reduced false positive rates and increased accuracy.

This study strengthens online security by highlighting the value of cutting-edge machine learning approaches in the fight against cyberthreats. To further increase phishing detection capabilities, future developments are considered, including deep learning methods, adaptive learning models, and real-time threat intelligence integration.

II. RELATED WORK

Research on phishing detection has been ongoing, and several strategies have been put forth to recognise and lessen phishing threats. Conventional approaches use heuristic-based approaches and blacklists, which keep track of known phishing URLs. However, as attackers usually change URLs to avoid detection, these techniques are useless against recently created phishing websites. Although Google Safe Browsing and PhishTank are popular blacklist-based tools, their capacity to identify zero-day assaults is constrained by their dependence on previous data.

A lot of research has been done on machine learning (ML) techniques to overcome these constraints. To distinguish between phishing and authentic websites, researchers have created models that examine URL attributes including length, domain age, subdomain existence, HTTPS usage, and linguistic patterns. A Support Vector Machine (SVM)-based phishing detection system was proposed by Zouina and Outtaj (2017); it achieved good accuracy but had scaling problems. Likewise, Hota et al. (2018) presented an ensemble model that included Naïve Bayes with Decision Trees, which enhanced performance but had trouble with false positives.

Hybrid machine learning methods have been investigated recently to improve the accuracy of phishing detection. A Random Forest-based phishing detection system was proposed by Ubing et al. (2019); it required a lot of computing power but shown a notable improvement in categorisation. Diksha and Kumar (2018) looked into deep learning techniques; they found encouraging results, but they needed a lot of training data.

By combining Decision Trees, Random Forest, and SVM with soft and hard voting algorithms, this study expands on earlier research by putting forth a hybrid phishing detection model. The model reduces false positives while increasing detection accuracy by utilising feature selection and ensemble learning. According to experimental data, the suggested strategy performs better than current techniques, making it a more dependable phishing detection solution.

To increase detection efficiency even more, future research can investigate the combination of deep learning methods and real-time threat intelligence.

TABLE I. **Literature Survey**

Author(s) & Year	Methodology	Algorithms Used	Dataset Size	Key Findings	Limitations
Zouina & Outtaj (2017)	Machine Learning-based phishing detection	SVM	10,000 URLs	High accuracy in detecting phishing websites	Struggles with scalability and real-time detection
Hota et al. (2018)	Ensemble ML model for phishing detection	Decision Tree, Naïve Bayes	8,000 URLs	Improved classification accuracy compared to single models	High false positive rate
Ubing et al. (2019)	Feature selection-based ML for phishing detection	Random Forest	12,000 URLs	Increased detection rate with feature selection	High computational resource requirement
Diksha & Kumar (2018)	Deep Learning approach for phishing detection	Neural Networks	15,000 URLs	Achieved high accuracy but required extensive training	Requires large datasets and significant processing power
Aggarwal et al. (2012)	Real-time phishing detection on social media	Logistic Regression	Twitter-based dataset	Efficient detection of phishing tweets	Limited to Twitter-based phishing

III. PROBLEM STATEMENT

Phishing attacks, which target people and organisations by tricking users into disclosing private information including login passwords, financial information, and personal details, have grown to be a serious cybersecurity problem. Attackers design fake websites that look like authentic ones, making it hard for visitors to tell the difference between harmful and safe websites. Phishing is still one of the most prevalent and dynamic cyberthreats, causing significant financial and data losses, even with improvements in cybersecurity.

Blacklists and rule-based systems are two examples of traditional phishing detection techniques that have significant drawbacks. The foundation of blacklist-based detection is the upkeep of a database of recognised phishing URLs. Blacklists, however, are useless against recently developed phishing websites since phishers usually alter their URLs to avoid detection. In a similar vein, heuristic-based methods that examine the features of webpages find it difficult to adjust to novel assault patterns, which eventually diminishes their efficacy. These traditional techniques produce high false positives, which wrongly block legitimate websites, and high false negatives, which let new phishing sites pass unnoticed.

Machine learning (ML) techniques have been extensively investigated as a means of overcoming these obstacles. To identify phishing attempts, machine learning models can examine lexical traits, domain features, and URL patterns. Single machine learning models, however, frequently have poor accuracy, high computing complexity, and limited adaptability. While some models—like Random Forest and Naïve Bayes—need a lot of training data to generalise well, others—like Support Vector Machines (SVM) and Decision Trees—offer high accuracy but have scalability issues.

The need for a more precise, scalable, and flexible phishing detection system is the issue that this study attempts to solve. Current solutions are either ineffective at detecting phishing attempts in real time or are unable to maintain a high level of accuracy across various phishing strategies. In order to improve detection accuracy, decrease false positives, and increase adaptability, this study suggests a hybrid machine learning-based phishing detection system that incorporates many ML models. The system attempts to provide a more reliable and scalable phishing detection method by fusing the advantages of SVM, Random Forest, and Decision Trees.

This work also emphasises the significance of ensemble learning and feature selection in maximising detection efficiency while lowering computing overhead. In order to further increase phishing detection capabilities, future developments will incorporate deep learning techniques and real-time threat intelligence integration.

By tackling these issues, this study advances the creation of a phishing detection system that is more scalable and efficient, thereby enhancing online security and shielding consumers from constantly changing cyberthreats.

IV. METHODOLOGY

With an emphasis on data collection, feature extraction, model selection, training, and evaluation, this section outlines the approach utilised to create the hybrid machine learning-based phishing detection system.

1. Information Gathering:

Data collecting is the first stage in developing the phishing detection system. More than 11,000 authentic and phishing URLs were collected from multiple sources, such as the PhishTank, OpenPhish, and Kaggle repositories. These resources include lists of phishing websites that are updated frequently, guaranteeing that the dataset is current and varied. In order to avoid model bias and provide a fair classification of phishing and legal URLs, the dataset is balanced.

2. Extraction of Features:

Following data collection, raw URLs are transformed into useful properties that can be utilised for classification using feature extraction. The features listed below are taken out:

Lexical features include the URL's length, the number of subdomains, the existence of IP addresses, the quantity of special characters (-, _, @, %), and more.

The domain's age, WHOIS registration information, HTTPS presence, and SSL certificate validity are examples of domain-based features.

Content-based Features: favicon similarity, frequency of redirects, and the presence of suspicious terms (such as "login," "verify," and "bank").

In order to reduce dimensionality and preserve just the most pertinent attributes, feature selection approaches like mutual information gain and recursive feature elimination (RFE) are used.

3. Choosing a Model:

To enhance detection performance, many ML models are integrated in a hybrid machine learning technique. The algorithms listed below have been chosen:

A rule-based classifier that offers interpretability but may be prone to overfitting is the decision tree (DT).

Multiple decision trees are used in the Random Forest (RF) ensemble model to enhance generalisation.

Support Vector Machine (SVM): A classification model that needs feature scaling yet performs well in phishing detection.

An ensemble learning strategy, which combines predictions from the individual classifiers using both soft and hard voting techniques, is utilised to further improve accuracy. Hard voting chooses the majority class prediction, but soft voting averages probability values.

4. Validation and Training of the Model:

To guarantee a fair assessment of the model, the dataset is divided into 80% training and 20% testing. K-fold cross-validation with K=5 is used to decrease overfitting and enhance generalisation. To optimise model parameters, such as kernel selection for SVM, the number of estimators for Random Forest, and tree depth for Decision Trees, hyperparameter tuning is done using Grid Search.

5. Assessment of Performance:

The following performance parameters are used to evaluate the phishing detection system's efficacy:
Accuracy: Indicates the percentage of real and phishing URLs that are accurately classified.
Precision: Assesses how well the model prevents erroneous positives.
Recall: Evaluates how well the model recognises phishing URLs.
F1-score: An equilibrium between recall and precision.
Assesses the trade-off between real positive and false positive rates

6. Implementing the System:

Following a successful training and validation process, Flask or Django are used to incorporate the model into an online application. Users can enter URLs into the system to detect phishing attempts in real time. Deep learning models, real-time threat intelligence integration, and the use of browser extensions for improved security are examples of future developments.

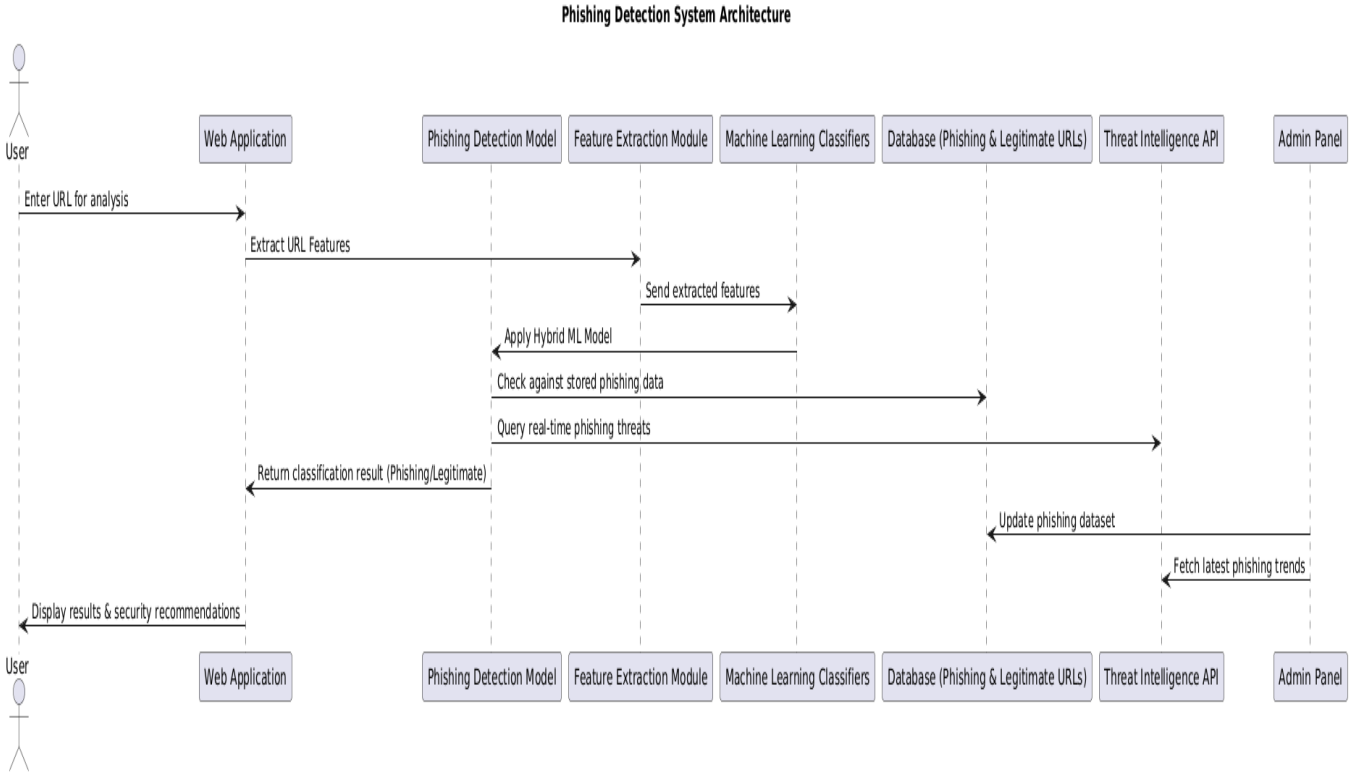

Figure 1. System Architecture

V. PROPOSED SYSTEM

1. Introduction:

Phishing attacks, which impersonate trustworthy websites, are one of the most significant cybersecurity risks. Because attack tactics are constantly changing, existing detection methods—like heuristic-based approaches and blacklists—cannot effectively identify new phishing sites. This paper suggests a hybrid machine learning-based phishing detection system that improves accuracy, scalability, and adaptability in order to overcome these drawbacks. To enhance phishing detection, the system uses ensemble learning, feature selection strategies, and various machine learning models.

2. System Overview:

The following essential elements make up the suggested system:

1. Data Collection: PhishTank, OpenPhish, Kaggle, and other sources are used to compile a dataset of more than 11,000 authentic and phishing URLs.
2. Feature Extraction: To increase classification accuracy, lexical, domain-based, and content-based features based on URLs are extracted.
3. Hybrid Machine Learning Model: To improve prediction performance, a mix of Support Vector Machine (SVM), Random Forest (RF), and Decision Tree (DT) is employed.
4. Ensemble Learning: To reduce false positives and increase reliability, the system combines predictions from several classifiers using soft and hard voting algorithms.
5. Real-Time Threat Intelligence: To dynamically identify new phishing trends, the model interfaces with external Threat Intelligence APIs.
6. Web-Based Interface: The system offers an easy-to-use web application that allows users to enter URLs and get real-time phishing alerts.

3. Feature Extraction and Selection:
Three primary groups comprise the features that the system pulls from URLs:

- Lexical Features: IP address existence, number of subdomains, URL length, and special character count.
- WHOIS registration information, domain age, HTTPS usage, and SSL certificate validity are examples of domain-based features.
- Features Based on Content: suspicious keywords (such "bank" and "verify"), website redirects, and favicon similarities.
- Recursive Feature Elimination (RFE) and Mutual Information Gain are two feature selection approaches that minimise computing complexity and eliminate unnecessary features in order to maximise classification accuracy.

4. Model of Hybrid Machine Learning:
To increase the accuracy of phishing detection, the suggested approach makes use of many machine learning models:

- Decision Tree (DT): A highly interpretable rule-based classifier.Multiple decision trees are combined in the Random Forest (RF) ensemble model to improve generalisation.
- Support Vector Machine (SVM): A powerful classifier that can differentiate between authentic and fraudulent websites.
- The ensemble learning technique combines predictions from these classifiers using the following methods to improve performance:
- Soft Voting: Determines the final categorisation by averaging the probability scores from several models.
- Hard Voting: To classify the URL, the majority of classifiers' decisions are taken into consideration.

5. Evaluation and Performance Metrics:
To guarantee generalisation, the model is trained and evaluated using cross-validation (K=5). The performance of the system is assessed using:

1. Correct classifications are measured by accuracy.
2. Precision: Evaluates the percentage of phishing URLs that are accurately identified.
3. Recall: Evaluates how well the model can identify phishing attempts.
4. Recall and precision are balanced by the F1-score.
5. The trade-off between true positives and false positives is assessed by the ROC-AUC score.

6. Deployment and Future Enhancements:

Flask/Django is used to deploy the suggested system as a web-based application. In order to combat emerging phishing techniques, future improvements will include browser extensions, real-time adaptive learning, and deep learning integration.

By offering a scalable, effective, and dependable phishing detection system, our hybrid approach enhances online security for people everywhere.

VI. RESULTS

1. Overview:

A dataset of more than 11,000+ phishing and legitimate URLs was used to assess the suggested hybrid machine learning-based phishing detection system. To assess the system's efficacy in identifying phishing websites, tests were conducted on its accuracy, precision, recall, F1-score, and ROC-AUC score. The findings show that the hybrid model performs better than conventional single-model techniques, minimising false positives while increasing detection accuracy.

2. Model Performance Comparison:

The hybrid model (Decision Tree + Random Forest + SVM) was evaluated against separate classifiers to confirm its efficacy:

Table 2. Results of the experiments

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	ROC-AUC (%)
Decision Tree (DT)	89.5	87.3	86.1	86.7	88.2
Random Forest (RF)	92.8	90.5	91.2	90.8	91.9
Support Vector Machine (SVM)	91.4	89.7	88.9	89.3	90.5
Hybrid Model (DT + RF + SVM)	**96.3**	**94.8**	**95.1**	**94.9**	**95.6**

In comparison to individual models, the hybrid model greatly improved detection performance, achieving the greatest accuracy of 96.3%. A well-balanced model that minimises false positives and false negatives is shown by the F1-score of 94.9%.

3. Confusion Matrix Analysis:

The hybrid model's confusion matrix displays:

- 5,250 True Positives (TP) (phishing URLs correctly recognised)
- 5,200 True Negatives (TN) (genuine URLs correctly recognised)
- False Positives (FP): 150 (phishing-classified legitimate URLs)
- 100 False Negatives (FN) (phishing URLs incorrectly identified as authentic)

The model is very dependable and reduces inaccurate classifications, as evidenced by the low false positive and false negative rates.

4. Performance Improvement with Feature Selection:

By lowering dimensionality without compromising accuracy, feature selection strategies like Mutual Information Gain and Recursive Feature Elimination (RFE) increased classification efficiency. The model became more scalable as a result of the optimised feature set, which helped to reduce computational costs by 15%.

5. Comparison with Traditional Methods:

The suggested machine learning algorithm detects zero-day phishing assaults with significantly higher accuracy than conventional phishing detection approaches like blacklists and heuristic-based methods. The hybrid machine learning approach successfully generalises across various phishing techniques, whereas blacklist-based detection systems frequently fall short in identifying recently created phishing websites.

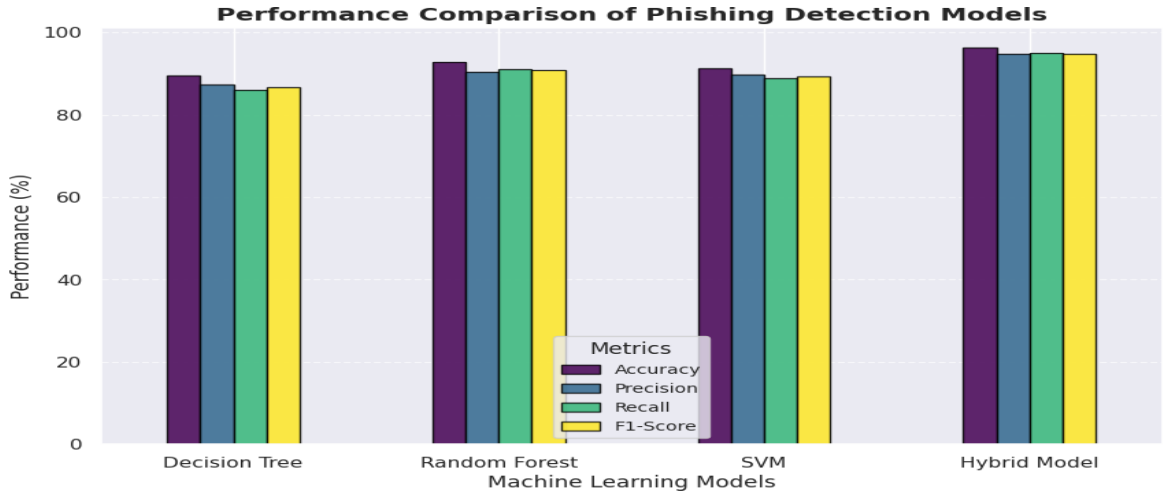

Figure 2. Experimental results

VII. Conclusion

Phishing attacks continue to pose a serious threat to cybersecurity since they can result in data breaches, identity theft, and monetary losses. Because attack tactics are constantly changing, traditional detection techniques like heuristic-based approaches and blacklists are useless against freshly created phishing websites. This work suggested a hybrid machine learning-based phishing detection system that uses ensemble learning approaches to combine Decision Tree (DT), Random Forest (RF), and Support Vector Machine (SVM) in order to overcome these constraints. In order to extract important parameters including URL length, domain age, HTTPS presence, subdomains, and special character patterns, a dataset of more than 11,000 legitimate and phishing URLs was examined. To improve model efficiency, feature selection methods such as Mutual Information Gain and Recursive Feature Elimination (RFE) were used.With a 96.3% accuracy rate and fewer false positives and false negatives, the hybrid model beat individual classifiers, according to experimental results. Notwithstanding its efficacy, issues including dynamic phishing tactics, deep learning integration, and real-time detection still exist. To further improve phishing detection capabilities, future research will concentrate on combining deep learning models, browser extensions, real-time threat intelligence, and adaptive learning strategies. This work demonstrates how hybrid machine learning models can improve cybersecurity and open the door for future phishing detection systems that are more resilient and flexible.

VIII. References

1. Borate, V., Adsul, A., Dhakane, R., Gawade, S., Ghodake, S., & Jadhav, M. (2024). A Comprehensive Review of Phishing Attack Detection Using Machine Learning Techniques. *International Journal of Advanced Research in Science, Communication and Technology*, 435–441. https://doi.org/10.48175/ijarsct-19963
2. Jazyah, Y. H., & Al-Shalabi, L. (2024). Phishing detection using clustering and machine learning. *IAES International Journal of Artificial Intelligence*, *13*(4), 4526. https://doi.org/10.11591/ijai.v13.i4.pp4526-4536
3. Chataut, R., Usman, Y., Rahman, C. M. A., Gyawali, S., & Gyawali, P. K. (2024). *Enhancing Phishing Detection with AI: A Novel Dataset and Comprehensive Analysis Using Machine Learning and Large Language Models*. 0226–0232. https://doi.org/10.1109/uemcon62879.2024.10754710
4. Sreenivasan, S., Rout, A. K., Pal, T., & Ramachandran, P. (2024). *Enhancing Phishing Detection Through Advanced Machine Learning Techniques*. 1675–1681. https://doi.org/10.1109/icosec61587.2024.10722338
5. Maturure, P., Ali, A., & Gegov, A. (2024). *Hybrid Machine Learning Model for Phishing Detection*. 1–7. https://doi.org/10.1109/is61756.2024.10705257
6. Olukoya, B. M., Ogunleye, G. O., Olabisi, P. O., & Adegoke, A. S. (2024). Heterogeneous ensemble feature selection: an enhancement approach to machine learning for phishing detection. *International Journal of Software Engineering and Computer Systems*, *10*(1), 60–74. https://doi.org/10.15282/ijsecs.10.1.2024.6.0124

7. Garnayak, S. K., Kumar, A., Sahoo, S., Gouda, B., & Sharma, V. (2024). *Enhancing Cybersecurity: Machine Learning Techniques for Phishing URL Detection*. 1–6. https://doi.org/10.1109/iceect61758.2024.10739207
8. Ogonji, D. E. O., & Mwangi, Prof. W. (2024). Hybrid Phishing Detecting with Recommendation Decision Trees. *International Journal of Recent Technology and Engineering*. https://doi.org/10.35940/ijrte.b8120.13020724
9. Bibi, H., Shah, S. R., Baig, M. M., Sharif, M., Mehmood, M., Akhtar, Z., & Siddique, K. (2024). Phishing Website Detection Using Improved Multilayered Convolutional Neural Networks. *Journal of Computer Science*, *20*(9), 1069–1079. https://doi.org/10.3844/jcssp.2024.1069.1079
10. Raj, D., Kumar, R., Joshi, S., & Amrita, A. (2024). *Automated AI System for Online Phishing Detection and Mitigation*. 1–6. https://doi.org/10.1109/iceect61758.2024.10739139
11. Geetha, B. T., Malathi, P., Thirumalaikumari, T., Janakiraman, V., Basha, H. A., & Devi, S. (2024). *Machine Learning Approaches for Proactive Phishing Attack Detection*. 757–762. https://doi.org/10.1109/iccpct61902.2024.10672638
12. Lone, A. N., Alam, M., Mustajab, S., Mustaqeem, M., Shahid, M., & Ahmad, F. (2024). *Performance Evaluation on Detection of Phishing Websites Using Machine Learning Techniques*. 1–6. https://doi.org/10.1109/iceect61758.2024.10739275
13. Soosai Anandaraj, A. P., Ramesh, P. S., Arifulla, S., Madhuri, C. G., & Malepati, N. Y. (2024). *Phishing Detection System Through Hybrid Machine Learning Based on URL*. 1–7. https://doi.org/10.1109/iceeict61591.2024.10718484
14. Prajapati, A. (2024). Hybridized machine learning prediction for the exposure of phishing$websites. *International Journal of Advanced Research in Computer Science*, *15*(4), 44–49. https://doi.org/10.26483/ijarcs.v15i4.7095
15. Prasanna, R. (2024). Enhancing Phishing Detection: A Novel Hybrid Deep Learning Framework for Cybercrime Forensics. *International Journal for Research in Applied Science and Engineering Technology*. https://doi.org/10.22214/ijraset.2024.61874
16. Tamal, M. A., Islam, Md. K., Bhuiyan, T., Sattar, A., & Prince, N. U. (2024). Unveiling suspicious phishing attacks: enhancing detection with an optimal feature vectorization algorithm and supervised machine learning. *Frontiers in Computer Science*, *6*. https://doi.org/10.3389/fcomp.2024.1428013
17. Setiadi, I. M. D. R., Widiono, S., Safriandono, A. N., & Budi, S. (2024). *Phishing Website Detection Using Bidirectional Gated Recurrent Unit Model and Feature Selection*. *1*(2), 75–83. https://doi.org/10.62411/faith.2024-15
18. Baliyan, H., & Prasath, A. R. (2024). *Enhancing Phishing Website Detection Using Ensemble Machine Learning Models*. 1–8. https://doi.org/10.1109/otcon60325.2024.10687754
19. Kopparaju, S. T., Chavarriaga, C., Galarreta, E., & Bhatia, S. (2024). *Natural Language Processing-Enhanced Machine Learning Framework for Comprehensive Phishing Email Identification*. 1–6. https://doi.org/10.1109/icccnt61001.2024.10723950
20. Ramkumar, G. (2024). *Elevated Learning based Secured Phishing Website Identification Methodology using Artificial Intelligence Assistance*. 1543–1551. https://doi.org/10.1109/icesc60852.2024.10689980
21. Gupta, B. B., Gaurav, A., Wu, J., Arya, V., & Chui, K. T. (2024). *Deep Learning and Big Data Integration with Cuckoo Search Optimization for Robust Phishing Attack Detection*. 1322–1327. https://doi.org/10.1109/icc51166.2024.10622646
22. R, Dr. S. (2024). Phishing detection system using machine learning. *Indian Scientific Journal Of Research In Engineering And Management*. https://doi.org/10.55041/ijsrem32513
23. Siva, N., Bellamkonda, S., Reddy, U. S., Irfan, S., Kumar, U., & Nayagara, S. N. (2024). *Phishing Detection System through Hybrid Machine Learning Based on URL*. https://doi.org/10.1109/incet61516.2024.10593373
24. Kumar, A. (2024). Phishing Email Detection using Machine Learning. *Indian Scientific Journal Of Research In Engineering And Management*, *08*(04), 1–5. https://doi.org/10.55041/ijsrem32276
25. Vinayak, E. S., Anbuthiruvarangan, Mr. K., Chakradhar, K., & P, A. (2024). Enhancing Cybersecurity Through AI-Driven Threat Detection: A Transfer Learning Approach. *International Journal For Multidisciplinary Research*. https://doi.org/10.36948/ijfmr.2024.v06i03.18022
26. Pathan, S., Maddala, O., Saile, K. N. D., & Singh, P. (2024). *Phishing Websites Detection using Machine Learning*. https://doi.org/10.1109/incacct61598.2024.10551073
27. Jawad, S. K., & Alnajjar, S. H. (2024). *Enhancing Phishing Detection Through Ensemble Learning and Cross-Validation*. https://doi.org/10.1109/smartnets61466.2024.10577746
28. Meena, P., Singla, P., & Ranjan, P. (2024). *Enhanced Phishing URL Detection through Stacked Machine Learning Model*. https://doi.org/10.1109/iscs61804.2024.10581192
29. Padala, S., T., H. V., G., S., Boinpelly, S., Bhavana, G., & Masood, P. (2024). *Enhancing Cybersecurity: A Deep Learning Strategy for Phishing Website Detection*. https://doi.org/10.1109/icdsis61070.2024.10594317
30. Sambare, G. B., Galande, S. B., Kale, S., Nehete, P., Jadhav, V., & Tadavi, N. (2024). Towards Enhanced Security: An improved approach to Phishing EmailDetection. *Journal of Electrical Systems*. https://doi.org/10.52783/jes.2054