WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal Homepage: www.ijrpr.com ISSN 2582-7421

# AI-Based Phishing Website Detection Using Machine Learning: A Comprehensive and Critical Literature Review

***Ms. Akansha S. Malthankar[1], Mrs. Shubhangi P. Bomble[2]***

*Student[1], Faculty[2]*
*Department of Masters of Computer Application, JCEI's Jaihind Institute of Research and Management, Vadgaon Sahani, Maharashtra*

**ABSTRACT:**

Phishing websites are a major cybersecurity threat in which attackers imitate legitimate websites to deceive users into revealing sensitive information, such as usernames, passwords, financial credentials, and personal data. Traditional phishing detection mechanisms such as blacklists, whitelists, and manually defined rules are useful for known threats but are often unable to detect newly created and rapidly changing phishing websites. Artificial intelligence (AI) and machine learning (ML) have therefore emerged as important approaches for automatically identifying phishing websites using URLs, domains, HTML, JavaScript, webpage content, and visual features.

This study presents a comprehensive and critical literature review of AI-based phishing website detection techniques. Sixty relevant studies published across journals, conferences, and scholarly sources are reviewed, covering classical machine learning, ensemble learning, deep learning, transformer-based models, feature engineering, visual similarity, dataset construction, explainable AI, adversarial robustness, and real-time deployment. The literature shows that random forest, support vector machine, gradient boosting, XGBoost, CNN, LSTM, and transformer-based models can achieve high classification performance under specific experimental conditions. However, reported performance depends strongly on dataset characteristics, feature representation, class balance, and evaluation methodology. Recent studies have also shown that models achieving high accuracy on randomly divided datasets may exhibit poor generalization when evaluated on newly generated domains or independent datasets. Therefore, accuracy alone is not sufficient to establish the practical effectiveness of a phishing detection system. This review identifies important research gaps related to temporal generalization, cross-dataset evaluation, feature engineering, explainability, adversarial robustness, computational efficiency, and real-time deployment. Finally, a research framework is proposed for developing adaptive, explainable, and lightweight AI-based phishing website detection systems.

***Keywords:*** *phishing website, machine learning, artificial intelligence, phishing URL, deep learning, random forest, ensemble learning, transformer, explainable AI, and cybersecurity.*

## 1. INTRODUCTION

The rapid expansion of Internet-based services has transformed banking, education, healthcare, commerce, communication, and other activities. However, increased dependence on online services has also resulted in increased cybersecurity risks. Among different cyber threats, phishing is one of the most common social-engineering attacks because it exploits both technical weaknesses and human trust [1]–[4].

A phishing attack generally attempts to make a malicious website appear similar to a legitimate website. An attacker may use a deceptive URL, copied webpage design, misleading domain name, malicious hyperlink, or fake login form to convince the victim to submit confidential information. Early phishing detection approaches used blacklist-based, heuristic, and visual-similarity techniques [5]–[8]. Although these techniques remain useful, they have limitations when attackers create new domains or modify webpage characteristics.

Visual-similarity approaches compare a suspicious webpage with a legitimate webpage using text, images, webpage layout, and other visual characteristics [6]–[10]. CANTINA+ demonstrated the use of a feature-rich machine learning framework for phishing website detection and showed the importance of combining multiple webpage characteristics [11].

The development of supervised machine learning has provided a more flexible approach. Instead of relying entirely on predefined rules, ML algorithms learn the characteristics of phishing and legitimate websites from labelled data. Algorithms such as decision trees, random forest, support vector machine (SVM), logistic regression, K-nearest neighbor (KNN), Naïve Bayes, and boosting algorithms have been widely investigated [12]–[20].

Deep learning has further extended this area by automatically learning complex representations from URLs and webpage data. CNN, DNN, LSTM, and hybrid models have been used for phishing detection [21]–[27]. More recently, transformer-based models have been investigated because of their ability to learn contextual relationships from sequential URL and webpage-content information [28]–[31].

However, the comparison of phishing detection models is not straightforward. A model may report 99% accuracy on one dataset and perform significantly worse on another dataset. Dataset size, class distribution, feature representation, and train-test splitting methodology can strongly influence the reported results [32]–[36].

Recent studies have specifically highlighted the generalization problem. Rashid et al. demonstrated that phishing URL models may perform effectively when training and testing data come from the same distribution but can lose performance when evaluated on fresh domains [37]. This observation is highly important because phishing websites are short-lived, and attackers continuously generate new domains.

Therefore, this study provides a critical review of AI-based phishing website detection with particular emphasis on machine learning, feature engineering, deep learning, transformers, datasets, generalization, explainability, adversarial robustness, and real-time deployment.

## 2. OBJECTIVES OF THE REVIEW

The major objectives of this literature review are as follows:

1. To study existing AI and ML techniques for phishing website detection.
2. Phishing detection approaches are classified according to their input features and learning algorithms.
3. To analyze commonly used phishing datasets
4. To compare classical ML, ensemble, deep learning, and transformer-based approaches.
5. To study the importance of feature engineering and feature selection
6. To analyze commonly used evaluation metrics
7. To investigate the dataset dependency and model generalization.
8. To study recent developments in explainable and adversarially robust phishing detection.
9. To identify major research gaps.
10. To propose future research directions for practical phishing detection systems

## 3. REVIEW METHODOLOGY

This review considers research papers related to phishing website and phishing URL detection using machine learning, deep learning, artificial intelligence, visual similarity, and hybrid approaches.

The literature was organized into the following categories.

- Traditional and visual-similarity approaches
- Classical machine learning
- Ensemble learning
- Deep learning
- Transformer-based detection
- Feature engineering
- Dataset and generalization studies
- Explainable AI and adversarial robustness
- Real-time and deployable systems

Systematic reviews by Catal et al., Safi and Singh, and other researchers demonstrate that phishing detection has developed into a broad research area involving multiple datasets and algorithmic approaches [38]–[42].

Recent reviews have also emphasized the importance of feature engineering, dataset limitations, evolving phishing tactics, and lightweight real-time solutions [43]–[45].

## 4. PHISHING:

### *4.1 WEBSITE DETECTION APPROACHES*

Phishing detection techniques can be broadly divided into the following categories:

1. List-based detection
2. Heuristic detection
3. Visual-similarity detection
4. Machine-learning-based detection
5. Deep-learning-based detection
6. Hybrid and transformer-based detection

### *4.1 List-Based Detection*

Blacklist-based systems maintain databases of known malicious URLs. When a user requests a URL, it is compared with a blacklist.

The main advantage is low computational complexity. However, the approach cannot reliably detect newly created phishing websites that have not yet been reported [4], [38].

### *4.2 Heuristic Detection*

Heuristic methods identify suspicious characteristics using pre-defined rules.

Examples include:

- Excessive URL length
- IP address in URL
- Multiple subdomains
- Suspicious keywords
- Abnormal redirections
- Missing HTTPS
- Suspicious forms

However, attackers can modify their URLs to avoid predefined rules [12], [38].

### *4.3 Visual-Similarity Detection*

Visual approaches compare suspicious webpages with trusted webpages using webpage screenshots, text, images, logos, and layout characteristics [6]–[10].

Visual-similarity research has demonstrated that phishing pages frequently attempt to imitate trusted websites. However, these methods can require webpage rendering and comparison, which may increase computational costs.

Recent deep learning visual approaches have attempted to improve the detection of zero-day and partially similar phishing webpages [46].

## 5. URL-BASED FEATURES

URL-based detection is one of the most commonly investigated approaches because URL can often be analyzed before the complete webpage is loaded.

Typical URL features include the following:

- URL length
- Number of dots
- Number of hyphens
- Number of digits

- Number of special characters
- Number of subdirectories
- Number of parameters
- Number of subdomains
- Presence of an IP address
- HTTPS usage
- Suspicious keywords
- URL entropy

Research has shown that URL lexical features can provide an efficient basis for phishing detection [14], [15], [17], [19], [32].

The main advantage of URL-only detection is its speed. However, URL-based models may miss phishing websites whose URLs appear relatively normal.

## 6. DOMAIN AND HOST-BASED FEATURES

Domain-based features provide additional information about websites.

Common domain features include the following:

- Domain age
- DNS information
- WHOIS information
- Registrar
- SSL certificate
- IP address
- Domain reputation

Hybrid approaches that combine URL and hyperlink or domain information have also been investigated [47].

However, external domain queries may introduce latency and may not always be available for use. Therefore, such features should be carefully selected when real-time detection is required in the future.

## 7. HTML AND WEBPAGE FEATURES

HTML-based detection examines the internal structure of webpages.

Common features include:

- Number of hyperlinks
- Number of forms
- Iframe usage
- External resources
- JavaScript functions
- Redirections
- Form actions
- Hidden elements
- Suspicious scripts

Machine learning models using such features have demonstrated good classification performance [12], [16], [18].

The main limitation is that webpages must usually be retrieved and processed before classification.

## 8. CLASSICAL MACHINE LEARNING

### *8.1 Logistic Regression*

Logistic regression is a simple and computationally efficient classification algorithm. It has been successfully applied to phishing URL detection, particularly with text-based representations, such as TF-IDF [19].

### *8.2 Decision Tree*

Decision trees use a sequence of feature-based decisions. They are relatively easy to interpret and have been frequently evaluated in phishing detection studies [13], [17].

### *8.3 Support Vector Machine*

The SVM constructs a decision boundary that separates phishing and legitimate samples. It has been widely investigated for URL and webpage feature classification [13], [48].

Nature-inspired optimization techniques have also been combined with SVM to improve the model parameter selection [48].

### *8.4 K-Nearest Neighbour*

KNN classifies a sample according to the nearby training samples. Although simple, the prediction may become computationally expensive for very large datasets.

### *8.5 Naïve Bayes*

Naïve Bayes provides a probabilistic approach and can be useful for URL- or text-based features.

### *8.6 Random Forest*

Random Forest combines multiple decision trees and has become one of the most commonly used algorithms for phishing detection [15], [18], [20], [49].

Its advantages include:

- Good performance
- Ability to handle nonlinear relationships
- Robustness to feature variations
- Relatively simple implementation

However, high performance on a single dataset does not establish universal superiority.

### *8.7 Gradient Boosting and XGBoost*

Boosting methods sequentially combine weak learners. XGBoost and gradient boosting have been increasingly used for phishing detection because of their ability to model nonlinear relationships [20], [34], [50].

## 9. ENSEMBLE LEARNING

Ensemble learning combines multiple models to improve the classification.

Common approaches include the following:

- Random Forest
- AdaBoost
- Gradient Boosting
- XGBoost
- Voting Classifier

- Stacking

Studies have shown that ensemble approaches can perform well on phishing datasets [20], [34], [50]–[51].

A recent ensemble-based framework combining CatBoost, LightGBM, and gradient boosting achieved 97.3% accuracy while explicitly considering feature robustness, generalization, and adversarial resilience [51].

This is important because future ensemble models should not be evaluated only based on accuracy. Robustness and generalization must also be considered.

## 10. DEEP LEARNING FOR PHISHING DETECTION

Deep learning models can automatically learn representations from raw or minimally processed datasets.

Common architectures include

- Deep Neural Networks
- CNN
- LSTM
- RNN
- Autoencoders
- CNN-LSTM
- Hybrid CNN-based models

Research has shown that deep learning can reduce the dependence on manually engineered URL features [21], [23], [24].

A 2024 study compared feature-engineered ML models with CNN and LSTM models and reported substantially higher performance for deep learning models [52].

Similarly, Yang et al. proposed a combination of deep CNN and random forest ensemble learning for phishing website detection [21].

## 11. CNN-BASED DETECTION

CNNs can learn local patterns from sequential data.

A URL can be represented as a character sequence for URL detection. The CNN filters can then identify the local patterns associated with phishing URLs.

CNN-based models have been used independently and in hybrid architectures [21], [52], [53].

However, CNNs may not capture long-range dependencies as effectively as transformer architectures do.

## 12. LSTM AND SEQUENTIAL MODELS

URLs are sequential strings. Therefore, recurrent architectures, such as LSTMs, can be used to model the dependencies between characters or tokens.

CNN-LSTM combinations have also been investigated because CNNs can extract local patterns, whereas LSTMs can model sequential dependencies [52].

The main limitations of these methods include higher computational requirements and increased model complexity.

## 13. TRANSFORMER-BASED DETECTION

Transformers have recently become an important research direction for phishing detection.

Transformer-based models can capture the contextual relationships between tokens and characters.

BERT-based approaches have been investigated for phishing URL detection [28].

More advanced integrated architectures combine deep learning components with pretrained transformers [29], [54].

A recent study proposed an integrated model combining ResNet-based URL representation, temporal convolution, multi-head self-attention, and MPNet and evaluated the model across four datasets [54].

Another recent study proposed an automatic phishing website detection system using a transformer deep belief network [55].

In 2026, transformer-based contextual content features were further investigated for phishing URL detection, indicating a continued movement toward context-aware phishing classification [56].

## 14. FEATURE ENGINEERING

Feature engineering is an important aspect of phishing detection.

Features can be categorized as follows:

**Table 1: Features of Phishing Detection**

| **Category** | **Examples** |
|---|---|
| Lexical | URL length, digits, symbols |
| Structural | Subdomains, directories |
| Domain | Domain age, DNS |
| Security | HTTPS, SSL |
| HTML | Forms, iframes, hyperlinks |
| Behavioural | Redirections, scripts |
| Content | Text and semantic features |
| Visual | Images, logos, layout |

Recent systematic research indicates that URLs and lexical features continue to dominate because they are relatively simple and efficient, while hybrid and content-based features are increasingly investigated [43]. The same review highlights research opportunities involving explainable AI, cross-lingual features, adversarial resilience, and lightweight real-time solutions [43].

## 15. DATASET ANALYSIS

The dataset is one of the most important factors affecting the phishing detection performance.

Commonly used sources include

- UCI phishing datasets
- PhishTank
- Kaggle
- OpenPhish
- Mendeley datasets
- Custom datasets
- Threat-intelligence datasets

The PhiUSIIL project introduced a large phishing URL dataset containing 235,795 legitimate and phishing URLs [57].

Large datasets can support deep learning; however, dataset size alone does not guarantee quality.

The important dataset characteristics include:

- Sample diversity
- Class balance
- Data freshness
- Source reliability
- Feature completeness
- Duplicate removal

- Temporal distribution

## 16. DATASET IMBALANCE

Class imbalance occurs when the numbers of legitimate and phishing samples differ significantly.

For example, if 95% of the samples are legitimate, a model that always predicts “legitimate” may achieve 95% accuracy while completely failing to detect phishing.

Therefore, studies have investigated balancing approaches, such as the following:

- Oversampling
- Undersampling
- SMOTE
- Class weighting

A 2023 study specifically investigated SMOTE for phishing website detection and evaluated CatBoost, Random Forest, and XGBoost on a PhishTank-based dataset [58].

## 17. EVALUATION METRICS

The most commonly used evaluation metrics are as follows:

**Accuracy**

Accuracy= (TP+TN)/(TP+TN+FP+FN)

**Precision**

Precision= (TP)/(TP+FP)

**Recall**

Recall= (TP)/(TP+FN)

**F1-score**

F1= (2*Precision*Recall)/(Precision + Recall)

## 18. COMPARATIVE ANALYSIS OF THE LITERATURE

| Approach | Typical Features | Algorithms | Main Strength | Main Limitation |
|---|---|---|---|---|
| Blacklist | Known URLs | Database | Very fast | Cannot detect new URLs |
| Heuristic | URL/webpage rules | Rule engine | Simple | Easily bypassed |
| Visual Similarity | Screenshot/logo | Image similarity/DL | Detects imitation | Computationally expensive |
| Classical ML | URL/domain/HTML | SVM, DT, RF, LR | Efficient | Feature engineering |
| Ensemble ML | Engineered features | RF, XGBoost, GBM | Strong performance | More complex |
| Deep Learning | Raw URL/content | CNN, LSTM, DNN | Automatic learning | Data/computation |
| Transformer | URL/content | BERT, MPNet | Contextual representation | High computational cost |
| Hybrid | Multiple feature types | CNN + ML/Transformer | Rich representation | Complex deployment |
| XAI | ML/DL features | SHAP/LIME | Interpretability | Additional processing |

**Table 2: Comparative Analysis of the Literature**

**ROC-AUC**

The ROC-AUC measures the model's ability to discriminate between phishing and legitimate samples over different classification thresholds.

For cybersecurity applications, recall is particularly important because a false negative indicates that a phishing website may be incorrectly classified as legitimate.

## 19. CRITICAL ANALYSIS

### *19.1 Accuracy Is Dataset Dependent*

Different studies report different accuracy values for similar algorithms.

For example, Random Forest has been reported to perform strongly in multiple studies [15], [20], [49], whereas other studies have found boosting or deep-learning approaches to perform better [50], [52].

Therefore, it is inappropriate to conclude that one algorithm is the best.

### *19.2 Same-Dataset Testing Can Overestimate Performance*

Many studies randomly divide a dataset into training and testing subsets.

This can produce an optimistic performance when both subsets contain similar URL patterns.

### *19.3 Cross-Dataset Generalization*

Rashid et al. specifically demonstrated the generalization challenge of phishing URL detection [37].

This suggests that a model should ideally be evaluated on the following:

- Training dataset
- Independent dataset
- Recent dataset
- Previously unseen domains

### *19.4 Temporal Generalization*

Phishing attacks are rapidly changing. A model trained on historical data may lose its effectiveness as attacker strategies evolve.

Research using login URLs and datasets collected from different years demonstrated the degradation of model performance over time [19].

### *19.5 Manual Feature Engineering*

Traditional ML systems strongly depend on manually engineered features.

This may limit their ability to recognize previously unobserved attack patterns.

### *19.6 Computational Complexity*

Deep learning and transformer approaches may provide better representation learning but require more computational resources than other methods.

Therefore, lightweight models may remain attractive for real-time browser applications [15], [43].

## 20. EXPLAINABLE AI

A major emerging research direction is explainable AI (XAI).

Ideally, a phishing detection system should explain why a URL is classified as malicious.

Possible explanations include the following:

- Excessive URL length
- Suspicious keyword
- High number of subdomains
- Abnormal character distribution

- Suspicious domain properties
- Unusual webpage structure

Recent research has combined machine learning with XAI for phishing URL detection [59].

Explainability can be improved by

- User trust
- Security analyst interpretation
- Model debugging
- Feature validation
- Regulatory transparency

## 21. ADVERSARIAL ROBUSTNESS

Attackers may deliberately modify phishing URLs to deceive machine learning models.

Possible adversarial modifications include the following:

- Adding or removing characters
- Changing subdomains
- Replacing keywords
- Modifying webpage elements
- Changing HTML structures

Therefore, future systems should be tested using adversarial examples.

Recent research has proposed ranking ML models according to feature robustness, generalization, and adversarial resilience before combining them into an ensemble [51].

Visual-similarity approaches have also been investigated for their robustness against adversarial samples [46].

## 22. REAL-TIME PHISHING DETECTION

A practical phishing detection system should provide a decision before the user submits sensitive information.

Therefore, a real-time system should include the following:

- Low latency
- Low memory consumption
- High recall
- Low false-positive rate
- Continuous updating
- Robustness against new attacks

Recent research has moved toward web-based frameworks, browser-oriented systems, and real-time notification mechanisms [60].

A web-based ML framework has also been combined with URL classification, embedded-link analysis, and WHOIS-based validation [35].

## 23. MAJOR RESEARCH GAPS

Based on the reviewed literature, the following research gaps are identified.

**Gap 1: Dataset Dependency**

Many studies depend on a single dataset.

**Gap 2: Limited Cross-Dataset Validation**

Independent datasets are not always used for final evaluation.

**Gap 3: Temporal Generalization**

Fresh phishing domains are not consistently used for testing.

**Gap 4: Manual Feature Engineering**

Classical ML methods often depend on handcrafted features.

**Gap 5: Explainability**

Many high-performance models behave as black boxes.

**Gap 6: Adversarial Robustness**

Limited studies systematically test manipulated phishing URLs.

**Gap 7: Real-Time Deployment**

Many experiments remain offline.

**Gap 8: Computational Complexity**

Transformer and deep-learning models can be expensive for lightweight systems.

**Gap 9: Multilingual Phishing**

Multilingual and cross-lingual webpage content requires further investigation.

**Gap 10: Standardized Evaluation**

Differences in datasets and experimental methodologies make direct comparison difficult.

## 24. FUTURE RESEARCH DIRECTIONS

Future research should focus on:

1. Cross-dataset evaluation.
2. Temporal validation.
3. URL and webpage-content fusion.
4. Transformer-based contextual analysis.
5. Explainable AI.
6. Adversarially robust learning.
7. Lightweight deep-learning models.
8. Browser-extension deployment.
9. Continuous learning.
10. Multilingual phishing detection.
11. Privacy-preserving/federated learning.
12. Human-readable phishing risk scores.

## 25. PROPOSED FRAMEWORK

Based on the literature, the following generalized framework is proposed:

**URL / Webpage Input**

↓

**URL + Domain + HTML + Content Extraction**

↓

**Preprocessing**

↓

**Feature Engineering / Representation Learning**

↓

**Feature Selection**

↓

**ML / DL / Transformer Models**

↓

**Ensemble Decision Layer**

↓

**Explainable AI**

↓

**Phishing Risk Score**

↓

**Legitimate / Suspicious / Phishing**

This framework combines the efficiency of traditional machine learning with the representation-learning capabilities of deep learning and transformers.

## 26. DISCUSSION

The reviewed literature demonstrates that AI-based phishing detection has progressed from simple blacklist systems toward sophisticated machine-learning and deep-learning architectures.

Classical algorithms such as Random Forest, SVM and Decision Tree remain useful because of their comparatively lower computational requirements and good performance on structured feature datasets [13]–[20].

Ensemble models can improve predictive performance by combining multiple learners [20], [34], [51].

Deep-learning models reduce the need for manual feature engineering and can learn complex URL and webpage representations [21], [52], [53].

Transformer models provide a promising direction for contextual understanding of URL sequences and webpage content [28], [29], [54]–[56].

However, the most important finding of the literature review is that reported accuracy should not be considered independently of dataset and evaluation methodology.

For example, one study reported 94.5% accuracy for Random Forest [20], another reported 99% for an ML-based URL detector [50], while a CNN-LSTM study reported 98.1% accuracy and 98.7% F1-score [52]. These values cannot be directly compared because the datasets, features, preprocessing methods and experimental conditions are different.

The literature therefore suggests that future research should emphasize **robustness and generalization rather than accuracy alone**.

## 27. CONCLUSION

Phishing websites remain a major cybersecurity challenge because attackers continuously modify domains, URLs and webpage structures to deceive users. Machine Learning and Artificial Intelligence provide effective approaches for automatically identifying phishing websites using URL, domain, HTML, JavaScript, webpage-content and visual characteristics.

The review of 60 studies shows that classical machine-learning algorithms such as Random Forest, SVM, Decision Tree, Logistic Regression and boosting methods remain important because of their efficiency and effectiveness. Ensemble models provide improved classification capability, while deep-learning methods such as CNN and LSTM can automatically learn complex representations. Transformer-based approaches represent a newer research direction capable of learning contextual information from URLs and webpage content.

Nevertheless, high accuracy obtained on a particular dataset does not necessarily indicate strong real-world performance. Dataset dependency, temporal distribution changes, cross-dataset generalization, adversarial manipulation, feature engineering, explainability and computational complexity remain significant challenges.

Therefore, future phishing detection systems should move beyond simple accuracy-based evaluation and adopt cross-dataset validation, temporal testing, explainable AI, adversarial robustness and real-time deployment evaluation.

The overall direction of the literature suggests that a practical phishing detection system should combine machine learning, deep learning or transformer-based representation, robust feature engineering, explainability and continuous adaptation. Such systems can provide a stronger foundation for intelligent and reliable cybersecurity protection.

**ACKNOWLEDGMENT**

The completion of this research paper would not have been possible without the support and guidance of Mrs. S. P. Bomble, Faculty, Jaihind Institute of Research and Management, Kuran, Pune, Maharashtra and Management, Santiniketan, Birbhum, Jaihind Institute of Research and Management, Kuran, Pune, Maharashtra, India. Her dedication and overwhelming attitude towards helping us is solely responsible for completing our research paper. The encouragement and insightful feedback were instrumental in accomplishing this task.

**REFERENCES**

[1] A. K. Jain and B. B. Gupta, "Phishing Detection: Analysis of Visual Similarity Based Approaches," *Security and Communication Networks*, 2017, Article ID 5421046, doi: 10.1155/2017/5421046.

[2] E. Medvet, E. Kirda, and C. Kruegel, "Visual-Similarity-Based Phishing Detection," *Proceedings of SecureComm*, 2008, doi: 10.1145/1460877.1460905.

[3] W. Liu, G. Huang, X. Liu, M. Zhang, and X. Deng, "Detection of Phishing Webpages Based on Visual Similarity," *Proceedings of WWW*, 2005, pp. 1060–1061, doi: 10.1145/1062745.1062868.

[4] A. Safi and S. Singh, "A Systematic Literature Review on Phishing Website Detection Techniques," *Journal of King Saud University – Computer and Information Sciences*, vol. 35, no. 2, pp. 590–611, 2023, doi: 10.1016/j.jksuci.2023.01.004.

[5] G. Xiang, J. Hong, C. P. Rose, and L. Cranor, "CANTINA+: A Feature-Rich Machine Learning Framework for Detecting Phishing Web Sites," *ACM Transactions on Information and System Security*, vol. 14, no. 2, 2011, doi: 10.1145/2019599.2019606.

[6] S. Hutchinson, Z. Zhang, and Q. Liu, "Detecting Phishing Websites with Random Forest," *Machine Learning and Intelligent Communications*, 2018, doi: 10.1007/978-3-030-00557-3_46.

[7] J.-L. Chen, Y.-W. Ma, and K.-L. Huang, "Intelligent Visual Similarity-Based Phishing Websites Detection," *Symmetry*, vol. 12, no. 10, 1681, 2020, doi: 10.3390/sym12101681.

[8] "Visual Similarity Based Anti-phishing with the Combination of Local and Global Features," *IEEE TrustCom*, 2014, doi: 10.1109/TrustCom.2014.28.

[9] A. K. Jain and B. B. Gupta, "Phishing Detection: Analysis of Visual Similarity Based Approaches," *Security and Communication Networks*, 2017, doi: 10.1155/2017/5421046.

[10] M. Wang, L. Song, L. Li, Y. Zhu, and J. Li, "Phishing Webpage Detection Based on Global and Local Visual Similarity," *Expert Systems with Applications*, vol. 252, 124120, 2024, doi: 10.1016/j.eswa.2024.124120.

[11] G. Xiang, J. Hong, C. P. Rose, and L. Cranor, "CANTINA+: A Feature-Rich Machine Learning Framework for Detecting Phishing Web Sites," *ACM TISSEC*, 2011, doi: 10.1145/2019599.2019606.

[12] "Survey on Detection and Prevention of Phishing Websites Using Machine Learning," *IEEE ICACITE*, 2021, doi: 10.1109/ICACITE51222.2021.9404714.

[13] "Phishing Website Detection Using Random Forest and Support Vector Machine: A Comparison," *IEEE AiDAS*, 2021, doi: 10.1109/AiDAS53897.2021.9574282.

[14] "URL Phishing Detection Using Machine Learning Techniques Based on URLs Lexical Analysis," *IEEE ICICS*, 2021, doi: 10.1109/ICICS52457.2021.9464539.

[15] A. Al-Alyan and S. Al-Ahmadi, "Robust URL Phishing Detection Based on Deep Learning," *KSII Transactions on Internet and Information Systems*, vol. 14, no. 7, 2020, doi: 10.3837/tiis.2020.07.001.

[16] "Malicious URL Detection Using NLP, Machine Learning and FLASK," *IEEE ICSES*, 2021, doi: 10.1109/ICSES52305.2021.9633889.

[17] "A Comparative Analysis of Machine Learning-Based Website Phishing Detection Using URL Information," *IEEE PRAI*, 2022, doi: 10.1109/PRAI55851.2022.9904055.

[18] "Phishing Website Detection Using Machine Learning Methods," *IEEE ICIICS*, 2023, doi: 10.1109/ICIICS59993.2023.10420933.

[19] "Phishing URL Detection: A Real-Case Scenario Through Login URLs," *IEEE Access*, vol. 10, pp. 42949–42960, 2022, doi: 10.1109/ACCESS.2022.3168681.

[20] "Phishing URL Detection Using Machine Learning: A Comparative Study," *IEEE ICMCSI*, 2025, doi: 10.1109/ICMCSI64620.2025.10883082.

[21] R. Yang et al., "Phishing Website Detection Based on Deep Convolutional Neural Network and Random Forest Ensemble Learning," *Sensors*, vol. 21, no. 24, 8281, 2021, doi: 10.3390/s21248281.

[22] "Phishing Website Detection Using Machine Learning with URL Analysis," *IEEE AIC*, 2022, doi: 10.1109/AIC55036.2022.9848895.

[23] "Phishing Website Detection Using LGBM Classifier With URL-Based Lexical Features," *IEEE SILCON*, 2022, doi: 10.1109/SILCON55242.2022.10028793.

[24] M. Selvakumari, M. Sowjanya, S. Das, and S. Padmavathi, "Phishing Website Detection Using Machine Learning and Deep Learning Techniques," *Journal of Physics: Conference Series*, vol. 1916, 012169, 2021, doi: 10.1088/1742-6596/1916/1/012169.

[25] Y. Mourtaji et al., "Hybrid Rule-Based Solution for Phishing URL Detection Using Convolutional Neural Network," *Wireless Communications and Mobile Computing*, 2021, Article ID 8241104, doi: 10.1155/2021/8241104.

[26] "Phishing Website Detection: How Effective Are Deep Learning-Based Models and Hyperparameter Optimization?" *Security and Privacy*, 2022, doi: 10.1002/spy2.256.

[27] J. K. Joshma and V. Sankar P, "Phishing Website Detection," *Indian Journal of Data Mining*, 2024, doi: 10.54105/ijdm.A1642.04010524.

[28] "Intelligent Deep Machine Learning Cyber Phishing URL Detection Based on BERT Features Extraction," *Electronics*, vol. 11, no. 22, 3647, 2022, doi: 10.3390/electronics11223647.

[29] "Detecting Phishing URLs Using the BERT Transformer Model," *IEEE BigData*, 2023, doi: 10.1109/BigData59044.2023.10386782.

[30] "PhishTransformer: A Novel Approach to Detect Phishing Attacks Using URL Collection and Transformer," *Electronics*, vol. 13, no. 1, 30, 2024, doi: 10.3390/electronics13010030.

[31] "Automatic Phishing Website Detection and Prevention Model Using Transformer Deep Belief Network," *Computers & Security*, vol. 147, 104071, 2024, doi: 10.1016/j.cose.2024.104071.

[32] M. Bahaghighat, M. Ghasemi, and F. Özen, "A High-Accuracy Phishing Website Detection Method Based on Machine Learning," *Journal of Information Security and Applications*, vol. 77, 103553, 2023, doi: 10.1016/j.jisa.2023.103553.

[33] A. Chawla, "Phishing Website Analysis and Detection Using Machine Learning," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 10, no. 1, pp. 10–16, 2022, doi: 10.18201/ijisae.2022.262.

[34] "Phishing Attacks Detection Using Ensemble Machine Learning Algorithms," *Computers, Materials & Continua*, vol. 80, no. 1, pp. 1325–1345, 2024, doi: 10.32604/cmc.2024.051778.

[35] R. Choutapally and T. Das, "Web-Based Machine Learning Framework for Phishing URL Detection and Analysis," *IEEE Conference on Artificial Intelligence*, 2025, doi: 10.1109/CAI64502.2025.00170.

[36] "Website Phishing Detection of Machine Learning Approach Using SMOTE Method," *IEEE ICECCT*, 2023, doi: 10.1109/ICECCT56650.2023.10179745.

[37] F. Rashid, B. Doyle, S. C. Han, and S. Seneviratne, "Phishing URL Detection Generalisation Using Unsupervised Domain Adaptation," *Computer Networks*, vol. 245, 110398, 2024, doi: 10.1016/j.comnet.2024.110398.

[38] "Phishing or Not Phishing? A Survey on the Detection of Phishing Websites," *IEEE Access*, vol. 11, pp. 18499–18519, 2023, doi: 10.1109/ACCESS.2023.3247135.

[39] C. Catal, G. Giray, B. Tekinerdogan, S. Kumar, and S. Shukla, "Applications of Deep Learning for Phishing Detection: A Systematic Literature Review," *Knowledge and Information Systems*, vol. 64, pp. 1457–1500, 2022, doi: 10.1007/s10115-022-01672-x.

[40] S. Safi and S. Singh, "A Systematic Literature Review on Phishing Website Detection Techniques," *Journal of King Saud University – Computer and Information Sciences*, 2023, doi: 10.1016/j.jksuci.2023.01.004.

[41] S. Kavya and D. Sumathi, "Staying Ahead of Phishers: A Review of Recent Advances and Emerging Methodologies in Phishing Detection," *Artificial Intelligence Review*, vol. 58, article 50, 2025, doi: 10.1007/s10462-024-11055-z.

[42] J. Islam, C. Patra, P. K. Mani, S. Biswas, D. Giri, and T. Maitra, "Phishing URL Detection via Machine Learning: A Comprehensive Survey," *Lecture Notes in Networks and Systems*, vol. 1405, 2025, doi: 10.1007/978-981-96-6348-4_12.

[43] Y. A. Kustiawan and K. I. Ghauth, "Feature Engineering for Phishing Website Detection Using Machine Learning: A Systematic Review," *IEEE Access*, vol. 13, pp. 192080–192104, 2025, doi: 10.1109/ACCESS.2025.3630334.

[44] D. Popescul and L. D. Radu, "AI in Phishing Detection: A Bibliometric Review," *Frontiers in Artificial Intelligence*, vol. 8, 1496580, 2025, doi: 10.3389/frai.2025.1496580.

[45] F. L. Santa Cruz-Rufasto and C. A. Dios-Castillo, "Diagnosing the Performance of Machine Learning Models for Phishing Website Detection: A Literature Review," *LACCEI*, 2025, doi: 10.18687/LACCEI2025.1.1.274.

[46] M. Wang, L. Song, L. Li, Y. Zhu, and J. Li, "Phishing Webpage Detection Based on Global and Local Visual Similarity," *Expert Systems with Applications*, vol. 252, 124120, 2024, doi: 10.1016/j.eswa.2024.124120.

[47] S. Guptta, K. T. Shahriar, H. Alqahtani, D. Alsalman, and I. H. Sarker, "Modeling Hybrid Feature-Based Phishing Websites Detection Using Machine Learning Techniques," *Annals of Data Science*, vol. 11, 2024, doi: 10.1007/s40745-022-00379-8.

[48] S. Anupam and A. K. Kar, "Phishing Website Detection Using Support Vector Machines and Nature-Inspired Optimization Algorithms," *Telecommunication Systems*, vol. 76, 2021, doi: 10.1007/s11235-020-00739-w.

[49] "Machine Learning Based Phishing Website Detection," *IEEE INDIACom*, 2024, doi: 10.23919/INDIACom61295.2024.10498854.

[50] "Advanced Learning for Phishing URLs Detection to Secure Consumer-Centric Applications," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 3, pp. 5756–5763, 2024, doi: 10.1109/TCE.2024.3404459.

[51] "An Optimized Machine Learning Framework for Phishing Website Detection Integrating Feature Robustness and Adversarial Resilience Ranking," *IEEE ICPCSN*, 2025, doi: 10.1109/ICPCSN65854.2025.11035371.

[52] "Phishing URL Detection Using Machine Learning and Deep Learning," *IEEE World AI IoT Congress*, 2024, doi: 10.1109/AIIoT61789.2024.10579005.

[53] K. Barik, S. Misra, and R. Mohan, "Web-Based Phishing URL Detection Model Using Deep Learning Optimization Techniques," *International Journal of Data Science and Analytics*, vol. 20, pp. 4449–4471, 2025, doi: 10.1007/s41060-025-00728-9.

[54] "An Integrated Model Based on Deep Learning Classifiers and Pre-Trained Transformer for Phishing URL Detection," *Future Generation Computer Systems*, vol. 161, pp. 269–285, 2024, doi: 10.1016/j.future.2024.06.031.

[55] "Automatic Phishing Website Detection and Prevention Model Using Transformer Deep Belief Network," *Computers & Security*, vol. 147, 104071, 2024, doi: 10.1016/j.cose.2024.104071.

[56] "Phishing URL Detection Using Transformer-Based Architecture and Contextual Content Features," *Computers*, vol. 15, no. 6, 335, 2026, doi: 10.3390/computers15060335.

[57] "PhiUSIIL: A Diverse Security Profile Empowered Phishing URL Detection Framework Based on Similarity Index and Incremental Learning," *Computers & Security*, vol. 136, 103545, 2024, doi: 10.1016/j.cose.2023.103545.

[58] "Website Phishing Detection of Machine Learning Approach Using SMOTE Method," *IEEE ICECCT*, 2023, doi: 10.1109/ICECCT56650.2023.10179745.

[59] "Enhancing Online Safety: Phishing URL Detection Using Machine Learning and Explainable AI," *IEEE ICCCNT*, 2024, doi: 10.1109/ICCCNT61001.2024.10723976.

[60] "Phishing Website Detection Using Machine Learning and Real-Time Email Notification System," *IEEE ICSSAS*, 2025, doi: 10.1109/ICSSAS66150.2025.11081299.