# A Comparative Analysis of Phishing Detection Techniques: Exploring Strengths, Weaknesses, and Research Gaps

**Ashvini Jadhav**[1]
MIT School of Computing, MIT Art Design and Technology University,
Loni, Pune, India ashvinigjadhav@ gmail.com

**Pankaj Chandre**[2]
MIT School of Computing, MIT Art Design and Technology University,
Loni, Pune, India pankajchandre30@gmail.com

## Abstract

Phishing attacks remain a significant threat in the digital landscape, causing financial losses, data breaches, and eroding user trust. This paper presents a comprehensive analysis of existing phishing detection techniques, categorized by their core functionalities: list-based, visual similarity, heuristic, machine learning, and deep learning. We evaluate the effectiveness, strengths, and limitations of each approach, drawing insights from recent research. Additionally, the paper explores potential research gaps in the field, highlighting areas for future investigation to enhance phishing detection capabilities and stay ahead of evolving threats .The analysis reveals the promising potential of machine learning for accurate and scalable phishing detection. However, challenges such as data dependence, computational cost, and the need for continuous adaptation remain. By identifying these gaps and exploring advanced techniques like deep learning and user behavior analysis, researchers can contribute to a more robust and user-friendly defense against phishing attacks.

**Keywords**
Automatic, Lists-Based, Visual Similarity, Heuristic, Machine Learning, Deep Learning, URL-based detection, content-based detection, reputation-based detection, behavioral-based detection, SMTP Envelope

## 1. INTRODUCTION

1. Introduction

1.1 Background Phishing attacks, characterized by fraudulent attempts to obtain sensitive information, continue to proliferate, posing serious risks to individuals and organizations. Detecting and mitigating these attacks is crucial for safeguarding digital assets and maintaining trust in online communications.

1.2 Scope of the Study This systematic literature review (SLR) aims to comprehensively analyze existing phishing detection techniques, covering a broad spectrum of methodologies and approaches employed in recent research. The study provides insights into the evolution of phishing threats and the corresponding advancements in detection strategies.

1.3 Objectives The primary objectives of this SLR are to:

- Identify and categorize phishing detection techniques described in recent scholarly literature.
- Evaluate the effectiveness, strengths, and limitations of different detection approaches.
- Synthesize key findings to inform the development of robust cyber security measures against phishing attacks

## 2. LITERATURE SURVEY

(Geng et al., 2018) focused on analyzing a website's resource request patterns, but it could only detect phishing attempts mimicking a specific brand. Other studies explored combining machine learning with various techniques: Awan et al. (2019) achieved high accuracy using a hybrid approach with a genetic algorithm, but it relied on excluding the original URL which might limit effectiveness. Similarly, Stobbs et al. (2020) achieved high accuracy with random forests, but faced limitations in dataset size and computational cost. Deep learning approaches (Wei et al., 2020) also showed promise but suffered from similar limitations regarding data and research scope.

Another approach combined visual similarity with a DNS blacklist for real-time detection (Nathezhtha et al., 2020), achieving good results but with a limited dataset. Lexical-based machine learning techniques (Gupta et al., 2021) were successful in detecting websites mimicking legitimate ones, but require ongoing development to stay ahead of evolving threats. Website fraud detection systems have proven valuable in combating online threats. However, there's always space for improvement. This analysis explores the current workflow and identifies potential areas for enhancement.

Website fraud detection systems have proven valuable in combating online threats. However, there's always space for improvement. This analysis explores the current workflow and identifies potential areas for enhancement.

**Common Workflow:**

Our research revealed a common workflow across various fraud detection systems, with some minor variations:

1. **Machine Learning for Website Classification:** Training machine learning models allows for real-time website classification based on extracted features. This can be applied to individual user visits or large-scale website analyses, as highlighted in the paper by Mr. Annappa Swamy et al. (2023).

2. **Feature Engineering and URL-Content Analysis:** Several studies explored feature engineering techniques. For instance, the work by AliAljofey et al. (2022) introduced eight new features analyzing the relationship between a webpage's URL and its content, leading to significant accuracy improvements.

3. **Automated Approaches with Feature Engineering:** Research suggests that automated approaches with feature engineering outperform traditional methods in detecting phishing websites. Md Sajadul Islam et al. (2023) demonstrated this by using feature engineering to identify malicious URLs and applying machine learning algorithms for training. Their method achieved high accuracy, emphasizing the importance of feature engineering.
4. **Ensemble Learning for Enhanced Accuracy:** Hesham Abusaimeh and Yusra Alshareef (2021) proposed a method combining multiple machine learning algorithms (decision tree, random forest, and SVM) into a single model. This "ensemble learning" approach aims to achieve superior accuracy in phishing website detection.
5. **Addressing False Positives:** While not directly related to the core workflow, the 2013 paper by Hetal Rahul Rajpura and Hiteishi Diwanji highlights the importance of reducing false positives in Decision Tree algorithms used for fraud detection. Their work suggests using feature selection and filtering techniques to achieve this.

**Room for Improvement:**

Despite the success of these systems, there's potential for improvement in user experience and streamlining operations:

- **User Experience:** Fraud detection systems should be designed with a user-centric approach, minimizing disruptions and maintaining a smooth browsing experience.
- **Streamlined Operations:** Optimizing system efficiency and minimizing processing time for fraud checks can further enhance user experience.

By addressing these areas and leveraging the strengths of existing techniques, website fraud detection can become even more robust and user-friendly.

**SWOT of a phishing detection model:**

**Strengths:**

- **Accuracy:** A well-designed model can identify phishing attempts with high accuracy, protecting users from malicious emails.
- **Automation:** Automating phishing detection frees up human resources for other tasks and provides 24/7 protection.
- **Scalability:** Phishing models can be trained on massive datasets, allowing them to adapt to new phishing tactics and maintain effectiveness as email volume grows.
- **Customization:** Models can be tailored to specific user needs and industries, focusing on the types of phishing attempts most relevant to a particular group.

**Weaknesses:**

- **False Positives:** Like any detection system, models can incorrectly flag legitimate emails as phishing, leading to user frustration and wasted time investigating false alarms.
- **Evolving Threats:** Phishing techniques constantly evolve. Models need to be updated regularly to stay effective against new tactics.
- **Data Dependence:** Model performance relies on the quality and quantity of training data. Insufficient or biased data can lead to inaccuracies.
- **Computational Cost:** Training and running complex models can require significant computing power, potentially posing a challenge for resource-constrained organizations.

**Opportunities:**

- **Machine Learning Advancements:** Improvements in machine learning algorithms can lead to even more accurate and robust phishing detection models.
- **Integration with Email Platforms:** Direct integration with email platforms can streamline the detection and filtering process, making it seamless for users.
- **User Education:** Combining phishing detection models with user education can create a layered defense, enhancing overall security awareness.
- **Collaboration:** Sharing threat intelligence across organizations can help identify emerging phishing tactics and improve model effectiveness for everyone.

**Threats:**

- **Zero-Day Attacks:** New, unseen phishing tactics can bypass even the most advanced models until they are updated with new data.
- **Social Engineering Techniques:** Phishing attacks that rely on social manipulation and psychological pressure can be harder to detect with purely technical models.

- **Privacy Concerns:** Collecting user data for model training raises privacy concerns that need to be addressed with ethical data practices and strong data governance.

## 3. MOTIVATION

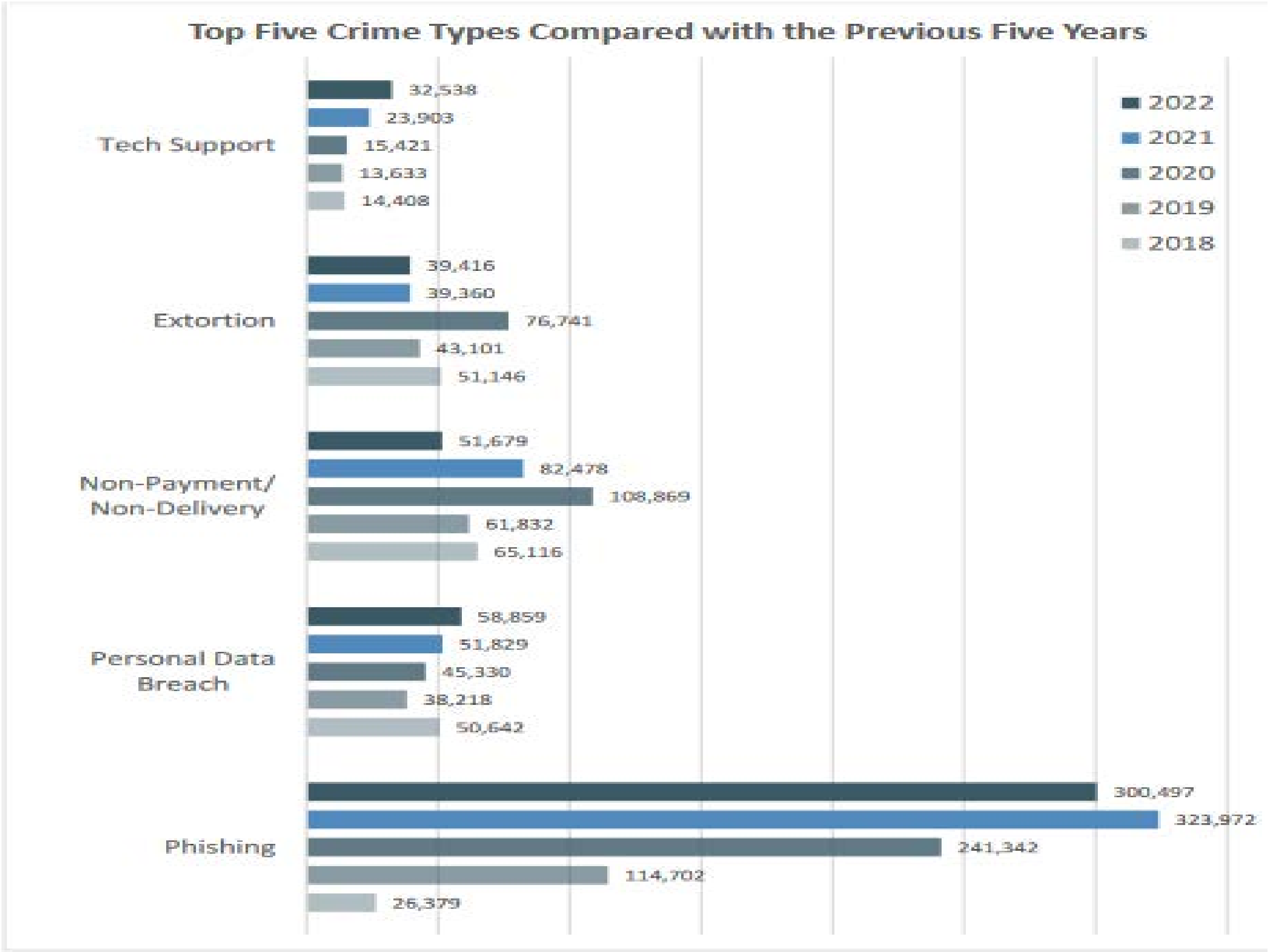
The motivation for research in phishing detection is driven by the ever-growing threat of cybercrime, as highlighted by the concerning statistics from the Internet Crime Complaint Center (IC3). Here's a breakdown of the key motivators:

- **Escalating Cybercrime:** The significant rise in cybercrime complaints reported to the FBI (over 300,000 more in 2020 compared to the previous year) demonstrates the urgency of developing better defenses. Phishing attacks are a major component of cybercrime, making effective detection crucial.
- **Financial Losses:** Phishing attacks often aim to steal financial information or redirect users to fraudulent websites, resulting in significant financial losses for individuals and businesses. Research in detection helps prevent these attacks and protects financial security.
- **Adversarial Attacks:** Sophisticated attackers might develop techniques to manipulate or trick phishing detection models.
- **Data Breaches:** Phishing emails can be used to trick users into revealing sensitive information or clicking malicious links that compromise their data. Effective detection techniques can help prevent data breaches and protect user privacy.
- **Evolving Threats:** Phishing tactics are constantly evolving, with attackers becoming more sophisticated in their methods. Research is necessary to stay ahead of these advancements and develop robust detection mechanisms that can identify even novel phishing attempts.
- **Protecting Users:** Ultimately, research in phishing detection aims to create a safer online environment for everyone. By developing accurate and efficient detection techniques, users can be better protected from falling victim to phishing scams.

In essence, the alarming rise in cybercrime, particularly phishing attacks, necessitates continuous research to safeguard individuals, businesses, and the overall security of the digital landscape.

## 4. STATISTICS

## TOP FIVE CRIME TYPE COMPARISON[4]



Ref. Markets Research Future

| Sr no | Criteria | V7Encase Forensic | FTK | MailXamine V4 | eMailTrackerPro V10 | Autopsy | Paraben EMX V8.6.5277 | Aid4Mail v3.8 |
|---|---|---|---|---|---|---|---|---|
| 1 | Language Interface | English | English | English | English | English | English | Chinese, English |
| 2 | User Interface | Requires training | Requires training | Easy to use | Easy to use | Easy to use | Easy to use | Easy to use |
| 3 | Programming Language | Python | Java | Not specified | Python | Java | Java | Java |
| 4 | Creation of Image File | Supports | Supports | Not specified | Not specified | Supports | Supports | Supports |
| 5 | Calculation of Hash Value | MD5 & SHA | MD5, SHA-1 | | MD5 | MD5 | MD5 | Supports |
| 6 | Cost | Expensive | Expensive | Open Source | Expensive | Free | Open Source | Expensive |
| 7 | Regular Expressions | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 8 | Header Analysis Tools | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 9 | Natural Language Processing (NLP) | ✓ | ✓ | ✓ | | | | |
| 10 | Clustering Algorithms | ✓ | ✓ | ✓ | | | | |
| 11 | Machine Learning (ML) | ✓ | ✓ | ✓ | | | | |
| 12 | Network Packet Capture | ✓ | ✓ | ✓ | | | | |
| 13 | NetworkMiner (PCAP Analysis) | ✓ | ✓ | ✓ | | | | |

Table 1 Comparison of email forensics tools and techniques.

**Research Gap**

| Category | Research Gap | Explore points for research |
|---|---|---|
| Understanding Phishing Techniques | Advanced Phishing Techniques | - Analyze impact of spear phishing, vishing, smishing on different user groups |
| | | - Investigate AI-driven phishing using machine learning for personalization |
| | | - Explore how the Internet of Things (IoT) can be exploited for phishing |
| Human Factors and Social Engineering | Behavioral Analysis and User Education | - Study user behavior in phishing attacks to identify patterns and improve education programs |
| | | - Understand why individuals fall victim and how to enhance their resistance |
| | Analysis of Social Engineering Tactics | - Conduct detailed analysis of social engineering techniques and psychological aspects |
| | | - Inform targeted prevention strategies based on social engineering tactics |
| | Cross-Cultural Analysis of Phishing Perception | - Explore cultural factors influencing how people perceive and respond to phishing attempts |
| | | - Develop culturally sensitive anti-phishing strategies |
| Technological Advancements and Phishing | Impact of Deepfakes on Phishing | - Understand how deep fakes may be used to deceive individuals and develop countermeasures |
| | Machine Learning for Phishing Detection | - Research more sophisticated machine learning algorithms for faster and more accurate phishing detection |

| | | |
|---|---|---|
| | | - Consider the dynamic nature of phishing campaigns |
| | Zero-Day Exploits and Vulnerabilities | - Focus on identifying and patching vulnerabilities in software before exploitation |
| | Cryptographic and Authentication Protocols | - Improve cryptographic methods and authentication protocols for secure online communication |
| | | - Hinder phishers from intercepting or manipulating sensitive information |
| | Deep Learning-Enhanced Phishing Attacks | - Examine how deep learning techniques can be integrated into phishing attacks |
| | | - Analyze use of generative models for convincing content or adversarial machine learning to bypass security defenses |
| Emerging Phishing Threats | Cross-Platform Phishing | - Investigate how phishing attacks adapt to target users across various platforms (mobile, IoT) |
| | | - Improve security measures in diverse environments |
| | Context-Aware Phishing | - Analyze how phishers use contextual information (location, time, user behavior) to tailor attacks |
| | | - Understand and mitigate context-aware phishing techniques |
| | Voice Cloning in Vishing Attacks | - Research the feasibility of voice cloning in vishing scenarios |
| | | - Develop countermeasures to detect and prevent voice cloning vishing attacks |
| | Augmented Reality (AR) Phishing | - Explore the potential for phishing attacks in AR environments |
| | Cryptocurrency-Related Phishing | - Understand how attackers might exploit AR to deceive users and develop defenses against AR-based phishing |
| | | - Investigate how phishing attacks exploit the popularity of cryptocurrencies |
| | | - Analyze scams related to fake wallets, ICOs, or fraudulent investment schemes |
| | | - Develop preventive measures in the cryptocurrency space |
| | Blockchain Manipulation in Phishing | - Explore how attackers might leverage blockchain technology for deceptive purposes |
| | | - Analyze potential manipulation of transactions or exploitation of trust in blockchain-based authentication systems |
| Response and Mitigation Strategies | Dynamic Threat Intelligence Sharing | - Research and develop dynamic, automated systems for real-time threat intelligence sharing across organizations and sectors |
| | Usability of Security Solutions | - Evaluate the user-friendliness of anti-phishing tools |
| | | - Explore how design and implementation impact effectiveness of security solutions |
| | Human Factors in Incident Response | - Understand human factors involved in incident response to phishing attacks |
| | | - Explore decision-making processes and propose strategies to improve response effectiveness |
| | Impact of Psychological Trauma | - Explore the long-term psychological impact of successful phishing attacks on victims |
| | | - Analyze anxiety, stress, and loss of trust in online communication |
| | | - Inform support mechanisms and recovery strategies |
| | Ethical Hacking for Phishing Resilience | - Investigate the effectiveness of ethical hacking as a means to assess and improve an organization's resilience against phishing attacks |
| | | - Understand how ethical hacking can simulate real-world scenarios and identify vulnerabilities |

| | | |
|---|---|---|
| Economic Impact and Legal Issues | Quantitative Analysis of Economic Losses | - Develop models to estimate the economic impact of successful phishing attacks on individuals, businesses, and economies over the long term |
| | Legal and Regulatory Approaches | - Analyze existing legal frameworks and explore potential regulatory changes to deter phishing and hold attackers accountable |

Table2 Research Gap

| Sr no | **Authors** | **Year** | **Method Used/Techniques/Technology** | **Outcome** | **Limitation** |
|---|---|---|---|---|---|
| 1 | G.G. Geng et al. | 2018 | Pattern analysis | Website resource request pattern analysis | Only detects phishing mimicking a specific brand. |
| 2 | Awan, I., et al., & Heuristic "Iterative Dichotomiser-3 | 2019 | K-Nearest Neighbor, Decision tree, Random Forest, Genetic Algorithms | High accuracy with ID3 and Yet Another Generating Genetic Algorithm (YAGGA). | Relies on normalized features and excludes the original URL. |
| 3 | Stobbs, S.E., et al. | 2020 | Random Forest | Achieved 99.33% accuracy. | Limited dataset size and computational cost. |
| 4 | Wei, W., et al. | 2020 | Artificial neural networks | High accuracy. | Limited research and data size. |
| 5 | Nathezhtha, S.N., et al., | 2020 | Visual Similarity & DNS blacklist | Achieved 96.17% accuracy. | Limited dataset size (200 websites). |
| 6 | D.J. Liu et al. | 2021 | List-Based, Multistage detection with Content, Anchor, Style, and Environment (CASE) features | Efficient detection of known fraudulent websites. | Vulnerable to evasion tactics employed by sophisticated fraudsters. |
| 7 | Gupta, B.B., et al | 2021 | Detect phishing URLs in real-time, Lexical-based machine learning | Can detect websites mimicking legitimate ones. | Requires ongoing research and development to address evolving threats and improve accuracy. |
| 8 | Hidayat et al., | 2021 | Fuzzy set technique | Visual Similarity | Various (SVM, Decision Tree, Neural Network) |
| 9 | Barraclough et al | 2021 | PART algorithm | List-Based | Various (including Machine Learning in some studies) |
| 10 | C. Rajeswary, et al. | 2023 | Surveys automated phishing detection techniques | Provides insights into performance of ML techniques | Requires further research to improve accuracy. |

Table 3 Comparison Literature Analysis

## 5. GENERAL WORKING:

5.1 Initial Screening (Steps 1-5):

1. Blacklist Check: Compare email and URL against frequently updated blacklists to eliminate known phishing emails and URLs efficiently.
2. Whitelist Check: Prioritize emails from trusted senders or domains if a whitelist is available to reduce false positives.
3. Sender Information Analysis: a. Validate sender email address syntax for proper formatting. b. Check sender domain reputation using third-party services to identify suspicious domains. c. Compare the sender name with expected names for known contacts to detect spoofing attempts.
4. URL Link Analysis: a. Extract the domain name from the URL to analyze the destination. b. Verify the domain name against blacklists to identify potentially malicious URLs.
5. Basic Header Inspection: a. Look for inconsistencies in email headers, such as mismatch between sender name and email address. b. If feasible, perform sender IP validation against known phishing source IPs.

5.2 Feature Extraction and Analysis (6-15)

Content Analysis: 6 a. Extract textual content from the email body, excluding attachments. b. Apply text normalization techniques, such as lowercase conversion and punctuation removal. c. Identify common phishing indicators in the content, such as urgent requests or suspicious links. 7. Subject Line Analysis: a. Extract the subject line and analyze for patterns commonly used in phishing attempts. 8. Attachment Analysis: a. Extract attachment details, including file names, extensions, and sizes. b. Check for common phishing attachment types, such as executable or compressed files. c. Validate attachment file types to detect inconsistencies. 9. Visual Feature Extraction (Website-Specific): a. Capture screenshots or render the website's HTML/CSS to extract visual features, such as layout and logos. 10. Link Feature Extraction (Website-Specific): a. Extract internal website links and analyze their structure for suspicious patterns, such as URL shortness or typo squatting.

5.3 Machine Learning Model Scoring with Deep Learning (Steps 11-15): 11. Preprocess All Extracted Features: a. Apply appropriate scaling or normalization techniques to prepare features for deep learning models. b. Consider techniques like word embedding to represent textual content numerically. 12. Deep Learning Model Selection and Training (Optional): a. Choose a suitable deep learning architecture for the task, such as LSTM or RNN/CNN. b. Train the model on a large dataset of labeled phishing and legitimate emails/websites. c. Use techniques like regularization to prevent overfitting. 13. Hybrid Model Integration (Optional): a. Combine deep learning with other machine learning algorithms for improved performance. 14. Ensemble Classification: a. Combine results from various detection techniques using techniques like weighted averaging or voting. b. Assign a final risk score based on the combined evidence. 15. Advanced Feature Engineering (Optional): a. Explore advanced feature engineering techniques to create new features from existing ones, such as n-grams or part-of-speech analysis.

5.4 Advanced Analysis and Decision-Making (Steps 16-20): 16. Reputation-Based Scoring: a. Check the sender's domain reputation using third-party services. b. Assign a reputation score based on historical phishing activity associated with the domain. 17. Geographical Analysis: a. Consider the sender's IP location to detect anomalies or suspicious activity. b. Use geo location data to enhance the phishing detection process.

## 6. CONCLUSION

In conclusion, phishing attacks persist as a formidable threat in today's digital landscape, posing significant risks to individuals, organizations, and society as a whole. This paper has thoroughly examined existing phishing detection techniques, classifying them into distinct categories based on their underlying functionalities: list-based, visual similarity, heuristic, machine learning, and deep learning. Through our analysis, we have evaluated the efficacy, advantages, and limitations of each approach, drawing valuable insights from recent research endeavors. Moreover, this study has shed light on potential research gaps within the domain, pinpointing areas that warrant further investigation to bolster phishing detection capabilities and effectively counter evolving threats.Our findings underscore the promising potential of machine learning techniques in facilitating accurate and scalable phishing detection. However, it is essential to acknowledge and address challenges such as data dependency, computational complexity, and the necessity for continual adaptation to evolving tactics employed by malicious actors. Looking ahead, researchers are encouraged to explore advanced methodologies such as deep learning and user behavior analysis to fortify the defense against phishing attacks further. By identifying and bridging these gaps in knowledge and technology, we can collectively advance the development of more robust, adaptive, and user-friendly solutions for combating phishing threats. In summary, this comprehensive analysis serves as a foundational framework for enhancing our understanding of phishing detection methodologies and informs future research endeavors aimed at mitigating the risks posed by phishing attacks in an increasingly interconnected digital ecosystem.

## 7. REFERENCES

**[1]** An anti-phishing approach based on website resource request pattern analysis (2018) by Geng, G.G., et al.

**[2]** A hybrid approach for phishing website detection using machine learning and genetic algorithm (2019) by Awan, I., et al. link: https://link.springer.com/article/10.1007/s40745-022-00379-8

**[3]** A machine learning approach for phishing detection using random forests (2020) by Stobbs, S.E., et al. link: https://ieeexplore.ieee.org/document/9574282

**[4]** Phishing website detection based on deep learning (2020) by Wei, W., et al. link: https://ieeexplore.ieee.org/document/9661323

**[5]** A hybrid approach for real-time phishing website detection using visual similarity and DNS blacklist (2020) by Nathezhtha, S.N., et alFake website detection using Machine Learning (2021) by Liu, D.J., et al.

**[6]** A new approach to detect phishing URLs in real time using lexical-based machine learning techniques (2021) by Gupta, B.B., et al

**[7]** **Survey on Automated Phishing Detection Techniques: A Machine Learning Perspective** (2023) by Rajeswary, C., et al.

**[8]** Wang, J., & Zhang, X. (2020). Website Fraud Detection Based on Gradient Boosting Decision Tree Algorithm.

**[9]** Almahdi, R., Alghazzawi, D., & Al-Azzawi, H. (2020). Detecting Fake Websites using Machine Learning. International Journal of Advanced Computer Science and Applications.

**[10]** Roy, A., & Ramanathan, R. (2019). Detecting Phishing Websites using Machine Learning Techniques. International Journal of Advanced Computer Science and Applications.

**[11]** Chandrasekhar, A., Jain, A., & Sundararajan, R. (2018). Detecting Phishing Websites using Machine Learning.

**[12]** Dursun, M., & Catak, F. (2020). Detection of Phishing Websites with Machine Learning Techniques. Journal of Polytechnic.

**[13]** Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing attacks and defenses. International Journal of Security and Its Applications.

**[14]** Khan, A. & Sharma R.,(2018). A Survey Paper on Detection of Phishing Website by URL Technique. International Journal of Computer Science and Mobile Applications.

**[15]** Sakunthala R. & Shankar S.,(2018). Various Methods for Phishing Detection. EAI Endorsed Transactions on Energy Web and Information Technologies.

**[16]** Santhana Lakshmi V, Vijaya MS, Efficient prediction of phishing websites using supervised learning algorithms, International Conference on Communication Technology and System Design, 2011.

**[17]** A. Basit, M. Zafar, A. R. Javed and Z. Jalil, “A Novel Ensemble Machine Learning Method to Detect Phishing Attack”, 2020 IEEE 23rd International Multitopic Conference (INMIC), 2020