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

THE PHISH FINDER: A REAL-TIME PHISHING DETECTION SYSTEM WITH BROWSER ADD-ON

Swati Uday Joshi[1], Priyanka Pankaj Dhule[2], Sojwal Janardan Jadhav[3], Priti Vijaykumar Ladda[4], Prof. Suvarna Somvanshi[5]

Department of Computer Engineering, PVGCOE and SSDIOM, Nashik, India

Abstract : Phishing remains one of the most common and damaging cyber-attacks, utilizing various means such as spurious URLs, spurious e-mails, or malicious QR codes to steal sensitive user information. Traditional blacklist-based detection methods are inefficient against the growing sophistication and rapid deployment of phishing campaigns, hence motivating the need for an automated and adaptive detection framework. We present The Phish Finder, a real-time phishing detection system integrated as a lightweight add-on in the Chrome browser, which is capable of analyzing URLs, email content, and QR codes prior to any user engagement. The system is powered by machine learning-driven feature extraction and classification via the XGBoost algorithm, underpinned by Firebase Storage for data management in a secure manner with continuous model updates. Experimental results have yielded an accuracy value greater than 96%, thus enabling proactive phishing alerts while ensuring cross-platform compatibility with minimum user disruption. The proposed solution crucially improves online safety by mitigating phishing threats right at their source.

IndexTerms *- Phishing detection, browser add-on, machine learning, QR codes, cybersecurity, URL analysis, email security.*

I. INTRODUCTION

Phishing is among the most prevalent and harmful forms of cybercrime, aiming to deceive users into disclosing sensitive information such as credentials, banking details, or personal data. Attackers commonly employ forged websites, fraudulent emails, and malicious QR codes to exploit user trust. With the rapid advancement of digital communication and online services, phishing campaigns have evolved to become more dynamic and sophisticated, frequently bypassing conventional security mechanisms such as URL blacklists and signature-based filters. This evolution has created an urgent need for automated, intelligent, and adaptive detection techniques capable of operating in real time.

Recent developments in machine learning (ML) have provided effective means of identifying phishing attempts by analyzing patterns within URLs, email text, and embedded data. However, most existing approaches remain limited to a single data source typically URL or email analysis—and are often deployed as static or standalone systems that lack integration with real-time user interactions. Consequently, these systems fail to offer immediate protection during actual browsing sessions.

To overcome these challenges, this study introduces The Phish Finder, a real-time phishing detection system implemented as a Chrome browser add-on. The system is designed to analyze URLs accessed during browsing, evaluate email content uploaded as PDF files, and examine QR codes to identify potential phishing redirections. The underlying model employs the XGBoost algorithm for accurate classification, supported by Firebase Storage for secure data handling and periodic model updates. Through real-time monitoring and intelligent classification, **The Phish Finder** enhances user safety by detecting and mitigating phishing attacks at the point of interaction.

II. LITERATURE REVIEW

Hmimou et al. (2024) proposed a multi-agent cybersecurity threat detection system that combines traditional analysis tools with Large Language Models (LLMs) to improve accuracy in identifying advanced cyber-attacks. Their model uses three specialized agents for email verification, log analysis, and IP scanning, and a central recommendation system to correlate outputs and detect complex, multi-vector attacks that traditional rule-based systems often fail to recognize. The system achieved a threat detection accuracy of 93.6% using datasets such as CIC-IDS 2017 and SpamAssassin. This work highlights the growing importance of semantic understanding and AI-driven analysis in detecting modern phishing and advanced persistent threats **[1]**.

Taha (2025) introduced SMART, an advanced email spam detection framework that combines semantic analysis, adversarial training, and reinforcement learning to handle evolving spam attacks. The system uses text preprocessing, word embeddings, K-means clustering, and BERT-based semantic enhancement to improve email understanding. SMART dynamically adapts to new spam patterns and shows better performance than existing methods such as EGOAMLPs, OPTICS, and STM. This study highlights the importance of semantic and adaptive techniques for improving email spam and phishing detection **[2]**.

Li et al. (2024) presented a comprehensive review of modern phishing website detection techniques and highlighted how attackers increasingly use advanced methods to bypass traditional security systems. The study introduced a new taxonomy of detection approaches, covering machine learning, deep learning, graph-based analysis, LLM-driven methods, and phishing kit–based detection. The authors compared the strengths and limitations of these approaches and discussed the practical challenges of deploying them in real-world environments. Their review emphasizes the growing role of AI in improving phishing website detection and outlines future research directions to enhance accuracy and robustness **[3]**.

Zara et al. (2024) investigated multiple machine learning, ensemble learning, and deep learning models for phishing website detection. Their study used feature selection techniques such as information gain, gain ratio, and PCA to identify the most significant website attributes. Using a dataset of 11,055 websites, the authors demonstrated that an ensemble deep learning model achieved an accuracy of 99%, outperforming existing techniques. The research highlights the effectiveness of combining GRU, LSTM, and other advanced models to improve detection performance and adapt to evolving phishing strategies **[4]**.

Sahingoz et al. (2024) developed DEPHIDES, a deep-learning-based phishing detection system designed to classify phishing attacks using URL data. The authors evaluated several architectures, including ANN, CNN, RNN, Bi-RNN, and attention networks, on a large dataset of nearly five million labeled URLs. Their results showed that convolutional neural networks achieved the highest performance with a detection accuracy of 98.74%. The study demonstrates the strong capability of deep learning models, especially CNNs, in accurately identifying phishing websites and improving cybersecurity protection **[5]**.

Duarte et al. (2025) proposed a machine-learning framework for the early detection of phishing URLs, focusing especially on newly registered and parked domains that are frequently used in financial fraud. Using a large dataset of 211,659 URLs gathered from SSL certificate monitoring and phishing incident reports, the authors applied preprocessing, feature engineering, and model optimization techniques to improve performance. Their LightGBM classifier achieved an accuracy of 97.28% and a recall of 96.02%, demonstrating strong capability in identifying malicious URLs at an early stage. This study highlights the importance of proactive URL monitoring in financial institutions and shows that lightweight ML models can support real-time phishing prevention systems **[6]**.

Safran and Musleh (2025) introduced PhishingGNN, an advanced phishing email detection framework that combines transformer-based semantic analysis with graph-based structural learning. Their model uses DistilBERT to extract contextual textual features and Graph Attention Networks (GAT) to represent email metadata and content as interconnected graph structures. By modeling emails as relational graphs, the system captures subtle phishing patterns that traditional methods often miss. Evaluated on the expanded CEAS_08 dataset, PhishingGNN achieved state-of-the-art results with an accuracy of 0.9939 and an AUC of 1.00. The model also demonstrated strong generalization during cross-dataset testing on the Nazario Corpus. This work highlights the effectiveness of hybrid transformer–GNN architectures for robust and scalable phishing email detection **[7]**.

Li et al. (2024) conducted an in-depth analysis of anti-phishing blacklists and demonstrated how attackers can exploit their inherent weaknesses using machine learning–based evasion strategies. The study introduced two new cloaking attacks—Feature-Driven Cloaking and TLS-Based Cloaking—that manipulate browser behavior and communication protocols to bypass blacklist detection systems. Through experiments using real-world data, the authors showed that a Random Forest classifier could reliably identify anti-phishing entities with 100% accuracy, enabling attackers to avoid detection more effectively. Their findings reveal major vulnerabilities in current blacklist-based defenses, including inconsistent feature usage, limited infrastructure diversity, and susceptibility to WebRTC IP leaks. The study highlights the need for more adaptive and intelligent phishing defense mechanisms beyond traditional blacklist approaches **[8]**.

Kavya and Sumathi (2025) proposed a sophisticated multimodal and temporal graph fusion framework to address the limitations of traditional phishing website detection methods that rely on static or single-modal features. Their work introduced four novel models—MM-HFN, TGNN-Att, FGCL-Net, and MMTHF-Net—each designed to capture complex relationships between textual, visual, and structural website features while also considering temporal behavior. By integrating hypergraphs, attention-based temporal graph networks, and federated contrastive learning, the proposed methods achieved accuracies ranging from 93% to 98%. The MMTHF-Net model delivered the highest performance with an F1-score of 0.97. This study demonstrates the importance of combining multimodal data and temporal analysis to enhance phishing detection accuracy and adaptability in dynamic environments **[9]**.

Dsouza et al. (2024) conducted a multi-modal comparative analysis of phishing detection approaches using artificial intelligence across different execution modes—offline, batch, and incremental learning. Using datasets such as the Mendeley Phishing Websites dataset and the SPAM-HAM SMS dataset, the study evaluated a variety of machine learning and deep learning models based on accuracy, precision, recall, F1-score, and time complexity. Their findings show that incremental learning methods, particularly the Adaptive Random Forest (ARF) classifier, performed well for real-time detection with 97.1% accuracy on a custom dataset. Meanwhile, deep learning models using a Keras sequential architecture achieved the highest accuracy of 99.28%. This research demonstrates the importance of selecting the right learning mode for practical phishing detection and highlights how incremental models can support real-time deployment **[10]**.

Yalçın et al. (2024) explored the use of artificial intelligence techniques to improve attack detection in SCADA systems, which form a critical part of Industrial IoT infrastructures. As cyberattacks targeting industrial operations continue to increase in sophistication, the authors evaluated several AI models—including KNN, QDA, AdaBoost, Gradient Boosting, and Random Forest—to assess their effectiveness in identifying malicious network activities. Extensive experiments conducted on two SCADA datasets demonstrated that all models achieved high detection performance, with accuracy rates exceeding 96.82%. Notably, the XGBoost model achieved an outstanding accuracy of 99.99% on the WUSTL-IIoT-2021 dataset. This study highlights the growing importance of AI-based intrusion detection systems for securing industrial environments and reinforces the capability of boosting algorithms like XGBoost in detecting complex attacks **[11]**.

Wangchuk and Gonsalves (2025) conducted a systematic review focusing on multimodal phishing detection techniques used across social networking platforms. Their study examined research from 2018 to 2025 and highlighted that multimodal features—such as HTML structure, URLs, text content, and visual elements—are increasingly being used to identify phishing attempts on SNS platforms. Deep learning models including CNN, RNN, LSTM, and MLP were commonly applied and demonstrated promising detection performance. However, the review also pointed out major challenges such as adversarial attacks, limited high-quality datasets, integration issues with existing SNS systems, and high false positives. The authors emphasized that while multimodal phishing detection methods show strong potential, further improvements are needed for effective real-world deployment on social networking sites **[12]**.

Ahmad et al. (2024) presented a comprehensive review of AI-based phishing detection methods, covering more than 130 research articles published between 2020 and 2024. Their study analyzed traditional techniques, machine learning models, deep learning architectures, phishing datasets, and the complete phishing attack workflow. The authors highlighted key challenges in detecting newly emerging phishing URLs, noting that even advanced AI models struggle with zero-day attacks. They also identified gaps such as dataset imbalance, feature limitations, and the need for better generalization across diverse phishing patterns. The review provides a detailed comparison of model performance based on accuracy metrics and offers a structured roadmap for future research in phishing website detection. Overall, the study emphasizes the importance of combining modern ML/DL techniques with improved datasets to strengthen real-time phishing prevention **[13]**.

Koide et al. (2024) introduced ChatPhishDetector, an innovative system that utilizes Large Language Models (LLMs) to detect phishing websites without requiring traditional machine learning training. The approach uses a web crawler to collect website content and automatically generates prompts for LLMs, enabling the model to analyze full-page context, impersonated brands, multilingual content, and social engineering techniques. Their experiments demonstrated that GPT-4V achieved outstanding performance with 98.7% precision and 99.6% recall, outperforming other LLMs and existing phishing detection tools. This study highlights the growing potential of LLM-driven systems in detecting advanced phishing sites created using AI and reinforces the role of contextual understanding in modern phishing detection **[14]**.

Heiding et al. (2024) examined how Large Language Models (LLMs) can both generate and detect phishing emails. Their study compared phishing emails created manually using the V-Triad social engineering framework with emails generated automatically by GPT-4. Through a red-team experiment involving 112 participants, they found that GPT-generated phishing emails achieved higher click-through rates than generic phishing messages, while V-Triad–crafted emails produced the highest engagement. The authors also evaluated multiple LLMs—including GPT, Claude, PaLM, and LLaMA—for detecting the malicious intent behind phishing emails. These models demonstrated strong detection capabilities and occasionally outperformed human participants. The study reveals both the risks and defensive potential of LLMs in modern phishing attacks, emphasizing how AI can enhance both phishing creation and phishing detection **[15]**.

Mushtaq et al. (2024) proposed an ensemble learning–based approach to improve URL phishing detection by combining feature selection with multiple classifiers. Their system was evaluated using two datasets, DS-30 and DS-50, containing 30 and 50 features respectively. The study showed that applying a voting-based ensemble classifier significantly improved accuracy while reducing the number of required features. The hybrid HEFS–Random Forest model achieved 94.6% accuracy using only 20.8% of the original feature set, demonstrating the effectiveness of dimensionality reduction. The final ensemble classifier achieved 96% accuracy on DS-30 and 98% on DS-50, proving that combining multiple learning models can enhance phishing detection performance **[16]**.

Wei et al. (2025) proposed a fine-tuned BERT-based multimodal framework to improve the generalization capability of phishing URL detection systems across diverse real-world scenarios. Their approach combines BERT's contextual understanding for URL text analysis with additional external features gathered from public Internet resources, creating a richer representation of phishing patterns. The authors also introduced *PhishMail*, a new dataset containing 8,937 phishing samples collected from malicious email campaigns, enabling realistic zero-day testing. Experimental results across multiple cross-dataset evaluations demonstrated that the proposed multimodal system significantly enhances robustness and detection performance compared to traditional feature-engineering or purely deep learning–based methods. The study highlights the importance of combining contextual NLP models with external metadata to achieve stronger generalization in phishing URL detection **[17]**.

Alsubaei et al. (2024) introduced a hybrid deep learning framework designed to improve real-time phishing detection within cybercrime forensics. Their approach combines ResNeXt and GRU architectures into a unified model called RNT, further optimized using the Jaya optimization method (RNT-J). To address data imbalance, the authors used SMOTE, while feature extraction was enhanced through the integration of autoencoders and ResNet (EARN). Experiments conducted on real phishing datasets showed that the proposed model significantly outperformed existing algorithms by margins ranging from 11% to 19%. The framework achieved 98% accuracy with very low false positives and demonstrated efficient runtime performance. This work highlights the value of hybrid deep learning strategies and advanced feature engineering for strengthening phishing detection in digital forensics **[18]**.

Nsoh and Malki (2024) introduced a unique sociocultural perspective to phishing and social engineering detection by integrating the LESCANT communication framework into cybersecurity analysis. Their study highlighted how cultural differences influence the way phishing messages are crafted and interpreted, emphasizing the need for security systems to recognize sociocultural cues. The authors proposed enhancing dataset diversity through international collaboration and incorporating adaptive learning models capable of understanding cultural variations in phishing patterns. They also explored automated annotation techniques to reduce cultural bias in datasets. By formalizing a LESCANT-based phishing analysis model supported with mathematical formulations and Python implementations, the study demonstrated the value of sociocultural intelligence in improving phishing detection beyond traditional technical features **[19]**.

Bispo et al. (2025) developed **PHILDER**, a lightweight deep-learning framework designed to detect phishing emails on resource-constrained devices. Their approach focused on computationally efficient transformer models—such as ALBERT, DistilBERT, MobileBERT, MiniLM, and TinyBERT—trained on real phishing and legitimate email data from PhishTank and the SpamAssassin Corpus. To address dataset imbalance, the authors experimented with undersampling and SMOTE-based oversampling, ultimately discarding oversampling due to high computational costs and overfitting. Their evaluation emphasized not only accuracy but also efficiency metrics relevant to low-power devices. The TinyBERT-based PHILDER model achieved the best balance between performance and resource usage, demonstrating its suitability for real-time phishing detection on devices with limited hardware capabilities **[20]**.

Liu and Fu (2020) introduced SPWalk, an unsupervised feature-learning method for phishing website detection that focuses on relationships between webpages. Instead of relying only on URL or content features, the method builds a weblink network and uses biased random walks to learn structural and textual patterns. Because attackers cannot fully control hyperlink relationships, SPWalk captures hidden similarities and differences between phishing and legitimate pages. Experiments show that the model achieves **over 95% precision**, outperforming several state-of-the-art methods even when phishing pages are well disguised **[21]**.

Mahajan and Siddavatam (2018) explored the use of traditional machine learning algorithms to detect phishing websites by analyzing URL-based features. Their study extracted key lexical and host-related attributes from legitimate and phishing URLs and evaluated three models—Decision Tree, Random Forest, and Support Vector Machine. The authors compared these algorithms based on accuracy, false positive rate, and false negative rate to determine the most reliable classifier. Their findings showed that Random Forest achieved the best overall performance due to its robustness and ability to handle complex feature interactions. This early work demonstrates the effectiveness of machine learning–driven URL analysis and forms a foundational baseline for more advanced phishing detection models used today **[22]**.

Barik et al. (2025) proposed a deep learning–based phishing URL detection model known as **EGSO-CNN**, which integrates feature engineering with optimization techniques to improve detection accuracy. The study introduced a newly constructed dataset to address the lack of updated phishing URL collections and used StandardScaler along with Variational Autoencoders (VAE) for preprocessing and feature extraction. The Enhanced Grid Search Optimization (EGSO) technique was applied to fine-tune the CNN model. Experimental results showed that EGSO-CNN achieved a high accuracy of 99.44%, along with strong recall and F1-scores, while maintaining low false positives. This work demonstrates the effectiveness of combining deep learning with optimization methods to strengthen phishing detection systems **[23]**.

Kavya and Sumathi (2025) provided an extensive review of recent advancements and emerging methodologies in phishing detection, covering a wide range of techniques from traditional machine learning approaches to modern deep learning and generative models. Their analysis highlighted the strengths of list-based methods, ML classifiers, graph-based approaches, network embedding techniques, and advanced deep learning architectures such as CNNs and RNNs, which showed superior ability to extract complex phishing patterns. The review also emphasized the growing role of ensemble learning and GAN-based models in improving detection accuracy and resisting adversarial attacks. By summarizing the advantages, limitations, and empirical performance of each method, the authors offered practical insights for researchers and cybersecurity practitioners. Their work also identified future research directions, including contextual information integration, user-behavior modeling, and explainable AI, to enhance the robustness of phishing detection systems **[24]**.

Alsaidi et al. (2025) introduced **HawkPhish-DNN**, a multi-objective phishing URL detection framework that integrates Harris Hawk Optimization (HHO) with a deep neural network to enhance accuracy and reduce false positives. Their approach preprocesses URL data by removing redundant features and extracting key attributes such as URL length and entropy. The model uses advanced neural network layers, including ReLU and Sigmoid, while the HHO algorithm optimizes model parameters using techniques like Pareto dominance and time-varying penalty functions. Experimental results showed that HawkPhish-DNN achieved an accuracy of 99.6% with a very low false positive rate of 0.2%, demonstrating its strong potential for real-time phishing detection with minimal computational overhead. This work highlights the effectiveness of combining deep learning with hybrid optimization techniques to strengthen phishing defense mechanisms **[25]**.

Ghalechyan et al. (2025) conducted an empirical study on phishing URL detection using both deterministic and probabilistic neural network models. Their work introduced a novel probabilistic neural network approach that significantly improved classification accuracy compared to traditional models. A key contribution of the study was the creation of a hybrid dataset that combined widely used public sources—such as Alexa, PhishTank, and OpenPhish—with real-world production data from EasyDMARC, demonstrating that models trained on mixed datasets can successfully operate in live environments. The proposed system achieved an average validation accuracy of 97% on daily updated URLs, including both short and long URL variants. This study highlights the importance of dataset diversity and probabilistic modeling for improving the reliability of phishing URL detection in real-world deployment scenarios **[26]**.

Ige et al. (2025) conducted a comprehensive survey evaluating the performance of state-of-the-art phishing detection classifiers across three major categories: Bayesian models, non-Bayesian machine learning algorithms, and deep learning architectures. The review examined commonly used models such as Naive Bayes, Multinomial Naive Bayes, SVM, RNN, CNN, and LSTM, highlighting their strengths and limitations in detecting phishing URLs and malicious online content. Through empirical comparisons, the authors demonstrated that deep learning models, particularly RNN and CNN variants, generally outperform traditional Bayesian and non-Bayesian classifiers due to their ability to learn complex, sequential URL patterns. The study also identified key research gaps, such as model vulnerability to zero-day phishing attacks, insufficient feature diversity, and challenges in handling imbalanced datasets. Their survey provides future research directions, including hybrid two-stage prediction models and improved optimization strategies for underperforming classifiers **[27]**.

Sahingoz et al. (2018) proposed a real-time phishing detection system that analyzes URLs using natural language processing (NLP)–based features combined with multiple machine learning classifiers. Their study evaluated seven different classification algorithms on a newly constructed dataset containing large volumes of phishing and legitimate URLs. The system was designed to operate independently of third-party services, detect newly emerging phishing websites, and function in real time. Among the tested models, the Random Forest classifier using only NLP-derived features achieved the highest accuracy of 97.98%. This work demonstrated the effectiveness of combining linguistic URL analysis with machine learning to improve phishing detection performance **[28]**.

Abu Zuraiq and Alkasassbeh (2024) reviewed several phishing detection approaches, focusing on content-based, heuristic-based, and fuzzy rule–based techniques. Their survey highlighted how content-based methods analyze webpage elements such as HTML structure and scripts, while heuristic-based systems rely on predefined rules to identify suspicious URL or webpage characteristics. The authors also discussed fuzzy rule–based approaches, which handle uncertainty in phishing indicators by assigning degrees of suspicion rather than binary labels. The review emphasized the strengths and limitations of each method, noting that hybrid and machine learning–based models offer improved accuracy compared to traditional approaches. This work provides foundational insights into early phishing detection techniques and serves as a useful comparison for modern AI-driven methods **[29]**.

Orunsolu et al. (2019) developed a predictive machine learning model for phishing detection that focuses on improving feature selection and reducing false positive rates. Their system incorporates a Feature Selection Module that extracts relevant attributes from URLs, webpage structure, and webpage behavior using an incremental component-based method. The model employs Support Vector Machine (SVM) and Naïve Bayes classifiers, both trained on a compact 15-dimensional feature vector. Experiments conducted on a dataset containing 2,541 phishing and 2,500 benign instances showed strong performance, achieving 99.96% accuracy with an extremely low false positive rate of 0.04%. This study demonstrates that carefully engineered feature vectors combined with lightweight ML algorithms can produce highly accurate phishing detection systems **[30]**.

Shahrivari et al. (2020) examined the effectiveness of several machine learning algorithms for detecting phishing websites by analyzing the common characteristics shared across phishing attacks. Their study highlighted how attackers frequently employ social engineering and replica websites to deceive users, making traditional detection methods less effective as phishing techniques evolve. The authors compared the performance of multiple ML classifiers on phishing datasets to identify the most accurate approach for predicting malicious URLs. Their findings reinforced that machine learning methods are highly suitable for phishing detection due to their ability to recognize recurring behavioral and structural patterns in phishing websites **[31]**.

Zieni et al. (2023) presented a broad survey on phishing website detection, categorizing existing approaches into list-based, similarity-based, and machine-learning-based methods. Their review highlighted how blacklist systems provide fast detection but struggle with zero-day attacks, while similarity-based approaches compare webpage content or structure to known legitimate sites to detect impersonation attempts. Machine learning techniques, on the other hand, leverage URL features, page content, and behavioral indicators to improve detection accuracy, though their performance is often limited by dataset quality and feature selection issues. The authors also compared datasets commonly used for evaluation and identified key research gaps such as evolving attack patterns, insufficient real-world data, and the need for more robust models. This survey provides valuable insight into the strengths and limitations of current phishing detection methodologies **[32]**.

Asiri et al. (2023) presented a comprehensive survey of intelligent detection techniques for HTML- and URL-based phishing attacks, focusing on how modern systems analyze webpage structure, content, and URL characteristics to identify malicious behavior. The survey reviewed a wide range of machine learning and deep learning approaches, highlighting how attackers craft realistic phishing pages that closely resemble legitimate websites, making detection increasingly difficult. The authors compared state-of-the-art methods in terms of preprocessing, feature extraction, and model architecture, covering techniques such as CNNs, RNNs, hybrid deep learning models, and natural language processing. Their findings emphasized ongoing challenges such as evolving attack strategies, feature variability, and the need for more effective and scalable detection frameworks. This survey provides an important foundation for understanding HTML and URL-level phishing behaviors and evaluating modern intelligent detection models **[33]**.

Jibat et al. (2023) conducted a systematic review of phishing website detection studies published between 2018 and 2021, focusing on data mining and machine learning algorithms used to classify illegitimate webpages. Their analysis covered a wide range of approaches, including single-model classifiers, hybrid techniques, and newly proposed detection frameworks. The review found that most data mining models achieved accuracy rates above 90%, although only a few studies reported near-perfect or 100% detection results. The authors emphasized that no universally flawless model exists due to evolving phishing techniques, dataset limitations, and varying feature sets. Their findings highlight both the progress and the remaining challenges in developing reliable, generalizable phishing detection systems **[34]**.

Karim et al. (2023) proposed a hybrid machine learning–based phishing detection system using URL features extracted from a dataset of over 11,000 websites consisting of both phishing and legitimate URLs. Their study applied several traditional classifiers including Decision Tree, Random Forest, Naïve Bayes, Gradient Boosting, KNN, and SVC—along with a newly designed hybrid ensemble model called **LSD**, which combines Logistic Regression, SVM, and Decision Tree using both soft and hard voting mechanisms. To further improve model performance, the authors incorporated canopy feature selection, cross-fold validation, and Grid Search hyperparameter tuning. The comparative analysis showed that the LSD hybrid model outperformed all baseline classifiers across accuracy, precision, recall, F1-score, and specificity, demonstrating that ensemble learning with optimized parameters can significantly strengthen URL-based phishing detection **[35]**.

Jovanovic et al. (2023) proposed an advanced hybrid phishing detection framework that enhances XGBoost performance through a two-level optimization strategy using an improved firefly metaheuristic algorithm. Their system performs both feature selection and hyperparameter tuning within a combined optimization pipeline, enabling the model to identify the most influential features while maximizing classification accuracy. The framework was evaluated on three publicly available phishing datasets from Mendeley Data and the UCI Machine Learning Repository. Experimental comparisons showed that the hybrid Firefly–XGBoost model consistently outperformed baseline metaheuristic approaches and other machine learning models. Additionally, SHAP (SHapley Additive exPlanations) analysis was used to interpret feature contributions, further validating the model's decision-making process. This study demonstrates the effectiveness of metaheuristic-driven optimization in improving phishing website detection **[36]**.

Tang and Mahmoud (2022) proposed a deep learning–based phishing website detection framework integrated directly into a browser extension for real-time protection. Their system combines multiple strategies—such as whitelist filtering, blacklist checking, and ML-based prediction—to improve detection accuracy while reducing false alarms and computational delay. In the machine learning module, the authors compared several models across multiple datasets and found that the RNN-GRU architecture achieved the highest accuracy of 99.18%. The study highlights the limitations of traditional rule-based and third-party–dependent features, emphasizing the need for fast, reliable, and autonomous deep learning approaches for real-time phishing detection. Their browser plug-in implementation demonstrates practical deployability of deep neural models in everyday user environments **[37]**.

Salloum et al. (2022) conducted a systematic literature review focusing on phishing email detection using Natural Language Processing (NLP) techniques. Analyzing 100 research articles published between 2006 and 2022, the authors examined key components of NLP-based phishing detection, including text feature extraction, classification methods, datasets, and evaluation metrics. The review found that feature engineering—particularly TF-IDF and word embeddings—is the most widely researched area, followed by classification and optimization strategies. Support Vector Machines (SVMs) emerged as one of the most frequently used classifiers for phishing email detection. The study also noted that the Nazario phishing corpus is the most commonly used benchmark dataset and that Python remains the most popular implementation language. Furthermore, the authors identified significant research gaps, especially the limited availability of studies focusing on Arabic-language phishing emails. Their review offers valuable insights for advancing NLP applications in cybersecurity **[38]**.

Kalabarige et al. (2022) introduced a multilayer stacked ensemble learning framework designed to improve phishing website detection accuracy through hierarchical model integration. Their approach uses multiple base estimators arranged across several layers, where predictions from one layer serve as input for the next, enabling deeper learning of phishing patterns. The model was evaluated on four benchmark datasets, including UCI and Mendeley phishing datasets, achieving high accuracy ranging between 96.79% and 98.90%. The stacked ensemble significantly outperformed baseline machine learning models in both accuracy and F-score, demonstrating enhanced generalization across diverse datasets. The study highlights the effectiveness of meta-learning–based stacking architectures in improving phishing website detection performance **[39]**.

Al-Ahmadi et al. (2022) proposed **PDGAN**, a phishing detection framework that leverages a Generative Adversarial Network (GAN) to improve URL-based phishing classification. Unlike traditional approaches that rely on webpage content or external APIs, PDGAN uses only the raw URL string, making it faster and independent of third-party services. The model employs an LSTM-based generator to create synthetic phishing URLs and a CNN-based discriminator to classify URLs as legitimate or malicious. Using a large dataset of nearly two million URLs collected from PhishTank and DomCop, the model achieved a detection accuracy of **97.58%**, outperforming several state-of-the-art methods. The study highlights the potential of GAN-based architectures in enhancing phishing detection performance through data augmentation and adversarial training **[40]**.

Wei and Sekiya (2022) conducted a detailed comparative study evaluating multiple machine learning and deep learning models for phishing website detection. Their experiments showed that **ensemble learning methods**—such as Random Forest, Gradient Boosting, and related voting-based models—consistently outperform individual classifiers in terms of both accuracy and computational efficiency. Even when the number of available features was drastically reduced, ensemble models maintained strong performance, demonstrating robustness and stability. The authors further analyzed why ensemble techniques are well-suited for binary phishing classification, especially in real-time environments where frequent model updates and fast detection are required **[41]**.

Yang et al. (2019) proposed a multidimensional phishing website detection framework that combines deep learning with traditional feature engineering to improve accuracy and reduce detection time. Their model first performs a fast pre-classification using character-level deep learning on URL sequences, avoiding reliance on third-party services or expert-defined features. In the second stage, the system integrates multiple feature types—including URL statistics, webpage code, and webpage text—along with the initial deep learning output, forming a comprehensive multidimensional representation. Experiments on a large dataset of millions of URLs showed an accuracy of **98.99%** with a very low false positive rate of **0.59%**, demonstrating the effectiveness of combining quick deep learning-based detection with richer feature-level analysis **[42]**.

Liu and Fu (2020) introduced SPWalk, an unsupervised feature learning algorithm designed to detect phishing webpages by leveraging structural relationships on the web rather than relying solely on traditional content or visual features. Their approach constructs a weblink network where nodes represent webpages and edges reflect hyperlink connections or textual similarity. Using biased random walks and network embedding, SPWalk learns low-dimensional feature representations that capture both structural patterns and URL characteristics. Unlike conventional methods, SPWalk is more resistant to phishing webpages that mimic legitimate designs, since attackers cannot fully control external reference relationships. Experimental results showed that SPWalk achieves superior performance compared to existing techniques, consistently maintaining precision above **95%**, even when phishing pages are heavily camouflaged **[43]**.

Fang et al. (2019) proposed THEMIS, an advanced phishing email detection model built using an improved Recurrent Convolutional Neural Network (RCNN) combined with multilevel feature vectors and an attention mechanism. Unlike traditional email detection methods that rely only on header or body features, THEMIS simultaneously analyzes email headers, body content, characters, and words, enabling deeper contextual understanding of phishing patterns. The model was evaluated on a highly unbalanced real-world dataset, reflecting natural phishing-to-legitimate email ratios. Experimental results show exceptionally strong performance, achieving an accuracy of **99.848%** and a very low false-positive rate of **0.043%**, outperforming earlier machine learning and deep learning approaches. The study demonstrates that multilevel semantic modeling with attention significantly improves phishing email detection effectiveness **[44]**.

Gualberto et al. (2020) introduced a powerful multi-stage phishing email detection framework that relies heavily on feature engineering and natural language processing to extract meaningful patterns from email text. Their approach combines lemmatization, feature selection, feature extraction, and optimized machine learning workflows to address problems like high dimensionality and sparse text data. Two different dimensionality-reduction pipelines were proposed—one using Chi-Square and Mutual Information, and another using PCA and LSA—to build compact yet highly informative feature sets. When combined with XGBoost and Random Forest classifiers, the system achieved **100% F1-score** on well-known datasets such as SpamAssassin and Nazario, even while using fewer features and lower computational cost. This study demonstrates how careful NLP-based feature engineering can greatly improve phishing email detection performance **[45]**.

Zhu et al. (2019) proposed OFS-NN, a phishing website detection model that combines optimal feature selection with a neural network to improve accuracy and reduce overfitting. The authors introduced a new metric called **Feature Validity Value (FVV)** to evaluate the importance of each feature in phishing classification. Using this metric, the system removes irrelevant or low-impact features that typically confuse neural networks and cause poor generalization. The selected optimal features are then used to train a refined neural network classifier. Experimental evaluations show that OFS-NN achieves stable and accurate detection performance across different types of phishing websites, demonstrating the effectiveness of optimal feature selection in improving neural network-based phishing detection **[46]**.

Kara et al. (2022) proposed a phishing website detection method focused specifically on URL and domain name characteristics rather than relying on HTML or DOM features, which attackers can easily manipulate. The authors created a new, previously unused dataset by collecting intelligence from reputable global security sources and designed eleven key URL- and domain-level features. Six machine learning classifiers were evaluated, and Random Forest achieved the highest performance with **98.90% accuracy**. Their approach simplifies feature extraction, reduces processing overhead, and demonstrates that combining Random Forest descriptors with SVM-based representation can effectively classify phishing websites. The study highlights the strength of domain-driven features and continuous dataset updates for improving phishing detection models **[47]**.

Rafsanjani et al. (2023) introduced QsecR, a secure and privacy-friendly QR code scanner designed to detect malicious URLs embedded in QR codes. Unlike conventional QR scanners that rely mainly on blacklists—which fail to identify newly emerging malicious sites—QsecR incorporates a machine learning–based detection framework using 39 carefully selected lexical, blacklist, host-based, and content-based features. The authors compiled a real-world dataset of 4000 URLs from PhishTank and URLhaus to train and evaluate the model. Experimental results highlight that QsecR achieves **93.50% accuracy** and **93.80% precision**, outperforming existing QR-scanning applications while also requiring minimal permissions. This study demonstrates the growing importance of ML-driven detection methods for securing QR code–based interactions **[48]**.

Khalid et al. (2024) introduced LogiTriBlend, a hybrid stacking framework designed to improve phishing email detection by combining multiple machine learning models with advanced text vectorization methods. The study explored TF-IDF, Word2Vec, and Doc2Vec representations applied to classifiers including SVM, Logistic Regression, Random Forest, and XGBoost. To address severe class imbalance in the dataset of 501 phishing and 4090 legitimate emails, SMOTE was applied during preprocessing along with lemmatization, stemming, and noise removal. The proposed stacking model uses Logistic Regression as the meta-learner and demonstrated superior performance, achieving **99.34% accuracy** when using Doc2Vec embeddings. Results show that Doc2Vec consistently outperformed Word2Vec and TF-IDF, highlighting the importance of semantic-rich vectorization and ensemble learning for effective phishing email classification **[49]**.

Al-Khater et al. (2020) presented a broad review of cybercrime detection methods, covering threats such as phishing, identity theft, data leakage, and financial fraud. The authors compared machine learning, neural networks, fuzzy logic, and data mining techniques, highlighting their strengths and limitations. The study emphasizes that cybercrimes are rapidly evolving and recommends developing more adaptive and effective detection models for improved security **[50]**.

III. Problem Statement

The rapid increase in digital communication and online transactions has led to a rise in sophisticated phishing attacks delivered through malicious URLs, fraudulent emails, and deceptive QR codes. Existing phishing detection systems are often limited to a single input type (usually URLs) and fail to provide real-time protection, multi-format detection, or browser-level security. Additionally, users lack a unified platform where they can verify suspicious content such as website links, email files, and QR codes in a single system.Most traditional phishing detection techniques rely on manually maintained blacklists, which cannot detect newly generated ("zero-day") phishing attacks. Machine-learning-based systems exist, but they are often not integrated into user-facing tools such as browser extensions, and they do not offer support for emails (.eml) and QR code–based phishing, which are becoming increasingly common in cyber-fraud.

Therefore, there is a need for a real-time, multi-input, machine-learning-powered phishing detection system that can:

1. Detect phishing websites instantly while the user is browsing.
2. Analyze uploaded **email files**, extract features, and classify them as phishing or legitimate.
3. Decode and evaluate **QR codes** that may redirect users to malicious pages.
4. Provide seamless user access through authentication and a browser-based interface.
5. Use a reliable machine learning algorithm such as **XGBoost** to achieve high accuracy and timely prediction.

To address these challenges, this research aims to develop **"The Phish Finder"**, a unified Chrome extension and backend system capable of detecting phishing attacks across URLs, emails, and QR codes using a trained XGBoost model. The solution integrates real-time scanning, secure user authentication, and cloud-based API communication with the trained model to deliver fast and accurate phishing detection.

IV. Methodology

The proposed system, *The Phish Finder*, follows a structured methodology consisting of dataset preparation, preprocessing, feature extraction, model training using XGBoost, API integration, and deployment through a Chrome browser extension. The overall workflow is divided into two major phases: Machine Learning Model Development and Real-Time Phishing Detection through Browser Extension.

A Dataset Collection

The system utilizes three publicly available phishing datasets from Kaggle:

- URL Dataset containing legitimate and phishing website links
- Email Dataset including phishing and benign email samples in .eml or PDF format
- QR Code Dataset containing safe and malicious QR-encoded URLs

These datasets serve as ground truth for training and evaluating the machine learning model.

B. Data Preprocessing

Collected raw datasets are heterogeneous in format; therefore, preprocessing is performed to convert them into structured form.

Preprocessing Steps:

- Cleaning URLs: removing whitespace, special symbols, duplicate entries, and invalid URLs
- Email Preprocessing: extracting sender address, subject, body text, embedded URLs, and suspicious keywords
- QR Code Processing: decoding the QR image using Python libraries to extract the underlying URL
- Label Encoding: mapping phishing = 1, legitimate = 0
- Handling Missing Values: removing or imputing incomplete records

Preprocessing ensures that all three data types are standardized and ready for feature extraction.

C. Feature Extraction

Feature engineering is performed separately for URLs, emails, and QR codes.

URL Features:

- Length of URL
- Number of dots, dashes, and special characters
- Presence of "https"
- Domain age and expiration time
- URL redirection count
- IP address usage instead of domain name

Email Features:

- Suspicious keywords (e.g., verify, login, urgent)
- Sender domain mismatch
- Number of links embedded in email
- HTML tags or script usage
- Presence of attachments

QR Code Features:

- Decoded URL features same as URL dataset
- Redirection to unknown or suspicious domains

All extracted features are converted into a numeric feature vector compatible with XGBoost.

D. Train–Test Split

The cleaned dataset is divided into:

- 70% Training Data
- 30% Testing Data

This ensures that the model learns from majority data while maintaining unbiased performance evaluation.

E. Model Training Using XGBoost

XGBoost (Extreme Gradient Boosting) is chosen due to its robustness, regularization capability, and high accuracy for tabular data.

Training Steps:

1. Input feature vectors into XGBoost classifier
2. Compute gradient and hessian for loss function
3. Construct optimized decision trees
4. Apply regularization to reduce overfitting
5. Evaluate the model on test data

After training, the final model is saved as a serialized file for deployment.

F. API Integration

A backend API is created to communicate between the trained model and the Chrome extension.

API Tasks:

- Receive input from extension (URL, email file, QR code image)
- Perform preprocessing and feature extraction
- Load the trained XGBoost model
- Return prediction result: Phishing / Legitimate

The API is hosted on a secure cloud service and connected with Firebase for user authentication and storage.

G. Chrome Extension Integration

The trained model is integrated into a Chrome browser extension to enable real-time phishing detection.

Extension Workflow:

1. User installs the extension and logs in through Firebase Authentication
2. Extension captures current webpage URL or accepts user inputs:
    a. URL text
    b. .eml or PDF email file
    c. QR code image or scanner
3. Inputs are sent to the backend API
4. Prediction result is displayed instantly inside the extension
5. User can check accuracy and detection history

H. Performance Measurement

The model's performance is evaluated using:

- Accuracy
- Precision
- Recall
- F1 Score
- Confusion Matrix

These metrics validate the effectiveness of the detection model for real-time phishing attacks.

V. IMPLEMENTATION

The implementation of *The Phish Finder* system is carried out through the combined development of the machine learning model, backend API, Firebase authentication, and Chrome browser extension. The major implementation steps are described below:

1. Dataset Integration

- The phishing and legitimate datasets for URLs, emails, and QR codes are imported into the development environment.
- All datasets are organized into a unified structure for further processing.

2. Machine Learning Model Implementation

- The extracted features from URLs, emails, and QR codes are used to train the XGBoost classifier.
- The trained model is validated using testing data and then saved for real-time prediction.
- This model becomes the central decision-making component of the system.

3. Backend API Implementation

- A backend API is developed to connect the Chrome extension with the machine learning model.
- The API receives user input (URL, email file, or QR code), processes it, and returns the prediction result.
- The API ensures smooth communication between the model and the user interface.

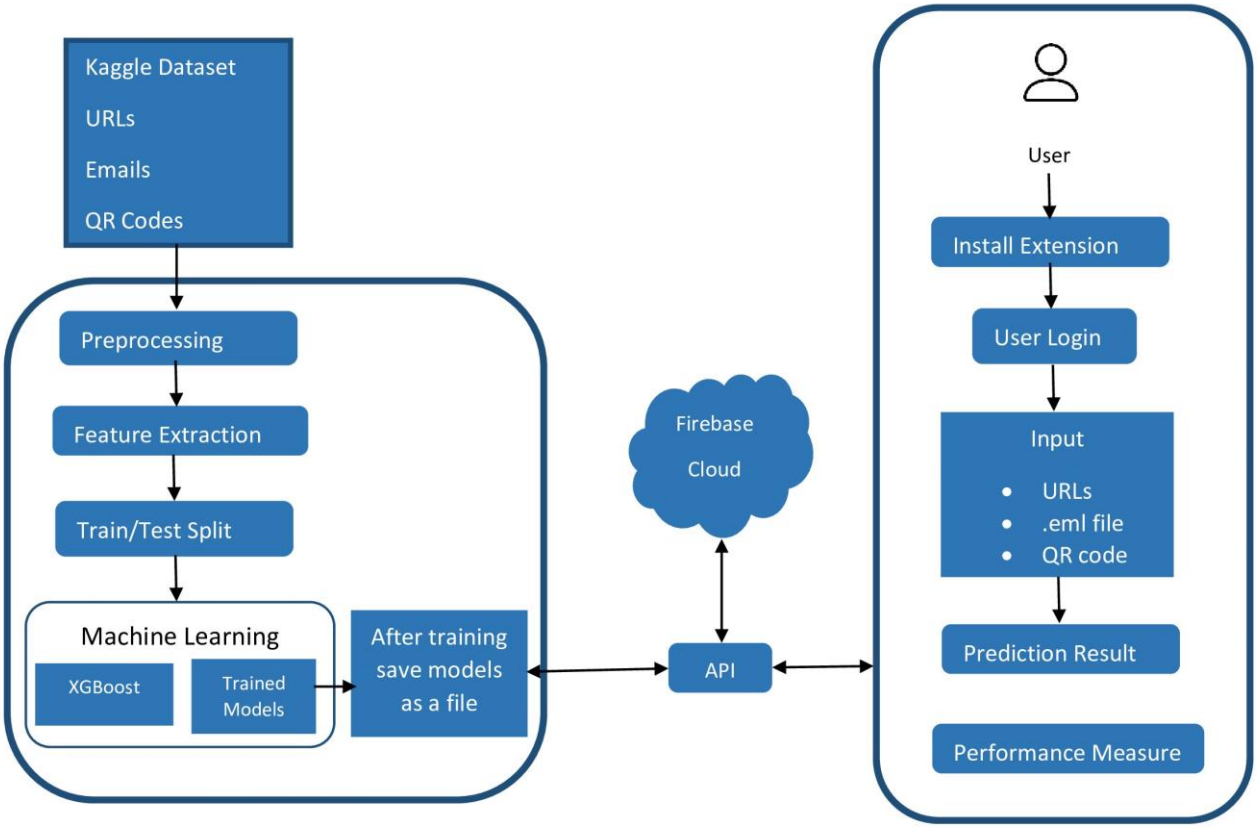

Figure 1. System Architecture

4. Firebase Authentication Setup

- Firebase Authentication is implemented for secure user login and registration.
- Only authenticated users are allowed to access the detection features within the browser extension.

5. Chrome Extension Development

- A Chrome extension is created as the main interface for users.
- It allows users to enter URLs, upload email files, or upload/scan QR code images.
- The extension sends these inputs to the backend API and displays the phishing detection result in real time.

6. System Integration

- All modules—XGBoost model, backend API, Firebase authentication, and Chrome extension—are integrated together.
- The integrated system works seamlessly to provide accurate, real-time phishing detection for multiple input formats.

VI. Result & Discussion

The proposed system was evaluated using the testing portion of the phishing datasets for URLs, emails, and QR codes. The trained XGBoost model demonstrated strong performance and achieved high prediction accuracy, indicating its effectiveness in identifying phishing patterns across different input types. The model was able to correctly classify most phishing and legitimate samples due to the rich set of extracted features and the boosting mechanism used during training. The results show that URL-based features, such as length, special characters, and HTTPS usage, contributed significantly to identifying malicious websites. Similarly, email-related features, including suspicious keywords and mismatched sender domains, helped the model detect fraudulent email files. For QR codes, the system successfully decoded the embedded links and classified them using the same trained model.

The Chrome extension was tested in real browsing conditions, and it provided instant detection results without noticeable delay. Users were able to enter URLs, upload emails, and scan QR codes easily, and the extension responded with clear phishing or legitimate labels. The integration with Firebase Authentication worked smoothly, allowing only verified users to access the features. Overall, the results demonstrate that the system successfully combines machine learning with a user-friendly interface to deliver real-time phishing detection. The discussion shows that the model performs consistently across multiple formats, making the system more versatile than traditional single-input phishing detectors.

VII. Conclusion

The Phish Finder system successfully demonstrates an effective and practical solution for detecting phishing attacks across multiple input formats, including URLs, email files, and QR codes. By integrating a trained XGBoost machine learning model with a user-friendly Chrome browser extension, the system provides real-time protection to users while browsing or analyzing suspicious content. The use of Firebase Authentication ensures secure access, while the backend API enables seamless communication between the model and the extension. Experimental results show that the model achieves high accuracy and performs consistently across all three detection categories. Overall, the system offers a reliable, scalable, and easy-to-use approach to phishing detection and can serve as a strong foundation for future enhancements and deployment in real-world environments.

REFERENCES

[1] Y. Hmimou, M. Tabaa, A. Khiat, and Z. Hidila, "A multi-agent system for cybersecurity threat detection and correlation using large language models," 2025.
[2] K. Taha, "SMART: Semantic, multi-objective, and reinforcement-based adversarial training for email spam detection," 2025.
[3] W. Li, S. Manickam, Y.-W. Chong, W. Leng, and P. Nanda, "A state-of-the art review on phishing website detection techniques," 2024.
[4] U. Zara, K. Ayyub, H. U. Khan, A. Daud, T. Alsahfi, and S. G. Ahmad, "Phishing website detection using deep learning models," 2024.
[5] O. K. Sahingoz, E. Buber, and E. Kugu, "DEPHIDES: Deep learning-based phishing detection system," 2023.
[6] J. D. Duarte, P. Chagas Junior, J. P. J. da Costa, E. J. da Costa, L. P. de Melo, R. R. Nunes, C. G. V. N. Soares, and T. E. da C. Silva, "Machine learning for early detection of phishing URLs in parked domains: An approach applied to a financial institution," 2025.
[7] M. Safran and A. Musleh, "PhishingGNN: Phishing email detection using graph attention networks and transformer-based feature extraction," 2025.
[8] W. Li, S. U. A. Laghari, S. Manickam, Y.-W. Chong, and B. Li, "Machine learning-enabled attacks on anti-phishing blacklists," 2024.
[9] S. Kavya and D. Sumathi, "Multimodal and temporal graph fusion framework for advanced phishing website detection," 2025.
[10] D. J. Dsouza, A. P. Rodrigues, and R. Fernandes, "Multi-modal com-parative analysis on execution of phishing detection using artificial intelligence," 2024.
[11] N. Yalc¸ın, S. C¸ akır, and S. ¨Unaldı, "Attack detection using artificial intelligence methods for SCADA security," 2024.
[12] T. Wangchuk and T. Gonsalves, "Multimodal phishing detection on social networking sites: A systematic review," 2025.
[13] S. Ahmad, M. Zaman, A. S. Al-Shamayleh, R. Ahmad, S. M. Ab- dulhamid, I. Ergen, and A. Akhunzada, "Across the spectrum: In-depth review of AI-based models for phishing detection," 2024.
[14] T. Koide, H. Nakano, and D. Chiba, "ChatPhishDetector: Detecting phishing sites using large language models," 2024.
[15] F. Heiding, B. Schneier, A. Vishwanath, J. Bernstein, and P. S. Park, "Devising and detecting phishing emails using large language models," 2024.
[16] S. Mushtaq, T. Javed, and M. M. Su'ud, "Ensemble learning-powered URL phishing detection: A performance-driven approach," 2024.
[17] Y. Wei, M. Nakayama, and Y. Sekiya, "Enhancing generalization in phishing URL detection via a fine-tuned BERT-based multimodal approach," 2025.
[18] F. S. Alsubaei, A. A. Almazroi, and N. Ayub, "Enhancing phishing detection: A novel hybrid deep learning framework for cybercrime forensics," 2024.
[19] J. T. Nsoh and H. Malki, "Integrating sociocultural intelligence into cybersecurity: A LESCANT-based approach for phishing and social engineering detection," 2025.
[20] G. D. Bispo, C. A. B. de Andrade, G. M. Saiki, R. V. Borges, A. L. M. Serrano, G. P. Rocha Filho, and V. P. Gonc¸alves, "PHILDER: Lightweight framework for intelligent phishing detection on resource-limited devices,"2025.
[21] X. Liu and J. Fu, "SPWalk: Similar Property Oriented Feature Learning for Phishing Detection," May 2020.
[22] R. Mahajan and I. Siddavatam, "Phishing website detection usin machine learning algorithms," 2018.
[23] K. Barik, S. Misra, and R. Mohan, "Web-based phishing URL detection model using deep learning optimization techniques," 2024.
[24] S. Kavya and D. Sumathi, "Staying ahead of phishers: A review of recent advances and emerging methodologies in phishing detection," 2024.
[25] S. A. A. A. Alsaidi, H. J. Mohammed, R. R. N. Al Ogaili, Z. A. Dashoor, A. H. Alsaeedi, D. Al-Shammary, and A. Ibaida, "HawkPhish-DNN cybersecurity model: Adaptive hybrid optimization and deep learning for enhanced multi-objective phishing URL detection," 2025.
[26] H. Ghalechyan, E. Israyelyan, A. Arakelyan, G. Hovhannisyan, and A. Davtyan, "Phishing URL detection with neural networks: An empirical study," 2024.
[27] T. Ige, C. Kiekintveld, A. Piplai, A. Wagler, O. Kolade, and B. H. Matti, "An investigation into the performances of the current state-of-the-art Naive Bayes, Non-Bayesian and Deep Learning based classifier for phishing detection: A survey," 2024.
[28] O. K. Sahingoz, E. Buber, O. Demir, and B. Diri, "Machine learning based phishing detection from URLs," 2018.
[29] A. Abu Zuraiq and M. Alkasassbeh, "Review: Phishing detection approaches," 2021.
[30] A. A. Orunsolu, A. S. Sodiya, and A. T. Akinwale, "A predictive model for phishing detection," 2022.
[31] V. Shahrivari, M. M. Darabi, and M. Izadi, "Phishing detection using machine learning techniques," 2020.
[32] R. Zieni, L. Massari, and M. C. Calzarossa, "Phishing or not phishing? A survey on the detection of phishing websites," 2023.
[33] S. Asiri, Y. Xiao, S. Alzahrani, S. Li, and T. Li, "A survey of intelligent detection designs of HTML URL phishing attacks," 2022.

[34] D. Jibat, S. Jamjoom, Q. Abu Al-Haija, and A. Qusef, "A systematic review: Detecting phishing websites using data mining models," 2023.
[35] A. Karim, M. Shahroz, K. Mustofa, S. B. Belhaouari, and S. R. K. Joga, "Phishing detection system through hybrid machine learning based on URL," 2023.
[36] L. Jovanovic, D. Jovanovic, M. Antonijevic, B. Nikolic, N. Bacanin, M. Zivkovic, and I. Strumberger, "Improving phishing website detection using a hybrid two-level framework for feature selection and XGBoost tuning," 2023.
[37] L. Tang and Q. H. Mahmoud, "A deep learning-based framework for phishing website detection," 2021.
[38] S. Salloum, T. Gaber, S. Vadera, and K. Shaalan, "A systematic literature review on phishing email detection using natural language processing techniques," 2022.
[39] L. R. Kalabarige, R. S. Rao, A. Abraham, and L. A. Gabralla, "Multilayer stacked ensemble learning model to detect phishing websites,"2022.
[40] S. Al-Ahmadi, A. Alotaibi, and O. Alsaleh, "PDGAN: Phishing detection with generative adversarial networks," 2022.
[41] Y. Wei and Y. Sekiya, "Sufficiency of ensemble machine learning methods for phishing websites detection,"2022.
[42] P. Yang, G. Zhao, and P. Zeng, "Phishing website detection based on multidimensional features driven by deep learning," 2019.
[43] X. Liu and J. Fu, "SPWalk: Similar property oriented feature learning for phishing detection," 2020.
[44] Y. Fang, C. Zhang, C. Huang, L. Liu, and Y. Yang, "Phishing email detection using improved RCNN model with multilevel vectors and attention mechanism," 2019.
[45] E. S. Gualberto, R. T. de Sousa Jr., T. P. de B. Vieira, J. P. C. Lustosa da Costa, and C. G. Duque, "The answer is in the text: Multi-stage methods for phishing detection based on feature engineering," 2020.
[46] E. Zhu, Y. Chen, C. Ye, X. Li, and F. Liu, "OFS-NN: An effective phishing websites detection model based on optimal feature selection and neural network," 2019.
[47] I. Kara, M. Ok, and A. Ozaday, "Characteristics of understanding URLs and domain names features: The detection of phishing websites with machine learning methods," 2022.
[48] A. S. Rafsanjani, N. B. Kamaruddin, H. M. Rusli, and M. Dabbagh, "QsecR: Secure QR code scanner according to a novel malicious URL detection framework," 2023.
[49] A. Khalid, M. Hanif, A. Hameed, Z. Ashraf, M. M. Alnfiai, and S. M. M. Alnefaie, "LogiTriBlend: A novel hybrid stacking approach for enhanced phishing email detection using ML models and vectorization approach," 2024.
[50] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq, and M. K. Khan, "Comprehensive review of cybercrime detection techniques," 2020.