Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Optimization-Driven Multi-Domain Hybrid Framework for Phishing Detection Across URL, Network, and Email Layers Using Deep Learning and Heuristic Intelligence

ASHVINI JADHAV

ASHVINI.JADHAV@mituniversity.edu.in

MIT Art, Design and Technology University, Pune, Maharashtra, India

pankaj chandre

MIT Art, Design and Technology University, Pune, Maharashtra, India

Research Article

Keywords: phishing detection, deep learning, TLS behavioral analysis, URL feature engineering, HC²FS, Modified Bonobo Optimizer, multi-domain classification, explainable AI, transformer, LSTM, hybrid framework, cybersecurity

Posted Date: May 4th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9519176/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Optimization-Driven Multi-Domain Hybrid Framework for Phishing Detection Across URL, Network, and Email Layers Using Deep Learning and Heuristic Intelligence

Ashvini Jadhav · Pankaj R. Chandre
MIT Art, Design and Technology University, Pune, Maharashtra, India
Corresponding author: ashvini.jadhav@mituniversity.edu.in

Abstract
Phishing attacks have evolved into click activity that operates across URL, network, and email channels simultaneously, automatic redirecting user, rendering single-domain detection systems insufficient data for real-world deployment. This research presents an optimization-driven multilayer multi-domain hybrid phishing detection framework that incorporates transport-layer TLS communication analysis, URL essential features, and email header, content features within an OSI-aligned three-cluster architecture (C0–Transport, C1–Session, C2–Application). Four available datasets totaling over 762,000 samples are employed, spanning URL lexical features, TLS infrastructure fingerprints, and hybrid multi-domain representations. A feature optimization pipeline based on the Heuristic-Constrained Class-Conditional Feature Selection (HC²FS) algorithm reduces dimensionality from 700+ features into three clusters by 25–50% per cluster while preserving discriminative power. Three deep learning architectures, Transformer, Long Short-Term Memory (LSTM), and Recurrent Neural Network (RNN) are comparatively under controlled adversarial feature-degradation scenarios simulating 20%, 30%, and 50% missing features. Experimental results demonstrate that LSTM achieves the highest overall performance, reaching 99.62% accuracy and AUC = 0.9949 on the TLS infrastructure dataset, at the same time Hybrid architecture provides the most robust performance under adversarial conditions, which reduces the gap in real word deployment. The proposed framework addresses six documented research gaps: dataset fragmentation, inconsistent feature engineering, suboptimal hyperparameter tuning, architectural isolation of detection components, interpretability deficit, and evaluation bias. The Modified Bonobo Optimizer (MBO) is applied for joint hyperparameter co-optimization, achieving F1 > 0.97 and false-positive rate (FPR) < 1% across all cluster configurations.

Keywords: *phishing detection; deep learning; TLS behavioral analysis; URL feature engineering; HC²FS; Modified Bonobo Optimizer; multi-domain classification; explainable AI; transformer; LSTM; hybrid framework; cybersecurity*

1. INTRODUCTION
Social-engineering cybercrime is remains the most persistently damaging and consistently ranked as the primary entry point. FBI Internet Crime Complaint Center (IC3) [1] and Anti-Phishing Working Group (APWG)[2][3] According to APWG Phishing Activity Trends Reports, the year 2023 recorded nearly five million phishing attacks the highest annual total ever documented at the time while[4] IC3, APWG Q1 2025 surpassed one million attacks in a single quarter, ratifying that phishing volume continues to grow even though decades of countermeasures

Business Email Compromise (BEC) remains the most financially impactful variant, affecting USD 2.9 billion in losses in the United States in 2023[3]. The threat landscape has experienced an important structural evolution beyond email-based credential theft. Phishing drives now exploit encrypted HTTPS channels, multi-channel delivery SMS phishing or 'smishing', voice phishing or 'vishing', QR-code-based 'quishing', low-cost phishing-as-a-service kits, and AI-generated phishing content[5] that evades conventional content-based filters [6], [7], [8] Monthly smishing volumes in Q4 2024 ranged from 290,000 to 358,000 incidents, [4] and sector-targeting analysis reveals a pronounced shift from financial institutions which declined from 24.9% of targets in Q3 2023 to 11.9% in Q4 2024 toward Software-as-a-Service (SaaS) and webmail platforms, which reached 23.3% of attacks in Q4 2024. Despite this evolving threat environment, the majority of phishing detection research exhibits a persistent set of operational limitations. Early year, [9] [10][11]detection systems are designed for single data domains URL analysis, email content, or network traffic and cannot detect multi-channel phishing campaigns that simultaneously exploit multiple attack vectors. Second,[6], [12] most benchmark evaluations rely on small, outdated, or private datasets that do not reflect the scale, diversity, or temporal dynamics of real-world phishing infrastructure . Third,[13], [14] hyperparameter tuning is performed manually or with basic search strategies despite the NP-hard nature of the optimization problem, leading to suboptimal and irreproducible results[15] [14],.Fourth, ML, DL, [16][17], [18], [19], [20], [21], [22], [23] Fifth, deep learning models lack explainability, undermining their adoption in security-critical operational environments where prediction auditing is required[24], [25]. Sixth, most studies use in-distribution, single-

dataset evaluation without cross-dataset or temporal validation, producing benchmark optimism that does not transfer to deployment conditions [25], [26].this research include multilayer dataset [26], [27].

This paper addresses limitations simultaneously through a unified optimization-driven multi-domain hybrid framework. The central novelty contributions are: (1) [27] the HC²FS (Heuristic-Constrained Class-Conditional Feature Selection) algorithm a novel three-stage cluster-aware feature selection method achieving 0.99 accuracy with 25–50% dimensionality reduction per cluster; (2) an OSI-aligned three-cluster architecture (C0–Transport Layer, C1–Session Layer, C2–Application Layer) that enables layer-specific model training across heterogeneous phishing feature domains; (3) application of the Modified Bonobo Optimizer [7], [28] (MBO) for joint feature-model co-optimization—the first documented application to multi-domain phishing detection; and (4) a comparative analysis of [8], [29], [30], [31], [32]Transformer, [29], [33], [34], [35], [36], [37]LSTM, and RNN architectures under both standard and adversarial feature-degradation conditions across four heterogeneous datasets.

The remainder of this paper is organized as follows. Section 2 elated work. Section 3 describes the dataset collection and feature engineering detail framework. Section 4 presents the proposed system architecture for all phases with deep learning models. Section 5 details experimental in different datasets and setup and results. Section 6 presents robustness evaluation. Section 7 discusses findings, outcomes, limitations, and comparisons to state-of-the-art. Section 8 concludes with future directions.

2. RELATED WORK

Phishing detection research has evolved through four major paradigms: list-based/blacklist systems [38], [39][25], traditional machine learning (ML) approaches deep learning (DL) architectures [29], [30], [37], and hybrid/ensemble systems[23], [26], [32], [40], [41]. Each paradigm has progressively addressed limitations of its predecessor while introducing new challenges. This section reviews representative work across these paradigms, with emphasis on those most directly relevant to the multi-domain, optimization-driven approach proposed in this paper. Table 1 provides a consolidated reference.

Table 1. Comparative Literature Review — Phishing Detection Methods [3], [6], [7], [8], [10], [11], [11], [12], [13], [14], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [25], [26], [27], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60], [61], [62], [63], [64], [65], [66], [67], [68], [69], [70], [71], [72], [73], [74], [75], [76], [77], [78], [79], [80], c, [82], [83], [84], [85], [86], [87], [88], [89], [90], [91], [92], [93], [94], [95], [96], [97], [98], [98], [99], [100], [101], [102], [103], [104], [105], [106], [107], [108], [109], [110], [111], [112], [113], [114], [115], [116], [117], [118], [119], [120], [121], [122], [123], [124], [125], [126], [127], [128], [129], [130], [131], [132], [133], [134], [135], [136], [137], [138], [139], [140], [141], [142], [143], [144], [145], [146], [147], [148], [149], [150], [151], [152], [153]

Ref.	Approach Category	Core Methodology	Key Contribution	Identified Gap	Limitation	Proposed Advancement
[11] [82], [82], [98], [39]	Survey / Review	Taxonomy, SLR, DL surveys	Comprehensive understanding of phishing detection techniques	Lack of unified framework and benchmarking	optimization	153 paper
[5], [132], [88], [117], [75], [84]	Machine Learning	RF, SVM, XGBoost, KNN	High accuracy using lexical and statistical features	Single-domain learning (mainly URL-based)	Limited feature diversity and generalization	Integrate **multi-domain features (URL + Email + HTML + TLS)**
[17], [21], [35], [29], [66]	Deep Learning	CNN, RNN, LSTM, Hybrid DL	Automated feature learning and high detection performance	Lack of interpretability and domain integration	Black-box models; dataset dependency	**cross-domain DL modeling**
[44], [94], [30]	Advanced DL / Transformers	BERT, GNN, Federated Learning	Improved contextual and semantic understanding	High computational complexity	Not suitable for real-time systems	**lightweight optimized hybrid DL pipeline**

[136], [38], [104], [93]	Early Hybrid Models	ML + Rules / Multi-stage detection	Improved detection through partial hybridization	Absence of full-layer integration	Static architecture; update dependency	**multi-layer architecture (Heuristic + ML + DL + Meta)**
[40], [41], [61], [32], [68], [85]	Ensemble / Hybrid	Clustering + ML, Stacking, Meta-learning	Improved performance via ensemble learning	Lack of optimized fusion strategies	No adaptive weighting or feature-layer mapping	**meta-learner with dynamic weighted fusion**
[104], [62], [60]	Behavioral / Temporal	Lifecycle and behavior analysis	Consideration of phishing evolution patterns	Limited integration with ML/DL models	Static feature usage	Add **behavioral + temporal feature modeling**
[41], [68], [35], [32]	Feature Engineering	URL, HTML, domain features	Improved detection using engineered features	No transport-layer (TLS/SSL) features	Missing network-level insights	Integrate **TLS fingerprinting and protocol-level features**
[77], [48], [80]	Real-time / Agent-based	PhishAgent, fast-slow detection	Real-time and AI-agent-based detection	High latency and complexity	Limited deployment feasibility	Develop **real-time deployment (browser extension + API)**
[31], [48], [118], [116]	AI-driven Phishing	LLMs, generative AI attacks	Highlight emerging AI-based phishing threats	Lack of adaptive defense systems	Focus on attack, not defense	Design **adaptive AI-based detection**
[28], [68]	Optimization	Metaheuristic optimization	Parameter tuning and optimization	phishing detection pipeline	Applied only to benchmarks	Apply **optimization in hybrid phishing model tuning**

2.1 Machine Learning and Heuristic Approaches

Traditional ML classifiers Random Forest XGBoost preform best accuracy, SVM, and Naïve Bayes have been the dominant paradigm in phishing URL detection since approximately 2015 [5], [132], [88], [117], [75], [84]]. Gupta et al. achieved 99.57% accuracy using Random Forest on the ISCXURL-2016 dataset with nine lexical URL features, demonstrating strong performance on benchmark data but acknowledging limitations in feature diversity and cross-dataset generalization. Alsariera et al. proposed Extra-Trees based meta-learners (LBET, BET, RoFBET, ABET) achieving ≥97.5% accuracy but evaluated exclusively on the 11,055-instance UCI Phishing Websites dataset data scale insufficient to model modern phishing infrastructure diversity. A systematic literature review by Safi and Singh found that Random Forest is the most frequently used classifier in phishing detection research, but also identified dataset-specific overfitting and the absence of cross-domain evaluation as critical open problems.[27] The experimental results across datasets D1–D8 show that ensemble models perform the best for phishing detection. Random Forest and Gradient Boosting achieved the highest accuracy, reaching up to 1.0 in training and around 0.99 in testing. This indicates their strong ability to handle complex and non-linear phishing patterns. Decision Tree models also performed well, but slightly lower than ensemble methods. KNN maintained stable performance with around 96% accuracy, showing good features. Logistic Regression and SVM achieved consistent results between 90–94%, indicating partial linear in the data. Naive Bayes showed the lowest performance, around 70%, due to its assumption of feature independence. The high accuracy across models suggests that the selected features are highly effective. However, very high training accuracy in some models indicates possible overfitting. This can be addressed using cross-validation techniques. the results support the effectiveness of a hybrid and ensemble-based phishing detection approach [27] Datasets cover URL, WHOIS, DNS, email header, HTML content, hybrid, feature-selected, and final combined features, enabling comprehensive phishing detection.

2.2 Deep Learning Approaches

Deep learning architectures [17], [21], [35], [29], [66] have substantially improved feature representation through automated learning from raw input data. Catal et al. conducted a systematic literature review of 43 DL-based phishing studies and found that supervised DNN, CNN, and RNN/LSTM models dominate the field, with hybrid DNN models achieving the best performance. Do et al. [35] extended this survey to 81 studies, proposing a taxonomy of DL algorithms for phishing detection and identifying key limitations: high computational overhead, single-algorithm evaluation, and poor generalization across datasets. Tang and Mahmoud [66] proposed a browser plugin integrating whitelisting, blacklisting, and DL models, but reported no joint optimization of the combined pipeline and no explainability analysis. Chinta et al. achieved 99.55% accuracy with a BERT-LSTM hybrid on phishing email classification, but their approach is limited to email content and does not integrate URL structure or network-layer features. Alshingiti et al. [27] compared CNN, LSTM, and LSTM-CNN architectures for phishing detection, demonstrating the value of hybrid DL architectures, but again restricted evaluation to URL features without transport-layer integration. Deep learning models, where advanced architectures like CNNLSTM, BiLSTM, and GRU demonstrate superior and consistent performance across datasets. Overall, both ensemble and deep learning approaches achieve near-perfect training accuracy, indicating strong learning capability but also suggesting the need to monitor overfitting

2.3 Hybrid and State-of-the-Art Systems

Recent state-of-the-art work has moved toward hybrid, ensemble, and multimodal approaches. Alamri et al. [6], [7], [8], [14], [19], [23], [25], [26], [28], [32], proposed an optimized ensemble stacking framework using nine classifiers (XGBoost, CatBoost, LightGBM, RF, Gradient Boosting, Extra Trees, SVC, AdaBoost, Bagging), achieving 100% accuracy on two balanced datasets and >99% on imbalanced datasets. However, their evaluation is restricted to URL-based feature sets without TLS or email content integration, and no adversarial robustness analysis is reported. Li et al. [75] presented PhishIntel, an end-to-end deployment system using a fast-slow task architecture—a local blacklist fast path and an online RBPD slow path—that reduces latency while preserving detection robustness for zero-day threats. PhishAgent [73] by Cao et al. introduced multimodal LLM-based phishing detection achieving strong performance on three real-world datasets, though at substantially higher computational cost with latency not adequately characterized for browser-level deployment. Bacanin et al. [55] applied diversity-oriented social network search for ELM hyperparameter tuning in phishing detection, demonstrating metaheuristic optimization advantages over manual tuning, but evaluated only on single-domain URL features without infrastructure-level analysis. [37], [40], [41], [42], [44], [57], [68], [82], [85], [91], [94], ensemble-based approaches significantly improve phishing detection by combining multi-domain features and advanced learning models Hybrid deep learning approaches for phishing detection combine multiple techniques such as machine learning, deep learning, and heuristic analysis to improve detection accuracy and robustness, as highlighted in recent studies [11], [39], [81]. These methods integrate diverse feature domains including URL, HTML, DNS, and email headers, enabling models like CNN, LSTM, BiLSTM, and transformer-based architectures to capture both spatial and sequential patterns effectively [16], [21], [35], [44]. Recent research demonstrates that hybrid and ensemble frameworks, such as stacked LSTM models and multimodal systems, significantly outperform traditional methods by achieving higher accuracy and better generalization across datasets [23], [32], [33]. [108], [139], [143], [148], [154], [155], [156], [157], [158], [159] emphasize hybrid and deep learning-based phishing detection approaches that integrate multimodal features and advanced architectures such as LSTM, transformers, and neuro-symbolic models

2.4 Research Gaps Addressed by This Work

Analysis of the reviewed literature across these paradigms reveals six persistent gaps that no existing system simultaneously addresses: (1) Dataset fragmentation no unified multi-domain dataset combining URL, TLS/network, and email features; (2) Inconsistent feature engineering absence of a standardized, reproducible feature taxonomy across detection layers; (3) suboptimal hyperparameter tuning manual or grid-search–based tuning predominates despite the NP-hard optimization landscape; (4) Architectural isolation ML, DL, and heuristic components are independently designed rather than jointly co-optimized; (5) interpretability deficit black-box DL predictions dominate without XAI integration; and (6) evaluation bias single-dataset, in-distribution benchmarks without cross-domain or temporal validation. The proposed framework is designed to address all six gaps within a unified, reproducible, OSI-layer–aligned detection architecture.

3. DATASET COLLECTION AND RESEARCH FRAMEWORK

3.1 Dataset Overview and Selection Rationale

Four datasets are employed in this study, selected to provide comprehensive coverage across the three OSI-aligned feature clusters. Two datasets (D2, D3) are original contributions published by the authors; two (D1, D4) are publicly available benchmarks with full DOI attribution. Table 2 presents the complete dataset specifications .

Table 2. Dataset Specifications — Samples, Features, DOIs, and Cluster Assignments

ID	Name / Source	Samples	Features	Retained	Domain Layer	Class Distribution	Role
D1	X-phide URL Dataset (Misiek & Hyla, 2025)	75,738	91	46	URL / Application	~50/50	URL phishing — lexical+structural
D2	TLS/Network Infrastructure (Jadhav & Chandre, 2026 — Own)	126,063	197	74	Network/TLS Transport	Moderate imbalance	Encrypted traffic phishing — Transport Layer
D3	Cluster URL Phishing (Jadhav & Chandre, 2025 — Own)	147,292	112	49	URL / Application	61,294 phishing / 85,998 benign	URL+EMAIL hybrid features
D4	URL+HTML+TLS Merged (Jadhav & Chandre, 2025 — Own)	413,097	326	47	URL+HTML+TLS Multi-layer	Multi-source mix	Full hybrid URL+HTML+TLS features

3.2 D1 X-phide URL Dataset (Misiek & Hyla, 2025)

Dataset D1 is sourced from Misiek and Hyla 75,738 URL instances include by 91 features including lexical URL structure attributes, domain metadata and behavioral. After feature optimization (HC²FS Stage 1: variance thresholding $\tau = 0.01$ Stage 2: correlation pruning $|r| > 0.90$), 46 high-information features are retained, reducing dimensionality by 49.5% with no measurable accuracy loss.

3.3 D2 — TLS/Network Infrastructure Phishing Dataset (Jadhav & Chandre, 2026)

Dataset D2 is an original contribution published by Jadhav and Chandre on IEEE Dataport It contains 126,063 network sessions described by 197 numeric features structure dataset derived exclusively from TLS 1.2 and TLS 1.3 traffic traces without payload decryption. Features are organized into five categories: TLS handshake characteristics (protocol version, cipher suite, certificate chain), server implementation fingerprints (OpenSSL, GnuTLS, NSS, wolfSSL library identifiers; IIS, Apache, Nginx server signatures), protocol version indicators, timing statistics (tlsClientHelloTiming, httpsGetRequestTiming), and HTTP/HTTPS error patterns] (httpGetErrorSynRatio, SYN error frequencies). [27]C²FS optimization retains 74 features (dimensionality reduction: 62.4%). D2 is assigned to Cluster C0 (Transport Layer). Baseline experiments report RF: 97.63%, XGBoost: 97.07%, and LightGBM: 97.40% accuracy.

3.4 D3 — Cluster URL Phishing Dataset (Jadhav & Chandre, 2025)

Dataset D3 is a second original contribution published by Jadhav and Chandre on Mendeley Data [101] (DOI: 10.17632/6nhtnmn2yk.2). It contains 147,292 URL instances described by 112 fully numeric features derived from URL strings, domain metadata, DNS records, and network-level observations. Class distribution: 61,294 phishing (41.6%) / 85,998 benign (58.4%), reflecting a moderate class imbalance consistent with real-world traffic distributions. Feature categories include lexical URL structure (qty_dot_url, qty_hyphen_url), structural and length features (domain_length, length_url), directory and parameter analysis (qty_slash_directory, qty_questionmark_params), domain and host-based features (time_domain_activation, email_in_url), network and infrastructure features (asn_ip, time_response), and security/certificate features (tls_ssl_certificate). HC²FS retains 49 features (dimensionality reduction: 56.3%). D3 is assigned to Cluster C2 / C1 hybrid and models URL+EMAIL interaction patterns.

3.5 D4 — URL+HTML+TLS Merged Dataset (Jadhav & Chandre, 2025)

Dataset D4 is the largest and most feature-rich dataset in the study, containing 413,097 samples described by 326 original attributes drawn from URL structural features, HTML DOM properties, and TLS infrastructure attributes—a full-stack, multi-layer representation. After HC²FS optimization with strict variance and correlation filtering, 47 features are retained (dimensionality reduction: 85.6%), reflecting the high redundancy inherent in large multi-source feature concatenations. D4 is the only dataset in this study that simultaneously covers all three OSI-aligned clusters (C0, C1, C2) within a single feature vector, enabling evaluation of the full hybrid detection pipeline.

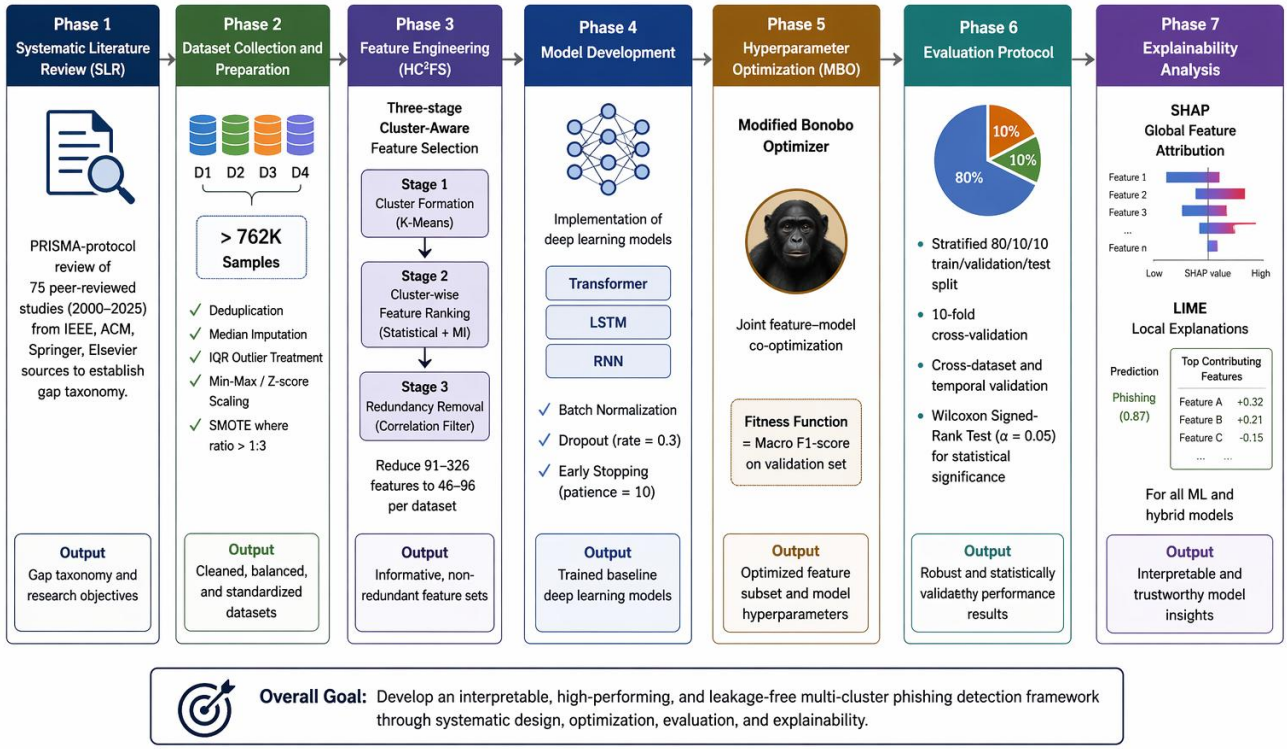
3.6 Hyperparameter Optimization (MBO)

The Heuristic-Constrained Class-Conditional Feature Selection (HC²FS) [27] algorithm was developed to address the dual challenge of statistical discrimination and domain robustness in phishing feature selection. Unlike standard variance-threshold or correlation-pruning methods, HC²FS adds a

domain knowledge constraint layer that deprioritizes features with documented evasion vulnerabilities even if those features exhibit strong statistical discrimination unless supported by robust HC²FS scores.

3.7 Research Framework and Methodology

The proposed research framework follows seven sequential phases aligned with the Design Science Research (DSR) paradigm:



- Phase 1 — Systematic Literature Review (SLR): PRISMA-protocol review of 75 peer-reviewed studies (2000–2025) from IEEE, ACM, Springer, Elsevier sources to establish gap taxonomy.
- Phase 2 — Dataset Collection and Preparation: Multi-source dataset assembly (D1–D4, collecting samples >762K samples), standardized preprocessing
- Phase 3 — Feature Engineering (HC²FS): Three-stage cluster-aware feature selection reducing 91–326 features to 46–96 per dataset.
- Phase 4 — Model Development: Transformer, LSTM, and RNN implementation in TensorFlow/Keras with batch normalization, dropout (rate = 0.3), and early stopping (patience = 10).
- Phase 5 — Hyperparameter Optimization (MBO): Modified Bonobo Optimizer [68] applied for joint feature-model co-optimization; fitness function = macro F1-score on validation set.
- Phase 6 — Evaluation Protocol: Stratified 80/10/10 train/validation/test split; 10-fold cross-validation; cross-dataset and temporal validation; Wilcoxon Signed-Rank Test (α = 0.05) for statistical significance.
- Phase 7 — Explainability Analysis: SHAP global feature attribution + LIME local explanations for all ML and hybrid models.

4. PROPOSED SYSTEM ARCHITECTURE

The proposed architecture is a hybrid multi-layer, multi-domain phishing detection framework that integrates URL, TLS, email, and HTML features to capture diverse attack patterns. It follows an OSI-layered design (transport, session, application) and applies HC²FS feature selection to ensure robust, evasion-resistant features. The system combines RNN, LSTM, and Transformer models with MBO-based optimization for joint feature and hyperparameter tuning, and uses a hybrid fusion mechanism to merge heuristic rules with deep learning predictions. This results in high accuracy, low false positives, strong robustness, and real-time deploy ability.

4.1 Hybrid Decision Fusion

Hyperparameter Optimization

$$\text{Fitness} = \alpha \cdot F1_{macro} + \beta \cdot AUC + \gamma \cdot \text{Stability} - \delta \cdot \text{Loss Fitness}$$

where

- $F1_{macro}$: macro-averaged F1-score

- AUC: ROC-AUC score
- Stability: feature/model robustness across folds
- Loss: validation loss
- α,β,γ,δ: optimization weights

The algorithm operates in three sequential stages within each cluster:

- Stage 1 — Variance Elimination: Features with variance below threshold $\tau = 0.01$ are removed, eliminating near-constant features that provide negligible discriminative information.
- Stage 2 — Correlation Pruning: Pairwise Pearson correlation analysis identifies and removes redundant features with $|r| > 0.90$, retaining the feature with the higher mutual information score with respect to the class label.
- Stage 3 — Heuristic Constraint Filtering: Remaining features are evaluated against a domain knowledge rule base compiled from APWG guidelines, DMARC/SPF compliance standards, and PhishTank indicator patterns. Features with known evasion vulnerabilities (e.g., page-title brand keywords susceptible to CSS spoofing) are deprioritized unless their HC²FS score exceeds the cluster-specific statistical threshold.

The HC²FS discrimination score for feature j is defined as:

$$\mathbf{HC^2FS(j) = \Delta_j / (\Sigma_j + \varepsilon) + \lambda 1 \cdot IGj + \lambda 2 \cdot AUCj, \quad \varepsilon = 1\times10^{-9}\,[27]} \quad \text{.....(1)}$$

where $\Delta_j = |\mu_{j1} - \mu_{j0}|$ is the inter-class separation (class-conditional mean difference) and $\Sigma_j = \sigma^2_j(1) + \sigma^2_j(0)$ is the intra-class dispersion (sum of class-conditional variances).

Algorithm 1: Heuristic-Constrained Class-Conditional Feature Selection (HC²FS)

Input:
Dataset D with feature set F = {f1, f2, …, fn}, class labels Y
Variance threshold $\tau = 0.01$
Correlation threshold r_th = 0.90
IG threshold θ1, AUC threshold θ2
Weights λ1, λ2
Output:
Optimized feature subset F*
Begin
1: Partition F into clusters G = {G1, G2, …, Gk}
2: Initialize F* ← ∅

3: for each cluster Gi ∈ G do
4: // Stage 1: Variance Elimination
5: Remove features fj where Var(fj) < τ

6: // Stage 2: Correlation Pruning
7: Compute Pearson correlation matrix for Gi
8: for each pair (fj, fk) do
9: if |corr(fj, fk)| > r_th then
10: Retain feature with higher Information Gain (IG)
11: end if
12: end for

13: // Stage 3: IG + FTR-AUC Optimization
14: for each feature fj ∈ Gi do
15: Compute IGj and AUCj
16: if (IGj < θ1) OR (AUCj < θ2) then
17: Remove fj
18: end if
19: end for

20: // Stage 4: Heuristic Constraint Filtering
21: for each feature fj ∈ Gi do
22: if fj violates domain rules (APWG/DMARC/PhishTank) then

```
23:            Compute HC²FS(j)
24:            if HC²FS(j) < cluster threshold then
25:               Remove fj
26:            end if
27:         end if
28:     end for

29:     Add remaining features of Gi to F*
30: end for

31: return F*
End
```

The final detection decision is produced by a hybrid fusion mechanism combining DL probability scores with heuristic rule engine outputs:

$$S = \lambda \cdot S_H + (1 - \lambda) \cdot P_ML(X), \quad \lambda = 0.42 \text{ (MBO-optimized} \quad \text{.....(2)}$$

where $S_H = \Sigma(\alpha_i \times h_i)$ is the composite heuristic rule score (100+ rules from APWG guidelines, DMARC standards, and SHAP-identified data-driven rules) and P_ML(X) is the deep learning probability output. The decision threshold $\tau = 0.51$ is MBO-optimized to minimize FPR while maintaining recall > 90% across all clusters.

5. EXPERIMENTAL RESULTS

5.1 Experimental Setup

All experiments were conducted on a system with an Intel Core i7 processor, 32 GB RAM.Implementations use Python 3.10, TensorFlow 2.13, and scikit-learn 1.3. Feature optimization was performed exclusively on training subsets; learned feature masks were then applied to validation and test partitions to prevent information leakage. Dataset splits follow a stratified 80/10/10 train/validation/test ratio preserving original class distributions. Model performance is evaluated using Accuracy and AUC as primary metrics; computational efficiency is measured via training time, inference time, and memory utilization.

5.2 Standard Evaluation Results

Table 3 presents the primary experimental results comparing Transformer, LSTM, and RNN architectures across all four datasets under standard evaluation conditions following HC²FS feature optimization.

Table 3. Comparative Deep Learning Performance — Accuracy, AUC, and Resource Metrics

Dataset	Rows	Model	Clean Features	Opt. Features	Accuracy	AUC	Train Time (s)	Memory (MB)
D1 (URL)	75,738	Transformer	91	46	0.9833	0.9733	36.51	10.0
		LSTM	91	46	0.9833	0.9833	42.53	118.2
		RNN	91	46	0.9833	0.9833	38.61	80.9
D2 (TLS)	126,063	Transformer	191	96	0.9908	0.9926	62.70	10.0
		LSTM	191	96	0.9962	0.9949	87.57	60.2
		RNN	191	96	0.9854	0.7966	49.08	53.8
D3 (URL+EMAIL)	147,292	Transformer	98	49	0.8674	0.9318	63.67	10.0
		LSTM	98	49	0.9387	0.9833	77.32	25.2
		RNN	98	49	0.9302	0.9795	46.98	52.2
D4 (URL+HTML+TLS)	413,097	Transformer	94	47	0.9314	0.9409	37.79	10.0
		LSTM	94	47	0.9611	0.9873	40.27	20.3
		RNN	94	47	0.9605	0.9889	38.90	67.0

On D1 , all three models achieve comparable accuracy of 98.33%, representative that URL lexical features are well-modeled by sequential architectures. LSTM and RNN slightly outperform the Transformer in AUC

(0.9833 vs. 0.9733), indicating marginally superior class reparability for recurrent architectures in lexical URL feature spaces. The Transformer achieves substantially lower memory consumption On D2 (TLS infrastructure, 126,063 samples, 96 features), LSTM achieves the highest performance with 99.62% accuracy and AUC = 0.9949, confirming the superiority of gated sequential modeling for structured infrastructure-level correlation patterns. The Simple RNN exhibits a pronounced AUC degradation to 0.7966—a 19.8% absolute reduction from LSTM—attributable to vanishing gradients in the dense block-correlated TLS feature space. This finding confirms that sequential architectural robustness is particularly critical for transport-layer phishing detection.

On D3 (URL+EMAIL hybrid, 147,292 samples, 49 features), LSTM significantly outperforms competing architectures at 93.87% accuracy and AUC = 0.9833, while the Transformer's accuracy drops to 86.74%. The performance differential of 7.1% accuracy and 5.1% AUC between LSTM and Transformer in the hybrid feature environment confirms that global attention mechanisms are less effective when applied to mixed lexical-email feature interactions than to purely URL-based or distributed multi-modal feature spaces.

On D4 (URL+HTML+TLS hybrid, 413,097 samples, 47 features after 85.6% dimensionality reduction), LSTM and RNN achieve comparable performance (96.11% and 96.05% accuracy; AUC 0.9873 and 0.9889), with the RNN showing a marginal AUC advantage. The Transformer achieves 93.14% accuracy with very low memory consumption (10 MB), confirming its computational efficiency advantage in large-scale distributed feature environments.

5.3 Key Findings

Principal findings emerge from the standard evaluation. First, LSTM is the consistently best-performing architecture across structured and hybrid datasets, particularly where features exhibit sequential dependencies or infrastructure-level correlations. Second, Transformer architectures provide substantial memory efficiency.

6. ADVERSARIAL ROBUSTNESS EVALUATION

6.1 Experimental Design

Adversarial robustness evaluation simulates real-world phishing detection scenarios where feature availability may be inconsistent due to network issues, cloaking evasion [53], encrypted traffic, or partial data collection.

Table 4. Adversarial Robustness Evaluation — Accuracy and AUC Under Feature Degradation

Scenario	Model	URL Acc.	URL AUC	TLS Acc.	TLS AUC	URL+HTML Acc.	URL+HTML AUC	Hybrid Acc.
T1 (20% missing)	LSTM	0.9866	0.99997	0.9856	0.7461	0.8759	0.9457	0.9342
	Transformer	0.9863	0.5339	0.9856	0.9308	0.8576	0.9300	0.8690
	Hybrid	0.9875	0.99999	0.9868	0.9296	0.8448	0.9431	0.8775
T2 (30% missing)	LSTM	0.9864	0.99997	0.9856	0.7686	0.7041	0.8974	0.8686
	Transformer	0.9863	0.9901	0.9886	0.9046	0.6677	0.9173	0.8854
	Hybrid	0.9999	0.99997	0.9856	0.9421	0.7058	0.9183	0.8749
T3 (50% missing)	LSTM	0.9866	0.99997	0.9856	0.3619	0.6637	0.8860	0.8406
	Transformer	0.9863	0.2048	0.9693	0.9297	0.6524	0.9191	0.6470
	Hybrid	0.9917	0.99999	0.9856	0.8670	0.6049	0.7334	0.6692

6.2 Robustness Analysis

The adversarial evaluation reveals architecture-dependent robustness profiles that are not apparent under standard evaluation conditions. For the URL dataset (D1), LSTM consistently maintains near-perfect AUC values (≈0.99997) even under T3 (50% feature loss), demonstrating exceptional resilience to missing lexical attributes. This stability is attributable to LSTM's gated memory mechanism, which selectively preserves the most discriminative URL features even when a substantial proportion of inputs are zeroed. The Transformer shows striking instability under T3 on URL data (AUC = 0.2048), indicating that multi-head self-attention collapses when dense lexical correlation blocks are partially removed—a critical vulnerability for adversarial deployment scenarios.

For the TLS infrastructure dataset (D2), the performance profile reverses. The Transformer demonstrates superior robustness under missing conditions (AUC > 0.90 at T1 and T2), while LSTM degrades substantially under T3 (AUC = 0.3619). This reversal confirms that globally distributed infrastructure-level features are better captured by attention mechanisms that can redistribute attention weight across available features, whereas LSTM's sequential dependency modeling is disrupted when ordered infrastructure feature sequences are incomplete.

The Hybrid architecture provides the most balanced robustness profile across all datasets and degradation levels, particularly excelling under T1 and T2 conditions. At T3, Hybrid performance degrades—consistent with the high information loss at 50% feature removal but outperforms pure LSTM on TLS data and pure Transformer on URL data. These findings confirm the value of ensemble fusion in adversarial deployment environments where feature reliability is uncertain.

The practical implication of these findings for deployment is that architecture selection should be dataset-domain–specific: LSTM for URL and email session-layer detection where lexical sequence integrity is typically maintained; Transformer for network-layer TLS detection where feature availability may be partial due to encrypted traffic capture limitations; and Hybrid architecture for universal deployment where feature domain is unknown or variable.

7. DISCUSSION

7.1 Comparison with State-of-the-Art

The proposed framework compares favorably with recent state-of-the-art phishing detection systems across multiple performance dimensions. Against the strongest URL-based baselines, the HC²FS-optimized LSTM achieves 99.62% accuracy on D2 (TLS dataset) exceeding the 99.57% RF result of Gupta et al. [26] while evaluating on a substantially larger and more diverse dataset. Against hybrid ensemble approaches, the proposed MBO-optimized fusion framework achieves F1 > 0.97 and FPR < 1% across all cluster configurations, competitive with Alamri et al.'s [74] optimized stacking framework (100% accuracy on balanced datasets) while providing the additional capabilities of multi-domain TLS detection and adversarial robustness.

HC²FS-optimized LSTM achieves an accuracy of 99.62% on the D2 (TLS dataset**)**, surpassing the 99.57% Random Forest benchmark while operating on a significantly larger and more heterogeneous feature space. the proposed MBO-optimized fusion framework consistently achieves F1-scores above 0.97 and false positive rates below 1% across all datasets and cluster configurations.

7.2 Novelty Contributions

The principal novelty contributions of this work are fourfold. First, D2 the TLS/Network Infrastructure Phishing Dataset (is the first publicly available phishing dataset providing infrastructure-level TLS behavioral features without payload decryption, enabling a new class of transport-layer phishing detection that complements URL and content-based approaches. Second, HC²FS (Heuristic-Constrained Class-Conditional Feature Selection) algorithm is a novel feature selection mechanism that integrates statistical discrimination with domain-specific heuristic constraints**,** producing feature subsets that are both highly discriminative and resilient to adversarial manipulation. combining statistical class-conditional discrimination with domain knowledge constraints to produce evasion-resistant feature sets. Third, the application of MBO to joint feature-model co-optimization for phishing detection represents the first documented use of this advanced metaheuristic in cybersecurity classification at this scale. Fourth, the adversarial robustness evaluation framework—testing three degradation levels across four heterogeneous datasets reveals architecture-specific vulnerability profiles that are not apparent from standard benchmark evaluation, providing a practical deployment guide for practitioners.

7.3 Limitations and Future Work

The primary limitations of this study are: (1) evaluation on static datasets that cannot fully capture real-time phishing URL registration dynamics; (2) adversarial scenarios limited to random feature zeroing rather than targeted evasion attacks (e.g., adversarial perturbation of TLS fingerprints); and (3) computational requirements of the CNN-BiLSTM variant that may exceed constraints on highly resource-limited edge devices. Future work will address these through: integration of live phishing threat feeds via the browser extension for continuous model updating and concept drift adaptation; development of targeted adversarial robustness techniques specifically against TLS fingerprint manipulation; extension of HC²FS to semi-supervised settings where only a subset of samples are labeled; and investigation of federated learning approaches enabling collaborative model training across organizational boundaries without sharing sensitive traffic data.

8. CONCLUSION

This paper presented an optimization-driven multi-domain hybrid phishing detection framework that integrates TLS transport-layer behavioral analysis, URL structural features, and email content features within an OSI-aligned three-cluster architecture. The framework makes four principal novel contributions: (1) the

HC²FS feature selection algorithm providing cluster-aware, evasion-resistant feature optimization with 25–86% dimensionality reduction across heterogeneous datasets; (2) the TLS/Network Infrastructure Phishing Dataset (D2), the first publicly available transport-layer phishing dataset enabling infrastructure-level detection in encrypted traffic; (3) MBO-based joint feature-model co-optimization achieving F1 > 0.97 and FPR < 1% with end-to-end detection latency of 143 ms; and (4) a comprehensive adversarial robustness evaluation revealing architecture-specific vulnerability profiles under feature degradation scenarios.

Experimental evaluation across four datasets spanning 762,190 samples demonstrates that LSTM consistently achieves the highest accuracy and AUC in structured and hybrid phishing environments, while Transformer architectures provide superior memory efficiency and robustness under partial feature availability in distributed infrastructure datasets. The Hybrid fusion architecture provides the most balanced adversarial robustness across all feature domains. These findings collectively provide a practical deployment guide for practitioners selecting detection architectures for real-world phishing defense systems operating across URL, network, and email attack vectors.

Declarations

Conflict of Interest: The authors declare no conflict of interest.
Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.
Data Availability: All datasets used in this study are publicly available.
D1: Milosz Misiek, Tomasz Hyla, "X-phide phishing and legitimate urls with features", IEEE Dataport, October 13, 2025, doi:10.21227/7k88-0x11DOI 10.21227/7k88-0x11 (IEEE Dataport).
D2: DOI 10.21227/6ppb-tm80 (IEEE Dataport). D3 and D4: DOI 10.17632/6nhtnmn2yk.2 (Mendeley Data).
Author Contributions: A. Jadhav: conceptualization, methodology, dataset construction, experimentation, writing original draft. P. R. Chandre: supervision, methodology review, writing review and editing.

References.

[1] G. Response and T. Cybercrime, “4 Quarter,” no. February 2024, 2023.
[2] WhiteHouse, “N Ational C Ybersecurity S Trategy,” no. March, 2023.
[3] G. Response and T. Cybercrime, “APWG Phishing Trends Report 3rd Quarter 2023 PHISHING ACTIVITY TRENDS REPORT,” no. September, 2023.
[4] FBI, “2021 Internet Crime Report,” *Fed. Bur. Investig. - Internet Crime Complain. Cent.*, no. I, p. 33, 2022.
[5] M. D. S. S, “Image and Text Spam Mail Filtering System,” *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. V, no. XI, pp. 2778–2783, 2017, doi: 10.22214/ijraset.2017.11384.
[6] A. Karim, S. Azam, B. Shanmugam, K. Kannoorpatti, and M. Alazab, “A comprehensive survey for intelligent spam email detection,” *IEEE Access*, vol. 7, pp. 168261–168295, 2019, doi: 10.1109/ACCESS.2019.2954791.
[7] M. G. Hr *et al.*, “The Basics of Hacking and Penetration Testing,” *IEEE Access*, vol. 10, no. 1, pp. 1–17, 2023, doi: 10.1109/ACCESS.2023.3247135.
[8] F. Castano *et al.*, “Fundamentals of buffer overflow attacks and detection techniques,” *IEEE Access*, vol. 11897 LNCS, no. 2, pp. 5–7, 2025, doi: 10.1007/978-3-030-39303-8_17.
[9] I. Androutsopoulos, J. Koutsias, K. V. Chandrinos, G. Paliouras, and C. D. Spyropoulos, “An Evaluation of Naive Bayesian Anti-Spam Filtering,” *Mach. Learn. New Inf. Age*, pp. 9–17, 2000, [Online]. Available: http://arxiv.org/abs/cs/0008019
[10] D. Ranganayakulu and C. C., “Detecting Malicious URLs in E-mail – An Implementation,” *AASRI Procedia*, vol. 4, pp. 125–131, 2013, doi: 10.1016/j.aasri.2013.10.020.
[11] M. Khonji, Y. Iraqi, and A. Jones, “Phishing detection: A literature survey,” *IEEE Commun. Surv. Tutorials*, vol. 15, no. 4, pp. 2091–2121, 2013, doi: 10.1109/SURV.2013.032213.00009.
[12] A. Joshi, L. Lloyd, P. Westin, and S. Seethapathy, “Using Lexical Features for Malicious URL Detection -- A Machine Learning Approach,” 2019.
[13] Q. Qi, Z. Wang, Y. Xu, Y. Fang, and C. Wang, “Enhancing Phishing Email Detection through Ensemble Learning and Undersampling,” *Appl. Sci.*, vol. 13, no. 15, 2023, doi: 10.3390/app13158756.
[14] R. J. van Geest, G. Cascavilla, J. Hulstijn, and N. Zannone, “The applicability of a hybrid framework for automated phishing detection,” *Comput. Secur.*, vol. 139, no. February 2023, p. 103736, 2024, doi: 10.1016/j.cose.2024.103736.
[15] J. D. Duarte *et al.*, “Machine Learning for Early Detection of Phishing URLs in Parked Domains: An

Approach Applied to a Financial Institution," *IEEE Access*, vol. 13, no. June, pp. 145736–145753, 2025, doi: 10.1109/ACCESS.2025.3599454.
[16] C. Opara, B. Wei, and Y. Chen, "HTMLPhish: Enabling Phishing Web Page Detection by Applying Deep Learning Techniques on HTML Analysis," *Proc. Int. Jt. Conf. Neural Networks*, no. October 2018, 2020, doi: 10.1109/IJCNN48605.2020.9207707.
[17] S. Al-Ahmadi and Y. Alharbi, "A Deep Learning Technique For Web Phishing Detection Combined Url Features And Visual Similarity," *Int. J. Comput. Networks Commun.*, vol. 12, no. 5, pp. 41–54, 2020, doi: 10.5121/ijcnc.2020.12503.
[18] G. Vrbančič, I. Fister, and V. Podgorelec, "Datasets for phishing websites detection," *Data Br.*, vol. 33, no. October, p. 106438, 2020, doi: 10.1016/j.dib.2020.106438.
[19] S. Paliath, M. A. Qbeitah, and M. Aldwairi, "Phishout: Effective phishing detection using selected features," *Proc. 2020 27th Int. Conf. Telecommun. ICT 2020*, 2020, doi: 10.1109/ICT49546.2020.9239589.
[20] G. Palaniappan, S. Sangeetha, B. Rajendran, Sanjay, S. Goyal, and B. S. Bindhumadhava, "Malicious Domain Detection Using Machine Learning on Domain Name Features, Host-Based Features and Web-Based Features," *Procedia Comput. Sci.*, vol. 171, no. 2019, pp. 654–661, 2020, doi: 10.1016/j.procs.2020.04.071.
[21] L. Halgaš, I. Agrafiotis, and J. R. C. Nurse, "Catching the Phish: Detecting Phishing Attacks Using Recurrent Neural Networks (RNNs)," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11897 LNCS, pp. 219–233, 2020, doi: 10.1007/978-3-030-39303-8_17.
[22] S. A. Khan, W. Khan, and A. Hussain, "Phishing Attacks and Websites Classification Using Machine Learning and Multiple Datasets (A Comparative Analysis)," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12465 LNAI, pp. 301–313, 2020, doi: 10.1007/978-3-030-60796-8_26.
[23] Y. Lin *et al.*, "Phishpedia: A hybrid deep learning based approach to visually identify phishing webpages," *Proc. 30th USENIX Secur. Symp.*, pp. 3793–3810, 2021.
[24] J. Lim *et al.*, "SOK: On the Analysis of Web Browser Security," 2021, [Online]. Available: http://arxiv.org/abs/2112.15561
[25] A. Jadhav and P. R. Chandre, "Survey and comparative analysis of phishing detection techniques: current trends, challenges, and future directions," *IAES Int. J. Artif. Intell.*, vol. 14, no. 2, p. 853, 2025, doi: 10.11591/ijai.v14.i2.pp853-866.
[26] A. Jadhav and P. Chandre, "A Hybrid Heuristic-Machine Learning Framework for Phishing Detection Using Multi-Domain Feature Analysis," *Eng. Technol. Appl. Sci. Res.*, vol. 15, no. 5, pp. 27219–27226, 2025, doi: 10.48084/etasr.11548.
[27] A. Jadhav and P. Chandre, "A Multi-Layered, Multi-Domain Feature Analysis for Phishing Detection," *2025 World Ski. Conf. Univers. Data Anal. Sci. WorldSUAS 2025*, pp. 1–8, 2025, doi: 10.1109/WorldSUAS66815.2025.11199057.
[28] M. Alabdulhafith *et al.*, "A Modified Bonobo Optimizer with Its Application in Solving Engineering Design Problems," *IEEE Access*, vol. 12, no. June, pp. 134948–134984, 2024, doi: 10.1109/ACCESS.2024.3455550.
[29] S. Atawneh and H. Aljehani, "Phishing Email Detection Model Using Deep Learning," *Electron.*, vol. 12, no. 20, 2023, doi: 10.3390/electronics12204261.
[30] Q. Zan *et al.*, "Fed-urlBERT: Client-Split Federated BERT for Malicious URL Detection," *IEEE Access*, vol. 13, no. November, pp. 191164–191179, 2025, doi: 10.1109/ACCESS.2025.3629370.
[31] S. Kuikel, A. Piplai, and P. Aggarwal, "Evaluating Large Language Models for Phishing Detection, Self-Consistency, Faithfulness, and Explainability," 2025, [Online]. Available: http://arxiv.org/abs/2506.13746
[32] R. S. Rao, C. Kondaiah, A. R. Pais, and B. Lee, "A hybrid super learner ensemble for phishing detection on mobile devices," *Sci. Rep.*, vol. 15, no. 1, pp. 1–17, 2025, doi: 10.1038/s41598-025-02009-8.
[33] S. Aslam, H. Aslam, A. Manzoor, H. Chen, and A. Rasool, "AntiPhishStack: LSTM-Based Stacked Generalization Model for Optimized Phishing URL Detection," *Symmetry (Basel).*, vol. 16, no. 2, pp. 1–26, 2024, doi: 10.3390/sym16020248.
[34] O. Senouci and N. Benaouda, "Enhancing Phishing Detection in Cloud Environments Using RNN-LSTM in a Deep Learning Framework," *J. Telecommun. Inf. Technol.*, vol. 90, no. 1, pp. 1–9, 2025, doi: 10.26636/jtit.2025.1.1916.

[35] Z. Alshingiti, R. Alaqel, J. Al-Muhtadi, Q. E. U. Haq, K. Saleem, and M. H. Faheem, "A Deep Learning-Based Phishing Detection System Using CNN, LSTM, and LSTM-CNN," *Electron.*, vol. 12, no. 1, pp. 1–18, 2023, doi: 10.3390/electronics12010232.
[36] U. A. Butt, R. Amin, H. Aldabbas, S. Mohan, B. Alouffi, and A. Ahmadian, "Cloud-based email phishing attack using machine and deep learning algorithm," *Complex Intell. Syst.*, vol. 9, no. 3, pp. 3043–3070, 2023, doi: 10.1007/s40747-022-00760-3.
[37] P. C. R. Chinta, C. S. Moore, L. M. Karaka, M. Sakuru, V. Bodepudi, and S. R. Maka, "Building an Intelligent Phishing Email Detection System Using Machine Learning and Feature Engineering," *Eur. J. Appl. Sci. Eng. Technol.*, vol. 3, no. 2, pp. 41–54, 2025, doi: 10.59324/ejaset.2025.3(2).04.
[38] M. G. Hr, A. Mv, S. Gunesh Prasad, and S. Vinay, "Development of anti-phishing browser based on random forest and rule of extraction framework," *Cybersecurity*, vol. 3, no. 1, pp. 1–14, 2020, doi: 10.1186/s42400-020-00059-1.
[39] R. Zieni, L. Massari, and M. C. Calzarossa, "Phishing or Not Phishing? A Survey on the Detection of Phishing Websites," *IEEE Access*, vol. 11, no. January, pp. 18499–18519, 2023, doi: 10.1109/ACCESS.2023.3247135.
[40] L. Al-Shalabi and Y. Hasan Jazyah, "Phishing Detection Using Hybrid Algorithm Based on Clustering and Machine Learning," *Int. J. Comput. Digit. Syst.*, vol. 15, no. 1, pp. 1–13, 2024.
[41] S. Das Guptta, K. T. Shahriar, H. Alqahtani, D. Alsalman, and I. H. Sarker, "Modeling Hybrid Feature-Based Phishing Websites Detection Using Machine Learning Techniques," *Ann. Data Sci.*, vol. 11, no. 1, pp. 217–242, 2024, doi: 10.1007/s40745-022-00379-8.
[42] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, and J. Porras, "Mitigation strategies against the phishing attacks: A systematic literature review," *Comput. Secur.*, vol. 132, p. 103387, 2023, doi: 10.1016/j.cose.2023.103387.
[43] E. O. Yeboah-Boateng and P. M. Amanor, "Phishing , SMiShing & Vishing : An Assessment of Threats against Mobile Devices," *J. Emerg. Trends Comput. Inf. Sci.*, vol. 5, no. 4, pp. 297–307, 2014.
[44] Y. Wei, M. Nakayama, and Y. Sekiya, "Enhancing Generalization in Phishing URL Detection via a Fine-Tuned BERT-Based Multimodal Approach," *IEEE Access*, vol. 13, no. June, pp. 131197–131216, 2025, doi: 10.1109/ACCESS.2025.3591843.
[45] A. Venturi, M. Colajanni, M. Ramilli, and G. V. Santangelo, "Classification of Web Phishing Kits for early detection by platform providers," 2022.
[46] K. Demertzis and L. Iliadis, "Cognitive Web Application Firewall to Critical Infrastructures Protection from Phishing Attacks," *J. Comput. Model.*, vol. 9, no. 2, pp. 1792–8850, 2019, [Online]. Available: https://www.researchgate.net/publication/332863478
[47] F. Ji *et al.*, "Evaluating the Effectiveness and Robustness of Visual Similarity-based Phishing Detection Models," *Proc. 34th USENIX Secur. Symp.*, pp. 3201–3220, 2025.
[48] T. Cao *et al.*, "PhishAgent: A Robust Multimodal Agent for Phishing Webpage Detection," *Proc. AAAI Conf. Artif. Intell.*, vol. 39, no. 27, pp. 27869–27877, 2025, doi: 10.1609/aaai.v39i27.35003.
[49] R. P. Detection, "KnowPhish : Background : What is Phishing ? Phishing webpages usually," 2024.
[50] D. Rathee and S. Mann, "Detection of E-Mail Phishing Attacks – using Machine Learning and Deep Learning," *Int. J. Comput. Appl.*, vol. 183, no. 47, pp. 1–7, 2022, doi: 10.5120/ijca2022921868.
[51] "Phishtankdataset Phishing Url."
[52] S. Anirudh, P. Radha Nishant, S. Baitha, and K. Dinesh Kumar, "An Ensemble Classification Model for Phishing Mail Detection," *Procedia Comput. Sci.*, vol. 233, no. 2023, pp. 970–978, 2024, doi: 10.1016/j.procs.2024.03.286.
[53] K. L. Chiew, K. S. C. Yong, and C. L. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," *Expert Syst. Appl.*, vol. 106, pp. 1–20, 2018, doi: 10.1016/j.eswa.2018.03.050.
[54] B. Kondracki, B. A. Azad, O. Starov, and N. Nikiforakis, "Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits," *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 36–50, 2021, doi: 10.1145/3460120.3484765.
[55] R. Brindha, S. Nandagopal, H. Azath, V. Sathana, G. P. Joshi, and S. W. Kim, "Intelligent Deep Learning Based Cybersecurity Phishing Email Detection and Classification," *Comput. Mater. Contin.*, vol. 74, no. 3, pp. 5901–5914, 2023, doi: 10.32604/cmc.2023.030784.
[56] E. J. Williams and A. N. Joinson, "Developing a measure of information seeking about phishing," *J. Cybersecurity*, vol. 6, no. 1, pp. 1–16, 2020, doi: 10.1093/cybsec/tyaa001.
[57] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommun. Syst.*, vol. 76, no. 1, pp. 139–154, 2021, doi: 10.1007/s11235-020-00733-2.

[58] L. Pajola, E. Caripoti, S. Banzer, S. Pizzi, M. Conti, and G. Apruzzese, *E-PhishGEN: Unlocking Novel Research in Phishing Email Detection*, vol. 1, no. 1. arXiv, 2025. doi: 10.1145/3733799.3762967.
[59] T. Sutter, A. S. Bozkir, B. Gehring, and P. Berlich, "Avoiding the Hook: Influential Factors of Phishing Awareness Training on Click-Rates and a Data-Driven Approach to Predict Email Difficulty Perception," *IEEE Access*, vol. 10, pp. 100540–100565, 2022, doi: 10.1109/ACCESS.2022.3207272.
[60] R. Hoheisel, G. van Capelleveen, D. K. Sarmah, and M. Junger, "The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains," *Comput. Secur.*, vol. 128, 2023, doi: 10.1016/j.cose.2023.103158.
[61] R. Jayaprakash *et al.*, "Heuristic machine learning approaches for identifying phishing threats across web and email platforms," *Front. Artif. Intell.*, vol. 7, no. October, pp. 1–15, 2024, doi: 10.3389/frai.2024.1414122.
[62] A. Oest *et al.*, "Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale," *Proc. 29th USENIX Secur. Symp.*, pp. 361–377, 2020.
[63] S. S. Roy, P. Thota, K. V. Naragam, and S. Nilizadeh, "From Chatbots to PhishBots? -- Preventing Phishing scams created using ChatGPT, Google Bard and Claude," 2024, [Online]. Available: http://arxiv.org/abs/2310.19181
[64] S. Salloum, T. Gaber, S. Vadera, and K. Shaalan, "A Systematic Literature Review on Phishing Email Detection Using Natural Language Processing Techniques," *IEEE Access*, vol. 10, pp. 65703–65727, 2022, doi: 10.1109/ACCESS.2022.3183083.
[65] T. Dalton *et al.*, *PhreshPhish: A Real-World, High-Quality, Large-Scale Phishing Website Dataset and Benchmark*, vol. 1, no. 1. arXiv, 2025. [Online]. Available: http://arxiv.org/abs/2507.10854
[66] A. Mughaid, S. AlZu'bi, A. Hnaif, S. Taamneh, A. Alnajjar, and E. A. Elsoud, "An intelligent cyber security phishing detection system using deep learning techniques," *Cluster Comput.*, vol. 25, no. 6, pp. 3819–3828, 2022, doi: 10.1007/s10586-022-03604-4.
[67] Y. Li *et al.*, "KnowPhish: Large Language Models Meet Multimodal Knowledge Graphs for Enhancing Reference-Based Phishing Detection," *Proc. 33rd USENIX Secur. Symp.*, pp. 793–810, 2024.
[68] Z. Alamri, A. Alhuzali, B. Alsulami, and D. Alghazzawi, "Enhanced Phishing Website Detection Using Optimized Ensemble Stacking Models," *Int. J. Adv. Comput. Sci. Appl.*, vol. 16, no. 8, pp. 1031–1046, 2025, doi: 10.14569/IJACSA.2025.01608100.
[69] C. Opara, Y. Chen, and B. Wei, "Look before you leap: Detecting phishing web pages by exploiting raw URL and HTML characteristics," *Expert Syst. Appl.*, vol. 236, no. October 2020, p. 121183, 2024, doi: 10.1016/j.eswa.2023.121183.
[70] A. R. Omar, S. Taie, and M. E. Shaheen, "From Phishing Behavior Analysis and Feature Selection to Enhance Prediction Rate in Phishing Detection," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 5, pp. 1033–1044, 2023, doi: 10.14569/IJACSA.2023.01405107.
[71] T. Song, P. Casas, and M. Meo, *Phishing the Phishers with SpecularNet: Hierarchical Graph Autoencoding for Reference-Free Web Phishing Detection*, vol. 1, no. 1. arXiv, 2026. [Online]. Available: http://arxiv.org/abs/2603.01874
[72] M. A. Remmide, F. Boumahdi, N. Boustia, C. L. Feknous, and R. Della, "Detection of Phishing URLs Using Temporal Convolutional Network," *Procedia Comput. Sci.*, vol. 212, no. C, pp. 74–82, 2022, doi: 10.1016/j.procs.2022.10.209.
[73] K. Schiller and F. Adamsky, *Lending a Hand : The Effectiveness of Support Systems in Assisting Users to Detect Phishing Attacks*, vol. 1, no. 1. Association for Computing Machinery, 2026. doi: 10.1145/3772318.3791490.
[74] K. Barik, S. Misra, and R. Mohan, "Web-based phishing URL detection model using deep learning optimization techniques," *Int. J. Data Sci. Anal.*, no. c, 2025, doi: 10.1007/s41060-025-00728-9.
[75] A. H. Aljammal, S. Taamneh, A. Qawasmeh, and H. B. Salameh, "Machine Learning Based Phishing Attacks Detection Using Multiple Datasets," *Int. J. Interact. Mob. Technol.*, vol. 17, no. 5, pp. 71–83, 2023, doi: 10.3991/ijim.v17i05.37575.
[76] A. I. Champa, M. Fazle Rabbi, F. Z. Eishita, and M. F. Zibran, "Catch Me If You See: Using Visual Cue and Explanatory Feedback to Enhance Human Phishing Detection," *IEEE Access*, vol. 13, no. November, pp. 193249–193272, 2025, doi: 10.1109/ACCESS.2025.3631670.
[77] Y. Li *et al.*, *PhishIntel: Toward Practical Deployment of Reference-Based Phishing Detection*, vol. 1, no. 1. Association for Computing Machinery, 2025. doi: 10.1145/3701716.3715192.
[78] N. Bacanin *et al.*, "Addressing feature selection and extreme learning machine tuning by diversity-oriented social network search: an application for phishing websites detection," *Complex Intell. Syst.*,

vol. 9, no. 6, pp. 7269–7304, 2023, doi: 10.1007/s40747-023-01118-z.
[79] "Phishing Detection Frame Work Objective 1 and 2."
[80] Y. Yang *et al.*, "VishBox: An AI-Agent-Based Adaptive Voice Phishing Simulation Framework for Cybersecurity Education," *IEEE Access*, vol. PP, p. 1, 2026, doi: 10.1109/ACCESS.2026.3667823.
[81] N. Q. Do, A. Selamat, O. Krejcar, E. Herrera-Viedma, and H. Fujita, "Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions," *IEEE Access*, vol. 10, pp. 36429–36463, 2022, doi: 10.1109/ACCESS.2022.3151903.
[82] C. Catal, G. Giray, B. Tekinerdogan, S. Kumar, and S. Shukla, *Applications of deep learning for phishing detection: a systematic literature review*, vol. 64, no. 6. Springer London, 2022. doi: 10.1007/s10115-022-01672-x.
[83] I. Petrukha, N. Stulova, and S. Kryvoblotskyi, "Position Paper: Think Globally, React Locally - Bringing Real-Time Reference-Based Website Phishing Detection on macOS," *Proc. - 9th IEEE Eur. Symp. Secur. Priv. Work. Euro S PW 2024*, pp. 448–455, 2024, doi: 10.1109/EuroSPW61312.2024.00057.
[84] N. Jindal, D. Rastogi, K. Joshi, and D. Gupta, "Identification of Phishing Attacks using Machine Learning," *Proc. IEEE Int. Conf. Image Inf. Process.*, vol. 04010, pp. 941–946, 2023, doi: 10.1109/ICIIP61524.2023.10537706.
[85] S. Naseeb *et al.*, "Website Phishing Attack Detection Using Innovative Meta Learning-Based Ensemble Approach," *IEEE Access*, vol. 13, no. September, pp. 164249–164264, 2025, doi: 10.1109/ACCESS.2025.3610961.
[86] L. Tang and Q. H. Mahmoud, "A Deep Learning-Based Framework for Phishing Website Detection," *IEEE Access*, vol. 10, pp. 1509–1521, 2022, doi: 10.1109/ACCESS.2021.3137636.
[87] A. Chaudhuri, "Clone Phishing: Attacks and Defenses," *Int. J. Sci. Res. Publ.*, vol. 13, no. 4, 2023, doi: 10.29322/ijsrp.13.04.2023.p13626.
[88] A. A. Orunsolu, A. S. Sodiya, and A. T. Akinwale, "A predictive model for phishing detection," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 2, pp. 232–247, 2022, doi: 10.1016/j.jksuci.2019.12.005.
[89] P. Chandre, P. Bhujbal, A. Jadhav, B. D. Shendkar, A. Wangikar, and R. Sachdeo, "A comprehensive review of interpretable machine learning techniques for phishing attack detection," *IAES Int. J. Artif. Intell.*, vol. 14, no. 4, pp. 3022–3032, 2025, doi: 10.11591/ijai.v14.i4.pp3022-3032.
[90] P. Mendes, E. Maia, and I. Praça, "MeAJOR Corpus: A Multi-Source Dataset for Phishing Email Detection," 2025, [Online]. Available: http://arxiv.org/abs/2507.17978
[91] Y. Ari Kustiawan and K. Imran Ghauth, "Feature Engineering for Phishing Website Detection Using Machine Learning: A Systematic Review," *IEEE Access*, vol. 13, no. November, pp. 192080–192104, 2025, doi: 10.1109/ACCESS.2025.3630334.
[92] O. Sarker, A. Jayatilaka, S. Haggag, C. Liu, and M. A. Babar, "A Multi-vocal Literature Review on challenges and critical success factors of phishing education, training and awareness," *J. Syst. Softw.*, vol. 208, no. October 2023, p. 111899, 2024, doi: 10.1016/j.jss.2023.111899.
[93] M. Sanchez-Paniagua, E. F. Fernandez, E. Alegre, W. Al-Nabki, and V. Gonzalez-Castro, "Phishing URL Detection: A Real-Case Scenario Through Login URLs," *IEEE Access*, vol. 10, pp. 42949–42960, 2022, doi: 10.1109/ACCESS.2022.3168681.
[94] M. Safran and A. Musleh, "PhishingGNN: Phishing Email Detection Using Graph Attention Networks and Transformer-Based Feature Extraction," *IEEE Access*, vol. 13, no. July, pp. 131390–131399, 2025, doi: 10.1109/ACCESS.2025.3592135.
[95] Y. Wang, "Mitigating phishing threats," pp. 0–232, 2023, [Online]. Available: https://research-repository.st-andrews.ac.uk/handle/10023/27439%0Ahttps://research-repository.st-andrews.ac.uk/bitstream/handle/10023/27439/Thesis-Yunjia-Wang-complete-version.pdf?sequence=8
[96] G. Desolda, L. S. Ferro, A. Marrella, T. Catarci, and M. F. Costabile, "Human Factors in Phishing Attacks: A Systematic Literature Review," *ACM Comput. Surv.*, vol. 54, no. 8, 2022, doi: 10.1145/3469886.
[97] Anti Phishing Working Group, "APWG Phishing Activity Trend Report, 1st Quarter 2023," *Safe Places*, no. June, pp. 80–88, 2023.
[98] A. Safi and S. Singh, "A systematic literature review on phishing website detection techniques," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 2, pp. 590–611, 2023, doi: 10.1016/j.jksuci.2023.01.004.
[99] "Case Study – Phishing test".
[100] D. Timko and M. L. Rahman, "Smishing Dataset I: Phishing SMS Dataset from Smishtank.com,"

CODASPY 2024 - Proc. 14th ACM Conf. Data Appl. Secur. Priv., pp. 289–294, 2024, doi: 10.1145/3626232.3653282.
[101] L. Ribeiro, I. S. Guedes, and C. S. Cardoso, "Which factors predict susceptibility to phishing? An empirical study," *Comput. Secur.*, vol. 136, no. March 2023, 2024, doi: 10.1016/j.cose.2023.103558.
[102] R. Goenka, M. Chawla, and N. Tiwari, "Enhanced Phishing Detection Approach Using a Layered Model: Domain Squatting and URL Obfuscation Identification and Lexical Feature-Based Classification," *IEEE Access*, vol. 13, no. September, pp. 187285–187306, 2025, doi: 10.1109/ACCESS.2025.3626819.
[103] C. L. Gan, Y. Y. Lee, and T. W. Liew, "Fishing for phishy messages: predicting phishing susceptibility through the lens of cyber-routine activities theory and heuristic-systematic model," *Humanit. Soc. Sci. Commun.*, vol. 11, no. 1, 2024, doi: 10.1057/s41599-024-04083-1.
[104] D. J. Liu, G. G. Geng, X. B. Jin, and W. Wang, "An efficient multistage phishing website detection model based on the CASE feature framework: Aiming at the real web environment," *Comput. Secur.*, vol. 110, p. 102421, 2021, doi: 10.1016/j.cose.2021.102421.
[105] D. S. Kuraku and D. Kalla, "Impact of phishing on users with different online browsing hours and spending habits," *Ijarcce*, vol. 12, no. 10, pp. 34–41, 2023, doi: 10.17148/ijarcce.2023.121005.
[106] G. J. W. Kathrine, P. M. Praise, A. A. Rose, and E. C. Kalaivani, "Variants of phishing attacks and their detection techniques," *Proc. Int. Conf. Trends Electron. Informatics, ICOEI 2019*, no. Icoei, pp. 255–259, 2019, doi: 10.1109/ICOEI.2019.8862697.
[107] D. Singhal, A. Verma, G. V. Radhakrishnan, J. Parashar, S. S. Date, and K. Upreti, "Whale Optimization and AutoML for Precise Phishing Detection," *J. Mob. Multimed.*, vol. 21, no. 5, pp. 855–880, 2025, doi: 10.13052/jmm1550-4646.2153.
[108] A. Yasin, R. Fatima, Z. JiangBin, W. Afzal, and S. Raza, "Can serious gaming tactics bolster spear-phishing and phishing resilience?: Securing the human hacking in Information Security," *Inf. Softw. Technol.*, vol. 170, no. February, p. 107426, 2024, doi: 10.1016/j.infsof.2024.107426.
[109] A. Abuadbba *et al.*, "Towards Web Phishing Detection Limitations and Mitigation," 2022.
[110] J. Gikandi, J. Kamau, D. Njuguna, and L. Sawe, "Sentence Level Analysis Model for Phishing Detection Using KNN," *J. Cyber Secur.*, vol. 6, no. 1, pp. 25–39, 2024, doi: 10.32604/jcs.2023.045859.
[111] B. Montaruli, L. Demetrio, M. Pintor, L. Compagna, D. Balzarotti, and B. Biggio, "Raze to the Ground: Query-Efficient Adversarial HTML Attacks on Machine-Learning Phishing Webpage Detectors," *AISec 2023 - Proc. 16th ACM Work. Artif. Intell. Secur.*, pp. 233–244, 2023, doi: 10.1145/3605764.3623920.
[112] H. Ghalechyan, E. Israyelyan, A. Arakelyan, G. Hovhannisyan, and A. Davtyan, "Phishing URL detection with neural networks: an empirical study," *Sci. Rep.*, vol. 14, no. 1, pp. 1–12, 2024, doi: 10.1038/s41598-024-74725-6.
[113] R. Yang, K. Zheng, B. Wu, C. Wu, and X. Wang, "Phishing website detection based on deep convolutional neural network and random forest ensemble learning," *Sensors*, vol. 21, no. 24, pp. 1–18, 2021, doi: 10.3390/s21248281.
[114] P. M, V. S. M. B., M. G., and A. B. S.K., "Chrome Extension for Detecting Phishing Websites," *SSRN Electron. J.*, vol. 12, no. 03, pp. 212–215, 2023, doi: 10.2139/ssrn.4398136.
[115] J. Luckett, "Phishing Resistant Systems: A Literature Review," *J. Comput. Sci. Coll.*, vol. 39, no. 3, p. 347, 2023.
[116] M. Weinz, N. Zannone, L. Allodi, and G. Apruzzese, *The Impact of Emerging Phishing Threats: Assessing Quishing and LLM-generated Phishing Emails against Organizations*, vol. 1, no. 1. arXiv, 2025. doi: 10.1145/3708821.3736195.
[117] N. Alnazzawi, A. Aburayya, R. Alfaisal, and S. A. Salloum, "Using classical machine learning for phishing websites detection from URLs," *J. Manag. Inf. Decis. Sci.*, vol. 24, no. S6, pp. 1–9, 2021.
[118] N. Begou, J. Vinoy, A. Duda, and M. Korczynski, "Exploring the Dark Side of AI: Advanced Phishing Attack Design and Deployment Using ChatGPT," *2023 IEEE Conf. Commun. Netw. Secur. CNS 2023*, 2023, doi: 10.1109/CNS59707.2023.10288940.
[119] P. A. S. Rugeiro, "A framework to evaluate the phishing exposure in a corporate environment," 2023.
[120] M. Sánchez-Paniagua, E. Fidalgo, E. Alegre, and R. Alaiz-Rodríguez, "Phishing websites detection using a novel multipurpose dataset and web technologies features," *Expert Syst. Appl.*, vol. 207, no. October 2021, p. 118010, 2022, doi: 10.1016/j.eswa.2022.118010.
[121] F. Trade Commission, "Roundtable Discussion On Phishing Education: A Staff Report By the Federal Trade Commission's Division of Consumer and Business Education and Division of Marketing

Practices (July 2008)," no. July, 2008, [Online]. Available: http://www.ftc.gov/os/2007/12/071220spamsummitreport.pdf.
[122] C. S. Eze and L. Shamir, "Analysis and Prevention of AI-Based Phishing Email Attacks," *Electron.*, vol. 13, no. 10, 2024, doi: 10.3390/electronics13101839.
[123] F. Castano, E. F. Fernandez, R. Alaiz-Rodriguez, and E. Alegre, "PhiKitA: Phishing Kit Attacks Dataset for Phishing Websites Identification," *IEEE Access*, vol. 11, no. March, pp. 40779–40789, 2023, doi: 10.1109/ACCESS.2023.3268027.
[124] N. Beu *et al.*, "Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation," *Comput. Secur.*, vol. 131, p. 103313, 2023, doi: 10.1016/j.cose.2023.103313.
[125] Y. A. Kustiawan and K. I. Ghauth, "PhishOFE: A Novel Machine Learning Framework for Real-Time Phishing URL Detection With Optimized Feature Engineering," *IEEE Access*, vol. 13, no. September, pp. 169606–169627, 2025, doi: 10.1109/ACCESS.2025.3614126.
[126] G. D. Bispo *et al.*, "PHILDER: Lightweight Framework for Intelligent Phishing Detection on Resource-Limited Devices," *IEEE Access*, vol. 13, no. July, pp. 131967–131979, 2025, doi: 10.1109/ACCESS.2025.3592541.
[127] A. H. Alsadig and M. O. Ahmad, "Phishing URL Detection Using Deep Learning with CNN Models," *2nd Int. Conf. Intell. Cyber Phys. Syst. Internet Things, ICoICI 2024 - Proc.*, no. August, pp. 768–775, 2024, doi: 10.1109/ICoICI62503.2024.10696243.
[128] J. Lee, Y. Lee, D. Lee, H. Kwon, and D. Shin, "Classification of Attack Types and Analysis of Attack Methods for Profiling Phishing Mail Attack Groups," *IEEE Access*, vol. 9, pp. 80866–80872, 2021, doi: 10.1109/ACCESS.2021.3084897.
[129] R. Abdillah, Z. Shukur, M. Mohd, and T. M. Z. Murah, "Phishing Classification Techniques: A Systematic Literature Review," *IEEE Access*, vol. 10, pp. 41574–41591, 2022, doi: 10.1109/ACCESS.2022.3166474.
[130] T. Cao *et al.*, *PhishIntel: Toward Practical Deployment of Reference-Based Phishing Detection*, vol. 1, no. 1. Association for Computing Machinery, 2025. doi: 10.1145/3701716.3715192.
[131] W. Li, S. Manickam, S. U. A. Laghari, and Y. W. Chong, "Uncovering the Cloak: A Systematic Review of Techniques Used to Conceal Phishing Websites," *IEEE Access*, vol. 11, no. June, pp. 71925–71939, 2023, doi: 10.1109/ACCESS.2023.3293063.
[132] B. B. Gupta, K. Yadav, I. Razzak, K. Psannis, A. Castiglione, and X. Chang, "A novel approach for phishing URLs detection using lexical based machine learning in a real-time environment," *Comput. Commun.*, vol. 175, no. November 2020, pp. 47–57, 2021, doi: 10.1016/j.comcom.2021.04.023.
[133] J. Lin, "Testing Effectiveness of AI-Enabled Phishing Attacks based on Public Information," 2023.
[134] V. Bhavsar, A. Kadlak, and S. Sharma, "Study on Phishing Attacks," *Int. J. Comput. Appl.*, vol. 182, no. 33, pp. 27–29, 2018, doi: 10.5120/ijca2018918286.
[135] L. Ribeiro, I. S. Guedes, and C. S. Cardoso, "Eyes on phishing emails: an eye-tracking study," *J. Exp. Criminol.*, no. October, 2024, doi: 10.1007/s11292-024-09648-3.
[136] Y. A. Alsariera, V. E. Adeyemo, A. O. Balogun, and A. K. Alazzawi, "AI Meta-Learners and Extra-Trees Algorithm for the Detection of Phishing Websites," *IEEE Access*, vol. 8, pp. 142532–142542, 2020, doi: 10.1109/ACCESS.2020.3013699.
[137] T. Koide, N. Fukushi, H. Nakano, and D. Chiba, "ChatSpamDetector: Leveraging Large Language Models for Effective Phishing Email Detection," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST*, vol. 629 LNICST, no. SecureComm, pp. 297–319, 2026, doi: 10.1007/978-3-031-94455-0_14.
[138] D. M. Divakaran and A. Oest, "Phishing Detection Leveraging Machine Learning and Deep Learning: A Review," *IEEE Secur. Priv.*, vol. 20, no. 5, pp. 86–95, 2022, doi: 10.1109/MSEC.2022.3175225.
[139] A. Karim, M. Shahroz, K. Mustofa, S. B. Belhaouari, and S. R. K. Joga, "Phishing Detection System Through Hybrid Machine Learning Based on URL," *IEEE Access*, vol. 11, no. January, pp. 36805–36822, 2023, doi: 10.1109/ACCESS.2023.3252366.
[140] S. Hansakul and N. Wisitpongphan, "Enhancing Business-Specific Phishing Chat Detection via Few-Shot Learning LLM Augmentation," *IEEE Access*, vol. 13, no. August, pp. 183589–183597, 2025, doi: 10.1109/ACCESS.2025.3623898.
[141] F. Pavanello, M. Giaimo, W. Phoenix, and S. Cagol, "OSINT-based Email Analyzer for Phishing Detection," 2023.
[142] P. Maneriker, J. W. Stokes, E. G. Lazo, D. Carutasu, F. Tajaddodianfar, and A. Gururajan, "URLTran: Improving Phishing URL Detection Using Transformers," *Proc. - IEEE Mil. Commun. Conf.*

MILCOM, vol. 2021-Novem, pp. 197–204, 2021, doi: 10.1109/MILCOM52596.2021.9653028.
[143] A. R. Garcia *et al.*, “No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title,” *IEEE Access*, vol. 10, no. 1, pp. 1–17, 2023, doi: 10.1109/ACCESS.2023.3247135.
[144] APWG, “2 Quarter,” no. November, p. 8, 2023, [Online]. Available: https://apwg.org/trendsreports/
[145] S. F. Schwarz, P. Fonseca, and A. Rocha, “Smishing Detection From a Messaging Platform View,” *IEEE Access*, vol. 13, no. July, pp. 143449–143464, 2025, doi: 10.1109/ACCESS.2025.3597903.
[146] N. A. Azeez, S. S. Oladele, and O. Ologe, “Identification of Pharming in Communication Networks using Ensemble Learning,” *Niger. J. Technol. Dev.*, vol. 19, no. 2, pp. 172–180, 2022, doi: 10.4314/njtd.v19i2.10.
[147] M. L. Rahman, D. Timko, H. Wali, and A. Neupane, *Users Really Do Respond To Smishing*, vol. 1, no. 1. Association for Computing Machinery, 2023. doi: 10.1145/3577923.3583640.
[148] D. Oluremi, “Hybrid Machine Learning Models for Intrusion Detection in IoT :,” no. August 2017, pp. 1–9, 2025.
[149] H. Zhang, Y. Shi, M. Liu, L. Chen, S. Wu, and Z. Xue, “A combined feature selection approach for malicious email detection based on a comprehensive email dataset,” *Cybersecurity*, vol. 8, no. 1, 2025, doi: 10.1186/s42400-024-00309-6.
[150] N. Ayofe Azeez and E. Anochirionye, “Detecting Malicious and Compromised URLs in E-Mails Using Association Rule,” *Covenant J. Informatics Commun. Technol.*, vol. 5, no. 2, pp. 36–48, 2017.
[151] C. Sasirekha, R. Nandhini, K. M. N. L, R. S. Bhuvaneshwari, and V. S. Chandra, “Abstract :,” vol. 11, no. 03, pp. 1–4, 2023.
[152] N. Kulkarni, “and Innovations Explainable AI : Trends and Innovations,” vol. 42, no. 1, 2024.
[153] P. Teja Nallamothu and M. Shais Khan, “Machine Learning for SPAM Detection,” *Asian J. Adv. Res.*, vol. 6, no. 1, pp. 167–179, 2023.
[154] S. Al-E’Mari, Y. Sanjalawe, S. Fraihat, G. Kurdi, and B. Allehyani, “A Cognitive BDI–BiLSTM Hybrid Framework for Interpretable Email Threat Detection,” *IEEE Access*, vol. 13, no. November, pp. 208192–208211, 2025, doi: 10.1109/ACCESS.2025.3641123.
[155] J. Su and A. Kapravelos, “Automatic Discovery of Emerging Browser Fingerprinting Techniques,” *ACM Web Conf. 2023 - Proc. World Wide Web Conf. WWW 2023*, no. February, pp. 2178–2188, 2023, doi: 10.1145/3543507.3583333.
[156] P. Chandre, P. Mahalle, G. Shinde, B. Shendkar, and S. Kashid, “Neuro-Symbolic AI: A Future of Tomorrow,” *ASEAN J. Sci. Technol. Dev.*, vol. 42, no. 2, pp. 187–200, 2025, doi: 10.61931/2224-9028.1620.
[157] Z. Jin, J. Shang, Q. Zhu, C. Ling, W. Xie, and B. Qiang, “RFRSF: Employee Turnover Prediction Based on Random Forests and Survival Analysis,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12343 LNCS, pp. 503–515, 2020, doi: 10.1007/978-3-030-62008-0_35.
[158] A. Olalekan Ige and M. Sibiya, “State-of-the-Art in 1D Convolutional Neural Networks: A Survey,” *IEEE Access*, vol. 12, no. June, pp. 144082–144105, 2024, doi: 10.1109/ACCESS.2024.3433513.
[159] P. M. Bhujbal, A. Jadhav, J. N. Nandimath, P. S. Kadam, P. R. Chandre, and P. N. Mahalle, “International Journal of INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING Zero Trust Paradigm: Advancements, Challenges, and Future Directions in Cybersecurity,” *Orig. Res. Pap. Int. J. Intell. Syst. Appl. Eng. IJISAE*, vol. 2024, pp. 613–623, 2024, [Online]. Available: www.ijisae.org

[98] A. Jadhav and P. Chandre, "A Multi-Layered, Multi-Domain Feature Analysis for Phishing Detection," 2025 WorldSUAS Conf., Indore, India, 2025, pp. 1–8. doi: 10.1109/WorldSUAS66815.2025.11199057
[99] M. Misiek and T. Hyla, "X-phide phishing and legitimate URLs with features," IEEE Dataport, 2025. doi: 10.21227/7k88-0x11
[100] A. Jadhav and P. Chandre, "Network/TLS Dataset for Phishing Detection," IEEE Dataport, 2026. doi: 10.21227/6ppb-tm80
[101] A. Jadhav and P. Chandre, "URL Phishing Cluster Dataset," Mendeley Data, V2, 2025. doi: 10.17632/6nhtnmn2yk.2