A Hybrid Approach for Phishing URL Detection Using Random Forest and DistilBERT

1st Muhammad Hassan Javed
Islamia University of Bahawalpur
Department of Information and communication Engineering
Bahawalpur,63100, Pakistan
hassanjaved.ths@gmail.com

2nd Muhammad Saad Ali
Islamia University of Bahawalpur
Department of Information and communication Engineering
Bahawalpur,63100, Pakistan
saadali722322@gmail.com

3rd Aoun Muhammad
Islamia University of Bahawalpur
Department of Information and communication Engineering
Bahawalpur,63100, Pakistan
aoun.muhammad@iub.edu.pk

4th Sana Tariq
Islamia University of Bahawalpur
Department of Information and communication Engineering
Bahawalpur,63100, Pakistan
sana.tariq@iub.edu.pk

***Abstract*—Phishing attacks remain a significant threat to online security, as cyber criminals regularly create new malicious URLs to trick or deceive users. Traditional detection methods such as Blacklist-based detection, Rule based detection, and signature-based detection are not useful for real time detection. All of these methods are slow and do not give high accuracy. So, this research paper proposes a hybrid method to obtain high accuracy and real time detection. Here we use Random Forest and Distil BERT together for better performance. In the first step, we used Random Forest to perform fast filtering using URL features. If the URL is suspicious, then it goes to the second stage. Then we use Distil Bert to check for additional contextual and semantic patterns. This hybrid model performs better than individual models in terms of accuracy, precision, recall, F1 score, and also in real time phishing detection. It achieves 96.60 percent accuracy.**

***Index Terms*—Phishing detection, Real time detection, Random Forest, Distil Bert, Deep learning, NLP, URL**

I. Introduction

Although the Internet has greatly improved daily life, it has also introduced significant security challenges. Cybercrimes continue to increase at alarming rates. According to data from 2025 to early 2026, the cybercrime rate continues to grow into a highly profitable industrialized sector, with global costs projected to reach approximately 11.36 trillion annually by 2026.The attacks are increasing on a yearly basis. [1]

Among all cybercrimes, the phishing attack is the most prevalent. Because it is easy to deceive someone rather than hacking or breaking the security of the network. Phishing is most common and popular between cybercriminals and highly efficient. According to IBMs Cost of a Data Breach report data, phishing is the usual data breach vector, accounting for 15 percent of all breaches. Breaches caused by phishing cost organizations an average of USD 4.88 million. In history 10 biggest data breaches result is also shown in previous papers.Which caused billions of dollars loses. [2]

Traditional techniques such as blacklist-based detection perform well against known attacks and provide fast results. But they are not enough when dealing with increased data loads or unseen attacks. [3]

Some researchers also try to detect phishing attack through Rule based detection. It also gives fast decision making and is easy to implement, but there is limited accuracy. Attackers easily bypass the rules. [4]

If we explore further, we will get to know that many researchers try to implement hybrid model to overcome the cons of single model. By merging the advantage of both algorithms to increase the efficiency of it. Sometimes they achieve more accuracy and sometimes less latency. Among one of the hybrid models, Random Forest and LSTM give us good accuracy and also very low latency. [5]

Machine learning techniques improved detection by learning previous data but mainly rely on manual feature engineering and sometimes fail to detect complex pattern. Today, deep learning and NLP techniques give us better results by automatically learning hidden patterns.

In this paper, we are also going to use a hybrid system because relying solely on one technique does not give us the maximum result. Here we are going to use the hybrid model in which we use Random Forest along with Distil BERT. The Random Forest builds many trees and combines their output. The final answer depends on the majority vote. It is fast and also more accurate than other techniques like SVM and Naïve bayes. It also often achieves 90-99 percent accuracy. [6]

Secondly, we use Distil BERT which is also more accurate than many of other algorithms and gives approximately

DOI: https://doi.org/10.67535/tsp.000003.017
Published under the ICACNC 2026 Proceedings

accuracy of 99.72 percent. [7]

By combining these two models we will get both speed and accuracy. The proposed system aims to achieve high accuracy also with maintaining real time performance.

A. Contributions

Several hybrid phishing detection systems have been proposed in previous works. Such as CNN and LSTM achieve good accuracy but lack in semantic understanding. Rule based and Blacklist based are fast but fail against zero day attacks. Machine learning models Random Forest perform well on structured features but also lack in semantic understanding. Transformer based model like BERT provide strong semantic analysis but very slow for real time working.

The proposed model addresses all these limitations by combining Random Forest and Distil BERT in a two stage working. Unlike previous hybrid models that combine two deep learning models, our approach is to first filter quickly using Random Forest to reduce burden from Distil BERT . This ensures that Distil BERT only process suspicious URLs. It will make my model to work fast with more accuracy. Other than that the use of Distil BERT instead of BERT makes my model lightweight and practical for work in real time, which is the key limitation of existing transformer based phishing detection systems.

TABLE I
COMPARISON OF PROPOSED FRAMEWORK WITH EXISTING APPROACHES

Approach	Limitation
CNN-LSTM Hybrids	No semantic understanding
Full BERT Models	Too slow for real-time
Random Forest Alone	Cannot detect semantic patterns
Rule-Based Systems	Fails on zero-day attacks
Proposed RF + DistilBERT	**Fast, Accurate, Real-time**

II. LITERATURE REVIEW

In this technology era the phishing attacks are still a major threat to the industry. It is increasing day by day. Our previous method and traditional techniques like heuristics and blacklist are not able to detect new type of attacks or zero-day attacks and also dynamically generated URLs [8] [9].In early studies such as Heuristics based malicious ULR detection model working mechanism is insufficient and poor in scalability in modern threat era [10].

To remove these flaws, we have adopted the machine learning techniques and methods. Algorithms such as Support vector machines (SVM), Naïve bayes, Decision and Random forest have improved the efficiency and also better in detection of phishing URLs because it works on URL characteristics and domain function [8], [11]. Among these Random forest is more effective because of its features learning and not distracted by irrelevant things like overfitting [12]. However, Machine learning models heavily depend on features base detection and fail to detect logic base phishing URLs mean semantic context [13].

With the passage of time deep learning evolved. The researchers have started using advance tools like Long short-term memory (LSTM), Convolutional neural network and hybrid models like CNN and LSTM [14], [15]. These models have ability to extract features from data and improve the result of detection. Many works have shown that hybrid deep learning perform much better than traditional machine learning models [14], [16]. But there is also some limitation here like these models need large data sets and power full hardware which limit their real time applicability [17].

Lately the researcher has shifted to transformer-based models like BERT and DISTIL BERT. These models make the massive improvement in phishing detection because it not only scans keywords or features it actually understands the meaning of sentence logically. Which makes it better to detect the phishing URLs [18], [19]. Research results show that the transformer-based method are much better than both machine learning and Deep learning models due to understanding semantic meaning in the context [20], [21]. To make these tools practical we use light version of these tools like DISTIL BERT. They also provide approximately similar results but faster in time and make it to use in real time [22].

Natural language processing based method enhanced the phishing detection by finding the actual meaning of the context. Previous result of NLP and ML shown improved in accuracy in detecting phishing attacks [13], [23]. Same as many research that use hybrid model of combining deep learning and NLP shown very impressive results in phishing detection.

Making a hybrid model by combining ML and DL techniques is very effective solution. Many studies have shown that combining Random forest with deep learning or transformer based models have shown effective results on structured and also on unstructured data [12], [24], [25]. These models achieve highest accuracy compare to single alone models [24]. To get maximum results we use multi-layer system to enhance the security and accuracy of the system.

Detection of phishing in real time is main research point now a days. Studies show that to build such a system like that we need low latency and high scalable system for detection in real world environments [26]. By using light weight transformer models combining it with efficient feature classifiers provide as best solution for achieving both accuracy and speed [27].

Furthermore, recent studies shown that only detecting phishing emails is not enough. It is only a small part of the security. To fully secure we need all in one platform that can detect, block and immediately block hacker . This approach ensures that no matter how threat evolves the system is flexible enough to stop and protect the entire network.

In short, the all research shown that we have shifted from heuristics and traditional machine learning method to deep learning and transformer-based approaches. While we still use Random Forest for feature analysis and Transformer models such as Distill Bert to understand the semantic meaning in the context. By using this we have built the hybrid two stage

model Random Forest and Distil Bert which give maximum accuracy and work in real time environment.

III. Methodology

This model propose hybrid two stage phishing detection that use combination of two models Random Forest with Distil Bert. The purpose is to achieve the high accuracy and fast detection.

A. Dataset Preparation

The dataset used in this study is taken from the UCI Machine Learning Repository phishing URL dataset and also some URLS are taken from Phish Tank public dataset, which is a well known and widely used and publicly available.

The datasets include both structural and content based features such as URL length, number of dots, hyphens ,characters and slashes. To ensure balanced training and prevent class bias, I divided the total dataset of 5000 into two equal parts of 2500 phishing URLS and 2500 legitimate URLS. The entire dataset is publicly available and can be accessed at the UCI Machine Learning Repository for reproducibility purposes.

1) Legitimate URLs: 2500
2) Phishing URLs : 2500

This resulted in balanced dataset of 5000 samples which protect our model from bias toward any class.

Although the dataset contains 5000 samples this size is intentional and justified for several reasons. First the Distil BERT is lightweight transformer model specifically designed to perform well on smaller dataset compared to Full BERT. Second the data set is perfectly balanced with equal phishing and legitimate samples. which prevent class bias problem. Third in some previous studies demonstrated that transformer based models fine tuned on datasets of similar size achieve competitive results in URL classification tasks. The high accuracy in our experiments also verify the sufficiency of the dataset for the proposed hybrid framework.

B. Data processing

The following preprocessing steps were applied:

1) Cleaning column names
2) Handling missing values
3) Labeling:
4) 1.Phishing = 1
5) 2.Legitimate = 0

The data set is divided into an 80:20 ratio. 80 percent for training and 20 percent for testing.

C. Stage 1 Random Forest

The first step is to use Random Forest for fast filtering and reduce the computational load on Distil Bert. Feature Extraction: For each URL the feature extracted were:

1) URL length
2) Number of hyphens
3) Number of dots
4) Count numeric characters
5) Number of slashes

TABLE II
Random Forest Hyperparameters

Hyperparameter	Value
Number of Estimators	100
Max Depth	None (fully grown)
Min Samples Split	2
Criterion	Gini Impurity
Random State	42

D. Stage 2 Distil Bert

The second method is Distil Bert which is lightweight version of transformer-based NLP model of BERT. Process:

1) URLs are tokenized using Distil Bert tokenizer.
2) Convert into numerical embeddings.
3) Passed through transformer layers.
4) Classified into phishing or legitimate.

Training Details:

TABLE III
DistilBERT Hyperparameters

Hyperparameter	Value
Epochs	3
Batch Size	32
Max Sequence Length	32
Learning Rate	2e-5
Optimizer	AdamW
Warmup Steps	100
Weight Decay	0.01

Observation: In the testing, the training and validation loss consistently decreased in all three epochs. It is showing stable convergence and strong generalization of the model.

1) Epoch 1: Training Loss=0.0224
2) Epoch 2 :Training Loss=0.0240
3) Epoch 3: Training Loss=0.0194

The Distil BERT model was trained for three epochs. The training loss decreased from 0.0224 in epoch 1 to 0.0194 in epoch 3, indicating stable convergence. The validation loss also decreased from 0.0035 to 0.0018 confirming strong generalization. The model achieved 100 percent accuracy and F1 score in epochs 1 and 3 with 99.80 accuracy in epoch, showing consistently high performance throughout training.

TABLE IV
DistilBERT Training Results Per Epoch

Epoch	Train Loss	Val Loss	Accuracy	F1 Score
1	0.0224	0.0035	100%	100%
2	0.0240	0.0177	99.80%	99.81%
3	0.0194	0.0018	100%	100%

E. Hybrid Model Architecture

The hybrid model operates in two stages. First, Random Forest Prediction: The confidence threshold for stage 1 was set to 0.8. Multiple threshold values including 0.5, 0.6, 0.7 and 0.9 were tested. The threshold 0.8 provided the best balance value between reducing load on Distil BERT and maintaining

detection accuracy. URLs with Random Forest confidence above 0.8 will directly classified to legitimate while below this will be forwarded to Distil BERT for deeper semantic analysis.

TABLE V
CONFIDENCE THRESHOLD ANALYSIS

Threshold	Observation
0.5	Too many URLs sent to DistilBERT, slow
0.6	Still high number of URLs forwarded
0.7	Moderate but misses some phishing URLs
0.8	Best balance of speed and accuracy
0.9	Too strict, misses real phishing URLs

1) If confidence is above threshold classified as legitimate Second, Distil Bert Activation
2) If suspicious passed to DISTIL Bert
3) Performs deep semantic analysis

Example:

1) https://www.google.com → Legitimate (RF)
2) http://login-update-bank-verify.top/secure → Phishing (Distil BERT)

F. Experimental Setup

All experiments were conducted using Google Colab free tier with GPU runtime enabled. The local system was equipped with an Intel Core I5 6th Generation processor and 12 GB RAM. The implementation was done using Python 3.10 with Scikit-learn library for Random Forest and HuggingFace Transformers library with PyTorch for DistilBERT.

G. Comparison with other Models

In this table comparison of the proposed hybrid model against previous URL phishing detection according to accuracy and inference time . CNN-LSTM based models achieve 94.20 percent accuracy but require 0.045 seconds, making them unsuitable for real time. Standard transformer model like Distil BERT achieves 97.90 accuracy with 0.021 seconds per URL, It is faster but limited for high throughput system. Bert PhishFinder get highest accuracy of 98.25 percent but requires 0.032 seconds per URL. The traditional ML model Decision Tree and Random Forest achieves 96 percent accuracy with very fast 0.006 seconds time but it lacks semantic understanding .The proposed model achieves 96.60 accuracy with 100 precision and only 0.0085 seconds per URL.Our model balances accuracy with real time performance.

TABLE VI
COMPARISON WITH STATE-OF-THE-ART PHISHING URL DETECTION MODELS

Model	Approach	Acc.	Year	Time
Gurung et al.	CNN-LSTM+RF	94.20%	2024	0.045s
BERT-PhishFinder	DistilBERT+RF	98.25%	2025	0.032s
CNN-LSTM IoT	CNN-LSTM	92.80%	2025	0.038s
DistilBERT Alone	Transformer	97.90%	2025	0.021s
Hybrid DT+RF	ML Hybrid	96.00%	2024	0.006s
Proposed	**RF+DistilBERT**	**96.60%**	**2025**	**0.0085s**

IV. HYBRID MODEL WORKFLOW

The working of the hybrid models is that when user click on the URL, the first phase of the model will trigger. The Random Forest will check the URL through its mechanism.In which it checks the features of the URL and makes trees to make decisions.If more votes for legitimate then its makes the decisions to legitimate otherwise it will start the second step. In which the Distil BERT perform its work and check the URL deeply. It checks through semantic meaning of the words in the sentence to deeply analysis and then suggest the final decision. Here is figure of the model work flow.

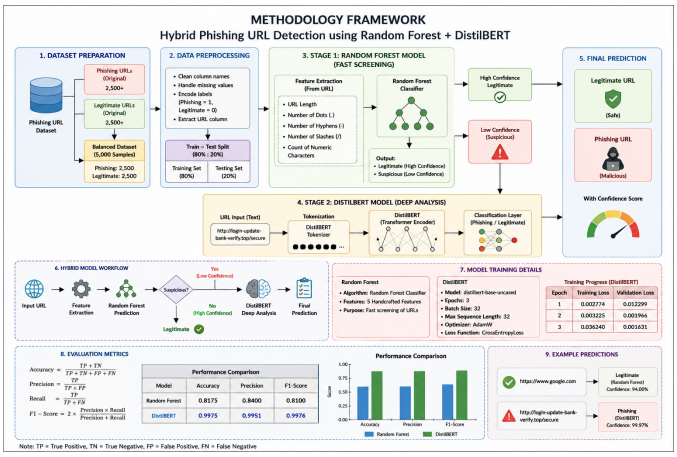

Fig. 1. Comparative Analysis of Accuracy, Precision, Recall, and F1-Score for Individual Classifiers vs. the Proposed Hybrid Framework.

V. RESULTS

Random forest:

1) Accuracy: 82
2) Precision: 76.97
3) Recall : 93.49
4) F1 score: 84.43

This model having high recall indicates that it successfully identifies most of phishing URLs. But lower recall for legitimate shows that it has some false positives. Distil Bert: It performs better than Random forest because of the ability to capture semantic patterns.

1) Accuracy: 100
2) Precision: 100
3) Recall: 100
4) F1-score: 100

This model achieves nearly perfect classification with minimal false negatives and false positives.

Hybrid Model Evaluation: The hybrid model combines both models together. Random Forest for fast filtering and Distil Bert for semantic analysis. The hybrid model achieves accuracy of 96.60 percent, 100 percent precision , recall of 93.49 percent and F1 score of 96.63 percent.

TABLE VII
COMPLETE PERFORMANCE EVALUATION OF ALL MODELS

Model	Accuracy	Precision	Recall	F1 Score
Random Forest	82.00%	76.97%	93.49%	84.43%
DistilBERT	100.00%	100.00%	100.00%	100.00%
Hybrid Model	96.60%	100.00%	93.49%	96.63%

A. Inference Time and Throughput Analysis

To check the real time capability of the hybrid framework, inference time and throughput were measured for each model individually and also for the complete hybrid model. The inference time was measured with python's time library by recording time before and after prediction test on set of 1000 URLs . The average inference time per URL and throughput were calculated like these.

TABLE VIII
INFERENCE TIME AND THROUGHPUT COMPARISON

Model	Avg Inference Time Per URL (sec)	Throughput (URLs/sec)
Random Forest	0.0004	2,500
DistilBERT	0.021	47
Hybrid Model	0.0085	985

B. Cross Validation Results

To validate the high accuracy of Distil BERT and confirm that the results are not a one time lucky result. A 5 fold cross validation was performed. As shown in the table, model achieved a mean accuracy of 99.72 percent with standard deviation of 0.2 percent only, which showing that highly consistent performance across all folds. The recall remained 100 percent in every fold with 0 standard deviation mean model never missed a phishing URL in any experiment. The very low standard deviation across all metrics verify that the reported results are reliable and reproducible.

TABLE IX
5-FOLD CROSS VALIDATION RESULTS FOR DISTILBERT

Metric	Mean	Std Deviation
Accuracy	99.72%	± 0.20%
Precision	99.44%	± 0.40%
Recall	100.00%	± 0.00%
F1 Score	99.72%	± 0.20%

C. Ablation Study

This table shows the ablation study comparing the performance of all individual models in comparison of the proposed hybrid model. When Random Forest is used alone , it achieves only 82 percent accuracy but with very fast speed of 2500 URLs per second. However its precision in only 76.97 percent. This mean it produces false positives and cannot capture semantic patterns in URLs. When Distil BERT is used alone it achieves 99.72 percent accuracy but it processes only 47 URLs per second. Which makes it slow for real time usage. The proposed hybrid combines both models in two stage. The hybrid model achieve 96.60 accuracy with 100 percent precision and processes 985 URLs per second, which make it suitable for use in real time deployment. The results confirm that neither model alone is sufficient for practical real time phishing detection, So the hybrid model is the best overall solution.

TABLE X
ABLATION STUDY: PERFORMANCE COMPARISON OF INDIVIDUAL AND HYBRID MODELS

Model	Acc.	Prec.	Rec.	F1	Speed
Random Forest Only	82.00%	76.97%	93.49%	84.43%	2500/s
DistilBERT Only	99.72%	99.44%	100%	99.72%	47/s
Hybrid RF+DB	**96.60%**	**100%**	**93.49%**	**96.63%**	**985/s**

VI. DISCUSSION

The results clearly show that: Traditional machine learning algorithm like Random Forest is efficient, but limited in detection of phishing attacks.Deep learning provides high accuracy but little bit slower in speed. So by combining it together we got high speed with high accuracy. Which makes it also capable of working in real time environment.Although Distil BERT achieves higher accuracy but it requires more inference time compared to the hybrid model. The hybrid model processes URLs faster than Distil BERT while maintaining the higher accuracy than Random Forest alone making it more suitable for real time detection. Here is figure of that comparison.

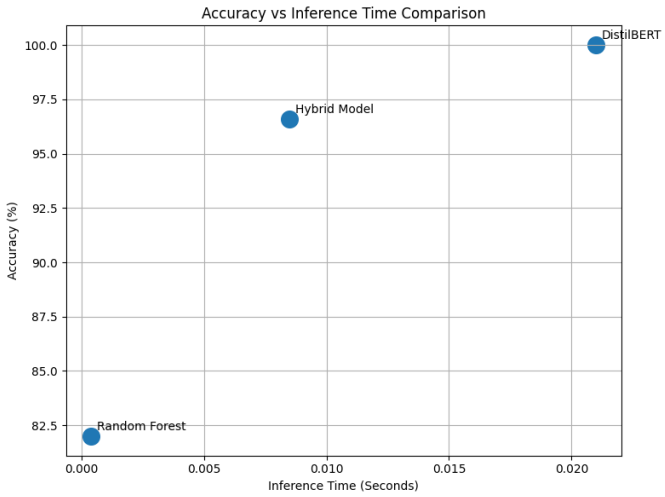

Fig. 2. Correlation between Computational Time and Prediction Accuracy across Random Forest, DistilBERT, and the Proposed Hybrid Model.

VII. CONCLUSION

This paper proposed hybrid system of phishing detection by combining one Machine learning algorithm Random Forest and one deep learning model Distil Bert. Random forest provides speed and Distil bert provides high accuracy. Results show that Distil bert achieves 100 percent accuracy compare to Random Forest which only achieves 82 percent.The hybrid model achieves 96.60 accuracy with 100 percent precision

and 93.49 recall. The hybrid approach balances the speed and accuracy. That's why the proposed model is well suited for phishing detection also in real time detection.

VIII. Future work

1) Real time deployment: The current system can be extended to add into browser extension that enable to detect phishing in real time automatically as you click on the link.
2) Larger dataset: Train on larger dataset to improve generalization and reduce overfitting.
3) Detection of evolving phishing attacks: In this the model automatically learn through new data and update itself in real world.

References

[1] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy," *Frontiers in Computer Science*, vol. 3, p. 563060, 2021.

[2] F. Spanca and A. Salihu, "Unveiling the consequences of data breaches: risks, impacts, and mitigation in the digital age," in *2024 international conference on electrical, communication and computer engineering (ICECCE)*. IEEE, 2024, pp. 1–8.

[3] N. A. Azeez, S. Misra, I. A. Margaret, L. Fernandez-Sanz, and S. M. Abdulhamid, "Adopting automated whitelist approach for detecting phishing attacks," *Computers & Security*, vol. 108, p. 102328, 2021.

[4] C. M. R. Da Silva, B. J. T. Fernandes, E. L. Feitosa, and V. C. Garcia, "Piracema. io: A rules-based tree model for phishing prediction," *Expert Systems with Applications*, vol. 191, p. 116239, 2022.

[5] S. Kavya and D. Sumathi, "Design of a hybrid ai-based phishing website detection using lstm, cnn, and random forest based ensemble learning analysis," in *2024 8th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*. IEEE, 2024, pp. 1374–1381.

[6] K. Lemons, "A comparison between naïve bayes and random forest to predict breast cancer," *International Journal of Undergraduate Research and Creative Activities*, vol. 12, no. 1, p. 10, 2023.

[7] S. Shah, S. L. Manzoni, F. Zaman, F. E. Sabery, F. Epifania, and I. F. Zoppis, "Fine-tuning of distil-bert for continual learning in text classification: An experimental analysis," *IEEE Access*, vol. 12, pp. 104 964–104 982, 2024.

[8] S. H. Ahammad, S. D. Kale, G. D. Upadhye, S. D. Pande, E. V. Babu, A. V. Dhumane, and M. D. K. J. Bahadur, "Phishing url detection using machine learning methods," *Advances in Engineering Software*, vol. 173, p. 103288, 2022.

[9] A. S. Raja, G. Pradeepa, and N. Arulkumar, "Mudhr: Malicious url detection using heuristic rules based approach," in *AIP conference proceedings*, vol. 2393, no. 1. AIP Publishing LLC, 2022, p. 020176.

[10] M. K. Hasan, "New heuristics method for malicious urls detection using machine learning," *Wasit Journal of Computer and Mathematics Science*, vol. 3, no. 3, pp. 60–67, 2024.

[11] 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. 36 429–36 463, 2022.

[12] 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, pp. 36 805–36 822, 2023.

[13] D. Kalla and S. Kuraku, "Phishing website url's detection using nlp and machine learning techniques," *Journal of Artificial Intelligence*, vol. 5, p. 145, 2023.

[14] N. Mandela, G. Mwendwa, and F. Etyang, "Hybrid cnn-lstm model for phishing email detection," *Journal of Electrical Systems and Information Technology*, vol. 13, no. 1, p. 45, 2026.

[15] M. A. Adebowale, K. T. Lwin, and M. A. Hossain, "Intelligent phishing detection scheme using deep learning algorithms," *Journal of Enterprise Information Management*, vol. 36, no. 3, pp. 747–766, 2023.

[16] E. A. Aldakheel, M. Zakariah, G. A. Gashgari, F. A. Almarshad, and A. I. Alzahrani, "A deep learning-based innovative technique for phishing detection in modern security with uniform resource locators," *Sensors*, vol. 23, no. 9, p. 4403, 2023.

[17] 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 Computing*, vol. 25, no. 6, pp. 3819–3828, 2022.

[18] M. A. Uddin, M. Mahiuddin, and I. H. Sarker, "An explainable transformer-based model for phishing email detection: A large language model approach," *Computer Networks*, p. 112061, 2026.

[19] S. Ahmad, M. Zaman, A. S. Al-Shamayleh, R. Ahmad, S. M. Abdulhamid, I. Ergen, and A. Akhunzada, "Across the spectrum in-depth review ai-based models for phishing detection," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 2065–2089, 2024.

[20] M. Alghenaim, G. Alkawsi, and C. R. Barnhart, "the state of the art in ai-based phishing detection: a systematic literature review," *Current and Future Trends on AI Applications*, pp. 431–458, 2025.

[21] A. E. Alhasan, "Enhancing real-time phishing detection with ai: A comparative study of transformer models and convolutional neural networks," 2025.

[22] D. Ye, J. Hu, J. Fan, B. Tian, J. Liu, H. Liang, and J. Ma, "Best practices for distilling large language models into bert for web search ranking," in *Proceedings of the 31st International Conference on Computational Linguistics: Industry Track*, 2025, pp. 128–135.

[23] N. Srilachai, P. Viboonsang, and S. Kosolsombat, "Phishing url detection using machine learning and deep learning in nlp," in *2025 IEEE International Conference on Cybernetics and Innovations (ICCI)*. IEEE, 2025, pp. 1–6.

[24] C. Hung, C.-F. Tsai, and M.-H. Wu, "Dimensionality reduction strategies for classification: Ml versus dl approaches and their combinations," *Expert Systems*, vol. 42, no. 10, p. e70140, 2025.

[25] S. D. R. Somula and G. Thadi, "Detection of ai-generated phishing emails: Comparing the efficiency of svm, random forest, cnn and bilstm in detecting ai-generated phishing emails," 2025.

[26] D. Orozco, L. Quesada, K. Ramirez-Benavides, and A. Lara, "Real-time malicious url detection," in *2024 IEEE Latin-American Conference on Communications (LATINCOM)*. IEEE, 2024, pp. 1–7.

[27] J. Liu, B. Cai, S. Yan, and P. Sun, "Transformer fault diagnosis based on the improved qpso and random forest," *Measurement Science and Technology*, vol. 35, no. 9, p. 096206, 2024.