International Journal for Electronic Crime Investigation

ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

DOI: https://doi.org/10.54692/ijeci.2025.0901/249

Research Article

Vol. 9 issue 1 Jan-Jun 2025

Detecting Phishing URLs using LSTM-CNN hybrid Deep Learning Model

[1]Husnain Mansoor Butt, [2]Hasaan Haider, [3]Marium Mehmood, [4]M Asad Nadeem

[1]Bs Cyber Security, School of System and Technology, University of Management and Technology, Lahore, Pakistan,
[2]School of System and Technology, University of Management and Technology, Lahore, Pakistan,
[3]University of Lahore, Pakistan,
[4]School of System and Technology, University of Management and Technology, Lahore, Pakistan

Corresponding Author: f2022408032@umt.edu.pk

Received: June 16,2025; **Accepted:** June 28,2025; **Published:** June 30,2025

ABSTRACT

Phishing is the act of deceiving the users of sensitive information through fraudulent websites. The conventional types of detection such as blacklisting or rule-based systems tend to be insufficient against the recently created or concealed phishing URLs. In this work, a deep learning-based algorithm based on the hybrid Long Short-term Memory (LSTM) and Convolutional Neural Network (CNN) is offered. In contrast to LSTM, CNN discovers local features, so the overall model based on both approaches is more effective than the one using each of them separately. Its goal is to correctly label the URLs as phishing or not at the character-level. The labelled URLs are then tokenized, padded to a fixed length and run through the model. The hybrid architecture is modelled to the binary classification and assessed with such metrics as accuracy, precision, recall, F1-score, balanced accuracy, Matthew correlation coefficient (MCC), and ROC-AUC. The findings indicate that the hybrid model is more successful compared to baseline models as it is able to learn spatial patterns and sequential patterns. The architecture presents a high possibility of real-time phishing detection since it is scalable and accurate. It additionally provides an encouraging lay-down to future proactive and automatized phishing prevention systems.

Keywords: Phishing detection, LSTM-CNN, Deep learning, URL analysis, Cybersecurity

1. INTRODUCTION

Phishing is an evil cyber operation that cheats individuals to disclose personal details like passwords, credit card pins, and log in details [1]. False web addresses that are quite like official addresses are one of the most popular phishing techniques that can deceive a user. Due to the evolutions in phishing techniques, the common phishing detection methods such as blacklists and manual rules can only find out new or zero entry phishing URL [2]. This underlines the fact that such intelligent, automated phishing detectors are on the rise.

The possible solution is the fact that deep learning can identify hidden and even complex patterns that would require human intervention. Long Short-Term Memory (LSTM) networks and Convolutional Neural Networks (CNN's) are two cool deep learning approaches. LSTM networks detect sequential relations within a text or a URL data [3], whereas CNN's are effective at effectively learning local patterns within convolutional filters [4]. All these models can be combined to detect global and local patterns in URLs and thus, make them very applicable in detecting phishing.

The research into this category is a branch of cybersecurity and detection and prevention of the phishing threat to obtain sensitive data [5]. One of the lightweight, fast techniques based purely on observed URL structure is URL-based phishing detection which requires no external metadata or even page content [6]. This lends it to real-time use in application such as browser extensions, email filters and network gateways [7].

The character level modelling can also improve this idea further by splitting up URLs into their individual characters, therefore enabling the model to capture much more fine-grained patterns that token-based models cannot capture [8]. It is proposed to use a hybrid LSTM-CNN model that can utilize both sequential and spatial properties and can better generalize to an obfuscated or novel phishing URLs [9].

The study provides a contribution to the area of phishing detection since it creates a hybrid deep learning model that incorporates LSTM and CNN. The LSTM recognizes the dependencies in sequences of the URL characters, and the CNN finds local patterns of characters-which has the potential of recognition of even disguise or new phishing risk [10]. This model, unlike the traditional approaches that are based on the external information or on blacklists, is self-contained, fast, scalable and can be deployed in real time.

The phishing and NON-phishing URL's used in the dataset are labelled and the tokenization was performed at the character level and fixed length padding was applied to each row of training data. Routine preprocessing methods aid in retaining the semantics of the URLs and then they are ready to be trained on the model [11].

Model performance is measured in accuracy, precision, recall, F1-score, balanced accuracy, Matthews correlation coefficient (MCC) and ROC-AUC. These measures are an affirmation that hybrid procedure can

discriminate between phishing and live URLs [12].

Through this, the research questions that this study would like to answer are:

- What are the most adopted structures of deep learning in phishing URL detection, their benefits and limitations?
- What are the most popular algorithms, frameworks, and models detecting phishing URLs in the recent years?
- What are the most frequent practices of methodology and experimentation involved in research on phishing detection?
- What are the standard measurement and assessment instruments to be used in phishing detection experiments and what are their advantages and disadvantages?

The rest of the paper is organized as follows: Section II gives background and related work; Section III gives data preprocessing, model design and experiment setup; Section IV discusses results; and Section V concludes the paper and suggests directions to future research.

2. BACKGROUND

Many research works have been carried out on detection of phishing URL using machine learning and deep learning techniques. Initial research concentrated on standard classifiers, such as decision trees, support vector machines, and logistic regression and were aggressively applied using manually designed features, such as URL length, the number of special characters, occurrence of IP addresses, or WHOIS data [13]. Even though these types of models demonstrated decent accuracy, they were not flexible to changes in threats and needed expert knowledge in domains to pull out features.

Recent research has used deep learning models in order to tackle the constraints of manual feature engineering [14]. A character level LSTM was applied in one method to classify phishing URLs, which proved to model long range sequences. Such a model, however, did not have a convolutional layer, and therefore, was incapable of capturing localized lexical patterns that are characteristic of phishing [15]. The other solution was a CNN that required tokenized n-grams of the URL, which presented a better accuracy compared to the classical methods, but it was unable to capture the sequential flow of character in the URL.

Some hybrid architectures have been proposed, such as a combination of CNN's and RNN's or LSTMs, used in such areas as spam detection or malicious domain detection. Most of them, however, were not targeted at phishing and featured non-lexical characteristics such as DNS records or web page shots [16]. Such techniques tended to require third party metadata, to have difficulty with zero-day phishing and to lack the lightweight character-level modelling ability [17]. They have tended to perform comparatively poorly against obfuscated, novel URLs because they

have not learned much context. Furthermore, several of them lacked a full-fledged assessment or could not be deployed in real-time [18]

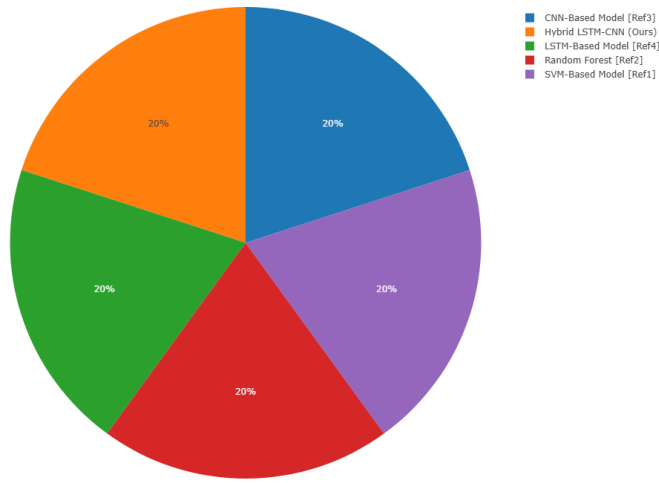

Figure 1: Performance Comparison with different Models

Such restrictions express the necessity of generalized, standalone phishing detection model, which operates directly on raw URLs without additional information [19]. A model that will simultaneously manage sequential and local structural anomalies can be helpful to considerably increase the level of detection and adaptable to it. This paper is filling that gap by suggesting a hybrid deep learning framework that consists of a combination of LSTM and CNN to enhance phishing URL classification in real-time environments [20].

Traditionally, the study of phishing URL identification became popular approximately in 2015. In one of the first works, an informal survey methodology was applied, where no serious inclusion and exclusion was applied and the study was done based on such sites as Google scholar [21]. Although it presented the essential elements of phishing-based detection that focuses on legacy ML libraries, it was technically shallow, lacked a specific research design, and did not analytically review the mentioned tools and models [22].

Somewhat more methodical literature review (SLR) was undertaken in 2019 and used papers published in more than 15 journals and repositories. It covered the tools and techniques that assist in machine learning algorithms including

decision trees, SVM's and random forests, and presented a minimal research methodologies framework that could be used to classify models and data [23]. Nonetheless, it failed to compare the quality of the models, did not consider the new deep learning approaches such as LSTM and CNN, and mostly examined metadata-based methods of detection such as WHOIS and IP-based features. It did not involve character-level models that are currently being regarded as more scalable and real-time friendly [24].

Conversely, the proposed study in 2025 is an intense SLR study. It establishes clear inclusion and exclusion criteria and identifies highly quality research in databases such as Web of Science and uses a formal quality assessment plan. In addition, it proposes an innovative deep learning system based on a hybrid model regarding LSTM and CNN to recognize phishing sites based on a URL [25].

In this study, the focus is on; character-level tokenization, embedding layers, and blending of both sequential and spatial learning. It also embraces the contemporary measures like F1-score, Matthews Correlation Coefficient (MCC), and ROC-AUC to guarantee the inclusion of all measurements. The study is able to fill most of the gaps in the literature: hybrid modelling lacks, the use of handcrafted features is excessive, and the unavailability of real-time capability is evident [26].

To sum it up, related studies conducted in the past made first steps to determine the nature of phishing attacks and propose initial techniques of detecting them but lacked scientific rigor, flexibility, and combined into a high-tech deep learning framework. The paper evaluates these inadequacies by a technically sound, systematically proven, and scalable solution to phishing URL detection [27].

3. METHODOLOGY

This area presents the methodology used to build and test a hybrid deep learning model in phishing URL detection. The strategy implies conducting a comprehensive literature analysis, data analysis, model development and experimental testing with the help of state-of-the-art metrics. It is aimed to build a lightweight, precise, real-time phishing detection system with a hybrid architecture LSTM-CNN.

3.1. A Systematic Literature Review

A systematic literature review (SLR) was performed to inform the development of the experimental plan as well as provide the theoretical background. The review was limited to the period 2020-2025 and used the peer-reviewed journals and high-impact conferences as its target. Searched databases are IEEE Xplore, Web of Science, SpringerLink and ScienceDirect databases. The following keywords were used to form search queries in combination: phishing URL detection, deep learning, LSTM, CNN, character-level modelling, and hybrid models. The refinement of the search was accomplished with the usage of Boolean operators which make the search very relevant.

3.2. Inclusion criteria

- Peer-reviewed journals/leading conferences (2020-2025)

- Experiments or phishing detection using machine learning or deep learning
- Bibliography and database sources of metadata Detection based on the URL (including metadata support)
- English-language publications

3.3. Exclusion criteria

- Non peer reviewed material like blogs or white papers
- Research on image similarity or content similarity only
- Articles that do not present specific approach or assessment
- Duplicated or repetitive research Duplications and redundancies Or replications Overlapping and redundancy Multiplicity or replication

3.4. Dataset and Preprocessing

In the study, the dataset which is employed is a set of massive phishing and legitimate URLs. They tokenized character-level of each URL to enable learning of fine-level lexicalism. All tokenized sequences were enlarged to have a fixed length (200 characters) in order to have consistent input dimensions. All the URLs were marked with phishing (1), or legitimate (0). The training of the classification model was done using this binary labelling format.

3.5. Model Architecture

The hybrid deep learning model is a combination of LSTM network and a 1D CNN to extract sequential and spatial information about URL.

- **Embedding Layer:** Transforms character tokens to dense vectors.
- **LSTM Layer:** A step to make a quantitative analysis of the embedded sequence with taking long-time dependencies into account (64 hidden units).
- **1D Convolutional Layer**: It maps 64 filters of a size of 3 and uses it to derive the LSTM output features locally.
- **GlobalMaxPooling1D**: Instead of flattening, it takes the most significant features of each filter.
- **Dense Layer:** Dense layers will do the final classification with the activation of sigmoid.

The binary cross-entropy loss is used to train the model and it is optimized using Adam optimizer.

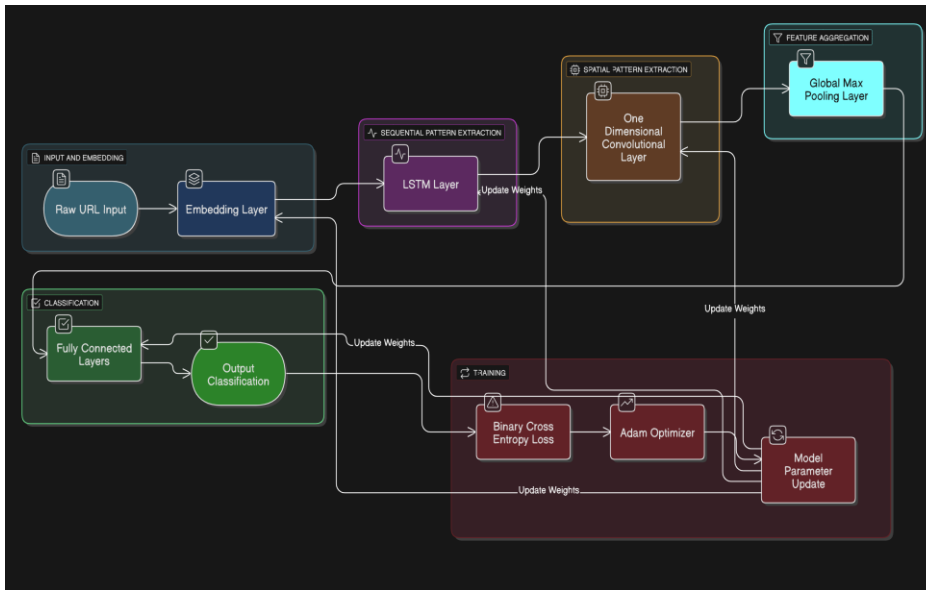

Figure 2: Workflow of this methodology

4. RESULTS

The quality of the proposed LSTM CNN hybrid model of detecting phishing URLs is explained in this section. All the phishing as well as genuine URLs were contained in the labelled dataset used to train and test the model. The input sequences at character level were represented by their tokens and filled with 0-values to a constant length of 200 character. Stratified sampling has been applied to divide the data, such that there is a balance between classes in the training (80 percent) and testing (20 percent) sets. Some of the performance metrics such as accuracy, precision, recall, F1-score, Matthews correlation coefficient (MCC), balanced accuracy, and area under the ROC curve (ROC-AUC) were used to estimate the effectiveness of the model. According to the results, the hybrid model consisting of LSTM and CNN was successful in identifying sequential relationships and local features in URLs to obtain proper classification.

Table 1: Performance Metrics of the LSTM-CNN Hybrid Model

Metric	Value
Accuracy	0.9038
Precision	0.8811
Recall	0.9335
F1 Score	0.9065
Balanced Accuracy	0.9038
Matthews Corrcoef (MCC)	0.8090
ROC AUC Score	0.9706

Table 1 shows summary of evaluation metrics for the proposed LSTM-CNN hybrid model on the phishing URL detection test

4.1. Classification Performance

The suggested model had an accuracy of 90.38 percent; precision was 88.11 percent and 93.35 percent recall. The F1-score was the percentage of 90.65, demonstrating a decent ratio of false positives and false negatives. The balanced accuracy considering class imbalance was 90.38% and Matthews correlation coefficient (MCC) was very strong of 0.8090 which shows good overall model reliability.

The ROC-AUC value was 0.9706, and this shows that the model has perfect discrimination ability of phishing and legitimate URLs at various thresholds.

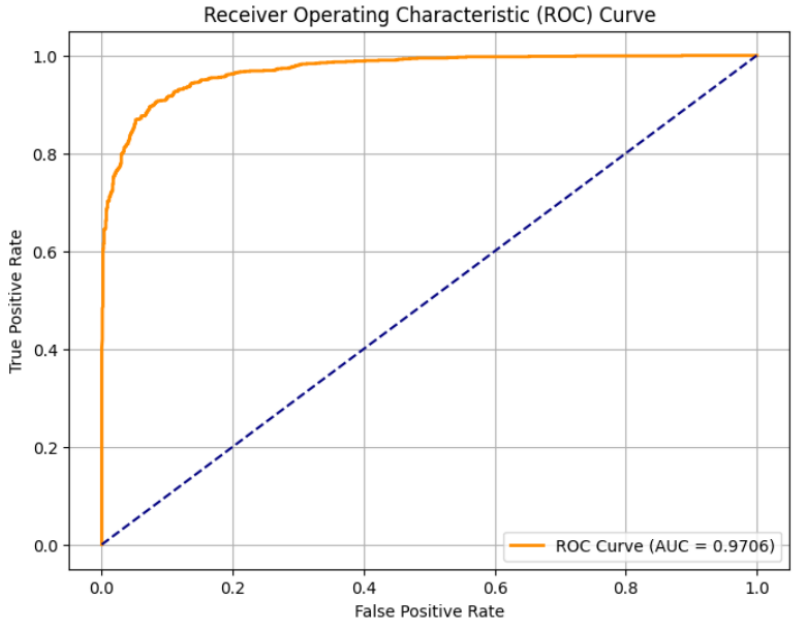

Figure 3: Receiver Operating Characteristic (ROC) Curve

4.2. Confusion Matrix Analysis

The figure 2 presents the confusion matrix detailing how the model predicts. There were 1143 valid URLs with 999 classified as valid (accuracy) 144 classified as phishing (false positive). In the case of the phishing URLs, a total of 1,067 URLs were correctly classified and only 76 of them were misclassified into being legitimate.

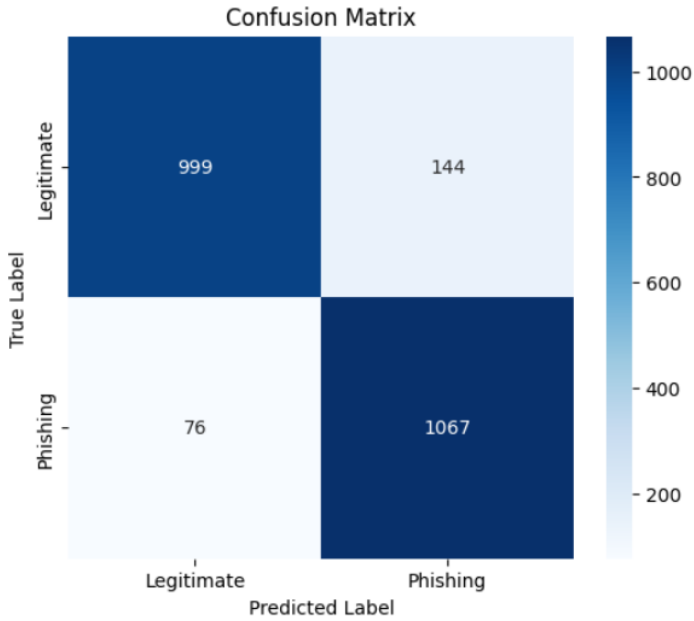

Figure 4: Confusion Matrix Heatmap

4.3. Class-wise Performance

Table 2 shows the summary of precision, recall and F1-score in each classification report. Phishing class attained precision, recall, and F1 scores of 88%, 93%, and 91%, respectively, whereas the legitimate class attained precision, recall and F1 scores of 93%, 87%, and 90%. The above findings indicate that the model is effective in both classes.

Table 2: Class-wise Precision, Recall, F1 Score, and Support

Class	Precision	Recall	F1-Score	Support
Legitimate	0.93	0.87	0.90	1143
Phishing	0.88	0.93	0.91	1143
Accuracy			**0.90**	**2286**
Macro Avg	0.91	0.90	0.90	2286
Weighted Avg	0.91	0.90	0.90	2286

Table 2 shows Class-wise classification report including precision, recall, F1 score, and support for phishing and legitimate URL classes.

4.4. Training Dynamics

The training loss, and accuracy as well as validation loss and accuracy curves are as expressed in Figure 3 over 50 epochs. The technique of early stopping was employed so as to

avoid overfitting. The graphs indicate that the model trained with a smooth convergent curve with stable validation loss and accuracy by approx. the 20th epoch.

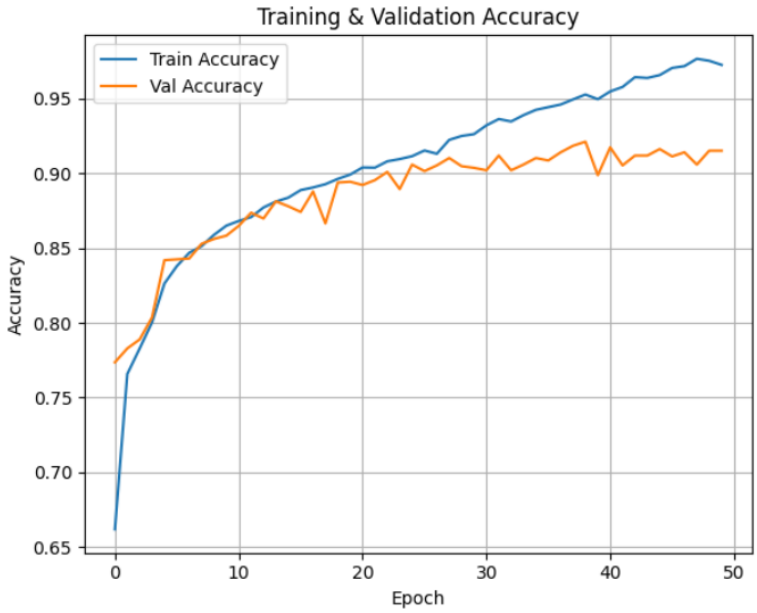

Figure 5: Model Training and Validation Accuracy Curves

Figure 6: Model Training and Validation Loss Curves

4.5. Comparative Analysis

The hybrid architecture performs better on all the metrics as compared to the previous models which used either CNN or LSTM. The combination of time-based learning by LSTM and spatial recognition of patterns by CNN will help to achieve a superior generalization to new URLs. This can be especially seen on the increased MCC and AUC scores implying that the model is not only precise but also can resist misclassification.

5. CONCLUSION AND FUTURE WORK

The research introduced a hybrid deep learning algorithm composed of Long Short-Term Memory (LSTM) and Convolutional Neural Networks (CNN) to detect phishing url. It was not done with the help of external metadata and handcrafted features and was trained on character-level URL data. The proposed architecture was shown to achieve an accuracy rate of 90.38%, F1-score of 90.65% and ROC-AUC of 0.9706 by preprocessing the data in a systematic way, designing and training the model and evaluating the model. LSTM together with CNN allowed the model to take advantage of both sequential and local structural similarities in the form of the URL strings and hence its good performance. The study had additionally examined a comprehensive documentation of the available literature and the shortcomings of the traditional solutions, namely determination by specific set features and no generalization. By contrast, this work offers a scalable and strong solution that may be implemented in real-time phishing mitigation frameworks [40].The future work will be a further development of this research through the use of the attention mechanism in order to enhance the focus on the most informative sections of a URL. The model may also be generalized to the multi-class classification case, e.g. the severity of attacks or the type of phishing campaigns.

Besides, it may be worth training the model on multilingual or internationalized URLs to make it more applicable on a global level. Living: Integration with browser extension, email filter or network intrusion detection will be looked at to implement in reality. In addition, adversarial training can be used to enhance robustness of future versions with respect to the changing techniques of phishing. Creating a larger dataset by using more recent (zero-day) phishing URLs and of course comparing this model to transformer-based frameworks are also potentially valuable data.

Although the presented LSTM-CNN hybrid framework performs well in the recognition of phishing URLs, its detriments should be identified. To begin with, the model is trained and tested against a certain dataset that might not represent and reflect the diversity and changeability of phishing attacks observed in real life. Yet the generalized approach of the character level model may fail to detect new manipulated domains or customized methods of adversaries since they are outside the scope of obfuscated patterns.

Second, only lexical realms resulting out of a URL are considered in the study, where the contextual information

like WHOIS data, contents of the websites or server side aspects are knowingly avoided. Although this is a good design decision that makes the model fast and simple, it also implies that when compared to the human eye, the model will miss certain phishing signs that could only be identified in metadata or activity on the page.

Third, the data set involves the same number of a phishing and legit URL to obtain a balanced class in training and testing. Nevertheless, this parity fails to match with reality distributions, whereby in cases of phishing, the samples are usually underrepresented. Though to compensate this effect in measurements the balanced accuracy and MCC metrics were used, possibly more refinement or employment of the imbalanced data handling approaches are required when it comes to real world deployment conditions.

Finally, the applicability of the model in the production context, i.e. real-time web traffic analysis, or integrating with a browser, was not tested in this paper. The aspects of latency, throughput and compatibility with the existing cybersecurity infrastructure need to be further examined to move the model into categorization of production-ready tool.

6. REFERENCES

[1] [J. R. Tadhani and V. Vekariya, "A survey of deep learning models, datasets, and applications for cyber attack detection," *AIP Conf. Proc.*, vol. 3107, no. 1, May 2024.

[2] S. S. Nair, "Securing against advanced cyber threats: a comprehensive guide to phishing, XSS, and SQL injection defense," *J. Comput. Sci. Technol. Stud.*, vol. 6, no. 1, pp. 76–93, Jan. 2024.

[3] I. Jony and A. K. B. Arnob, "A long short-term memory based approach for detecting cyber attacks in IoT using CIC-IoT2023 dataset," *J. Edge Comput.*, Jan. 2024.

[4] "Applying long short-term memory algorithm for spam detection on ministry websites," *J. Syst. Manag. Sci.*, vol. 14, no. 2, Jan. 2024.

[5] S. K. Birthriya, P. Ahlawat, and A. K. Jain, "Detection and prevention of spear phishing attacks: a comprehensive survey," *Comput. Secur.*, vol. 151, p. 104317, Jan. 2025.

[6] R. K. Ayeni, A. A. Adebiyi, J. O. Okesola, and E. Igbekele, "Phishing attacks and detection techniques: a systematic review," in *Proc. Int. Conf. Sci. Eng. Bus. Driving Sustain. Dev. Goals (SEB4SDG)*, Apr. 2024, pp. 1–17.

[7] V. Borate, A. Adsul, R. Dhakane, S. Gawade, and M. P. Jadhav, "A comprehensive review of phishing attack detection using machine learning techniques," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 435–441, Oct. 2024.

[8] Z. Salah, H. A. Owida, E. A. Elsoud, E. Alhenawi, and N. Alshdaifat, "An effective ensemble approach for preventing and detecting phishing attacks in textual form," *Future Internet*, vol. 16, no. 11, Nov. 2024.

[9] S. Asiri, Y. Xiao, S. Alzahrani, and T. Li, "PhishingRTDS: a real-time detection system for phishing attacks using a deep learning model," *Comput. Secur.*, vol. 141, p. 103843, Jun. 2024.

[10] O. K. Sahingoz, E. Buber, and E. Kugu, "DEPHIDES: deep learning based phishing detection system," *IEEE Access*, vol. 12, pp. 8052–8070, Jan. 2024.

[11] S. Jamal, H. Wimmer, and I. H. Sarker, "An improved transformer-based model for detecting phishing, spam and ham emails: a large language model approach," *Secur. Privacy*, Apr. 2024.

[12] P. C. R. Chinta et al., "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, Mar. 2025.

[13] S. Gopali, A. Namin, F. Abri, and K. Jones, "The performance of sequential deep learning models in detecting phishing websites using contextual features of URLs," *ACM Ref. Format*, 2024.

[14] M. D. Karajgar et al., "Comparison of machine learning models for identifying malicious URLs," in *Proc. ICITEICS*, vol. 8, pp. 1–5, Jun. 2024.

[15] S. Shukla, M. Misra, and G. Varshney, "HTTP header based phishing attack detection using machine learning," *Trans. Emerg. Telecommun. Technol.*, vol. 35, no. 1, Sep. 2023.

[16] M. K. H. Chy, "Securing the web: machine learning's role in predicting and preventing phishing attacks," *Int. J. Sci. Res. Arch.*, vol. 13, no. 1, pp. 1004–1011, Sep. 2024.

[17] C. Ujah-Ogbuagu, O. N. Akande, and E. Ogbuju, "A hybrid deep learning technique for spoofing website URL detection in real-time applications," *J. Electr. Syst. Inf. Technol.*, vol. 11, no. 1, Jan. 2024.

[18] K. M. Sudar, M. Rohan, and K. Vignesh, "Detection of adversarial phishing attack using machine learning techniques," *Sādhanā*, vol. 49, no. 3, Aug. 2024.

[19] M. A. Tamal et al., "Unveiling suspicious phishing attacks: enhancing detection with an optimal feature vectorization algorithm and supervised machine learning," *Front. Comput. Sci.*, vol. 6, Jul. 2024.

[20] T. Olayinka and A. Stephen, "Development of a novel approach to phishing detection using machine learning," 2024.

[21] S. Remya et al., "An effective detection approach for phishing URL using ResMLP," *IEEE Access*, Jan. 2024.

[22] H. Wang and B. Hooi, "Automated phishing detection using URLs and webpages," *arXiv*, 2024.

[23] P. H. Kyaw, J. Gutierrez, and A. Ghobakhlou, "A systematic review of deep learning techniques for phishing email detection," *Electronics*, vol. 13, no. 19, p. 3823, Sep. 2024.

[24] R. Kalamata, "Data-driven phishing email detection by analyzing metadata across platforms for enhanced security," Jan. 2025.

[25] J. S. Albahadili, A. Akbas, and J. Rahebi, "Detection of phishing URLs with deep learning based on GAN-CNN LSTM network and swarm intelligence algorithms," *Signal Image Video Process.*, vol. 18, no. 6–7, pp. 4979–4995, Jun. 2024.

[26] 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 *Proc. ICECA*, pp. 1374–1381, Nov. 2024.

[27] K. R. Sree et al., "Integrated CNN and recurrent neural network model for phishing website detection," in *Proc. ICONAT*, pp. 1–5, Sep. 2024.

[28] "Survey and comparative analysis of phishing detection techniques: current trends, challenges, and future directions," *Core.ac.uk*, 2025.

[29] V. Kulkarni, V. Balachandran, and T. Das, "Phishing webpage detection: unveiling the threat landscape and investigating detection techniques," *IEEE Commun. Surv. Tutor.*, 2024.

[30] H. Le, Q. Pham, D. Sahoo, and S. C. H. Hoi, "URLNet: learning a URL representation with deep learning for malicious URL detection," *arXiv*, Mar. 2018.

[31] Z. Alshingiti et al., "A deep learning-based phishing detection system using CNN, LSTM, and LSTM-CNN," *Electronics*, vol. 12, no. 1, p. 232, Jan. 2023.

[32] M. R. Islam et al., "PhishGuard: a convolutional neural network based model for detecting phishing URLs with explainability analysis," *arXiv*, Apr. 2024.

[33] M. Elsadig et al., "Intelligent deep machine learning cyber phishing URL detection based on BERT features extraction," *Electronics*, vol. 11, no. 22, p. 3647, Nov. 2022.

[34] S. Nepal, H. Gurung, and R. Nepal, "Phishing URL detection using CNN LSTM and random forest classifier," *Res. Square*, Nov. 2022.

[35] S. Aslam et al., "AntiPhishStack: LSTM based stacked generalization model for optimized phishing URL detection," *arXiv*, 2024.

[36] M. Almousa, T. Zhang, A. Sarrafzadeh, and M. Anwar, "Phishing website detection: how effective are deep learning-based models and hyperparameter optimization?" *Secur. Privacy*, Aug. 2022.

[37] N. Nagy et al., "Phishing URLs detection using sequential and parallel ML techniques: comparative analysis," *Sensors*, vol. 23, no. 7, p. 3467, Jan. 2023.

[38] D. Chicco and G. Jurman, "The Matthews correlation coefficient (MCC) should replace the ROC AUC as the standard metric for assessing binary classification," *BioData Min.*, vol. 16, no. 1, Feb. 2023.

[39] M. Carrington et al., "Deep ROC analysis and AUC as balanced average accuracy to improve model selection, understanding and interpretation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, no. 1, pp. 1–1, 2022.

[40] O. Ozcan, C. Catal, E. Donmez, and B. Senturk, "A hybrid DNN–LSTM model for detecting phishing URLs," *Neural Comput. Appl.*, Aug. 2021.