International Journal on Robotics, Automation and Sciences

Detection of Malicious URLs: A Deep Learning and Machine Learning Perspective

Shougfta Mushtaq* and Mazliham Mohd Su'ud

***Abstract* - Nowadays, as the cyber world is expanding rapidly, issues related to cybersecurity are also increasing. The criminal mind set try to breach the security of individual or organization by firstly, win confidence and secondly attack them for this purpose URL phishing is a most common way where phisher attach a link and share with victim. The proposed paper examines the various machine learning and deep learning approaches on state-of-the-art data set Crawling2024 by classifying the phishing and legitimate URLs. The study involves different machine learning algorithms like Random Forest, LR (Logistic Regression), XGBoost, MLP (Multilayer Perceptron) and Gated Recurrent Units (GRU) and deep learning algorithms like CNN (Convolutional Neural Network), MLP, etc. and analyze performance metrics accuracy, precision, F1 score, Recall, False Positive and False Negative. The RF (Random Forest) classifier achieved the highest precision (98.63%) and accuracy (96.24%), while Logistic Regression and GRU also achieved well. In addition to that LTRCN (Long-Term Recurrent Convolutional Network) achieved good precision but poor accuracy 48.23%. The experimental work shows that conventional algorithms such as Random Forest and advanced algorithms like GRU are efficient in detecting URL phishing, it also emphasizes that there is still need of some advanced approaches like CNN and LTRCN.**

Keywords---Phishing URLs, URL Classification, Machine Learning, Deep Learning, Cybersecurity.

I. INTRODUCTION

Phishing is a kind of cybercrime where phisher wants to harm an individual or an organization by breaching security and successfully deceive them to reveal their confidential data such as passwords, PINs, credit card numbers or loin credentials. The common phishing attacks are usually done through fake emails, messages, or websites that seems to be trustworthy. The common strategies included modification of domain names (e.g., "g00gle.com" instead of "google.com"), modification in logo, extra subdomains or hiding the true destination by shortening URLs. There is immense danger caused by phishing like economic loss, identity theft, financial frauds, and illegal access to accounts and making false transactions. Furthermore, breaching the security of an individual or an organization sometimes cause legal consequences and harm the reputation of organization. Phishing also includes the circulation of malware through links that effects security. A successful phishing attack can harm an organization image and break customer trust on a brand. Now, it is the need of the time to spread awareness regarding phishing, its prevention and, mitigate with attacks [1].

*Corresponding author email: shouguftawajid@yahoo.com, ORCID: 0009-0000-5794-8466

Shougfta Mushtaq : Faculty of Computing & Informatics, Multimedia University, Persiaran Multimedia, 63100 Cyberjaya, Selangor, Malaysia (e-mail: shouguftawajid@yahoo.com)

Mazliham Mohd Su'ud: Faculty of Information Science & Technology, Multimedia University, 63100, Cyberjaya, Selangor, Malaysia (e-mail: mazliham@mmu.edu.my)

International Journal on Robotics, Automation and Sciences (2026) 8, 1:1-11
https://doi.org/10.33093/ijoras.2026.8.1.1
Manuscript received: 15 May 2025 | Revised: 26 Jun 2025 | Accepted: 28 Oct 2025 |
Published: : 31 Mar 2026
Published by MMU PRESS. URL: http://journals.mmupress.com/ijoras

In cyber world several solutions related to phishing are also available like browser-based cautioning system, rule-based systems, heuristic -based methods and blacklists are also available each of them has limitations. Like in the case of blacklist used anti-phishing tool block the malicious sites but it is reactive approach and need continuous updating, which can permit new phishing techniques to attack until it is discovered. Heuristic-based approach detects the phishing by investigate the characteristics of URL, such as the length or the occurrence of the keywords, but new phishing techniques deceive them as well. Same like them Signature-based detection that is used in anti-viruses classifies based on signature of identified patterns but are fail to catch the zero-day attacks or new attacks launched by attackers [2].

The growing complexity of the phishing attacks is becoming more challenging as attackers continuously make new techniques that mimic and seems to be legitimate websites, it outperforms heuristic and rule-based approaches. Like in the case of zero-day which is immensely difficult to detect, signature-based methods and blacklist methods only catch the recognized threats. Furthermore, the false positive rate of traditional phishing detection approaches is also very high, that can block legitimate websites and prevent user to access websites. Scalability is also a big challenge; traditional methods are unable to deal with huge numbers of URLs created on daily bases. So, real time phishing detection is a big challenge [3].

From past decade ML (Machine Learning) and DL (Deep Learning) approaches are presented to deal with the phishing attacks. These solutions seem to be relevant in a case so train and learn automatically hence eliminate the problem to deal with the latest attacks. The flexibility provided by these approaches make them flexible to learn new kinds of the attacks and overcome the problems arose by traditional methods. Machine Learning and deep learning approaches also strengthen the system to extract the complex patterns and association from URLs names that can be missed out by the rule-based system or by the human professionals. So, it can be a better approach to use these models to recognize the hidden patterns and to boost the detection systems [4].

The major advantage of the Machine Learning and Deep learning approaches is to achieve the real-time detection of URLs by processing the huge amount of data faster than traditional techniques. The methods will constantly monitor and instantly detect the phishing attacks with quick response time. Moreover, deep learning and machine learning algorithms can be fined tuned to decrease the false positive ratio, that will guarantee the legitimate website are not consider as phishing [5].

Moreover, ML/DL models are well-suited to cope zero-day phishing attacks. By being trained on large datasets, they can generalize efficiently and detect earlier unseen phishing URLs. This knowingly improves the system's capability to catch zero-day attacks, where traditional methods trusting on predefined signatures or blacklists would characteristically fail [6].

II. RELATED WORK

M. Sanchez-Paniagua et al. [7] discovered phishing detection via URL analysis, highlighting the use of login page URLs instead of homepage URLs, that leads to lower false-positive rates. Phishing Index Login URL (PILU-90K) was analyzed that contains 60,000 legitimate URLs and 30,000 phishing URLs. The results showed that logistic regression model with TF-IDF achieved 96.50% accuracy and highlighting decay in model performance over time with older datasets and stressing the need for effectual training data.

A. Villanueva et al. [8] proposed phishing detection machine learning and deep learning models are that investigate through natural language processing NLP. These algorithms including Multi-Naïve Bayes and Logistic Regression, are used for classification, while deep learning methods as Gated Recurrent Units (GRU), and Long Short-Term Memory (LSTM) Model achieved high training and validation scores, as the top models reaching 97% accuracy. The results determine the efficiency of these models in predicting phishing URLs, which highpoints the need for further research to explore additional parameters and improve detection accuracy. Overall, the findings establish the important role of multiple deep learning methods in precisely classifying URLs for phishing detection.

C. Catal et al. [9] reviewed deep learning-based phishing detection models that include nine research questions, and by analyzing 43 high-quality journal articles. The study acknowledged commonly used deep learning algorithms, datasets, and evaluation metrics, highlighting the tasks and breaches in current approaches. Key future guidelines include developing semi-supervised models, bigger public datasets, and Explainable AI for phishing detection. The study accomplishes that deep learning models show capacity, with substantial improvements in accuracy and detection rates, but additional research is needed to improve real-time detection and model transparency.

I. Kara, M. Ok, and A. Ozaday [10] proposed a procedure to detect malicious websites by classifying URLs and domain names by using six classifiers and 11 predefined features, with Random Forest carrying the highest accuracy. Model was tested on a dataset of 32,928 entries, achieving 98.90% accuracy in detecting phishing websites and 98% total prediction success. The system can be combined into email security mechanisms to block phishing links, and a continuously updated list is used to enhance detection. Future work comprises refining the approach that will use a model for real-time detection and following changes in attacker practices to improve security.

N. Q. Do et al. [11] presented use of deep learning algorithms for phishing detection, author reviewed 81 papers to classify advanced techniques. Highpoints the weaknesses and strengths of the methods, observing issues such as long training times, manual parameter-tuning and incomplete detection accuracy. Future research guidelines include experimenting with different parameters, discovering underutilized techniques like GANs and DRL, using heterogeneous ensemble models. Study's empirical investigation shows that phishing detection still faces contests in accuracy and efficiency, particularly in managing imbalanced datasets where phishing attempts are much fewer than legitimate occurrences.

D. Rathee and S. Mann [12] presented Phishing emails have become a substantial cyber threat, exploiting sensitive information through deceptive strategies. In this paper, author review machine learning algorithms and deep learning algorithms for detecting phishing emails and highpoint their restrictions relative to handling new phishing tactics due to the support on manual feature engineering and third-party services. The study exposes a lack of research using advanced natural language processing (NLP) techniques for phishing detection. Future research should focus on using modern DL models like CNNs, RNNs, and Deep Reinforcement Learning to enhance detection accuracy. Results show that current methods are insufficient, imposing more advanced phishing detection technologies.

E. S. Vishva and D. Aju. [13] discussed how phishing attacks stance an important threat to cyberspace by inducing users to expose sensitive information over malicious URLs. The paper suggests use of BERT in phishing detection for feature extraction and a CNN is used for classification of phishing and legitimate websites. The proposed model then applied to a URL dataset. Here, BERT is used to extract meaningful text features from URLs, a CNN is employed to classify such features URLs. The method achieved 96.66% accuracy, beating traditional deep learning approaches. Future work aims to improve this model with dynamic feature selection for even more precise phishing detection results.

E. S. Vishva et al. [14] elaborated that Phishing is a chief cybercrime where attackers attempt to encourage individuals into exposing reformation through fake websites, with taken data sold on the dark web. Paper presents phishing detection system that based on a machine learning, applying TF-IDF for webpage content enquiry and methods like Logistic Regression, Random Forest, and Naive Bayes. The model named Phisher Fighter, achieved 90.68% accuracy, outperforming existing methods like Cantina (76.20%). Additional improvements are recommended by expanding the dataset, using deep learning techniques, and enhancing feature selection for even better detection results.

S. H. Ahammad et al. [15] presented Phishing as a major cybercrime, aims users through malicious URLs to snip sensitive data. This study mentions that machine learning solution to distinguish phishing and legitimate websites, using algorithms like Decision Trees, Random Forests, Light GBM, SVM and Logistic Regression. By investigative the language and domain-based features, the proposed model Light GBM algorithm obtained the best results. Though, limitations in the dataset, such as missing WHO-IS data, propose the need for more features and fresh URL data to enhance accuracy. Forthcoming work goals to develop a search engine and framework to perceive and block phishing attacks with advanced investigation capabilities.

M. Almousa et al. [16] focused on the emerging deep learning techniques that can be used to enhance hyperparameters to detect phishing websites having some issues in them in terms of robustness and replicability. The proposed models are based on Long Short-Term Memory (LSTM), Fully Connected Deep Neural Networks and Convolutional Neural Networks were built and then tested using four publicly available datasets, and it achieved an accuracy of 97.37%. Hyperparameter optimization through grid search and genetic algorithm enhanced performance by 0.1–1% Future work is presented to additional browser-based features and models with Gradient Boosting methods. The goal of this study is to develop a real-time phishing detection tool for end-users.

A. Dawabsheh et al. [17] focused Phishing attacks as a major security threat, where fake URLs betray users into trailing valuable assets. Traditional blacklist-based methods fight to keep up with newly flung phishing sites. To overcome this, an enhanced deep learning approach using Variational Autoencoders (VAE) and Deep Neural Networks (DNN) are projected for automatic feature extraction and URL classification. The model achieved high accuracy (97.85%) and a response time of 1.9 s by using the ISCX-URL-2016 and Kaggle datasets. Though, a false positive rate of 2.19% is detected, and future work focused on integrating generative models to decrease this rate.

M.A. Adebowale, K.T. Lwin, and M.A. Hossain, [18] presented Phishing attacks have become more refined, and efficient detection methods. The study established a model based on deep learning for phishing detection system (IPDS) merging with the Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) algorithms to examine

URLs images and text from websites. Taking 1 million URLs, and 10,000 images from the PhishTank and Common Crawl datasets, the proposed hybrid model obtained 93.28% accuracy with an average detection time of 25 s. The incorporation of CNN speed and LSTM efficiency improved phishing detection. Future plan of author is to improve accuracy of the proposed method and produce a plugin for browser to realize real-time protection.

S. R. Abdul Samad et al. [19] presented that the phishing attacks frequently exploit social engineering to betray users into clicking malicious URLs. These attacks are hard to detect, even for thoughtful users, leading researchers to develop a machine learning based models to enhance the detection method by using features taken from URLs and web. This study tried eight popular machine learning algorithms, applying data balancing, hyperparameter alteration, and feature selection crosswise two common phishing datasets. The results show that hyperparameter tuning and feature selection meaningfully improve model accuracy, with Random Forest and Gradient Boosting achieving up to 98.27% accuracy. Future research will discover cloud security and blockchain applications.

A. Karim et al. [20] focused on the phishing attacks that are among the most hazardous forms of cyber-attacks, that use phishing URLs to deceive users. It applies machine learning models to dataset of over 11,000 URLs from the Kaggle repository to increase phishing detection. The study estimates Random Forest, Decision Tree and a hybrid ensemble model (LR+SVC+DT) used soft and hard voting with feature selection through canopy, through cross-validation and Hyperparameter Optimization by Grid Search. Results indicate that the proposed LSD hybrid model outperforms existing models, which indicates high efficiency in detecting phishing URLs. In future work, author plan to combine list-based and machine-learning detection systems

Phishing attacks, which often start with false messages holding malicious links, steal sensitive information such as passwords and login particulars. Users must differentiate malicious and legitimate URLs to avoid falling victim. The study trains machine learning models such as Random Forest, KNN, Decision Tree, Logistic Regression, CNN, and RNN models, to classify URLs as phishing or legitimate. Among these CNN and Logistic Regression achieved the highest accuracy of 96% and 95%, respectively, in detecting phishing URLs, that indicates their efficiency in preventing such cyberattacks. Author suggested Hybrid models could be a better choice to improve phishing detection [21].

Y. Wang et al. [22] emphasized that phishing attacks persist an important cybersecurity threat, and current improvements in pretrained models have accessible promising solutions. Proposed PhishBERT model is a deep learning method that is projected specifically for URL phishing detection. PhishBERT was pre-trained on over 3 billion unlabeled URLs, permitting it to learn general URL patterns. Through supervised fine-tuning with adversarial methods, the proposed model achieved superior performance in detecting phishing websites compared to advanced models. The proposed PhishBERT model achieves improved accuracy, robustness, and efficiency, making it a broadly used phishing detection tool.

M. Shoaib and M. S. Umar, [23] elaborated Phishing combines with the social engineering attacks and with technical fraudulence to snip personal identity and economic data, with cultured attacks on the rise. Paper reviews various machine learning procedures employed to spot malicious URLs, prominence their effectiveness and the current challenges in this field. It recommends that a machine learning-based phishing detection model is personalized for accurately identifying phishing attacks. The study offers a complete overview of cybersecurity progressions, the phishing attack lifecycle, and the growth in malicious URL detection through machine learning methods. The proposed model establishes promising results, flooring the way for more advanced algorithms in detecting phishing.

W. Wang.[24] presented Phishing attacks are gradually sophisticated, encourage the need for innovative detection methods. This research recommends a layered classification model leveraging machine learning algorithms to spot phishing websites by examining URL structures, image, features and text. Applying a substantial dataset of 20,000 URLs, the model integrates text extracted from images for classification, attaining an impressive accuracy of 94% in training and 91% in testing phases with the XGBoost algorithm. The multilayer perceptron, random forest, and decision tree models similarly achieved accuracies of 91%, 91%, and 90% correspondingly. The study highpoints the importance of constant adaptation to developing phishing strategies and proposes further optimization and user education as critical areas for future research.

A. Ozcan et al. [25] presented that phishing attacks mimic official websites to snip sensitive user information, leading to considerable security challenges. The proposed deep learning approach combines character embedding and Natural Language Processing NLP features to detect phishing URLs. By applying Long Short-Term Memory (LSTM) and Bi-Directional LSTM (BiLSTM) models, this study recognized that the DNN-BiLSTM model achieves an accuracy of 98.79% on earlier used dataset and 99.21% on a new dataset, beating other machine learning and deep learning models. Hybrid architecture competently integrates multiple feature sets, which allows the model to capture deep connections in URLs. Furthermore, the superior performance of BiLSTM can be attributed to its ability to examine character relationships in both forward and backward directions, which improves its contextual understanding in natural languages.

P. Pavan Kumar, T. Jaya, and V. Rajendran, [26] proposed Web phishing is an important threat that focuses on stealing sensitive information by mimicking legitimate websites. A previous study proposed a deep learning model that exploits the Swarm Intelligence Binary Bat Algorithm (SI-BBA) to classify URLs as phishing or legitimate. The deep learning model, enhanced with the Adam optimizer that achieved a classification accuracy of 94.8% and a loss value is 0.2 when detecting phishing attacks. The results demonstrate the efficiency of the proposed SI-BBA algorithm in terms of enhancing neural network performance for phishing detection. Impending improvements, including modifications to the number of epochs, batch size and learning rate are expected to further enhance the accuracy and optimization of the NN model.

F. S. Alsubaei, A. A. Almazroi, and N. Ayub [27] Introduced an innovative deep learning method that merge with the ResNeXt method with an embedded Gated Recurrent Unit (GRU) mod which is referred to as the RNT model and for real-time phishing attack detection. Use of SMOTE to address data inequality and integrating autoencoders and ResNet to enhance feature extraction, the RNT model improved through the Jaya optimization method (RNT-J). The model determined exceptional performance, achieved 98% accuracy and outperform state-of-the-art algorithms by 11% to 19% while sustaining efficient computing with execution times averaging 36.99 seconds. RNT-J excels in classifying phishing behaviors and rapidly discovering new patterns associated with existing methods like ResNet, DenseNet, BERT, and ELMo. This study highlights the need for innovative algorithms in digital forensics, paving the way for future research into hybrid models to further improve phishing detection accuracy and efficiency.

O. K. Sahingoz, E. Buber, and E. Kugu,.[28] explored in today's digital age, the growth of internet-connected devices has made users susceptible to phishing attacks, which steal sensitive information through social engineering strategies. This study presents a deep learning-based phishing detection system that assesses five different architectures: artificial neural networks, Convolutional Neural Networks CNNs, Recurrent Neural Networks RNN, Bidirectional Recurrent Neural Networks, and attention networks, focusing on fast URL classification. Using a dataset of nearly five million labeled URLs, this study demonstrated that CNNs achieved the highest performance, with a detection accuracy of 98.74% for phishing attacks, which is superior to traditional machine learning methods. This study highlights the critical role of deep learning algorithms in establishing cybersecurity against evolving threats.

D. M. Linh et al.[29] proposed Phishing attacks exploit users' lack of awareness and understanding of online security, frequently leading to the theft of personal information via fake websites. The proposed browser extension is designed to avoid phishing by implementing a smart threat feature based on deep learning models. The extension assesses malicious URLs from a dataset of 651,191 samples and employs a convolutional neural network CNN to attain a high accuracy rate of 98.4% in detecting untrusted connections. The study compares CNN performance against six other machine learning algorithms, with CNN outclassing Logistic Regression, Random Forests, Decision Trees, Support Vector Machines, and CNN-LSTM, particularly with an 8:2 training-testing data ratio. The research team will release a trial version of the extension for public use, supported by the Posts and Telecommunications Institute of Technology, and will contribute to security advancements.

B. C. Ujah-Ogbuagu, O. N. Akande, and E. Ogbuju, [30] explained URL spoofing remains a predominant method for executing phishing attacks, misleading users into see-through personal information on malicious websites. Traditional blacklists and rule-based filters have become useless; thus, new detection techniques that use machine and deep learning methods. The study recommended a hybrid model which combines convolutional neural networks CNN and Long Short-Term Memory LSTM networks to improve their ability to detect spoofing URLs. Assessed on the UCL and PhishTank datasets, the hybrid CNN-LSTM model achieved accuracies of 98.9% and 96.8%, correspondingly, pointedly outperformed CNN and LSTM models, that attained accuracies of 90.4% and 94.6% on the UCL dataset and 89.3% and 92.6% on the PhishTank dataset. The results conclude the efficiency of the proposed hybrid method in fighting phishing, and future research can discover additional hybrid models and datasets.

S. Aslam et al. [31] presented increasing use of online web services entails exaggerated security risks, primarily phishing attacks that overtake traditional detection methods. In this paper, the AntiPhishStack presented two-phase stack generalized model is presented, which employs both URL and TF-IDF features for phishing detection. Phase I is a base machine learning classifier is trained using K-fold cross-validation and Phase II is a two-layer LSTM network is operated combined with five adaptive optimizers for enhanced predictions. Proposed model achieved accuracy of 95.67% and 96.04% on two benchmark datasets, outperforming existing methods, and demonstrated its ability to detect unidentified phishing URLs. The results highlight the potential of the propose AntiPhishStackk model as a progressive phishing detection solution. In future, author plan to implement this method using GRU to classifying fraudulent accounts.

S. Das Guptta et al. [32] described machine learning-based method for real-time detection of phishing websites is proposed in this study. The proposed method influences hybrid features taken from URLs and hyperlinks that are not trusted by third-party systems. Conventional anti-phishing methods often fail to classify new phishing, which increases the difficulty of real-time detection. The proposed strategy extracts feature exclusively from the client-side URL and hyperliability using a newly developed dataset for experiments. The results demonstrate high effectiveness by achieving accuracy of 99.17% with the XGBoost technique together with a true positive rate of 98.81% and false positive rate of only 0.49%. The results of this study highlight the importance of joining both feature sets and proposes that further feature inclusion can improve accuracy while noticing that mobile phishing may pose an increasing threat in the future.

F. Trad and A. Chehab [33] investigated the Large Language Models (LLMs) efficiency in detecting phishing URLs with the help of associating prompt-engineering methods with the support of fine-tuning tactics. Paper discovered numerous prompt-engineering methods that can be functional to chat bots GPT-3.5-turbo and Claude 2, achieving F1-score of 92.74% when test on the set of 1,000 samples. In addition to that fine-tuning LLMs like GPT-2, Baby LLaMA, Bloom and DistilGPT-2, completely used for phishing detection resulted in a peak F1-score of 97.29% and an AUC of 99.56%, that will outperformed existing advanced methods. These findings result that even prompt engineering made simple development of application, it did not match the presentation of the dedicated fine-tuned models. Work suggested hybrid approaches to enhance resilience in contradiction of adversarial attacks, optimize real-time detection and address partialities in LLMs to increase the detection of phishing tools.

R. Alazaidah et al [34] addressed that phishing attacks are growing in such a way that enlarges their scope from cybercrime and are planned at stealing sensitive information from users. Study has two main objectives: classifying the best classifier among 24 options representative six learning approaches for detecting phishing and defining the most effective feature selection method for phishing datasets. The results specified that the FilteredClassifier, J-48, and RandomForest classifiers outclassed in phishing detection, while the InfoGainAttributeEval method occurred as the top feature selection technique. These findings propose the potential for developing an ensemble model combining the three best classifiers to enhance detection capabilities. Future research could discover using metaheuristic algorithms to generate more operative feature selection methods.

A. Halili et al. [35] presented "NoPhish," a Chrome extension considered to battle web phishing attacks by acting as middleware between users and potentially damaging websites. Applying a training dataset from PhishTank, the extension influences 22 popular features appraised by the Alexa database and applied various types of machine learning algorithms, the algorithms like Support Vector Machine, Random Forest and k-Nearest Neighbor are used to detect phishing attempts. The experimental results showed Random Forest algorithm achieved the highest accuracy and precision, with small false negatives. These result-based findings indicate the efficiency of machine learning algorithms in phishing detection and propose that there is important potential for further research and the development of more advanced algorithms. Paper concludes that while Random Forest performs well, continuing enhancements and adaptations are essential to keep pace with developing phishing techniques.

S. Remya et al. [36] proposed Phishing websites pose serious risks by copying legitimate sites and stealing user information through misleading URLs, making traditional blacklists unproductive. This study presents a phishing URL detection method using an enduring pipeline that combines traditional and reversed residual blocks to extract common URL features, which are then classified by using Multi-Layer Perceptron (MLP). The approach integrates domain age analysis and a lexical study of URL structure to enhance detection accuracy. Tested on a Kaggle dataset, which then achieved high accuracy, precision, recall and F1 score. Proposed method confirmed an imposing accuracy of 98.29%, highlighting its potential in mitigating phishing threats.

III. DATASET DESCRIPTION

The dataset used for experiments is Crawling2024 contains two types of URLs; Phishing URLs and Legitimate URLs. The phishing URLs are designed to deceive users into providing delicate information, while the legitimate URLs represent trusted sites. This collection purposes to provide a complete range of URLs to train models and test the model efficiency.

The Crawling2024 dataset is organized in columns representing numerous characteristics of the URLs, which helps differentiate between phishing and legitimate sites.

The key features that are used to analyze the performance metrics and classify phishing and legitimate websites are

TABLE 1: Key features used to analyze performance metrics

Feature Name
url_url
url_url_pre
url_len_url
url_len_pre
url_pre_entropy

url_suf_entropy
url_pre_https_count
url_suf_https_count
url_pre_count/
url_pre_count%
url_pre_count=
url_pre_numbers_in_domain
url_suf_numbers_in_domain

Before the result-oriented experiment performed the certain preprocessing steps are taken i.e. to remove the null values from data set dropna() function of python is used. It ensured that the experiments to be performed on the cleaned data. TF-IDF is used for the textual data classification. TF-IDF is used to control the noise in data, detect the malicious patterns and converted the text-based data into numerical form. After TF-IDF data set is divided into testing and training groups using splits of 80/20 and 70/30. This will allow the ability of model to learn from one partition of the data and check rest of data to analyze its performance.

Several ML Models like RF, LR, XGBOOSt and the DL Models like CNN MLP RCN etc. are applied on the dataset. These models calculated various performance metrics, like accuracy, precision, F1 score, recall, false positives, false negatives and Area Under the Curve (AUC). These are the most important metrics for evaluating the efficiency of the model in classifying phishing and legitimate URLs.

IV. METHODOLOGY

To perform experimental work with ML and DL algorithms for the detection of phishing URLs different steps are performed. Firstly, dataset is loaded and then cleaned by removing null values from it. Feature extraction is held after that and then split the dataset for testing and training. Making it sure that the 80% of the data is used to train the model. TF-IDF is used the convert the text-based data into numerical data. After preprocessing and proper training of dataset different types of Machines Learning and Deep Learning models are used that ensured to learn patterns from phishing URLs.

After proper training of data set it is the time to test the dataset on different Machine Learning and deep learning models. To evaluate the model's efficiency dataset different performance metrics, like accuracy, precision, F1 score, recall, false positives, false negatives and Area Under the Curve (AUC) are tested. The performance evaluation's results are printed to compare their performance in detecting phishing URLs.

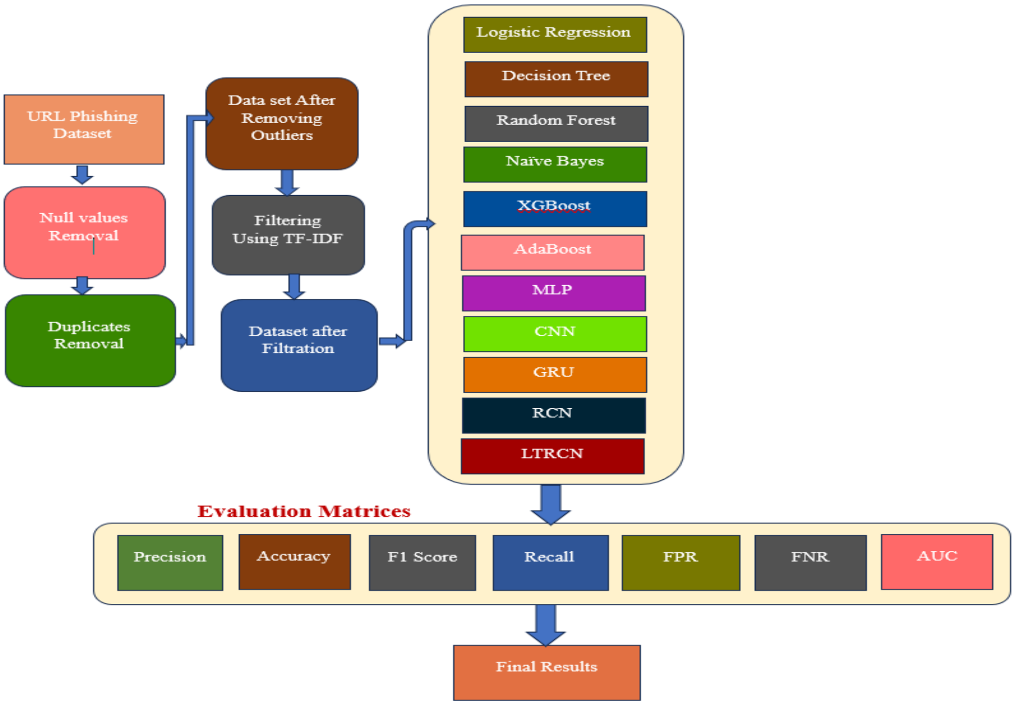

FIGURE 1. Classification of Phishing URL's Using ML and DL Models.

This flowchart outlines a phishing URL detection process that starts with a dataset undergoing cleaning steps like removing null values, duplicates, and outliers. The dataset is then filtered using TF-IDF to transform textual data into numerical form. Various machine learning models are applied, including Logistic Regression, Decision Tree, Random Forest, Naive Bayes, XGBoost, AdaBoost, MLP, CNN, GRU, RCN, and LTRCN. The performance of these models is evaluated using metrics such as precision, accuracy, F1 score, recall, false positive rate (FPR), false negative rate (FNR), and AUC. The final results indicate the most effective model for phishing detection based on these evaluation matrices.

The above architecture of the model highlights that the experimental work starts with the preprocessing i.e. cleaning of the data set by removing null values as well as duplicates to avoid misclassification. Secondly data is filtered by using TD-IDF approach that convert textual data into numeric. Then, Several ML Models like Random Forest, Logistic Regression XGBOOSt and DL Models like CNN MLP RCN etc. are applied on the dataset. For performance evaluation matrices like accuracy, precision, F1 score, recall, false positives, false negatives and Area Under the Curve (AUC) are analyzed. The experimental results show the which is the most effective Machine Learning Model or Deep Learning Model. On the basis of results one can classify to use appropriate algorithm that is suitable for specifically URL phishing attacks.

V. EXPERIMENTS AND RESULTS

In this study, ML algorithms like Random Forest, Logistic Regression, XGBoost, Naïve Bayes, Decision Tree, and Ada Boost and DL algorithms MLP, Gated Recurrent Units (GRU), CNN, RCN and LTRCN are evaluated to analyze the efficiency in detecting phishing URLs. The algorithms are analyzed on multiple performance metrics i.e. Precision, Accuracy, F1 Score, Recall, False Positive Rate (FPR), False Negative Rate (FNR) and Area Under the Curve (AUC).

TABLE 2. Results of Classification of Phishing URL's Using ML and DL Models

Algorithms /Classifier	Precision	Accuracy	F1 Score	Recall	(FPR)	(FNR)	(AUC)
Logistic Regression	97.77	93.69	93.07	88.81	1.85	11.19	98.08
Decision Trees	96.43	94.95	94.61	92.85	3.14	7.15	94.86
Random Forest	98.63	96.24	95.96	93.42	1.18	6.58	98.65
Naive Bayes	96.91	93.99	93.48	90.29	2.63	9.71	97.07
XGBoost	95.93	94.71	94.37	92.87	3.61	7.13	98.6
AdaBoost	82.32	84.28	83.85	85.44	16.78	14.56	92.02
Multilayer Perceptron (MLP)	97.94	94.38	93.87	90.12	1.73	9.88	98.37
Convolutional Neural Networks (CNN)	48.23	48.23	65.07	100	100	0	50
Gated Recurrent Unit (GRU)	98.23	94.62	94.13	90.36	1.49	9.64	98.56
Recurrent Convolutional Network (RCN)	84.23	70.82	61.07	47.9	8.21	52.1	79.96
Long-Term Recurrent Convolutional Networks (LTRCN)	100	51.27	0.27	0.14	0	99.86	50.01

The results confirmed that the Random Forest classifier attained the highest precision (98.63%) and accuracy (96.24%), making it a strong applicant for phishing detection. Logistic Regression and the Gated Recurrent Unit (GRU) also performed well, with precision scores of 97.77% and 98.23%, respectively. Particularly, the LTRCN model achieved perfect precision (100%), but it exhibited a lower accuracy of 51.27% and a regarding FNR of 99.86%, representing it struggled with false negatives. In distinction, CNNs performed poorly, with an accuracy of only 48.23%. General, the results specify that traditional algorithms like Random Forest and advanced models like GRU are more active for this task, while models like CNN and LTRCN require additional optimization for consistent performance in phishing URL detection.

The results confirmed that the Random Forest classifier attained the highest precision (98.63%) and accuracy (96.24%), making it a strong applicant for phishing detection. Logistic Regression and the Gated Recurrent Unit (GRU) also performed well, with precision scores of 97.77% and 98.23%, respectively. Particularly, the LTRCN model achieved perfect precision (100%), but it exhibited a lower accuracy of 51.27% and a regarding FNR of 99.86%, representing it struggled with false negatives. In distinction, CNNs performed poorly, with an accuracy

of only 48.23%. General, the results specify that traditional algorithms like Random Forest and advanced models like GRU are more active for this task, while models like CNN and LTRCN require additional optimization for consistent performance in phishing URL detection.

The results confirmed that the Random Forest classifier attained the highest precision (98.63%) and accuracy (96.24%), making it a strong applicant for phishing detection. Logistic Regression and the Gated Recurrent Unit (GRU) also performed well, with precision scores of 97.77% and 98.23%, respectively. Particularly, the LTRCN model achieved perfect precision (100%), but it exhibited a lower accuracy of 51.27% and a regarding FNR of 99.86%, representing it struggled with false negatives. In distinction, CNNs performed poorly, with an accuracy of only 48.23%. General, the results specify that traditional algorithms like Random Forest and advanced models like GRU are more active for this task, while models like CNN and LTRCN require additional optimization for consistent performance in phishing URL detection.

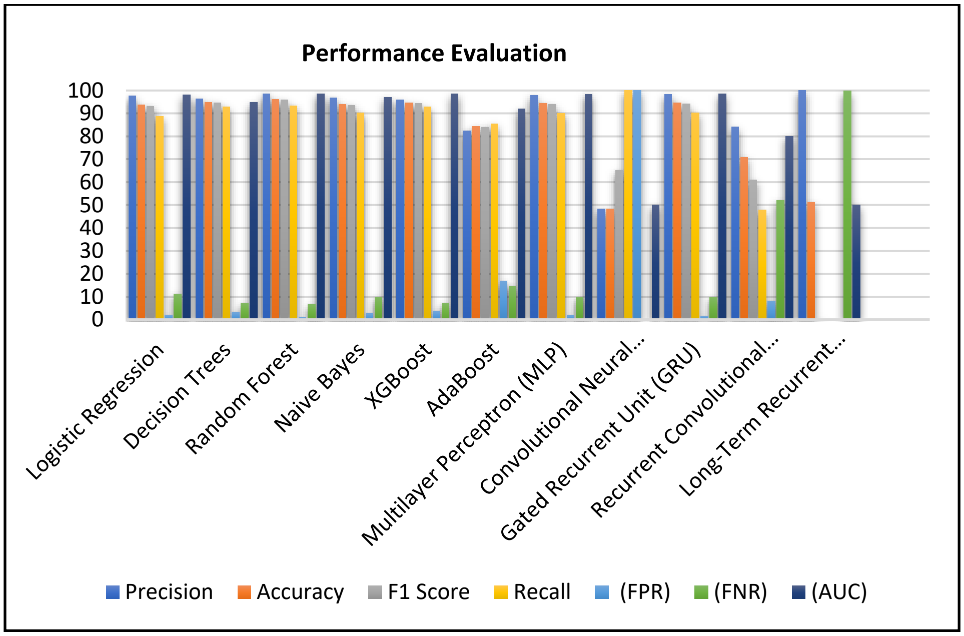

FIGURE 2. Experimental Results of Classification of Phishing URL's Using ML and DL Models

Experimental results confirmed that among the Machine Learning algorithm Random Forest classifier attained the highest precision (98.63%) and accuracy (96.24%). Other ML algorithms like Logistic Regression and the Gated Recurrent Unit (GRU) acquire the precision scores of 97.77% and 98.23%. In case of Deep learning algorithms LTRCN model achieved perfect precision of 100%, but its accuracy degrades as 51.27%, Moreover, its False Negative Rate is 99.86% that shows its poor performance.

When summarize the results it is cleared that Machine Learning Algorithm Random Forest achieve high precision and accuracy and from deep Learning GRU performance is best.

VI. CONCLUSION

This experimental based study evaluated different ML and DL algorithms for the detection of malicious URLs. Among all models Random Forest achieved highest precision 98.63% and accuracy 96.24%. Make them a good choice for phishing URLs. While the LTRCN model achieved perfect precision (100%), but it exhibited a lower accuracy of 51.27% and a regarding FNR of 99.86%, representing it struggled with false negatives indicate it is not a best choice.

Logistic Regression and Gated Recurrent Units (GRU) also show good performance and it can be increased by applying some other engineering techniques. While Convolutional Neural Networks (CNNs) not performed well in case of phishing URLs, its accuracy is only 48.23%.

To conclude the results, it is stated that Machine Learning model like Random Forest and the Deep Learning model like GRU showed better results in detecting the phishing URLs rather than CNNs and LTRCN that need further optimization. So, there is need of the time to do more work on ML and DL algorithms to increase the performance of phishing URLs detection in the domain of cybersecurity.

ACKNOWLEDGMENTS

My Sincere thanks to Prof. Dr. Muhammad Mansoor Alam for their supervision and constant guidance throughout my research. Their expertise and their support played a vital role in completion of the work. There are no funding agencies supporting the research work

AUTHOR CONTRIBUTIONS

Shougfta Mushtaq: Literature Review, Idea, Experimental work, Presentation and Formatting;

Mazliham Mohd Su'ud: Project Administration, Supervision, Topic and Experiments approval.

CONFLICT OF INTERESTS

No conflict of interests has been disclosed.

ETHICS STATEMENTS

The dataset used in the experiments were available at publicly available platform Kaggle, and all experiments are performed by using Kaggle cloud environment.

REFERENCES

[1] M.A. Tamal, M.K. Islam, T. Bhuiyan, A. Sattar and N.U. Prince, "Unveiling suspicious phishing attacks: enhancing detection with an optimal feature vectorization algorithm and supervised machine learning," *Frontiers in Computer Science*, vol. 6, 2024. DOI: https://doi.org/10.3389/fcomp.2024.1428013

[2] C. Opara, Y. Chen and B. Wei, "Look before you leap: Detecting phishing web pages by exploiting raw URL and HTML characteristics," *Expert Systems with Applications*, vol. 236, 2024. DOI: https://doi.org/10.1016/j.eswa.2023.121183

[3] J.A. Daniel, C.V. Chinnappan and J. Giri, "Heuristic machine learning approaches for identifying phishing threats across web and email platforms," *Frontiers in Artificial Intelligence*, 2024. DOI: https://doi.org/10.3389/frai.2024.1414122

[4] K.H. Chy, "Securing the web: Machine learning's role in predicting and preventing phishing attacks," *International Journal of Security and Risk Assessment*, 2024. DOI: https://doi.org/10.30574/ijsra.2024.13.1.1770

[5] T. Ige, C. Kiekintveld and A. Piplai, "Deep Learning-Based Speech and Vision Synthesis to Improve Phishing Attack Detection through a Multi-layer Adaptive Framework," *arXiv*, 2024. DOI: https://doi.org/10.20944/preprints202402.1557.v1

[6] A. Arun, "Next Generation of Phishing Attacks using AI powered Browsers," *arXiv*, 2024. DOI: https://doi.org/10.48550/arXiv.2406.12547

[7] 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, 2022. DOI: https://doi.org/10.1109/ACCESS.2022.3168681

[8] A. Villanueva, C. Atibagos, J.D. Guzman, J.C.D. Cruz, M. Rosales and R. Francisco, "Application of Natural Language Processing for Phishing Detection Using Machine and Deep Learning Models," *ICISS 2022 - Proceedings*, pp. 1–6, 2022. DOI: https://doi.org/10.1109/ICISS55894.2022.9915037

[9] C. Catal, G. Giray, B. Tekinerdogan, S. Kumar and S. Shukla, "Applications of deep learning for phishing detection: a systematic literature review," *Artificial Intelligence Review*, vol. 64, no. 6, 2022. DOI: https://doi.org/10.1007/s10115-022-01672-x

[10] I. Kara, M. Ok and A. Ozaday, "Characteristics of understanding URLs and domain names features: The detection of phishing websites with machine learning methods," *IEEE Access*, vol. 10, 2022. DOI: https://doi.org/10.1109/ACCESS.2022.3223111

[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, 2022. DOI: https://doi.org/10.1109/ACCESS.2022.3151903

[12] D. Rathee and S. Mann, "Detection of e-mail phishing attacks – using machine learning and deep learning," *International Journal of Computer Applications*, vol. 183, no. 47, 2022. DOI: https://doi.org/10.5120/ijca2022921868

[13] M. Elsadig et al., "Intelligent deep machine learning cyber phishing URL detection based on BERT features extraction," *Electronics*, vol. 11, no. 22, 2022. DOI: https://doi.org/10.3390/electronics11223647

[14] E.S. Vishva and D. Aju, "Phisher Fighter: Website phishing detection system based on URL and term frequency-inverse document frequency values," *Journal of Cyber Security and Mobilities*, vol. 11, no. 1, pp. 83–104, 2022. DOI: https://doi.org/10.13052/jcsm2245-1439.1114

[15] S.H. Ahammad et al., "Phishing URL detection using machine learning methods," *Advances in Engineering Software*, vol. 173, 2022. DOI: https://doi.org/10.1016/j.advengsoft.2022.103288

[16] M. Almousa, T. Zhang, A. Sarrafzadeh and M. Anwar, "Phishing website detection: How effective are deep learning-based models and hyperparameter optimization?" *Security and Privacy*, vol. 5, no. 6, 2022. DOI: https://doi.org/10.1002/spy2.256

[17] A. Dawabsheh, M. Jazzar, A. Eleyan, T. Bejaoui and S. Popoola, "Phishing Detection using Machine Learning Techniques," *2022 International Conference on Smart Applications, Communications and Networking (SmartNets)*, 2022. DOI: https://doi.org/10.1109/SmartNets55823.2022.9993984

[18] 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. DOI: https://doi.org/10.1108/JEIM-01-2020-0036

[19] S.R. Abdul Samad, A. Abdullah, M.F. Abdollah, A.A. Mutalib and S.A.M. Noah, "Analysis of the performance impact of fine-tuned machine learning model for phishing URL detection," *Electronics*, vol. 12, no. 7, 2023. DOI: https://doi.org/10.3390/electronics12071642

[20] 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. 36805–36822, 2023. DOI: https://doi.org/10.1109/ACCESS.2023.3252366

[21] U. Nishitha, R. Kandimalla, R.M. Mourya Vardhan and U. Kumaran, "Phishing detection using machine learning techniques," *2023 3rd Asian Conference on Innovation in Technology (ASIANCON)*, pp. 1–6, 2023. DOI: https://doi.org/10.1109/ASIANCON58793.2023.10270550

[22] Y. Wang, W. Zhu, H. Xu, Z. Qin, K. Ren and W. Ma, "A large-scale pretrained deep model for phishing URL detection," *ICASSP 2023*, pp. 1–5, 2023. DOI: https://doi.org/10.1109/ICASSP49357.2023.10095719

[23] M. Shoaib and M. S. Umar, "URL based phishing detection using machine learning," *6th International Conference on Information Systems and Computer Networks (ISCON)*, pp. 1–7, 2023.
DOI: https://doi.org/10.1109/ISCON57294.2023.10112184

[24] W. Wang, "Using Machine Learning," *Pro iPhone Development with SwiftUI*, pp. 313–336, 2023. DOI: https://doi.org/10.1007/978-1-4842-9544-1_17

[25] A. Ozcan, C. Catal, E. Donmez, and B. Senturk, "A hybrid DNN–LSTM model for detecting phishing URLs," *Neural Computing and Applications*, vol. 35, no. 7, pp. 4957–4973, 2023.
DOI: https://doi.org/10.1007/s00521-021-06401-z

[26] P. Pavan Kumar, T. Jaya, and V. Rajendran, "SI-BBA – A novel phishing website detection based on Swarm intelligence with deep learning," *Materials Today: Proceedings*, vol. 80, pp. 3129–3139, 2023.
DOI: https://doi.org/10.1016/j.matpr.2021.07.178

[27] F. S. Alsubaei, A. A. Almazroi, and N. Ayub, "Enhancing Phishing Detection: A Novel Hybrid Deep Learning Framework for Cybercrime Forensics," *IEEE Access*, vol. 12, pp. 8373–8389, 2024.
DOI: https://doi.org/10.1109/ACCESS.2024.3351946

[28] O.K. Sahingoz, E. Buber and E. Kugu, "DEPHIDES: Deep Learning Based Phishing Detection System," *IEEE Access*, vol. 12, pp. 8052–8070, 2024.
DOI: https://doi.org/10.1109/ACCESS.2024.3352629

[29] D.M. Linh, H.D. Hung, H.M. Chau, Q.S. Vu and T.N. Tran, "Real-time phishing detection using deep learning methods by extensions," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 3, pp. 3021–3035, 2024.
DOI: https://doi.org/10.11591/ijece.v14i3.pp3021-3035

[30] B.C. Ujah-Ogbuagu, O.N. Akande and E. Ogbuju, "A hybrid deep learning technique for spoofing website URL detection in real-time applications," *Journal of Electrical Systems and Information Technology*, vol. 11, no. 1, 2024.
DOI: https://doi.org/10.1186/s43067-023-00128-8

[31] 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, 2024.
DOI: https://doi.org/10.3390/sym16020248

[32] S.D. Gupta, K.T. Shahriar, H. Alqahtani, D. Alsalman and I. H. Sarker, "Modeling Hybrid Feature-Based Phishing Websites Detection Using Machine Learning Techniques," *Annals of Data Science*, vol. 11, no. 1, pp. 217–242, 2024.
DOI: https://doi.org/10.1007/s40745-022-00379-8

[33] F. Trad and A. Chehab, "Prompt Engineering or Fine-Tuning? A Case Study on Phishing Detection with Large Language Models," *Machine Learning and Knowledge Extraction*, vol. 6, no. 1, pp. 367–384, 2024.
DOI: https://doi.org/10.3390/make6010018

[34] R. Alazaidah et al., "Website Phishing Detection Using Machine Learning Techniques," *Journal of Statistics and Applications in Probability*, vol. 13, no. 1, pp. 119–129, 2024.
DOI: https://doi.org/10.18576/jsap/130108

[35] T. L. Halili, A. Halili, K. Vishi, and B. Rexha, "NoPhish: Efficient Chrome Extension for Phishing Detection Using Machine Learning Techniques," *ArXiv: Cryptography and Security*, 2024.
DOI: https://doi.org/10.48550/arXiv.2409.10547

[36] S. Remya, M.J. Pillai, K.K. Nair, S. Rama Subbareddy and Y.Y. Cho, "An Effective Detection Approach for Phishing URL Using ResMLP," *IEEE Access*, vol. 12, no. June, pp. 79367–79382, 2024.
DOI: https://doi.org/10.1109/ACCESS.2024.3409049