NABEA AL-AJYAL FOUNDATION PRESS
Online ISSN: 3078-5413
CyberSystem Journal (CSJ)
csj.nabea.pub
CyberSystem Journal Research Article

A Robust Intelligent Approach for Phishing URL Detection Using Hybrid Machine Learning

Hind Abdulkareem Abdalrazaq [1]

[1] Automobiles Engineering Department, College of Engineering AL Musayab , University of Babylon, Babylon, Iraq , 51001 Hillah, Babylon, Iraq

* Corresponding Author: **Hind Abdulkareem Abdalrazaq**, Email: eng925.hind.abdulkarim@uobabylon.edu.iq

Abstract: Phishing attacks are still the main and most severe vulnerability to cyber security through deceptive URLs for sensitive user information. Therefore, this paper proposes a framework based on deep learning techniques for phishing and legitimate URLs as an alternative to the currently employed blacklist-based detection approaches that have proven rather limited. The architecture includes one custom Convolutional Neural Network (CNN) and three Transfer Learning Architectures, ResNet50, InceptionV3, and VGG16 using representations of features based on URLs. All models under consideration shall be trained with Adam Optimizer and Binary Cross-Entropy loss function so that a fair comparison can be made under unified experimental set-up conditions. The set is broken down as 70% training, 10% validation, and 20% testing. Experimental results provide clear evidence that transfer learning models perform much better than the baseline CNN. The InceptionV3 model posted a validation accuracy of 100% leading the pack, followed by VGG16 at 98.96%. ResNet50 could muster only 97.92%. The proposed CNN model has also achieved quite competitive performance with a validation accuracy above 97%. Therefore, these results are explicit in confirming the effectiveness, robustness, and generalization capability of deep learning architectures toward the problem of phishing URL detection. This proposed framework will go a long way in ensuring web security is beefed up as it creates a barrier against all evolving cyber threats.

Access this article online

Keywords: Phishing URL detection, Deep learning, Cybersecurity, Convolutional neural networks, Transfer learning

1. Introduction

The Internet is the large-scale worldwide infrastructure that today supports communication, commerce, education, and government services all over the world. At a technical level, it can be generally described as "networks of networks" interconnecting hosts and servers over diverse telecommunications media—fiber backbones, wireless access, or satellite links—with standardized protocol suites (mainly TCP/IP) providing addressing and routing semantics plus reliable data transport for distributed systems. By decentralized governance principles, the Internet does not fall under any government or single authority; rather evolution and operation are determined by a complex ecosystem of standards bodies, service providers, research institutions, and universities. Therefore Internet-based service applications have rapidly proliferated to include support for information retrieval, electronic commerce and

Received September 20, 2025; Revised June 9, 2025; Accepted November 19, 2025; Published December 31, 2025
https://doi.org/10.57238/csj.2025.1017

online banking, e-health applications via telemedicine including social networking software supporting remote teamwork introduced as a critical tool during pandemics such as COVID-19 [1-5]

The more digital interactions take place, the more opportunities for attacks against individuals and organizations. Since email is one of the most popular communications for messages, documents, and links exchange - that makes it a sweet spot of attack because it's so well integrated into the workflows at institutions. Malware, ransomware, identity theft, denial-of-service attacks, and large-scale financial fraud are all able to be facilitated over the Internet via cybercriminal activity; phishing stands out among them due to how much more common it is since human vulnerabilities are so often exploited compared to technical ones [6]. A phishing attack involves an adversary pretending to be a reputable entity in order to trick one of its victims into revealing sensitive information - like credentials or personal identifiers or payment data - or performing some malicious action. The risks increase further when spear-phishing is applied because then even more specific messages can be crafted against a single employee or department based on knowledge about who is within which organization (or project work being conducted), and on formal communication styles [7-9].

At the heart of phishing and spear-phishing attacks are URLs, which direct users to web resources-whether legitimate or malicious. Like most syntactic components, scheme (HTTP/HTTPS), host/domain, path, and query parameters can be manipulated to look like trusted brands or official portals. Figure 1 gives a sample URL based on HTTP and marks its major structural components with references to emphasize how small lexical as well as structural variations may be exploited by attackers for fooling users [10].

While HTTPS does mean communication is encrypted using TLS/SSL and it is necessary for protection of data in transit, having a HTTPS site does not guarantee the site's legitimacy because adversaries can also obtain certificates for their fraudulent domains and then convincingly host imitation pages [11]. In recent years, the emergence of generative AI has fortified social engineering by allowing attackers to generate large volumes of well-written email content. This content is not only grammatically correct but also contextually relevant, significantly diminishing the effectiveness of traditional rule-based filters and keyword matching [12].

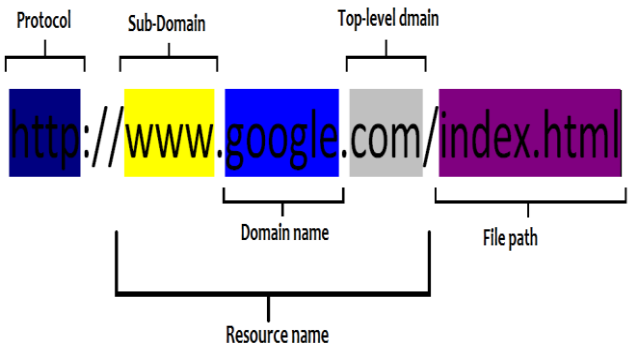

Figure 1. Representation of URLs using HTTP protocol attributes.

Thus, recent studies have increasingly centered their attention on the dimensions of machine learning and deep learning algorithms for robust email threat detection. It is spear-phishing detection that usually combines several categories of features and not only just textual cues from the body and subject of an email-appending information on intent, urgency, semantic patterns but also URL-based features lexical structure, obfuscation pattern, domain characteristics-and sender-based attributes including domain reputation, header anomalies, reply-to mismatches among others [13].

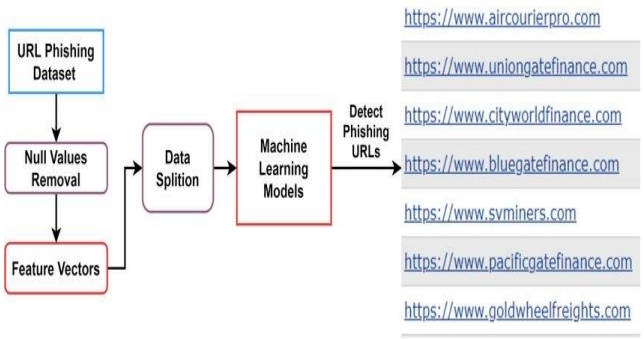

Figure 2. Phishing URL Detection and Architecture of the Proposed Approach.

Figure 2 represents a general workflow adopted in this study-the phishing dataset is preprocessed and then transformed into feature vectors split for training/testing to train machine learning models to detect malicious URLs as well as related phishing content within emails themselves. Utilizing such heterogeneous signals, AI-assisted classifiers can raise the bar much higher in accuracy with far more reduced false positives in terms of alerting capacity to give a better warning-this will bring about improved email security and shall reduce operational as well as financial impacts by intrusions based on phishing [14].

2. Related works

Phishing is among the major challenges that are currently being faced in network security and systems operating over the Internet. Several studies have therefore proposed different techniques in the protection of users against cyber threats as part of an overall system architecture—these include machine learning models, deep learning models, and blacklist as well as whitelist URL filtering approaches. Existing solutions to phishing detection can be broadly classified into two key categories: those that fall under list-based methods and those comprising machine learning-based identification systems. Consequently, this section comprises two parts in which existing works pertaining to these dimensions are reviewed.

1. This research proposes an intelligent machine learning-based phishing URL detection system using a benchmark dataset of more than 11,000 phishing and legitimate URLs. Several machine learning algorithms were implemented after data preprocessing to compare their performances. The hybrid model which is proposed here consists of Logistic Regression, Support Vector Machine, and Decision Tree classifiers with soft as well as hard voting for better accuracy in detecting phishing URLs. Canopy-based feature selection, k-fold cross-validation, and Grid Search optimization have been adopted for getting improved results. This approach proved better than the existing models by attaining 98.12% accuracy, 96.33% recall value, and a 95.89% F1-Score to establish its efficacy as well as its robustness in the detection of phishing URLs [15].
2. This study proposes a real-time machine learning setup, running at the client side, for detecting phishing URLs that can dynamically keep pace with changes in the nature of attacks. Differentiating features from URL and webpage source code are leveraged to differentiate phishing from legitimate sites without involving any third-party support. As per empirical analysis results, the proposed approach has attained 98.19% TPR with an FPR of only 1.59%, recording precision as well as accuracy figures of 98.39% along with a valuation on an F1-score metric standing at 98.29% [16].
3. Results of the experiment strongly prove that the proposed hybrid detection method is effective in identifying phishing URLs. A comparative study on several machine learning and deep learning models proves that deep learning techniques perform better. The convolutional neural network (CNN) model recorded the highest accuracy at 97.945%, followed by multilayer perceptron (MLP) at 93.216%. This will hence forth prove that the methodology being proposed is robust enough to present a solution towards distinguishing a legitimate website from a phishing one; thus, it can be considered practicable [17].
4. This paper proposes a machine learning approach to train classifiers on hybrid features, both URL-based and hyperlink-based. The features can be extracted in real-time from the webpage, such that the detection system will work completely at the client side without depending on any third-party service for detecting zero-day or newly launched phishing websites. A specific dataset was constructed for experimental evaluation where several machine-learning classifiers were trained and tested; meanwhile, this proposed hybrid feature-based approach proved highly effective since it achieved 99.17 % detection accuracy using an XGBoost classifier [18].
5. This study proposes a layered machine learning model that first checks the URL structure and then combines textual and image features for detecting phishing websites. A dataset was prepared with 20,000 URL samples having 22 different feature values along with text data extracted from images for classification purposes. Several algorithms- XGBoost, random forest, SVM, and multilayer perceptron were applied out of which XGBoost gave the highest result accuracy of 94% during training and 91% while testing on test data thereby strongly catching phishing sites leading to an advanced warning plus internet user security [19].
6. This study analyzes the tactics of phishers in their gradual approach to close imitation of legitimate URLs to fool users. A total of 10,000 URLs composed equally by half from phishing and another half from legitimate web pages collected between 2015-and 2017 were used. Forty-eight features were extracted out of these URLs on which Information Gain (IG) and Chi-Squared feature selection techniques have

been applied for comparison purposes. Further analysis has been done on selected features to find out common techniques adopted by phishers in URL manipulation using machine learning techniques [20]. The results discuss how well anti-phishing tool developers can use such information together with user awareness strategists.

7. This proposed Machine Learning-based approach for Cyber Attack Detection in Smart Power Systems using (Phasor Measurement Unit) PMU Data. Features were extracted from the PMU measurement data based on anomaly assessment and Random Forest Classifier under AdaBoost Ensemble used for detection. It has been validated over several smart grid event case studies that it can achieve 93.6% accuracy with a 93.91% detection rate beating the state-of-the-art methods by a fair margin. This method clearly proves the possibility of accurate anomaly detection inside critical infrastructure systems when applying machine learning and deep learning methodologies [21].
8. This study proposes a deep learning-based model using long-term Phasor Measurement Unit (PMU) data for event and cyber-attack detection in energy systems. Key features are extracted with the help of Principal Component Analysis(PCA), which reduces redundancy as well as learning time, keeping the main information intact. The model applies deep learning as well as Decision Tree classifiers for anomaly detection and is evaluated based on different metrics where the confusion matrix has been taken into account. Results have proven that proposed methodology attains 97% accuracy, thus security and efficiency increment of intelligent energy grids [22].
9. This study proposes an efficient machine-learning framework for detecting phishing URLs without visiting the website or relying on third-party services. The model extracts 30 key features from the URL, including protocol scheme, hostname, path, entropy, suspicious words, and brand name matching using TF-IDF. The framework was evaluated on six datasets using eight classifiers, with Random Forest achieving the highest accuracy. Experimental results demonstrate that the proposed approach outperforms existing methods, achieving up to 96.85% accuracy across benchmark datasets, providing an effective solution for real-world phishing detection [23].
10. This study proposes a real-time anti-phishing system that detects phishing websites using natural language processing (NLP) features and seven machine learning classifiers. The system is designed to be language-independent, capable of detecting new websites, and operates without relying on third-party services. A large dataset of phishing and legitimate URLs was constructed for evaluation, and experimental results show that the Random Forest classifier achieved the highest accuracy of 97.98% using only NLP-based features. The approach demonstrates effective and efficient detection of phishing URLs in real-time [24].
11. Recent studies highlight the success of machine learning and deep learning models in detecting phishing URLs as well as cyber-attacks against critical systems. Several works presented hybrid and layered frameworks based on features extracted from URL, text, image, hyperlink, etc., in combination with ensemble or deep learning classifiers such as Random Forest, XGBoost, CNN, and MLP [15–19]. These frameworks achieved very high accuracy between 91% to 99.17% which means robustness regarding detection of zero-day attacks on language-independent phishing and dynamically evolving threats [16,18,24]. Furthermore, studies about phisher strategies applying feature selection methods like Information Gain and Chi-Squared bring more information that can be harnessed when building powerful anti-phishing tools [20]. Outside of cybersecurity, machine learning models have also been equivalent to accuracy up to 97% for anomaly applications in smart power systems utilizing PMU data and are truly available in real time [21,22]. Collectively, this literature reveals a strong indication of the potential leverage of machine and deep learning methodologies toward an improved state of security, efficiency, and user protection on web-based systems as well as critical infrastructure. Table 1 shows the summary of related works.

Recent studies highlight the success of machine learning and deep learning models in detecting phishing URLs as well as cyber-attacks against critical systems. Several works presented hybrid and layered frameworks based on features

extracted from URL, text, image, hyperlink, etc., in combination with ensemble or deep learning classifiers such as Random Forest, XGBoost, CNN, and MLP [15–19]. These frameworks achieved very high accuracy between 91% to 99.17% which means robustness regarding detection of zero-day attacks on language-independent phishing and dynamically evolving threats [16,18,24].

Furthermore, studies about phisher strategies applying feature selection methods like Information Gain and Chi-Squared bring more information that can be harnessed when building powerful anti-phishing tools [20]. Outside of cybersecurity, machine learning models have also been equivalent to accuracy up to 97% for anomaly applications in smart power systems utilizing PMU data and are truly available in real time [21,22].

Collectively, this literature reveals a strong indication of the potential leverage of machine and deep learning methodologies toward an improved state of security, efficiency, and user protection on web-based systems as well as critical infrastructure. Table 1 shows the summary of related works.

Table 1. Summary of related works

Ref	Methods	Results	Limitations
[15]	Hybrid ML model combining Logistic Regression, SVM, and Decision Tree with soft and hard voting; Canopy-based feature selection, k-fold CV, Grid Search optimization	Accuracy 98.12%, Recall 96.33%, F1-Score 95.89%	Requires preprocessed benchmark dataset; may not generalize to unseen dynamic phishing URLs
[16]	Real-time client-side ML setup using URL and webpage source code features	TPR 98.19%, FPR 1.59%, Accuracy 98.39%, F1-Score 98.29%	Focused only on client-side detection; may not consider server-side or advanced evasion techniques
[17]	Hybrid ML and deep learning; CNN and MLP for URL classification	CNN Accuracy 97.945%, MLP 93.216%	Deep learning models require high computational resources; smaller datasets may limit generalizability
[18]	ML-based hybrid features from URLs and hyperlinks; client-side execution; multiple classifiers	XGBoost Accuracy 99.17%	Dataset construction limited; may not cover all types of zero-day attacks
[19]	Layered ML approach analyzing URL, text, and image features; algorithms: XGBoost, Random Forest, SVM, MLP	XGBoost Training 94%, Testing 91%	Image text extraction may fail for complex or obfuscated images; feature engineering required
[20]	ML analysis of phisher tactics; 48 features; feature selection: Information Gain, Chi-Squared	Identified 10 common URL manipulation techniques	Dataset from 2015–2017; older URLs may not represent current phishing strategies
[21]	ML-based anomaly detection in smart power systems; PMU data; Random Forest under AdaBoost	Accuracy 93.6%, Detection rate 93.91%	Focused on power systems; results may not generalize to other cyber-physical systems
[22]	Deep learning model on long-term PMU data; PCA for feature reduction; Deep learning & Decision Tree classifiers	Accuracy 97%	High dependency on quality and quantity of PMU data; computational cost high
[23]	ML framework for phishing URL detection; 30 key URL features; 8 classifiers	Accuracy up to 96.85%	Limited to URL features; may not detect phishing based on images or dynamic content
[24]	Real-time anti-phishing system; NLP features; 7 ML classifiers; language-independent	Random Forest Accuracy 97.98%	Depending on textual content; may fail on image-based phishing without text

3. PROPOSED APPROACH

This section presents a comprehensive description of the methodologies adopted in this study, offering a detailed explanation of the proposed framework for phishing URL detection. The performance of the proposed model is rigorously evaluated using standard evaluation metrics, including Accuracy, Precision, Recall, and F1-score, to assess its effectiveness and reliability in distinguishing phishing URLs from legitimate ones.

4. Dataset

The UCI PHIUSIIL Phishing URL Dataset [25] contains a wide and comprehensive diversity of features that makes it most appropriate to train resilient machine learning, as well as deep learning models for detecting phishing. One

major cyberattack vector is through malicious URLs; hence the dataset includes labeled collection URLs both malicious and legitimate websites with many different attributes such as structure or domain characteristics special characters present among others which could indicate phishing activity thus allowing detection not only known patterns but also emerging threats when heuristic based features are combined statistical attributes allow thorough analysis hence enhancing adaptability efficiency detection model current up-to-date phish data ensures model stay relevant evolving attack strategies therefore important tool discover battle against phish. The dataset contains 235,795 instances and 56 features. Several columns Filename, URL, Domain, Title, URLLength, DomainTitleMatchScore and URLSimilarityIndex were removed to eliminate redundancy. The remaining features were used to train the algorithm improving its detection capability and accuracy [26-27].

5. Evaluation matrix

A machine learning model can be evaluated in different ways, and multiple metrics of evaluation would add to the rigor of analytical research by giving a detailed comparison between machine learning algorithms [28,29]. The four basic measures used in this study are accuracy (AC, Eq. 1), precision (PR, Eq. 2), recall (RE, Eq. 3), and F1-score (FS, Eq. 4). All four metrics are calculated from a confusion matrix [30-31] ,which also shows how well classification has been performed by the model. The correctly identified false negatives have been emphasized because such errors bear important implications when predictions are made in the medical domain

$$\mathbf{Acuraccy} = \frac{\mathbf{TP+PN}}{\mathbf{TP+PN+FN+FP}} \quad (1)$$

$$\boldsymbol{Recall} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FN}} \quad (2)$$

$$\boldsymbol{Precision} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FP}} \quad (3)$$

$$\mathbf{F1-score} = \frac{\mathbf{2*Precision*Recall}}{\mathbf{Precision+Recall}} \quad (4)$$

6. Proposed system

The approach introduces an intelligent hybrid framework for phishing URL detection through the optimal combination of feature selection and deep learning/transfer learning paradigms. It makes high accuracy, robustness, and generalization promises not only on known attacks but also previously unseen attacks, zero-day attacks. Initially, the PhiUSIIL Phishing URL dataset is used. It contains a large scale collection of both legitimate and phishing URLs. Some discriminative features are extracted from the structures of the URLs and characteristics of web pages. Structure based features include length of URL , domain based attributes , lexical properties as well as similarity based hyperlink indicators . These features have shown relevance in capturing those behavioral patterns which mostly are and always become part of the execution plan for phishing attacks.

The data is cleaned, normalized using Standard Scaler, and split into train and test subsets as a minor step inside an extensive data preprocessing phase.Hybrid feature selection is initiated at the strength of Random Forest (RF) [32] together with Extra Trees Classifier (ETC) [33] to fight redundancy and noise of features. In parallel, these models calculate feature importance scores based on impurity reduction while learning. Rankings formed within both models are aggregated to find out which features are most influential and stable.

This hybrid selection mechanism ensures reduced dimensionality to a large extent, overfitting is taken care of, preserves very important discrimination information, and makes computation faster. Convolutional Neural Networks [34] (CNNs) use transfer learning [35,36] models such as ResNet50 [37], InceptionV3 [38], and VGG16 [39] to enhance high-level features of their representation. The proposed CNN architecture would entail a number of Conv2D [40] layers with ReLU [41] activation functions followed by MaxPooling2D layers that would be able to pick up spatial hierarchies and salient patterns inside the feature representations.

The resulting feature maps are then flattened and passed through fully connected Dense layers. Sigmoid activation will be used in the last layer for binary classification between legitimate and phishing URLs. In the end, a strict check of the proposed framework is done using standard evaluation metrics that come from the confusion matrix: Accuracy, Precision, Recall, and F1-score. Test results show that the proposed crossbreed setup attains trusty and effectual phishing spotting performance; showing strength ability in finding both known and zero-day phishing URLs without leaning on third-party blacklists. Figure 3 and algorithm 1 show the block diagram for proposed system [42].

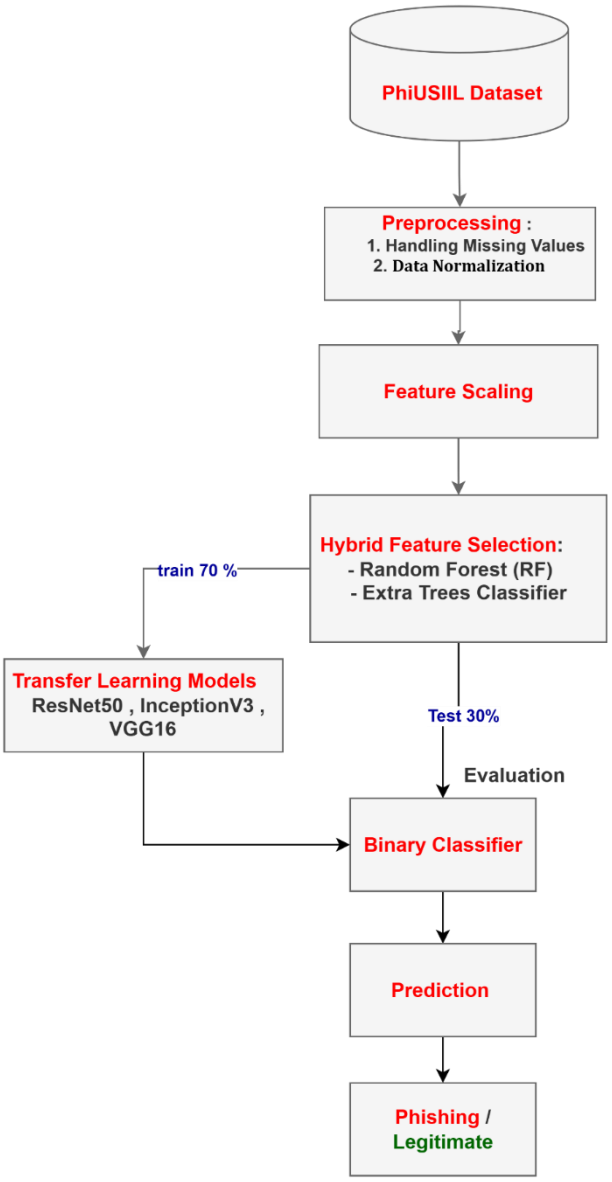

Figure 3. the Proposed Approach.

Algorithm: Proposed Phishing Detection Methodology

Input:
Phishing URL dataset (PhiUSIIL) containing legitimate and phishing URLs

Output:
Binary classification result (Legitimate / Phishing)

Begin

Load Dataset: Load the PhiUSIIL phishing URL dataset.

Data Preprocessing

Remove duplicate and inconsistent records.

Handle missing values if present.

Encode class labels (Legitimate = 0, Phishing = 1).

Feature Selection (Hybrid Approach)

Apply Random Forest (RF) to compute feature importance scores.

Apply Extra Trees Classifier (ETC) to compute alternative importance scores.

Aggregate importance scores from RF and ETC.

Select the most influential features based on average ranking.

Dimensionality Reduction: Construct an optimized feature subset using the selected features.

Train–Test Split: Split the dataset into training and testing sets using a sampling strategy.

Model Training (Transfer Learning / Deep Learning)

Train deep learning models using transfer learning approaches
(ResNet50, InceptionV3, VGG16).

Fine-tune convolutional layers for phishing detection.

Classification: Apply a sigmoid activation function for binary classification.

Model Evaluation
Evaluate the trained model using:

Accuracy

Precision

Recall

F1-score

Output Prediction: Predict whether a URL is legitimate or phishing.

7. Results and discussion

Transfer deep learning efforts at classifying phishing URLs include custom-designed neural architectures and well-known pre-trained deep learning models such as ResNet50, InceptionV3, and VGG16 retargeted toward feature representations based on URLs.

The proposed CNN model comprises several convolutional layers defined by ReLU activations followed by MaxPooling applied for pooling of extracted features to make the extraction more discriminative in regard to the characteristics of URLs. These features are then flattened into a one-dimensional vector-using Flatten layer-and sent through fully connected (Dense) layers, with Sigmoid activation function at output layer which produces a binary output representing whether a URL is phishing or legitimate.

The ResNet50 model uses weights that have been pre-trained on large scale benchmark datasets and is fine-tuned by adding extra Flatten and Dense layers to the base architecture so as to learn better any patterns within URL features relating to phishing. Similarly, InceptionV3 adds the base network without its final classification head followed by more Dense and Dropout layers which help in overfitting as well as generalization performance. The VGG16 model takes advantage of its deep yet stable architecture by freezing the base layers and then creating new trainable ones which are designed in particular for finding complicated signs of phishing embedded inside URL structures.

Training is performed with the Adam optimizer and Binary Cross-Entropy loss. Generalization capability Improved generalization capability diminished overfitting by applying proper data-level regularization techniques on the URL feature set via normalization and feature rebalancing strategies. A fair comparison among all tested models is guaranteed by training them using an identical split from the data—70% for training, 10% for validation, and 20% for testing—with a batch size of 32 over 20 epochs of learning. Early Stopping and TensorBoard are, respectively, tools to monitor when convergence has started to go into overfitting during model training. Training performance about the proposed model is in Figure 4-6 and Table 2.

Table 2. Training Results for approach system

Algorithm	Best Epoch	Best Accuracy	Minim Loss	Validation Accuracy	Validation Loss
CNN	18	0.97	0.11	0.98	0.05
ResNet50	17	0.93	0.20	0.98	0.10
InceptionV3	8	0.99	0.003	1.00	0.002
VGG16	8	0.99	0.04	0.99	0.04

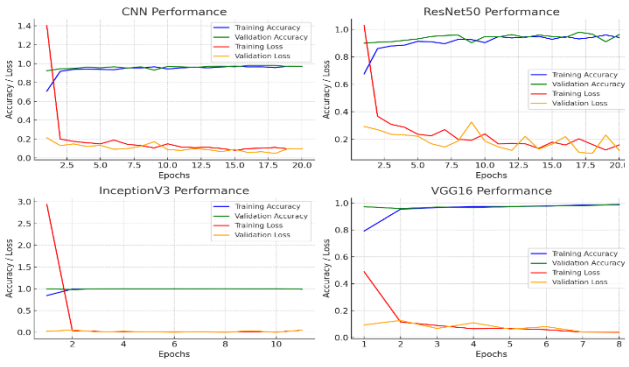

Figure 4.models performance curve.

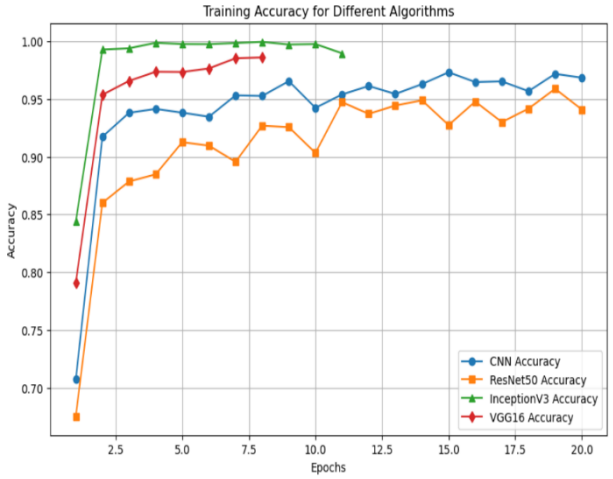

Figure 5.the training accuracy curve.

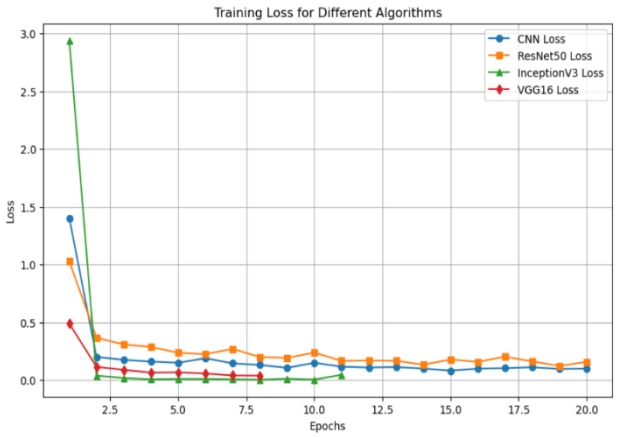

Figure 6.the training loss curve.

8. Conclusion

This study introduced a holistic deep learning framework for the classification of phishing URLs as a mitigation of the constraints brought about by conventional static rule-based or blacklist-oriented detection techniques. This approach made use of a custom CNN model and some transfer learning architectures, specifically ResNet50, InceptionV3, and VGG16 to establish the complicated nonlinear relationships that exist within URL feature representations. The results empirically validated all models under study with high classification accuracies where transfer learning models outperformed the baseline CNN model regarding the speed of convergence and validation performance.

InceptionV3 and VGG16 have been among the architectures evaluated with a relatively better stability generalization, hence highly probable to be used in real-world phishing detection systems. This is enabled by unified training which includes splitting the data and optimization settings equally for all the models being compared hence ensuring fair and reliable comparison. Other training control

mechanisms that would help reduce overfitting increase model robustness.

Overall, these results further solidify the fact that deep learning models have an effective and scalable solution toward the problem of phishing URL detection. Future research may pivot on aspects relating to real-time feature extraction, adversarial robustness, and hybridized elements where deep learning is fused with contextual or behavioral analysis in the quest for higher accuracies in detection regarding novel phishing methodologies.

Conflict of Interest: The authors declare no conflicts of interest.

Funding: This research received no external funding.

Author Contributions: The author contributed equally to this work. All authors read and approved the final version of the manuscript.

References

[1] J. Kline, E. Oakes, and P. Barford, ‘‘A URL-based analysis of WWW structure and dynamics,’’ in Proc. Netw. Traffic Meas. Anal. Conf. (TMA), Jun. 2019, p.800.doi:https://doi.org/10.23919/TMA.2019.8784665

[2] P. Flach and M. Kull, ‘‘Precision-recall-gain curves: PR analysis done right,’’ in Proc. Adv. Neural Inf. Process. Syst., 2015, pp. 838–846.

[3] R. S. Rao and A. R. Pais, ‘‘Detection of phishing websites using an efficient feature-based machine learning framework,’’ Neural Comput. Appl., vol. 31, no. 8, pp. 3851–3873, Aug. 2019.doi:https://doi.org/10.17577/IJERTV9IS050888

[4] H. Shahriar and S. Nimmagadda, ‘‘Network intrusion detection for TCP/IP packets with machine learning techniques,’’ in Machine Intelligence and Big Data Analytics for Cybersecurity Applications. Cham, Switzerland: Springer, 2020, pp. 231–247.doi: https://doi.org/10.1007/978-3-030-57024-8_10

[5] T. Nathezhtha, D. Sangeetha, and V. Vaidehi, ‘‘WC-PAD: Web crawling based phishing attack detection,’’ in Proc. Int. Carnahan Conf. Secur. Technol. (ICCST), Oct. 2019, pp. 1–6. (2020). Accessed:Jan.2020.doi:https://doi.org/10.1109/ccst.2019.8888416

[6] S. Bell and P. Komisarczuk, ‘‘An analysis of phishing blacklists: Google safe browsing, OpenPhish, and PhishTank,’’ in Proc. Australas. Comput. Sci. Week Multiconf. (ACSW), Melbourne, VIC, Australia. New York, NY, USA: Association for Computing Machinery, 2020, pp. 1–11, Art. no. 3, doi: https://doi.org/10.1145/3373017.3373020

[7] G. Diksha and J. A. Kumar, ‘‘Mobile phishing attacks and defence mechanisms: State of art and open research challenges,’’ Comput. Secur., vol. 73, pp. 519–544, Mar. 2018.doi: https://doi.org/10.1016/j.cose.2017.12.006

[8] V. Shahrivari, M. M. Darabi, and M. Izadi, ‘‘Phishing detection using machine learning techniques,’’ 2020, arXiv:2009.11116.doi: https://doi.org/10.52783/pst.1643

[9] S. Wang, S. Khan, C. Xu, S. Nazir, and A. Hafeez, ‘‘Deep learning-based efficient model development for phishing detection using random forest and BLSTM classifiers,’’ Complexity, vol. 2020, pp. 1–7, Sep.2020.doi: https://doi.org/10.1155/2020/8694796

[10] G. Sonowal and K. S. Kuppusamy, ‘‘PhiDMA—A phishing detection model with multi-filter approach,’’ J. King Saud Univ., Comput. Inf. Sci., vol. 32, no. 1, pp. 99–112, Jan. 2020.doi: https://doi.org/10.1016/j.jksuci.2017.07.005

[11] M. Babagoli, M. P. Aghababa, and V. Solouk, ‘‘Heuristic nonlinear regression strategy for detecting phishing websites,’’ Soft Comput., vol. 23, no. 12, pp. 4315-4327,Jun.2.doi: https://doi.org/10.1007/s00500-018-3084-2

[12] R. S. Rao and A. R. Pais, ‘‘Detection of phishing websites using an efficient feature-based machine learning framework,’’ Neural Comput. Appl., vol. 31, no. 8, pp. 3851–3873, Aug.

2019.doi: https://doi.org/10.1007/s00521-017-3305-0

[13] Y. Feng, Q. Wang, D. Wu, Z. Luo, X. Chen, T. Zhang, and W. Gao, ‘‘Machine learning aided phase field method for fracture mechanics,’’ Int. J. Eng. Sci., vol. 169, Dec. 2021, Art. no. 103587.doi: https://doi.org/10.1016/j.ijengsci.2021.103587

[14] A. Karim, M. Shahroz, K. Mustofa, S. B. Belhaouari and S. R. K. Joga, "Phishing Detection System Through Hybrid Machine Learning Based on URL," in IEEE Access, vol. 11, pp. 36805-36822, 2023, doi: https://doi.org/10.1109/ACCESS.2023.3252366

[15] M. M. Yadollahi, F. Shoeleh, E. Serkani, A. Madani and H. Gharaee, "An Adaptive Machine Learning Based Approach for Phishing Detection Using Hybrid Features," 2019 5th International Conference on Web Research (ICWR), Tehran, Iran, 2019, pp. 281-286, doi: https://doi.org/10.1109/ICWR.2019.8765265

[16] Y. Mourtaji, M. Bouhorma, D. Alghazzawi, G. Aldabbagh, and A. Alghamdi, “Hybrid rule-based solution for phishing URL detection using convolutional neural network,” Wireless Communications and Mobile Computing, vol. 2021, Article ID 8241104,pp. 1–14, Sep. 2021, doi: https://doi.org/10.1155/2021/8241104

[17] S. Das Gupta, K. T. Shahriar, H. Alqahtani, “Modeling hybrid feature-based phishing websites detection using machine learning techniques,”Annals of Data Science, vol. 11, pp. 217–242, 2024,doi: https://doi.org/10.1007/s40745-022-00379-8

[18] M. W. Shaukat, R. Amin, M. M. A. Muslam, A. H. Alshehri and J. Xie, “A Hybrid Approach for Alluring Ads Phishing Attack Detection Using Machine Learning,” Sensors, vol. 23, no. 19, Art. no. 8070, 2023, doi: https://doi.org/10.3390/s23198070

[19] J. S. Tharani and N. A. G. Arachchilage, “Understanding phishers' strategies of mimicking uniform resource locators to leverage phishing attacks: A machine learning approach,” Security and Privacy, vol. 3, no. 5, e120, Jul. 2020, doi: https://doi.org/10.1002/spy2.120

[20] M. W. Shaukat, R. Amin, M. M. A. Muslam, A. H. Alshehri, and J. Xie, “A Hybrid Approach for Alluring Ads Phishing Attack Detection Using Machine Learning,” Sensors, vol. 23, no. 19, Art. no. 8070, 2023, doi: https://doi.org/10.3390/s23198070

[21] A. Almalaq, S. Albadran, and M. A. Mohamed, “Deep Machine Learning Model-Based Cyber-Attacks Detection in Smart Power Systems,” Mathematics, vol. 10, no. 15, Art. no. 2574, 2022, doi: https://doi.org/10.3390/math10152574

[22] S. Jalil, M. Usman, and A. Fong, “Highly accurate phishing URL detection based on machine learning,” Journal of Ambient Intelligence and Humanized Computing, vol. 14, pp. 9233–9251, 2023, doi: https://doi.org/10.1007/s12652-022-04426-3

[23] O. K. Sahingoz, E. Buber, O. Demir, and B. Diri, “Machine learning based phishing detection from URLs,” Expert Systems with Applications, vol. 117, pp. 345–357, 2019, doi: https://doi.org/10.1016/j.eswa.2018.09.029

[24] A. Prasad and S. Chandra, "PhiUSIIL: A diverse security profile empowered phishing URL detection framework based on similarity index and incremental learning," Computers & Security, vol. 136, Art. no. 103545, Jan. 2024, doi: https://doi.org/10.1016/j.cose.2023.103545.

[25] A. Rawla, S. Singh, M. Daniyal, and P. Dubey, "Detection of Phishing Attacks in PhiUSIIL Dataset using Deep Learning," Procedia Computer Science, vol. 259, pp. 543–552, 2025, doi: https://doi.org/10.1016/j.procs.2025.04.003

[26] V. Vajrobol, V. Vajratiya, B. B. Gupta, and A. Gaurav, "Mutual information based logistic regression for phishing URL detection," Cyber Security and Applications, vol. 2, Art. no. 100044, 2024, doi: https://doi.org/10.1016/j.csa.2024.100044

[27] A. Sumayli, "Development of advanced machine learning models for optimization of methyl ester

biofuel production from papaya oil: Gaussian process regression (GPR), multilayer perceptron (MLP), and K-nearest neighbor (KNN) regression models," Arabian Journal of Chemistry, vol. 16, Art. no. 104833, Jul. 2023, doi: https://doi.org/10.1016/j.arabjc.2023.104833

[28] M. Grandini, E. Bagli, and G. Visani, "Metrics for Multi-Class Classification: an Overview," arXiv preprint arXiv:2008.05756, Aug. 2020.https://doi.org/10.48550/arXiv.2008.05756.

[29] J. Qi, J. Du, S. M. Siniscalchi, X. Ma, and C. H. Lee, "On Mean Absolute Error for Deep Neural Network Based Vector-to-Vector Regression," IEEE Signal Processing Letters, vol. 27, no. c, pp. 1485–1489, 2020,doi:https://doi.org/10.1109/LSP.2020.3016837

[30] O. Rainio, J. Teuho, and R. Klén, "Evaluation metrics and statistical tests for machine learning," Scientific Reports, vol. 14, Art. no. 6086, 2024, doi: https://doi.org/10.1038/s41598-024-56706-x

[31] S. Subbiah, K. S. M. Anbananthen, S. Thangaraj, S. Kannan and D. Chelliah, "Intrusion detection technique in wireless sensor network using grid search random forest with Boruta feature selection algorithm," in Journal of Communications and Networks, vol. 24, no. 2, pp. 264-273, April 2022, doi: https://doi.org/10.23919/JCN.2022.000002

[32] G. Alfian, M. Syafrudin, I. Fahrurrozi, N. L. Fitriyani, F. T. D. Atmaji, T. Widodo, N. Bahiyah, F. Benes, and J. Rhee, "Predicting Breast Cancer from Risk Factors Using SVM and Extra-Trees-Based Feature Selection Method," Computers, vol. 11, no. 9, Art. no. 136, 2022, doi: https://doi.org/10.3390/computers11090136

[33] L. Alzubaidi, J. Zhang, A. J. Humaidi, et al., "Review of deep learning: concepts, CNN architectures, challenges, applications, future directions," Journal of Big Data, vol. 8, Art. no. 53, 2021, doi: https://doi.org/10.1186/s40537-021-00444-8

[34] R. Ribani and M. Marengoni, "A Survey of Transfer Learning for Convolutional Neural Networks," 2019 32nd SIBGRAPI Conference on Graphics, Patterns and Images Tutorials (SIBGRAPI-T), Rio de Janeiro, Brazil, 2019, pp. 47-57, doi:https://doi.org/10.48550/arXiv.2008.05756 10.1109/SIBGRAPI-T.2019.00010

[35] A. Kaya, A. S. Keceli, C. Catal, H. Y. Yalic, H. Temucin, and B. Tekinerdogan, "Analysis of transfer learning for deep neural network based plant classification models," Computers and Electronics in Agriculture, vol. 158, pp. 20–29, Mar. 2019, doi: https://doi.org/10.1016/j.compag.2019.01.041

[36] A. Deshpande, V. V. Estrela, and P. Patavardhan, "The DCT-CNN-ResNet50 architecture to classify brain tumors with super-resolution, convolutional neural network, and the ResNet50," Neuroscience Informatics, vol. 1, no. 4, Art. no. 100013, Dec. 2021, doi: https://doi.org/10.1016/j.neuri.2021.100013.

[37] A. Minarno, L. Aripa, Y. Azhar, and Y. Munarko, "Classification of Malaria Cell Image using Inception-V3 Architecture," Journal of Informatics and Visualization, vol. 7, no. 2, 2023, doi: https://doi.org/10.30630/joiv.7.2.1301

[38] Z.-P. Jiang, Y.-Y. Liu, Z.-E. Shao, and K.-W. Huang, "An Improved VGG16 Model for Pneumonia Image Classification," Applied Sciences, vol. 11, no. 23, Art. no. 11185, 2021, doi: https://doi.org/10.3390/app112311185

[39] B. Kim, Y. Natarajan, S. D. Munisamy, A. Rajendran, K. R. S. Preethaa, D.-E. Lee, and G. Wadhwa, "Deep Learning Activation Layer-Based Wall Quality Recognition Using Conv2D ResNet Exponential Transfer Learning Model," Mathematics, vol. 10, no. 23, Art. no. 4602, 2022, doi: https://doi.org/10.3390/math10234602

[40] Y. Bai, "RELU-Function and Derived Function Review," SHS Web of Conferences, vol. 144, Art. no. 02006,2022,doi:https://doi.org/10.1051/shsconf/202214402006

[41] A. Zafar, M. Aamir, N. M. Nawi, A. Arshad, S. Riaz, A. Alruban, A. K. Dutta, and S. Almotairi, "A

Comparison of Pooling Methods for Convolutional Neural Networks," Applied Sciences, vol. 12, no. 17, Art. no. 8643, 2022, doi: https://doi.org/10.3390/app12178643

[42] H. Pratiwi, A. P. Windarto, S. Susliansyah, R. R. Aria, S. Susilowati, L. K. Rahayu, Y. Fitriani, A. Merdekawati, and I. R. Rahadjeng, "Sigmoid Activation Function in Selecting the Best Model of Artificial Neural Networks," Journal of Physics: Conference Series, vol. 1471, Art. no. 012010, 2020, doi:https://doi.org/10.1088/17426596/1471/1/012010

How to cite this article

H. A. Abdalrazaq,, "A robust intelligent approach for phishing URL detection using hybrid machine learning," *CyberSystem J.*, vol. 2, no. 2, pp. 91-97, 2025. doi: 10.57238/csj.2025.1017

Access this article online