Ensemble Fusion for Enhanced Malicious URL Detection by Integrating Machine Learning and Deep Learning Techniques

Raja Rao PBV[1(✉)], Kiran Sree Pokkuluri[1], M. Prasad[1], Neeraj Sharma[2], BSatya Narayana Murthy[3], and Adina Karunasri[4]

[1] Shri Vishnu Engineering College for Women(A), Bhimavaram, A.P, India
rajaraopbv@gmail.com
[2] VPPCOE and VA, Sion, Mumbai-22, Maharashtra, India
[3] BVC Engineering College(A), Odalarevu, A.P, India
[4] Vishnu Institute of Technology(A), Bhimavaram, A.P, India

Abstract. The exponential rise of malicious activities on the internet underscored the critical need for robust detection mechanisms to safeguard users from potential threats. In this paper, the authors propose an innovative method for enhancing malicious URL detection by utilizing ensemble fusion techniques that integrate both ML and DL methodologies. The proposed method began by loading and preprocessing a large-scale dataset comprising 5,49,346 URLs sourced from Kaggle. Through feature engineering and extraction, the dataset is transformed into a numerical format suitable for model training, employing TF-IDF to capture the importance of features. Subsequently, individual ML models are trained, including Random Forest, XGBoost, and Gradient Boosting, as well as the DL models Multi-Layer Perceptron (MLP), RNN, LSTM, and GRU, on the preprocessed data. Random Forest achieved a recall of 97% and an accuracy of 97.50%, while LSTM demonstrated a recall and accuracy of 97% and 97.50%, respectively. Then, ensemble fusion techniques, specifically stacking and the meta-learner approach, were used to combine the predictions from all individual models and produce a final prediction. Through comprehensive evaluation and performance analysis, the proposed method demonstrated the efficacy of ensemble fusion model in accurately detecting malicious URLs, achieving superior performance compared to individual models. The proposed ensemble model with logistic regression as a meta-learner achieved an accuracy of 98.4% and a recall of 98%. These findings underscore the robustness and superior performance of the ensemble fusion approach in accurately identifying malicious URLs.

Keywords: Malicious URL · RNN · LSTM · TF-IDF · MLP

1 Introduction

Cybersecurity is becoming a top priority due to the growing reliance on the internet for a variety of purposes. Malicious URLs represent a serious danger to users' online security, among the many other hazards that exist in cyberspace. Frequently disguising

P. Pareek et al. (Eds.): IC4S 2024, LNICST 597, pp. 339–349, 2025.
https://doi.org/10.1007/978-3-031-77075-3_27

themselves as authentic webpage addresses, these URLs are intended to trick visitors and enable illicit operations, including virus distribution, phishing, and identity theft. Safeguarding people, businesses, and vital infrastructure from cyberattacks requires the detection and mitigation of these threats. URLs are identified and categorized according to their purpose and content in order to detect malicious URLs. Manual inspection or pre-established criteria are the mainstays of traditional URL categorization techniques, which are frequently inadequate in the face of complex and dynamic threats. In order to avoid discovery, malicious actors are always changing their strategies and using cutting-edge methods like redirection, domain spoofing, and URL obfuscation. It is difficult to identify and block malicious URLs using conventional methods because of these complex techniques.

The sheer quantity and diversity of URLs on the internet is a significant challenge for detection systems. Millions of new URLs are created every day, making it increasingly difficult to distinguish between malicious and legitimate URLs. Consequently, there is a significant false-positive rate in detection methods. Threat landscapes for malicious URLs are always evolving as attackers find new ways to get past security measures. Cybersecurity specialists have a great challenge: security systems need to be updated often to meet new threats as attackers become more adept at evading defenses. To counter the threat posed by rogue URLs, user awareness and education remain crucial, even with the most powerful detection technology [1]. Phishing efforts to trick people into clicking on dangerous links frequently involve social engineering techniques. This emphasizes how important it is to inform customers about the risks associated with visiting unknown URLs. Some detection methods, particularly those that depend on deep learning and machine learning [2], can be computationally costly and resource-intensive. Using these detection technologies at scale may be more challenging for organizations with low resources since they may need significant infrastructure and computing resources.

The need to improve cybersecurity measures and automate the process of identifying harmful URLs has led to an increase in interest in the application of ML and DL techniques. In this work, a novel hybrid strategy is proposed that builds on the advantages of deep learning[3] and ML methods. This work created a reliable and efficient solution for malicious URL detection by utilizing the strengths of DL models MLP, RNN, LSTM, and GRU in conjunction with ML algorithms like Random Forest, XGBoost, and Gradient Boosting. By combining these models using ensemble fusion techniques such as stacking and meta-learning, then system obtained superior performance and accuracy in identifying malicious URLs, thereby enhancing cyber defense mechanisms and protecting users from online threats.

2 Literature Review

To find out the effectiveness of ML in identifying phishing domains, Shouq Alnemari et al. [4] created and contrasted four models. The models were assessed using the UCI phishing domains dataset for URLs. The models are based on ANN, SVC, DT, and RF approaches. The results demonstrated that the RF model outperformed other solutions in the literature and was the most accurate of the four approaches. S. Abad et al. [5] set out to develop ML models for the efficient identification and classification of hazardous

URLs in order to enhance cybersecurity. The study demonstrated how effective RFs are in achieving high accuracy, recall, and F1 scores using Bayesian optimization with SVMs, RFs, DTs, and KNNs. Instance selection methods, including random selection, BPLSH, and DRLSH, were used for computational efficiency. The results highlighted the importance of the instance selection method in the machine learning pipeline for the classification of hazardous URLs by showing how it substantially impacts model performance. In order to evaluate the effectiveness of phishing website detection methods during the last five years, a thorough literature review was carried out in [6]. After examining a dataset of 530 research items from five electronic libraries, the researchers used inclusion-exclusion criteria to reduce the sample to 80 articles. Research questions were the main focus of the study in order to identify the most widely used methods, datasets, and algorithms in the literature, especially the ones that achieved the finest in terms of accuracy.

In the cybersecurity domain, identifying malicious URLs presents a formidable hurdle, necessitating sophisticated approaches that amalgamate machine learning and deep learning methodologies. Inspired by the accomplishments in image caption generation, which hinge on a profound understanding of image content, this study aims to refine the detection of malicious URLs using an innovative ensemble fusion strategy. Proposed methodology harnesses the ResNet-50 Convolutional Neural Network (CNN) as a robust feature extractor and the Long Short-Term Memory (LSTM) recurrent neural network as an adept language model to encode crucial visual details from URLs and generate coherent textual descriptions. Following a methodology akin to the successful image captioning paradigm, the ResNet-50 CNN undergoes fine-tuning on an expansive dataset to adeptly capture the semantic essence of URLs. Simultaneously, the LSTM network [7], trained on a comprehensive set of URL-caption pairs, constructs descriptive text by iteratively generating captions. Empirical results highlight the efficacy of ensemble fusion model, surpassing current methods in terms of detection accuracy and demonstrating its proficiency in fortifying malicious URL detection through the integration of machine learning and deep learning techniques.

In [8], the authors used an ML-based approach for malicious URL detection and reported promising results. They used several ML models and achieved the highest accuracy with SVM. The authors of [9] discussed the most frequent and harmful assaults made possible by malicious URLs and included explanations of how they work as well as countermeasures. The emphasis was on a particular detection method that used machine learning techniques, providing a more detailed examination.

The authors of [10, 11] suggested an ML-based method for identifying rogue websites. For their tests, they made use of a dataset that had a sizable number of URLs. For text feature extraction, three methods were used: count vectorizer, hashing vectorizer, and IDF vectorizer. Four ML classifiers were then used to build a phishing website detection model: DT, RF, K-NN, and logistic regression. The ML model with a random forest and hash vectorizer had a 97% accuracy rate. Furthermore, a web application that uses Flask was created to determine whether or not a URL input is dangerous. A method for detecting phishing and preventing users from visiting fraudulent websites was described by K. Sushma et al. [12] and involved utilizing the unique features of the Uniform Resource Locator (URL). Two machine learning approaches, SVC and

RF, were applied to the task of categorizing webpages. People's growing reliance on the Internet for a wide range of daily chores has raised concerns about security flaws related to online apps. Many online application risks, including phishing, session hijacking, cross-site scripting (XSS), and denial-of-service attacks, pose a severe danger to information security. The research highlighted the need to implement new protocols to identify and prevent phishing attacks due to the potential for significant losses. The techniques now employed to recognize phishing, including content-based strategies, visual similarities, whitelisting, and blacklisting, were also underlined.

The goal was to examine consumer- and employee-focused tweets from the airline sector on Twitter. Using a dataset of 14,640 tweets about American airlines that were taken from the Kaggle repository, DL methods were used. In order to account for any flaws and guarantee accurate predictions [13], a similar dataset was utilized for training and testing. For efficient dataset splitting, the Python language was used. The dropout learning technique was used, with impressive results, to avoid overfitting related to the co-adaptation of feature detectors. In order to provide "inquiry extension grade (IEG)," a unique feature dimensionality technique, M. Prasad et.al [14] proposed a TF-IDF technique to recognize flower and took inspiration from the inquiry extension term weighting strategy. Additionally, "improved TF-IIDF," a modified version of the traditional TF-IDF approach, was developed specifically to handle unbalanced text collections. A number of simulations were conducted to evaluate the efficiency of the presented techniques. The outputs demonstrated that the combination of IEG-ITFIDF and Bi-LSTM with glove embeddings achieved high accuracy for the Twitter US Airline Sentiment dataset. M. Alsaedi et al. [15] developed a detection model based on cyber threat information using ensemble learning to increase the detection accuracy of hazardous URLs. Cyber threat intelligence (CTI) was created by compiling information from user input and cybersecurity analyst reports from across the world in order to boost detection accuracy. Rohit Rayala et al. [16] focused on developing a system for URL analysis and classification[17] in order to lessen cyberattacks. This system's primary goal was to detect potentially harmful URLs. The detection of potentially harmful URLs was framed by the binary classification task. The recommended approach made use of a machine learning-based automated URL classification algorithm called logistic regression. Using the logistic regression approach, the data was classified as malicious or legal following the use of feature extraction and tokenization in the first stage. Authentic websites were categorized as good, whereas malicious websites were categorized as bad.

Venkatesh et al. [18] described an ML-based phishing detection system that examined URLs on three distinct datasets using eight different methods. The outcomes of the experiment demonstrated that the recommended models had excellent performance and a high success rate. W. Ahmed et al. [19] developed a practical and lightweight MLP model that exclusively employs lexical features and integrates a DT approach for feature selection in order to enhance performance. Based only on URL lexical properties, the MLP achieved 94.51% accuracy, according to an experimental evaluation that measured accuracy, time, and error reduction. It employed 35 features. The model's time efficiency was increased along with a modest improvement in accuracy and loss by employing the DT for feature selection.

3 Proposed Methodology

The proposed method is depicted in Fig. 1. The methodology for detecting[20] malicious URLs combined the strengths of both ML and DL techniques to effectively combat cybersecurity threats. First, gathered a comprehensive Kaggle dataset comprising 5,49,000 URLs sourced from reputable repositories, ensuring a balanced representation of both legitimate and malicious URLs. Later, preprocessing of URLs is done. The preprocessing of the dataset involved rigorous cleaning and standardization procedures to remove noise such as special characters and unnecessary parameters, thereby enhancing the quality of the data. Next, feature engineering was performed with TF IDF. It plays a crucial role in extracting meaningful information from the URLs to represent their characteristics effectively. These features served as inputs to various ML and DL models employed in the detection process. Current methodology encompassed the training of individual models using a variety of algorithms, including Random Forest, XGBoost, and Gradient Boosting, as well as DL architectures such as MLP, RNN [21], LSTM, and GRU. This diverse set of models allowed us to capture both simple and complex patterns present in the data. Ensemble techniques were employed to combine the predictions from the individual models, enhancing the overall detection accuracy. The stacking method was applied, along with the introduction of a meta-learner as logistic regression to optimize the fusion of predictions and improve model performance. Following model training and ensemble integration, a thorough evaluation and performance analysis were conducted using established metrics.

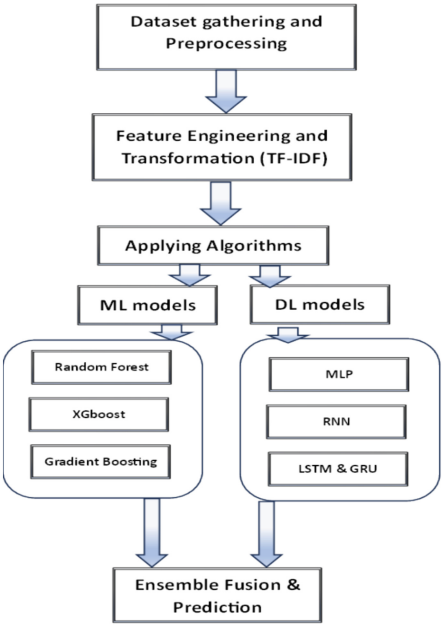

Fig. 1. Proposed Methodology

4 Experimentation and Results

4.1 Dataset Gathering and Preprocessing

In the initial phase of research, embarked on the task of gathering a substantial dataset comprising URLs sourced from reputable repositories and sources known for their reliability in cataloging both legitimate and malicious URLs. The malicious URLs dataset, obtained from Kaggle [22], comprises 549,340 URLs.

Among them, 156,420 URLs are classified as bad URLs (phishing URLs), while 392,920 URLs are categorized as good URLs. Datset consists of website information. Among these, Smilesvoegol.servebbs.org/voegol.php represents a known malicious source labeled as "bad," offering valuable insights into the characteristics of malicious URLs essential for robust detection mechanisms. Conversely, Creativeproductsgroup.com, labeled "good," serves as a legitimate website, aiding in distinguishing between benign and malicious URLs during model training. Once the dataset was assembled, rigorous preprocessing steps were applied to prepare the URLs for further analysis. This involved meticulous cleaning and standardization procedures aimed at removing any extraneous noise that could potentially interfere with the learning process of all models. Special characters and unnecessary parameters were systematically removed from the URLs, ensuring that only relevant information was retained for subsequent analysis. Text normalization techniques were employed to further increase the quality of the dataset. This involves standardizing the format of the URLs by converting them to a consistent representation, such as lowercase, to eliminate variations in capitalization that could otherwise introduce inconsistencies during the modeling process. The resulting dataset was clean, standardized, and well-suited for training ML and DL models to effectively detect and classify malicious URLs.

4.2 Feature Engineering and Transformation (TF-IDF)

Initially, basic DL algorithms, namely Simple RNN, LSTM, and GRU, were applied. The architecture used for the RNN model contains 3 hidden layers with 180, 100, and 80 neurons, respectively. The LSTM and GRU models used only two hidden layers with 180 and 90 neurons in each layer. The loss function used in three models is "binary_cross entropy." The "Adam" optimzer is utilized in all three models. The number of epoches used in the models is 30. The results of the three models are shown in Table 1. From Table 1, it is observed that RNN has 86% accuracy and 84% recall. The accuracy and recall achieved with LSTM are 91% and 90%, respectively. GRU gave 90% and 87.8% accuracy and recall values, respectively. Among the three, LSTM performed well.

4.3 Apply ML Models

In the phase of model training with ML techniques and objective was to build predictive models capable of accurately classifying URLs as either malicious or benign based on the features extracted from the preprocessed dataset with TF-IDF features. Began with training individual ML models, including Random Forest, XGBoost, and Gradient Boosting, on the prepared dataset. To train these models effectively, then optimized

their performance by tuning their hyperparameters. For that, a systematic exploration of different combinations of hyperparameter values using techniques was performed.

By fine-tuning the hyperparameters, identified the configuration that yielded the best performance for each model, thereby enhancing their predictive capabilities. After the models were trained and their hyperparameters optimized, proceeded to evaluate their performance using appropriate evaluation metrics. The results of these experiments are shown in Table 1 and Fig. 2.

Table 1. Model results

Method	*Accuracy*	*Recall*
Random Forest	97.5%	97%
Gradient Boosting	97%	96%
XGBoost	97.2%	96.9%

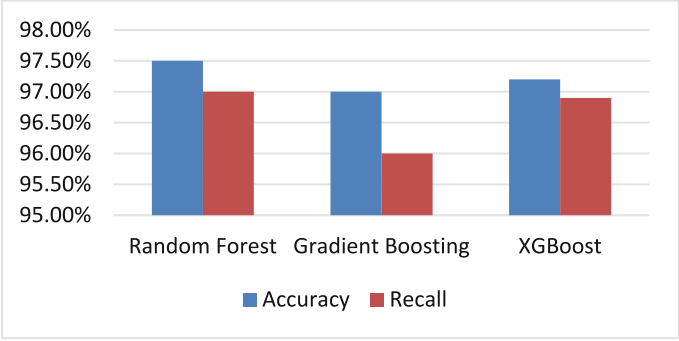

Fig. 2. ML Techniques accuracy, recall

4.4 Applying DL Techniques

Later, the model was trained a variety of DL models, including MLP, RNN, LSTM, and GRU, on the prepared dataset. During the training process, explored a range of architectural configurations, activation functions, and regularization techniques to optimize the performance of the DL models. This involved experimenting with different network architectures, adjusting the number of layers, neurons per layer, and activation functions to identify configurations that yielded the best results. The architectures for all these four models are different, but the number of epochs used in all models is 50. The number of hidden layers used in MLP, RNN, LSTM, and GRU is 3, 2, 2, and 2, respectively. Applied various regularization methods namely dropout and L2 regularization, to prevent overfitting and improve the models' generalization capabilities. The models underwent various hyperparameter settings. The optimizer used in all four models is "Adam.". The los function is used in "cross entropy." The results with DL techniques are shown in Fig. 3 and Table 2 (Table 3).

Table 2. DL Model results

Method	*Accuracy*	*Recall*
MLP	97%	96%
RNN	96%	95%
LSTM	97.5%	97%
GRU	97%	96%

Table. 3. Comparison with existing works

Method	*Accuracy*
Conventional DL	96%
Traditional Ensemble Approach	96%
Proposed Method	98.4%

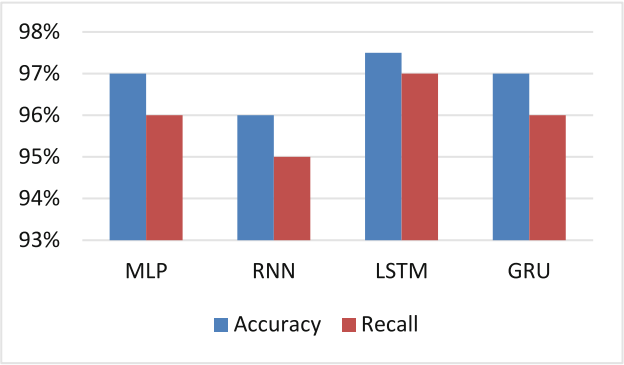

Fig. 3. DL Techniques accuracy, recall

4.5 Ensemble Fusion

In proposed ensemble fusion architecture, the stacking technique served as the cornerstone for integrating predictions from a diverse array of previously appled ML and DL models. Stacking, a widely-used ensemble method, capitalized on the unique strengths of individual models by treating their predictions as additional input features for a meta-learner. This approach enabled us to effectively capture diverse patterns in the data and exploit the collective intelligence of the ensemble. Specifically, predictions generated by these base models were fed into a meta-learner model implemented as logistic regression. The meta-learner then learned to combine these predictions in an optimal manner, weighting them based on their individual performance and contribution to the final prediction. By training the meta-learner on the predictions of base models, then aimed to capture the complex relationships between the predictions and improve the predictive

performance of the ensemble. This architecture ensured for ensemble fusion model was capable of making accurate predictions, achieving an accuracy rate of 98.4% and a recall rate of 98%, and outperformed individual models.

4.6 Performance Comparison

In the final phase, several ensemble fusion techniques employed to integrate the predictions from all individual models, including both ML and DL models. The final comparison of all models is shown in Fig. 4. From Fig. 4, it is observed that the proposed methods outperformed traditional ML and DL techniques. It is identified that the recall obtained with the proposed model is higher than conventional ML and DL techniques.

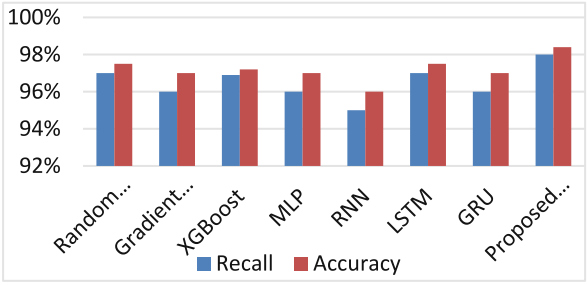

Fig. 4. Ensemble Performance

4.7 Comparison with Existing Work

Table 5 shows the comparison with existing works. Compared to existing methodologies, the proposed approach exhibits superior accuracy in identifying malicious URLs. Conventional Deep Learning (DL) approaches[23], as reported by, achieve an accuracy of 96%. Similarly, ensemble learning techniques, as outlined in, also attain a comparable accuracy of 96%. However, the proposed method surpasses both conventional DL and ensemble learning methodologies, achieving an impressive accuracy of 98.4%.

5 Conclusion

This paper aimed to address the escalating threat posed by malicious URLs through the development of an innovative detection mechanism leveraging ensemble fusion techniques. The method encompassed the application of both ML and DL algorithms.

The process started by preparing a dataset comprising over 549,000 URLs sourced from Kaggle. Through rigorous preprocessing and feature engineering, the dataset transformed the raw URL data into a structured numerical format, facilitating effective model training and evaluation. Then applied three traditional ML models: Random Forest, Gradient Boosting, and XGBoost, and achieved the best accuracy and recall of 97.5% and

97% with random forest. Later, several DL methods, including MLP, RNN, LSTM, and GRU, are applied. The highest accuracy and recall values of 97.5% and 97% were acquired with the LSTM model. Later, a novel ensemble fusion was applied with logistic regression as a meta-learner and achieved accuracy and recall of 98.4% and 98%, respectively. This study contributed to the advancement of cybersecurity measures, offering insights into the integration of ML and DL techniques for enhanced threat detection.

References

1. Sree, P.K., Chintalapati, P.V., Prasad, S.U.D.N,M., Babu, G.R., Raja Rao, P.B.V.: Waste management detection using deep learning. In: 2023 3rd International Conference on Computing and Information Technology (ICCIT), pp. 50–54. Tabuk, Saudi Arabia (2023). https://doi.org/10.1109/ICCIT58132.2023.10273898
2. Uppalapati, P.J., Gontla, B.K., Gundu, P., Hussain, S.M., Narasimharo, K.: A machine learning approach to ıdentifying phishing websites: a comparative study of classification models and ensemble learning techniques. EAI Endorsed Scal. Inf. Syst. **10**(5) (2023). https://publications.eai.eu/index.php/sis/article/view/3300
3. Pilli, B.V.R., Nagarajan, S., Devabalan, P.: Detecting the vehicle's number plate in the video using deep learning performance. Rev. Int. Geogr. Educ. (RIGEO), **11**(5), 4315–4324 (2021). https://doi.org/10.48047/rigeo.11.05.311
4. Alnemari, S., Alshammari, M.: Detecting phishing domains using machine learning. Appl. Sci. **13**(8), 4649. MDPI AG (2023). https://doi.org/10.3390/app13084649
5. Abad, S., Gholamy, H., Aslani, M.: Classification of malicious URLs using machine learning. Sensors **23**(18), 7760. MDPI AG (2023). https://doi.org/10.3390/s23187760
6. Safi, A., Singh, S.: A systematic literature review on phishing website detection techniques. J. King Saud Univ. Comput. Inf. Sci. **35**(2), 590–611. Elsevier BV (2023). https://doi.org/10.1016/j.jksuci.2023.01.004
7. Satti, S.K., Rajareddy, P., Maddula, N.V.: Vishnumurthy ravipati: ımage caption generation using ResNET-50 and LSTM. In: 2023 IEEE Silchar Subsection Conference (SILCON), 1–6. Silchar, India (2023). https://doi.org/10.1109/SILCON59133.2023.10404600 (2023)
8. Jain, S., Gupta, C.: A support vector machine learning technique for detection of phishing websites. In: 2023 6th International Conference on Information Systems and Computer Networks (ISCON), pp. 1–6. Mathura, India (2023). https://doi.org/10.1109/ISCON57294.2023.10111968
9. Bhavani, A., et al.: Detection of legitimate and phishing websites using machine learning. In: 2023 International Conference on Sustainable Computing and Smart Systems. Coimbatore, India (2023)
10. Lakshmanarao, A., Babu, M.R., Bala Krishna, M.M.: Malicious URL detection using NLP, machine learning and FLASK. In: 2021 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), pp. 1–4. Chennai, India (2021). https://doi.org/10.1109/ICSES52305.2021.9633889
11. Dharmaraju, G., Kumar, T.N., Mohan, P.P., Rao Pbv, R., Lakshmanarao, A.: Phishing website detection through ensemble machine learning techniques. In: 2024 2nd International Conference on Computer, Communication and Control (IC4), pp. 1–5. Indore, India (2024). https://doi.org/10.1109/IC457434.2024.10486530
12. Sushma, K., Jayalakshmi, M., Guha, T.: Deep learning for phishing website detection. In: 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), pp. 1–6. Mysuru, India (2022). https://doi.org/10.1109/MysuruCon55714.2022.9972621

13. Maddula, P., Srikanth, P., Sree, P.K., Rao, P.B.V.R., Murty, P.T.S.: COVID-19 prediction with Chest X-Ray images using CNN. In: 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), pp. 568–572. Bengaluru, India (2023). https://doi.org/10.1109/IITCEE57236.2023.10090951
14. Prasad, M., et al.: A CNN and TF techniques development for efficient ıdentification of floral recognition. In: 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), pp. 327–332. Greater Noida, India (2024). https://doi.org/10.1109/IC2PCT60090.2024.10486528
15. Alsaedi, M., Ghaleb, F., Saeed, F., Ahmad, J., Alasli, M.: Cyber threat ıntelligence-based malicious URL detection model using ensemble learning. Sensors **22**(9), 3373. MDPI AG (2022). https://doi.org/10.3390/s22093373
16. Rayala, R., Pasumarthi, S., Kuppa, R., Karthık, S.R.: Malicious URL detection using logistic regression. In: Institute of Electrical and Electronics Engineers (IEEE) (2021). https://doi.org/10.36227/techrxiv.14790381.v1
17. Josphineleela, R., Raja Rao, P.B.V., Shaikh, A., et al.: A multi-stage faster RCNN-Based iSPLInception for skin disease classification using novel optimization. J. Digit Imaging **36**, 2210–2226. https://doi.org/10.1007/s10278-023-00848-3 (2023)
18. Venkatesh, N., et al.: Malicious URL detection using machine learning. Turcomat **14**(2), 537–552 (2023)
19. Ahmed, W., Jameel, N.G.M.: Malicious URL detection using decision tree-based lexical features selection and multilayer perceptron model. In: UHD Journal of Science and Technology, vol. 6, no. 2, pp. 105–116. University of Human Development (2022). https://doi.org/10.21928/uhdjst.v6n2y2022.pp105-116
20. Satti, SK., Maddula, P., Ravipati, N.V.: Unified approach for detecting traffic signs and potholes on Indian roads. J. King Saud Univ.- Comput. Inf. Sci. **34**(10), Part B, 9745–9756 (2022). https://doi.org/10.1016/j.jksuci.2021.12.006. ISSN 1319–1578
21. Sree, P.K., Babu, G.R., Rao, P.R., Chintalapati, P.V., Prasad, M.: Fake news detection using cellular automata based deep learning. In: 2023 3rd International Conference on Computing and Information Technology (ICCIT), pp. 167–171. Tabuk, Saudi Arabia (2023). https://doi.org/10.1109/ICCIT58132.2023.10273875)
22. Kaggle. https://www.kaggle.com/datasets/taruntiwarihp/phishing-site-urls/data
23. Sree, P.K., Usha Devi N, S., Chintalapati, P.V., Babu, G.R., Raja Rao, P.: Drug recommendations using a reviews and sentiment analysis by RNN. In: Pareek, P., Gupta, N., Reis, M.J.C.S. (eds) Cognitive Computing and Cyber Physical Systems. IC4S 2023. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 536. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-48888-7_11