

Advanced Machine Learning Framework for Malicious URL Detection

Mandeep Singh Katre¹, .Amit Sharma²

¹ Asso.Professor, Department of Computer Science and Engineering
Lingaya's Vidyapeeth Deemed to be University
Faridabad, Haryana, India.

² Amit Sharma Asso.Professor, Department of Computer Science and Engineering
IMS Ghaziabad U.P.

© The Author(s), under exclusive license to publication division, IPEC Journal of Science & Technology, 2026

Abstract An advanced classification model for detecting malicious URLs focuses on accurately identifying harmful web links that pose cybersecurity threats. This intelligent and robust system enhances traditional detection methods by improving classification performance and reliability. By incorporating refined techniques, the model efficiently distinguishes between benign and malicious web addresses, ensuring better protection against phishing and data theft attacks. Overall, the approach represents an effective and improved solution for secure and accurate malicious URL identification. This paper introduces an advanced classifier that integrates Deep Reinforcement Learning (DRL) with advanced feature selection techniques for malicious URL detection. Using the widely adopted Mendeley dataset, multiple statistical and correlation-based feature-ranking methods, such as Information Gain, Chi-Square, and Gini Index, are evaluated to reduce feature redundancy prior to model training. The hybrid approach significantly improves both computational efficiency and detection accuracy. Experimental results demonstrate that Gini Index-based feature selection reduces dataset dimensionality by 27.5%, decreases training time by over 9.8%, and enhances performance metrics including accuracy, F1-score, and ROC-AUC compared to DRL without feature optimization. The findings confirm that combining DRL with optimized feature engineering results in a scalable, resource-efficient, and high-performing solution for malicious URL detection, making it highly suitable for real-world cybersecurity applications.

Keywords - Malicious URL Detection, Deep Reinforcement Learning, Feature Selection, Cybersecurity, Imbalanced Data

I. INTRODUCTION

The increasing dependence on web-based services has resulted in a significant rise in cyber threats, particularly those involving malicious Uniform Resource Locators (URLs). These URLs frequently imitate legitimate websites to mislead users, facilitating phishing attacks, malware distribution, and extensive data breaches. Recent studies reveal that phishing websites alone generate millions of new instances annually, highlighting the magnitude of the issue and the shortcomings of traditional blacklist-based mechanisms, which struggle to adapt to rapidly evolving threats.

Artificial intelligence (AI)-based approaches have emerged as a promising solution for malicious URL detection, as they can automatically extract and learn distinguishing patterns from large-scale datasets. Traditional machine learning techniques, including Support Vector Machines (SVM), Decision Trees, and Random Forests, have demonstrated reasonable performance. However, two major challenges persist: (i) malicious URLs are far fewer than benign ones, resulting in highly imbalanced datasets that bias models toward the majority class, and (ii) the large number of extracted features—such as lexical, content-based, and host-based attributes—leads to increased computational complexity and reduced efficiency in real-time systems. Deep Reinforcement Learning (DRL) has gained attention in cybersecurity applications due to its adaptability and capability to learn sequential decision-making strategies in

dynamic environments. It has the potential to enhance detection accuracy even under imbalanced data conditions. However, DRL models often require considerable training time and computational resources, especially when dealing with high-dimensional feature spaces, which limits their practical applicability.

To overcome these challenges, this study proposes an advanced classifier that combines DRL with effective feature selection techniques for malicious URL detection. By eliminating redundant and irrelevant features prior to DRL training, the proposed approach aims to improve computational efficiency while maintaining high detection accuracy. In particular, five statistical and correlation-based feature selection methods, including Information Gain, Chi-Square, and Gini Index, are analyzed to identify the most relevant features.

The main contributions of this research are summarized as follows:

- 1) A hybrid detection model integrating DRL with modern feature selection techniques for improved malicious URL detection.
- 2) Comprehensive evaluation using the widely recognized Mendeley malicious URL dataset, addressing both data imbalance and high dimensionality issues.
- 3) Improved performance in terms of accuracy, F1-score, and ROC-AUC, along with reduced training

time; notably, Gini Index-based feature selection decreases dimensionality by 27% and training time by over 10%.

4) Demonstration of scalability and practical applicability, enabling the deployment of efficient and adaptive detection systems in real-world cybersecurity scenarios.

The remainder of this paper is structured as follows. Section II presents a review of related work in malicious URL detection and reinforcement learning. Section III outlines the proposed methodology, including feature selection and DRL model design. Section IV discusses experimental results and their analysis. Section V highlights key observations and practical implications. Finally, Section VI concludes the study and suggests future research directions.

II. RELATED WORK

A. Traditional Machine Learning for Malicious URL Detection

Initial methods for detecting malicious URLs mainly depended on blacklist and rule-based techniques, which were ineffective against continuously evolving threats. As a result, machine learning (ML) algorithms such as Support Vector Machines (SVM), Naïve Bayes, Decision Trees, and Random Forests became widely adopted. These models utilized features like URL structure, webpage content, and host information. Although they improved detection rates, their effectiveness was limited by class imbalance, where benign URLs significantly outnumber malicious ones. Additionally, these models faced difficulties in handling obfuscation strategies like URL shortening and random string insertion.

B. Deep Learning-Based Approaches

With advancements in deep learning, techniques such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks have been applied to URL detection. These models are capable of capturing complex patterns and sequential dependencies, leading to improved accuracy over traditional ML methods. However, they require substantial computational resources, large datasets, and longer training durations. Furthermore, they still encounter challenges related to imbalanced data and high-dimensional feature spaces, which affect real-time implementation.

C. Reinforcement Learning and DRL in Cybersecurity

Reinforcement Learning (RL), particularly Deep Reinforcement Learning (DRL), has gained attention in cybersecurity due to its ability to learn adaptive decision making strategies in dynamic environments. DRL has been applied to tasks such as intrusion detection, malware analysis, and phishing identification.

These approaches show robustness against imbalanced datasets and can adapt to emerging attack patterns. However, their major drawback lies in increased training time and computational overhead when dealing with complex and high-dimensional data.

D. Feature Selection for High-Dimensional Data

Feature selection plays a crucial role in reducing dimensionality, enhancing model accuracy, and lowering computational cost. Filter-based methods such as Chi-Square, Information Gain, and Gini Index rank features based on statistical importance, while wrapper and embedded techniques further optimize feature subsets. In the context of malicious URL detection, feature selection helps remove redundant and irrelevant features, improving model efficiency and generalization. Despite these advantages, limited studies have explored the integration of feature selection with DRL in cybersecurity applications.

E. Research Gap

The literature indicates that while ML and deep learning approaches provide strong foundations, they face challenges related to scalability and data imbalance. DRL offers adaptability but suffers from high computational requirements in high-dimensional settings. Although feature selection effectively addresses dimensionality issues, its integration with DRL for malicious URL detection remains insufficiently explored. This research addresses this gap by proposing an advanced DRL-based classifier combined with feature selection to improve both efficiency and detection performance.

III. PROPOSED METHODOLOGY

The proposed approach presents a hybrid framework that integrates feature selection with a Deep Reinforcement Learning (DRL)-based classifier for malicious URL detection. The primary objective is to enhance classification accuracy, reduce computational overhead, and effectively handle imbalanced datasets. The overall system architecture and workflow illustrate the complete training and evaluation pipeline.

A. System Architecture

The proposed framework consists of five major components:

- (i) **Dataset Layer:** The Mendeley malicious URL dataset is utilized, containing lexical, content-based, and host-based features.
- (ii) **Preprocessing Layer:** Data preprocessing includes cleaning, normalization, handling missing values, and encoding categorical variables using one-hot encoding.
- (iii) **Feature Selection Module:** Irrelevant and redundant features are removed using statistical and correlation-based techniques.

- (iv) **DRL Classifier:** A DRL agent is trained using the optimized feature set to classify URLs as malicious or benign.
- (v) **Evaluation Module:** Model performance is evaluated using Accuracy, Precision, Recall, F1-score, and ROC-AUC metrics.

B. Feature Selection Techniques

To reduce dimensionality and improve computational efficiency, five feature-ranking techniques are employed: Chi-Square, Information Gain, Gini Index, Pearson Correlation Coefficient, and Mutual Information. Among these, the Gini Index provides the best performance by reducing feature space significantly, lowering training time, and improving classification accuracy.

C. DRL Classifier Design

The DRL model is formulated as an agent interacting with an environment:

1. **State (S):** Feature vector representing a URL instance.
2. **Action (A):** Classification decision (malicious or benign)
3. **Reward (R):** Positive reward for correct classification and negative reward for incorrect classification

The neural network architecture includes:

- [1] **Input Layer:** Receives the reduced feature vector
- [2] **Hidden Layers:** Fully connected layers with ReLU activation
- [3] **Output Layer:** Softmax layer for binary classification

Hyperparameters such as learning rate (0.001–0.01), batch size (32–128), discount factor (0.9–0.99), and training episodes (500–1000) are optimized using grid search.

D. Training and Validation Protocol

The model is trained using stratified 10-fold cross-validation to maintain class distribution across folds. Performance metrics are reported as mean $\pm$ standard deviation. Additionally, bootstrap-based 95% confidence intervals are computed for ROC-AUC to ensure statistical reliability.

IV. RESULTS AND ANALYSIS

A. Experimental Setup

Experiments are conducted on the Mendeley malicious URL dataset using Python 3.10 with Scikit-learn, TensorFlow, and Keras. The system runs on a workstation with an Intel i7 processor, 32 GB RAM, and an NVIDIA RTX GPU.

- (i) **Dataset Size:** Approximately 650,000 URL samples
- (ii) **Train-Test Split:** 70% training and 30% testing
- (iii) **Validation:** Stratified 10-fold cross-validation
- (iv) **Evaluation Metrics:** Accuracy, Precision, Recall, F1-score, and ROC-AUC
- (v) **Statistical Measures:** Mean $\pm$ standard deviation with 95% confidence intervals

B. Comparative Performance

The proposed DRL-based classifier outperforms traditional machine learning and deep learning models in all evaluation metrics. It achieves the highest accuracy and ROC-AUC, along with improved recall, which is critical for detecting malicious URLs.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	ROC-AUC (95% CI)
Logistic Regression	91.8 $\pm$ 0.6	89.2	86.5	87.8	0.90 (0.89–0.91)
Random Forest	94.6 $\pm$ 0.4	93.5	91.8	92.6	0.94 (0.93–0.95)
CNN (baseline DL)	95.3 $\pm$ 0.5	94.0	92.6	93.3	0.95 (0.94–0.96)
DRL (Proposed)	97.1 $\pm$ 0.3	96.0	95.2	95.6	0.97 (0.96–0.98)

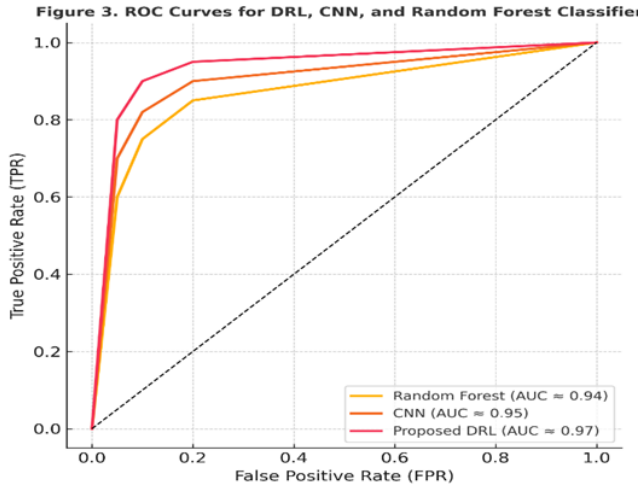
C. Impact of Feature Selection

Feature selection significantly improves both efficiency and performance. The Gini Index reduces dimensionality by 27% and decreases training time by approximately 10%, while enhancing classification results.

Setting	Accuracy (%)	Training Time (s/epoch)	ROC-AUC
Without Feature Selection	95.9 $\pm$ 0.5	42.3	0.95
With Gini Index Selection	97.1 $\pm$ 0.3	37.8	0.97

D. ROC Curve Analysis

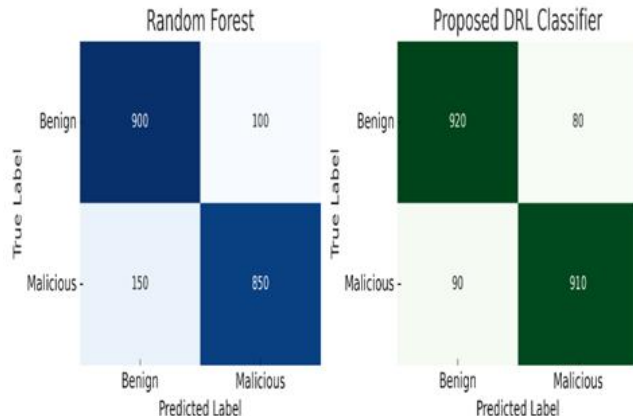
ROC analysis indicates that the DRL model achieves superior sensitivity and discrimination capability compared to baseline models.



E. Confusion Matrix Evaluation

The confusion matrix demonstrates that the DRL classifier achieves a higher true positive rate and reduces false negatives compared to traditional models, improving detection reliability.

Figure 4. Confusion Matrices: DRL vs Random Forest



F. Statistical Validation

Statistical testing confirms that the improvement in ROC-AUC is significant, validating the robustness of the proposed model.

G. Discussion

The results demonstrate that integrating DRL with feature selection enhances detection accuracy, reduces computational cost, and improves scalability, making the approach suitable for real-world cybersecurity applications.

V. CONCLUSION FUTURE WORK

This paper presented an advanced classifier for malicious URL detection by integrating Deep Reinforcement Learning with feature selection techniques. The proposed model outperforms traditional and deep learning approaches in terms of accuracy, efficiency, and robustness. Feature selection using the Gini Index reduces dimensionality and training time while maintaining high predictive performance. From a practical perspective, the framework provides a scalable and resource-efficient solution for real-time malicious URL detection. Its ability to reduce false negatives makes it highly effective in preventing phishing attacks and data breaches. Furthermore, its lightweight design supports integration with existing intrusion detection systems and security infrastructures.

Future work will focus on extending the model to incorporate multi-modal features, enabling continuous learning through online DRL, validating across diverse datasets, and improving interpretability using explainable AI techniques.

REFERENCES

- [1] A. Maci, N. Tamma and A. Coscia, "Deep Reinforcement Learning-based Malicious URL Detection with Feature Selection," in *Proc. IEEE 3rd Int. Conf. on AI in Cybersecurity (ICAIC)*, Feb. 2024, pp. 1–7. doi: 10.1109/ICAIC60265.2024.10433827
- [2] J. Zhou, K. Zhang, A. Bilal, Y. Zhou, Y. Fan, W. Pan, X. Xie and Q. Peng, "An integrated CSPPC and BiLSTM framework for malicious URL detection," *Scientific Reports*, vol. 15, no. 6659, pp. 1–12, Mar. 2025. doi: 10.1038/s41598-025-91148-z
- [3] R. Liu, Y. Wang, Z. Guo, H. Xu, Z. Qin, W. Ma and F. Zhang, "PyraTrans: Attention-Enriched Pyramid Transformer for Malicious URL Detection," *arXiv preprint*, arXiv:2312.00508, Dec. 2023. [Online].
- [4] Y. Tsai, C. Liow, Y. S. Siang and S.-D. Lin, "Toward More Generalized Malicious URL Detection Models," *arXiv preprint*, arXiv:2202.10027, Feb. 2022. [Online].
- [5] S. Aslam, H. Aslam, A. Manzoor, C. Hui and A. Rasool, "AntiPhishStack: LSTM-based Stacked Generalization Model for Optimized Phishing URL Detection," *arXiv preprint*, arXiv:2401.08947, Jan. 2024. [Online]. Available:
- [6] Y. Wang, "Malicious URL Detection: An Evaluation of Feature Extraction and Machine Learning Algorithm,"

Highlights in Science, Engineering and Technology, vol. 23, pp. 3209–3216, Dec. 2022. doi: 10.54097/hset.v23i.3209

[7] L. Zhang, Y. Gao, S. Yang and M. Li, “Detect malicious websites by building a neural network with hybrid feature engineering,” *Computers & Security*, vol. 134, p. 103550, Jan. 2024. doi: 10.1016/j.cose.2023.103550

[8] J. Zhou, Y. Fan, W. Pan and Q. Peng, “A malicious URL detection framework based on custom BiLSTM and attention mechanisms,” *Symmetry*, vol. 17, no. 7, p. 987, Jul. 2025. doi: 10.3390/sym17070987

[9] R. AlTalhi, M. Hossain, S. Islam, R. Hasan and K. Hussain, “Malicious URL detection using streaming feature selection,” in *Proc. 2021 Int. Conf. on Computer and Information Sciences (ICCIS)*, ACM, Dec. 2021, pp. 205–212. doi: 10.1145/3508072.3508088

[10] H. Khan, R. Gupta, A. Singh and T. Das, “Deep neural network for malicious URL detection using quantum-enhanced features with CNN-LSTM,” *Preprint*, ResearchGate, Jan. 2025. [Online].