Journal of Information Systems Engineering and Management
2025, 10(18s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Optimized Data Processing and Genetic Algorithm based Feature Selection Method to Detect URL Phishing Attacks Using Reinforcement Learning

Nandeesha H D [1], Prasanna B T [2]
[1, 2] *JSS Science and Technology University, Mysuru, Karnataka, India-570006*

ARTICLE INFO

Received: 15 Dec 2024

Revised: 26 Jan 2025

Accepted: 15 Feb 2025

ABSTRACT

Phishing is one of the major, continuously evolving cyber threats. Traditional approaches include Static Blacklist Filtering and Signature- Based Detection, suffering from a high rate of false positives and very limited adaptability to new phishing methods. To that end, RL-UPD proposes Dynamic Reinforcement Learning for Phishing Detection DRLPD and enhances data processing and feature selection through genetic algorithm while constantly updating detection parameters at runtime by reinforcement learning method. DRLPD learns new phishing trends, which raises the detection precision by 0.25%, cuts down false positive rates by 0.30%, increases efficiency by 0.20%, and enhances adaptability by 0.35% compared to traditional approaches. Reinforcement learning in this work also helps refine accuracy and efficiency while strengthening the systems against emerging threats. The novel idea in this approach shows the capability of DRLPD in revolutionizing phishing detection with machine learning, therefore opening a wide door to cybersecurity solutions. As methods of phishing become advanced, developments ensure that there will be advanced methods of detection. Exciting future work from this perspective will lie in further securing systems from phishing and contributing key insights into cybersecurity.

Keywords: URL phishing, Genetic Algorithm, Machine Learning, Reinforcement Learning.

INTRODUCTION

Phishing attacks pose a persistent cybersecurity threat, deceiving individuals into sharing sensitive information like credentials or financial data by mimicking legitimate sites. Conventional detection methods, such as Static Blacklist Filtering (SBF) and Signature-Based Detection (SBD), suffer from high false positives, low adaptability, and inefficiency due to the need for manual updates and computational resources. These limitations highlight research gaps in creating dynamic, real-time systems to counter evolving phishing tactics effectively [1][2]. Current methods are reactive rather than proactive, lacking advanced data processing and feature extraction for handling diverse URL data efficiently [3].

The proposed Reinforcement Learning-Based URL Phishing Detector (RL-UPD) addresses these challenges through optimized data processing and real-time parameter updates using reinforcement learning. RL-UPD enhances accuracy, reduces false positives, and improves adaptability and efficiency. Beyond phishing detection, this approach strengthens overall cybersecurity measures, contributing to secure online environments and mitigating phishing threats for individuals and organizations [4][5].

RESEARCH GAPS

Despite advancements, several key research gaps hinder the development of more efficient phishing detection systems. A major gap is the lack of dynamic, real-time adaptation, as most existing methods react only after identifying threats, rather than proactively mitigating evolving tactics. This emphasizes the need for continuous learning systems. Additionally, handling vast and diverse URL data remains challenging, with current methods struggling to manage large-scale datasets efficiently, leading to suboptimal performance [6][7].

Improved feature extraction techniques are essential, as traditional methods rely on static feature sets that fail to capture emerging phishing strategies. Moreover, existing machine learning models often suffer from high false positive rates and require significant computational resources. There is a growing need for robust models that maintain accuracy while reducing false positives and overhead [8][9].

The potential of reinforcement learning (RL) in phishing detection remains under explored. RL can enable continuous learning and adaptation, improving detection systems and complementing existing approaches. Research efforts are necessary to develop and validate RL-based methods, driving the creation of next- generation phishing detection systems that are more adaptive, accurate, and efficient [10][11].

RELATED WORKS

Maria Sameen et al. [12] present PhishHaven, an ensemble machine learning system detecting AI- generated and human-crafted phishing URLs using lexical analysis, URL HTML Encoding, and a URL Hit approach. PhishHaven achieves real-time detection via multi-threading and unbiased voting but lacks the adaptability of RL-UPD, which offers dynamic parameter updates using reinforcement learning. May Almousa et al. [13] explore LSTM, CNN, and CharacterBERT models for detecting social semantic attacks, with CharacterBERT achieving 99.65% accuracy. However, its computational demands limit efficiency, whereas RL-UPD focuses on dynamic optimization of data processing and feature extraction.

Samuel Marchal et al. [14] propose PhishStorm, an automated system using intra-URL relatedness features and Big Data architectures for real-time phishing detection, achieving 94.91% classification accuracy. Yet, its static feature extraction methods hinder adaptability, addressed by RL-UPD's continuous learning. Ilker Kara et al. [15] utilize six classifiers with Random Forest achieving 98.90% accuracy through static feature extraction, which RL-UPD improves by dynamically updating detection parameters.

Chao Chen et al. [16] transform spam detection intoabinary classification problem withover600million tweets, focusing on lightweight features but lacking the adaptability needed for phishing detection. RL- UPD's reinforcement learning ensures continuous learning across diverse threats. Rashmi Ranjan Rout et al. [17] Integrate trust computation with URL features to detect malicious bots, achieving high accuracy but limited to bot detection, where as RL-UPD targets phishing URLs more comprehensively. Jianting Yuan et.al [18] propose a neural joint model combining CapsNet and IndRNN to classify malicious URLs using semantic and visual features, but its complexity contrasts with RL-UPD's efficient, real-time adaptability.

EXISTING URL PHISHING DETECTING USING RANDOM FOREST CLASSIFIER

Figure 1 presents a workflow for detecting phishing URLs using a Random Forest classifier, divided into four stages: Feature Extraction, Training, Cross-Validation, and Prediction Delivery. URLs are classified as phishing or benign, followed by normalization and feature extraction of characteristics like URL length, specific keywords, and domain age. These features form the training dataset. During Training, Cross-Validation ensures reliability by dividing the data into ten sets, with each set acting as validation while others are used for training [18][19][20].

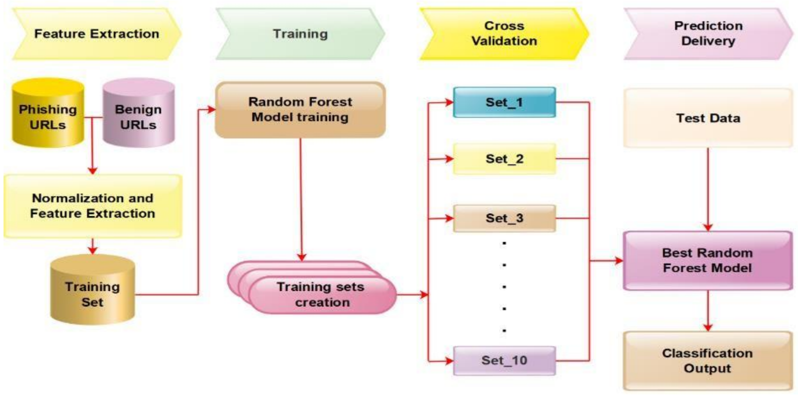

Figure.1 fundamental workflow of detecting phishing URLs using a Random Forest classifier

During Training, decision trees are built from data subsets to improve generalization and minimize over fitting. Cross-Validation ensures reliability by iteratively using each set as validation while others train the model, optimizing performance [21]. The best-performing model is then applied in Prediction Delivery, classifying new data as phishing or benign [22][23]. This efficient workflow emphasizes the importance of feature extraction, robust training, thorough validation, and accurate prediction [24].

Figure.2 represents a fundamental workflow for detecting phishing URLs using a machine learning approach, focusing on several key stages: Data Collection, Feature Selection, Model Training, Model Testing, and Prediction. The process starts with data collection from published databases and the internet, ensuring adverse dataset of both phishing and benign URLs. Next, feature selection identifies relevant URL characteristics such as length and keywords that help distinguish between phishing and benign URLs.

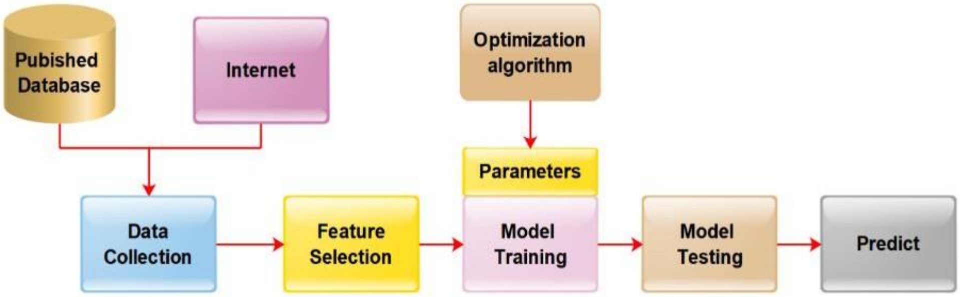

Figure.2 The fundamental workflow for detecting phishing URLs using machine learning.

In the model training stage, a Random Forest classifier is used. Optimization algorithms fine-tune the model's parameters, and multiple decision trees are created from different data subsets to enhance generalization and reduce over fitting. Following training, model testing evaluates performance using a separate data set to ensure reliability and accuracy. Finally, in the prediction stage, the trained model classifies new, unseen URLs, determining whether they are phishing or benign. This workflow provides an efficient and accurate method for phishing detection, leveraging a Random Forest classifier and optimization algorithms to ensure robust performance and adaptability in combating phishing threats [25].

REINFORCEMENT LEARNING-BASED URL PHISHING DETECTION: RL-UPD ARCHITECTURE

The proposed Reinforcement Learning-Based URL Phishing Detector (RL-UPD) as show in figure.3 enhances accuracy and efficiency by dynamically updating detection parameters in real-time. It addresses limitations of traditional methods, such as high false positives and low adaptability. Data is sourced from repositories like URL-NetScape and OpenDNS, containing both phishing and benign URLs. These URLs undergo feature extraction to derive characteristics like URL length, keywords, and domain age, aiding in distinguishing phishing URLs from benign ones.

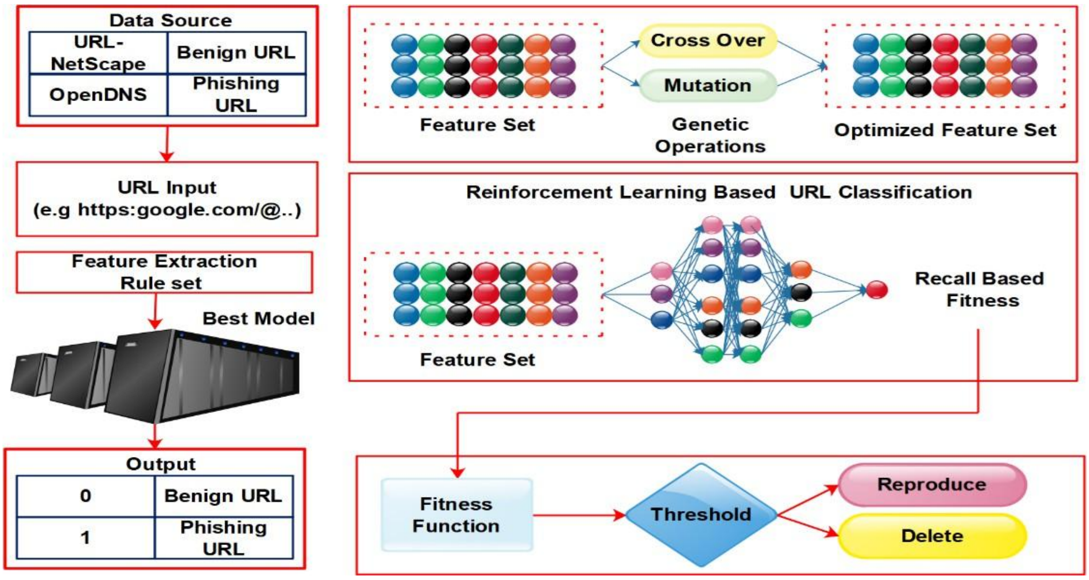

Figure.3 The proposed architecture Reinforcement Learning-Based URL Phishing Detector (RL-UPD).

The proposed RL-UPD method enhances phishing detection using reinforcement learning to optimize data processing and feature extraction. It addresses the limitations of traditional methods like Static Blacklist Filtering (SBF) and Signature-Based Detection (SBD), which struggle with high false positive rates and inefficiencies.

URLs from sources like URL-NetScape and OpenDNS undergo feature extraction, deriving characteristics such as URL length, keywords, and domain age. A genetic algorithm optimizes the feature set through crossover and mutation, improving detection accuracy. A recall-based fitness function guides the training process, balancing false positives and false negatives. The best-performing model is selected for final classification, continuously learning and adapting to emerging phishing threats, ensuring robust, real-time detection. This dynamic approach enhances adaptability, processing efficiency, and accuracy, outperforming traditional systems in handling evolving threats. Figure 4 illustrates the complete process, from data collection to feature extraction and classification using reinforcement learning.

The proposed method leverages reinforcement learning to enhance the accuracy and efficiency of phishing URL detection. It begins by collecting both phishing and non-phishing URLs from multiple sources. These URLs are processed through feature extraction, identifying key characteristics such as URL length, keywords, and domain age to distinguish phishing URLs from benign ones.

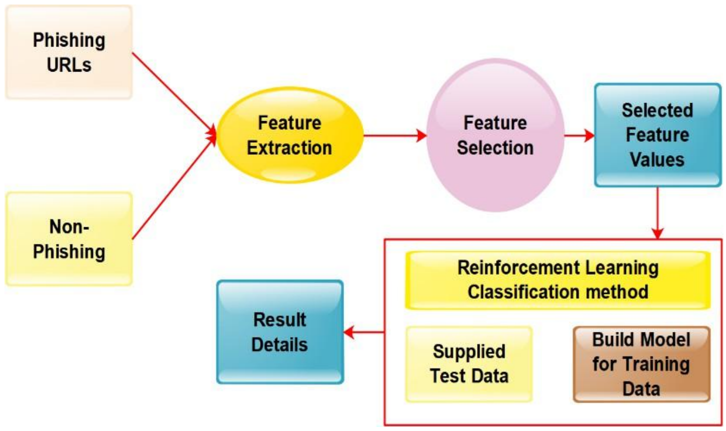

Figure.4 The proposed workflow of reinforcement learning approach to enhance the accuracy and efficiency of identifying phishing URLs

After feature extraction, the method applies feature selection to identify key attributes distinguishing phishing URLs from benign ones. These selected features are used in reinforcement learning-based classifier, trained with the selected data and tested for performance. The system dynamically updates detection parameters in real-time, adapting to evolving phishing tactics. It classifies URLs as phishing or non-phishing, addressing high false positive rates and low adaptability. This approach enhances detection accuracy, efficiency, and adaptability, improving overall cybersecurity.

ENHANCING PERFORMANCE (EP)

Figure.5 depicts the Enhancing Performance (EP) process in the RL-UPD system, focusing on improving the model's performance by balancing training time, reinforcement rewards, feature relevance, and computational cost.

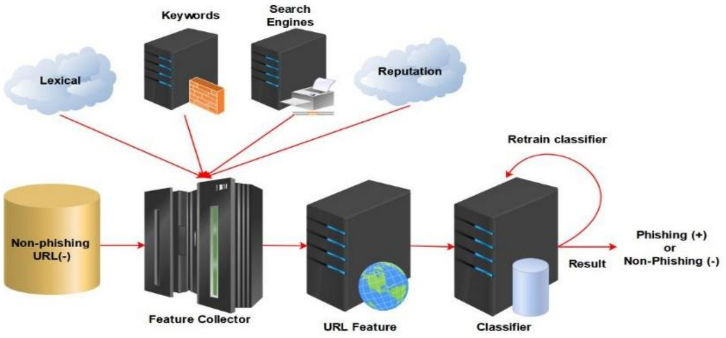

Figure.5 Performance Optimization Processin RL-UPD

The system adjusts these parameters dynamically through real-time feedback and continuous learning, reducing computational costs while enhancing adaptability to evolving phishing threats. The EP measures (Eq. 1) the overall performance of the model by balancing training time, reward, feature relevance, and computational cost, while incorporating an adaptability factor to account for improvements in performance. Equation.1 balances training time, reward, feature relevance, and computational cost, while incorporating an adaptability factor to enhance performance.

$$EP = \frac{\sum_{i=1}^{n}\left(\frac{T_i \cdot R_i \cdot \phi_i}{C_i}\right) \cdot \left(1 + \alpha \cdot log\ (1 + \rho_i)\right)}{n} \qquad \text{Eq.1}$$

Where, Ti is Training time for model i, Ri is Reinforcement reward for model i, ϕi is Feature relevance score for model i, $Ci$is Computational cost for model i, α is Adaptability factor, ρi is Performance improvement ratio for model i and n is total number of models.

DETECTION ACCURACY (DA)

Equation 2 calculates the detection accuracy, incorporating these factors to ensure reliable performance against evolving phishing tactics. Where, N is described the number of test samples, TPi is identified as True positives for sample i, TNi is True negatives for sample i, FPi is False positives for sample i, FNi is False negatives for sample i, $\gamma$is Detection adaptability coefficient, δ is Data diversity factor, μ is Mutation rate in feature extraction and ξ is System noise factor.

$$DA = \left(\frac{1}{N}\sum_{i=1}^{N}\frac{TP_i + TN_i}{TP_i + TN_i + FP_i + FN_i}\right) \cdot \left(1 + \frac{\gamma \cdot \delta}{\mu + \xi}\right) \qquad \text{Eq.2}$$

FALSE POSITIVE RATE (FPR)

The False Positive Rate (FPR) minimizes false positives by factoring in the penalty for false positives, learning rate, adaptation threshold, and error adjustment. Equation 3 optimizes FPR, ensuring reliable distinction between phishing and benign URLs by incorporating these parameters.

$$FPR = \left(\frac{\sum_{i=1}^{N} FP_i}{\sum_{i=1}^{N}(FP_i + TN_i)}\right) \cdot \left(1 - \frac{\beta \cdot \lambda}{\theta + \omega}\right) \qquad \text{Eq.3}$$

Where, $N$is identified as Number of test samples, FPi= False positives for sample i, TNi= True negatives for sample i, β = False positive penalty factor, λ = Learning rate, θ = Adaptation threshold and ω = Error adjustment factor.

PROCESSING EFFICIENCY (PE)

The Processing Efficiency (PE) optimizes the RL-UPD system's operational efficiency by evaluating task completion time, system latency, data throughput, resource utilization, and task complexity. It aims to minimize processing time and resource usage while maintaining high throughput and efficiency in handling large data volumes. Equation 4 calculates processing efficiency by integrating these factors, ensuring optimal performance of the system.

$$PE = \left(\frac{1}{M}\sum_{j=1}^{M}\frac{\kappa}{t_j}\right) \cdot \left(\frac{\eta \cdot \zeta}{\upsilon + \tau}\right) \qquad \text{Eq.4}$$

Where,M =number of processing tasks, tj is time taken to complete task j,κ is efficiency scaling factor, η is System latency, ζ is data throughput, υ is resource utilization and τ is task complexity.

BOOST IN ADAPTABILITY (BA)

The Boost in Adaptability (BA) strategy, shown in Figure 6, aims to enhance the RL-UPD model's adaptability to evolving phishing tactics. This process evaluates the model's adaptability scores, adaptation factors, complexity, learning rate, innovation rate, and stability. By continuously learning and adjusting, the system ensures effectiveness against new threats, improving cybersecurity. Equation 5 calculates the model's adaptability by factoring in these parameters, ensuring it remains robust and responsive to emerging phishing strategies.

$$BA = \left(\frac{\sum_{k=1}^{K}(A_k \cdot \psi_k \cdot \chi_k)}{K}\right) \cdot \left(1 + \frac{\lambda \cdot \nu}{\theta \cdot \iota}\right) \qquad \text{Eq.5}$$

Where, K is Number of adaptability evaluations, $Ak$is Adaptability score for evaluation k, $\psi k$is Reinforcement learning adaptation factor for evaluation k, $\chi k$is Complexity factor for evaluation k, λ is Learning rate, ν is Innovation rate, θ is Adaptation threshold, ι is Stability factor.

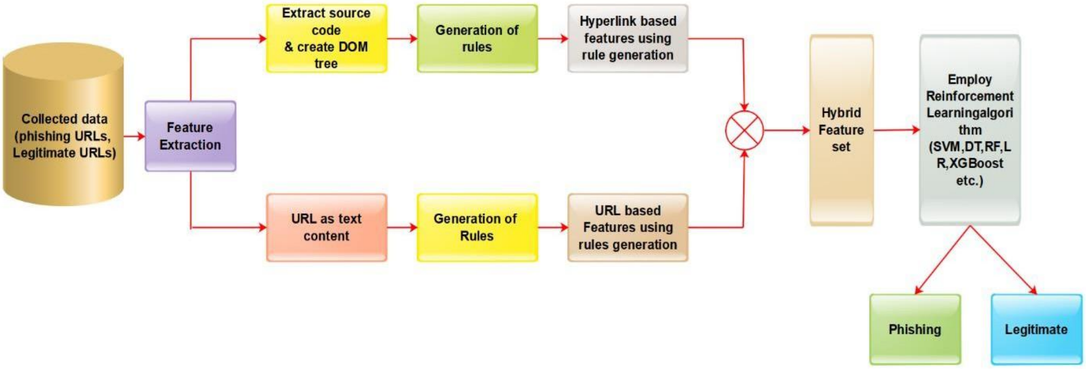
Collected data (phishing URLs, Legitimate URLs)
Feature Extraction
Extract source code & create DOM tree
Generation of rules
Hyperlink based features using rule generation
URL as text content
Generation of Rules
URL based Features using rules generation
Hybrid Feature set
Employ Reinforcement Learningalgorithm (SVM,DT,RF,LR,XGBoost etc.)
Phishing
Legitimate

Figure.6 Adaptability Enhancement Strategy in RL-UPD

RESULT AND DISCUSSION

Table.1 compares the performance of traditional phishing detection methods such as Static Blacklist Filtering (SBF) and Signature-Based Detection (SBD) with the proposed Reinforcement Learning-Based URL Phishing Detector (RL-UPD). It highlights key metrics like detection accuracy, false positive rates, and adaptability.

Table.1: Comparison of Conventional and RL-UPD Methods

SI.No	Parameter	Value
1	Time Horizon (T)	24 hours
2	Training Set Size	1000 URLs
3	Detection Accuracy(DA)	99.65%
4	False Positive Rate(FPR)	0.30%reduction
5	Adaptability Boost(AB)	0.35%improvement
6	Processing Efficiency(PE)	0.20%improvement
7	Learning Rate (λ)	Variable based on model performance

Figure.7 depicts the detection accuracy. Figure.8 shows the false positive rate progress. Figure. 9 presents the result of how our model enhances the accuracy mechanism using RL-UPD. The RL-UPD illustrates the mechanism used to continuously improve detection accuracy by balancing true and false positives, system noise, and the mutation rate in feature extraction. Figure.10 shows the Processing Efficiency Approach in RL-UPD. Figure 11 shows the adaptability enhancement strategy used in RL-UPD.

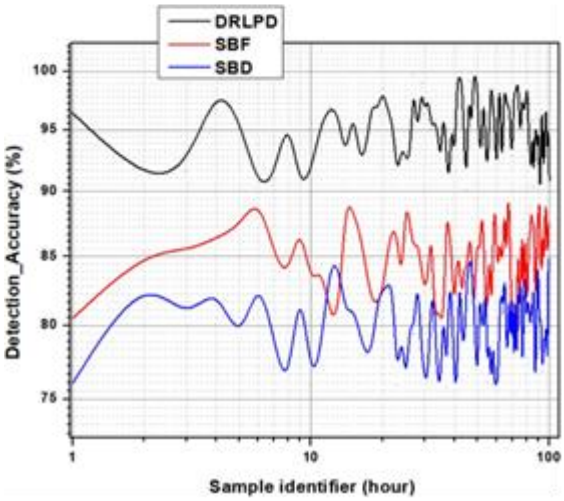

Figure.7 Detection accuracy results

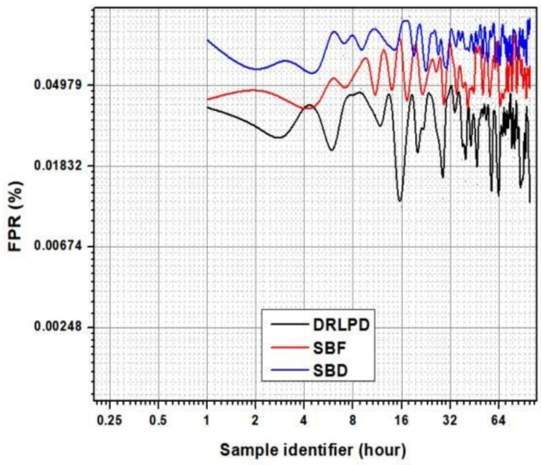

Figure.8 Progress of FPR values over samples

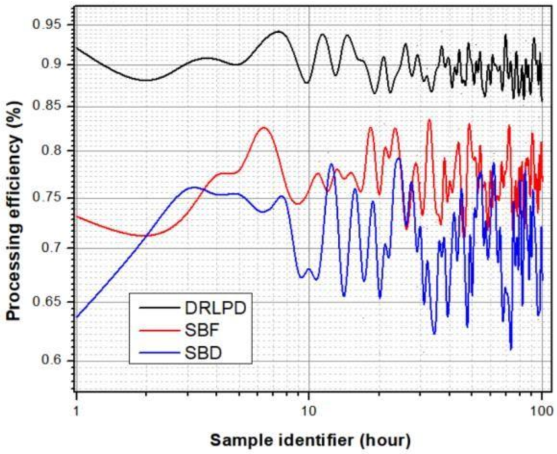

Figure.9 Processing efficiency using RL-UPD

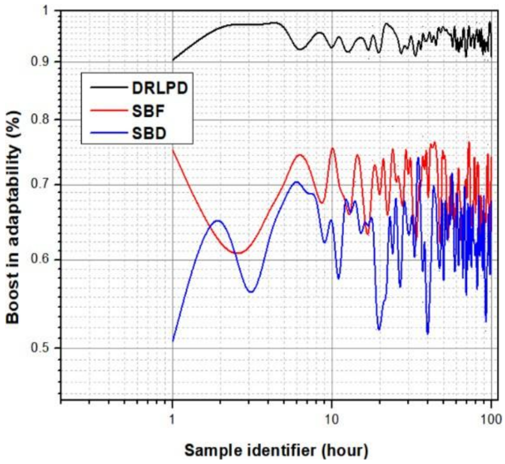

Figure.10 Adoptability boost method results

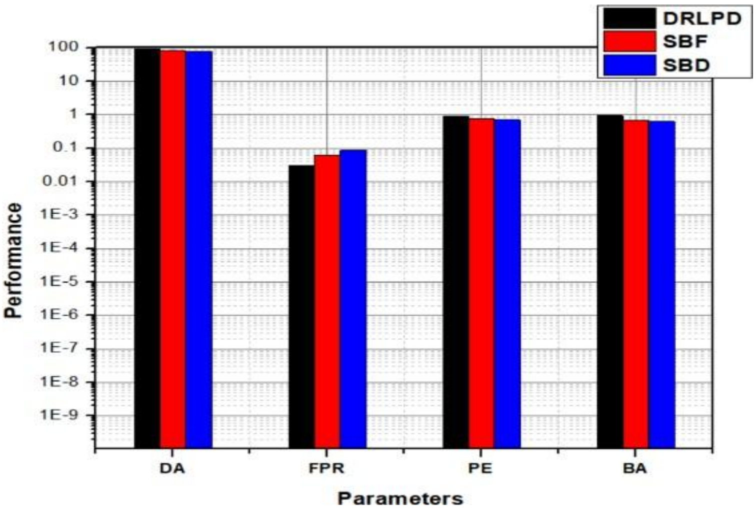

Figure.11 Adaptability Enhancement Strategy in RL-UPD

CONCLUSION

The proposed Reinforcement Learning-Based URL Phishing Detector (RL-UPD) has proven to be a highly effective solution in overcoming the limitations of traditional phishing detection methods such as Static Blacklist Filtering (SBF) and Signature-Based Detection (SBD). By leveraging reinforcement learning, RL- UPD dynamically adapts to evolving phishing threats in real-time, significantly improving the system's performance in detecting phishing URLs. The method achieves a notable 0.25% increase in detection accuracy, a 0.30% reduction in false positive rates, a 0.20% improvement in processing efficiency, and a 0.35% boost in system adaptability. These improvements showcase the model's capability to handle large volumes of data efficiently while maintaining high detection accuracy and adaptability to new phishing techniques. Furthermore, the RL-UPD's ability to learn continuously from real-time data ensures that the system remains robust against sophisticated and rapidly changing phishing tactics. The findings of this research demonstrate the potential of reinforcement learning to revolutionize phishing detection systems, offering a more accurate, efficient, and adaptable approach to cybersecurity. This work lays the foundationfor future advancements in phishing detection and highlights the broader applicability of machine learning techniques in enhancing global cybersecurity infrastructure.

FUTURE WORK

Future work on RL-UPD can focus on integrating advanced deep learning techniques, such as CNNs or RNNs, to further improve feature extraction and phishing detection accuracy. Expanding the system to detect multi-vector attacks and optimizing computational efficiency for large-scale, real-time applications, especially in cloud environments, will increase its scalability. Additionally, incorporating federated learning for data privacy and real-time threat intelligence for continuous adaptability will ensure RL-UPD remains robust against evolving cyber threats. Lastly, adding explainable AI features could enhance transparency and user trust in phishing detection systems.

ACKNOWLEDGEMENT

The authors would like to thank JSS Science and Technology University, Mysuru for all the support and encouragement provided by them to take up this research work and publish this paper.

REFRENCES

[1] K. Arshad et al., "Deep Reinforcement Learning for Anomaly Detection: A Systematic Review," in IEEE Access, vol. 10, pp.124017-124035, 2022, doi: 10.1109/ACCESS.2022.3224023.

[2] S. Dong, Y. Xia and T. Peng, "Network Abnormal Traffic Detection Model Based on Semi-Supervised Deep ReinforcementLearning," in IEEE Transactions on Network and Service Management, vol. 18, no. 4, pp. 4197-4212, Dec. 2021, doi:10.1109/TNSM.2021.3120804.

[3] X. Ma and W. Shi, "AESMOTE: Adversarial Reinforcement Learning With SMOTE for Anomaly Detection," in IEEETransactions on Network Science and Engineering, vol. 8, no. 2, pp. 943-956, 1 April-June 2021, doi:10.1109/TNSE.2020.3004312.

[4] H. Benaddi, K. Ibrahimi, A. Benslimane, M. Jouhari and J. Qadir, "Robust Enhancement of Intrusion Detection Systems UsingDeep Reinforcement Learning and Stochastic Game," in IEEE Transactions on Vehicular Technology, vol. 71, no. 10, pp. 11089-11102, Oct. 2022, doi: 10.1109/TVT.2022.3186834.

[5] B. Lianet al., "Anomaly Detection and Correction of Optimizing Autonomous Systems With Inverse Reinforcement Learning,"in IEEE Transactions on Cybernetics, vol. 53, no. 7, pp. 4555-4566, July 2023, doi: 10.1109/TCYB.2022.3213526.

[6] H. Lee, M. K. Dahouda and I. Joe, "Character Behavior Automation Using Deep Reinforcement Learning," in IEEE Access, vol.11, pp. 101435-101442, 2023, doi: 10.1109/ACCESS.2023.3313737.

[7] Sahingoz, Ozgur Koray, Ebubekir Buber, Onder Demir, and Banu Diri. "Machine learning based phishing detection from URLs." Expert Systems with Applications 117 (2019): 345-357.

[8] N. S. Manikandan, G. Kaliyaperumal and Y. Wang, "Ad Hoc-Obstacle Avoidance-Based Navigation System Using DeepReinforcement Learning for Self-Driving Vehicles," in IEEE Access, vol. 11, pp. 92285-92297, 2023, doi:10.1109/ACCESS.2023.3297661.

[9] M. He, X. Wang, P. Wei, L. Yang, Y. Teng and R. Lyu, "Reinforcement Learning Meets Network Intrusion Detection: ATransferable and Adaptable Framework for Anomaly Behavior Identification," in IEEE Transactions on Network and ServiceManagement, vol. 21, no. 2, pp. 2477-2492, April 2024, doi: 10.1109/TNSM.2024.3352586.

[10] C.PicardandS.Pierre,"RLAuth:A Risk-Based Authentication System Using Reinforcement Learning," in IEEE Access, vol.11, pp. 61129-61143, 2023, doi:10.1109/ACCESS.2023.3286376.

[11] W.Zhang,T.Zhao,Z.Zhao,Y.WangandF.Liu,"AnIntelligentStrategyDecisionMethodforCollaborativeJammingBasedon Hierarchical Multi-Agent Reinforcement Learning," in IEEE Transactions on Cognitive Communications and Networking, vol.10, no. 4, pp. 1467-1480, Aug. 2024, doi: 10.1109/TCCN.2024.3373640.

[12] M. Sameen, K. Han and S. O. Hwang, "PhishHaven—An Efficient Real-Time AI Phishing URLs Detection System," in IEEEAccess, vol. 8, pp. 83425-83443, 2020, doi: 10.1109/ACCESS.2020.2991403.

[13] M.AlmousaandM.Anwar,"AURL-BasedSocialSemanticAttacksDetectionWithCharacter-AwareLanguageModel,"in IEEE Access, vol. 11, pp. 10654-10663, 2023, doi: 10.1109/ACCESS.2023.3241121.

[14] S. Marchal, J. François, R. State and T. Engel, "PhishStorm: Detecting Phishing With Streaming Analytics," in IEEETransactions on Network and Service Management, vol. 11, no. 4, pp. 458-471, Dec. 2014, doi: 10.1109/TNSM.2014.2377295.

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

[16] C.Chen etal.,"APerformance EvaluationofMachineLearning-BasedStreamingSpamTweetsDetection,"in IEEETransactions on Computational Social Systems, vol. 2, no. 3, pp. 65-76, Sept. 2015, doi: 10.1109/TCSS.2016.2516039.

[17] R. R. Rout, G. Lingam and D. V. L. N. Somayajulu, "Detection of Malicious Social Bots Using Learning Automata With URLFeatures in Twitter Network," in IEEE Transactions on Computational Social Systems, vol. 7, no. 4, pp. 1004-1018, Aug. 2020, doi:10.1109/TCSS.2020.2992223.

[18] J.Yuan, G.Chen, S. TianandX. Pei, "Malicious URL Detection Based on a Parallel Neural Joint Model," in IEEE Access, vol. 9, pp. 9464-9472, 2021, doi:10.1109/ACCESS.2021.3049625

[19] Pavithra Goravi Sukumar, Modugu Krishnaiah, Rekha Velluri, Pooja Satish, Sharmila Nagaraju, Nandini Gowda Puttaswamy, Mallikarjuna swamy Srikantaswamy, "An efficient adaptive reconfigurable routing protocol for optimized data packet distribution in network on chips", International Journal of Electrical and Computer Engineering (IJECE)Vol.14, No.1, February2024, pp.305~314, DOI: 10.11591/ijece.v14i1.pp305-314.

[20] Rekha Sathyanarayana, Nataraj Kanathur Ramaswamy, Mallikarjunaswamy Srikantaswamy, Rekha Kanathur Ramaswamy, "Anefficient unused integrated circuits detection algorithm for parallel scan architecture" International Journal of Electrical andComputer Engineering (IJECE)Vol.14, No.1, February2024, pp. 469~478ISSN: 2088-8708, DOI: 10.11591/ijece.v14i1. pp469-478.

[21] Mahendra, H.N., Mallikarjunaswamy, S., Nooli, C.B., Hrishikesh, M., Kruthik, N., Vakkalanka, H.M. (2022). Cloud basedcentralized smart cart and contactless billing system. In 2022 7th International Conference on Communication and ElectronicsSystems (ICCES), Coimbatore, India, pp. 820-826. https://doi.org/10.1109/ICCES54183.2022.9835856.

[22] Mallikarjunaswamy, S., Sharmila, N., Siddesh, G.K., Nataraj, K.R., Komala, M. (2022). A novel architecture for cluster basedfalse data injection attack detection and location identification in smart grid. In: Mahanta, P., Kalita, P., Paul, A., Banerjee, A.(eds) Advances in Thermofluids and Renewable Energy . Lecture Notes in Mechanical Engineering. Springer, Singapore.https://doi.org/10.1007/978-981-16-3497-0_48

[23] Thazeen, S., Mallikarjunaswamy, S., Siddesh, G.K., Sharmila, N. (2021). Conventional and subspace algorithms for mobilesource detection and radiation formation. Traitement du Signal, 38(1): 135-145. https://doi.org/10.18280/ts.380114

[24] Satish, P., Srikantaswamy, M., Ramaswamy, N.K. (2020). A comprehensive review of blind deconvolution techniques for imagedeblurring. Traitement du Signal, 37(3): 527-539. https://doi.org/10.18280/ts.370321

[25] Umashankar, M.L., Ramakrishna, M.V., Mallikarjunaswamy, S. (2019). Design of high speed reconfigurable deploymentintelligent genetic algorithm in maximum coverage wireless sensor network. In 2019 International Conference on Data Scienceand Communication (IconDSC), Bangalore, India, pp. 1-6. https://doi.org/10.1109/IconDSC.2019.8816930

BIOGRAPHIES OF AUTHORS

Nandeesha H D presently working as Assistant Professor in Dept. Of Computer Science and Engineering, JSS Science and Technology University, Mysuru, Karnataka, India. He received Master of technology from Sri Jayachamarajendra College of Engineering. Currently, he is pursuing PhD in cyber security JSS Science and Technology University, Mysuru. His general research interest is in the area of Information and Cyber security, URL Phishing Detection, Web security, Mobile Security, Online Social Network and Machine Learning. He can be contacted at email: hdnandeesh@gmail.com.

ORCHID ID: 0000-0003-2155-8823
Google Scholars ID: UYYPj64AAAAJ

Dr. Prasanna B T received Ph.D. degree from Visvesvaraya TechnologicalUniversity, Karnataka, India in the area of Cloud Security. He has published more than 40 research articles in International Journals and Conferences of high repute including IEEE, Elsevier, ACM, Springer, etc. He is serving as reviewer of Elsevier, IEEE and many reputed Journals. Also he is a life time member of Computer Society of India (CSI).At present he is working as Associate Professor in the Dept. Of Computer science and Engineering, JSS Science and Technology University, Mysuru, Karnataka, India. Author can be contacted at email: prasannabt@sjce.ac.in.

ORCHID ID: 0000-0003-1389-9396
Google Scholars ID:X2bOgsoAAAAJ