*Grenze International Journal of Engineering and Technology, Jan Issue*

# Reinforcement Learning for Adaptive Cybersecurity: A Case Study on Intrusion Detection

Dr. Pratik S. Patel[1], Dr. Tanvi S. Navik[2] and Sakshi Ahuja[3]
[1]National Forensic Science University, Gandhinagar, India
Email: pratik.patel@nfsu.ac.in
[2]C.K Pithawala College of Commerce -Management-Computer Application, Surat, India
Email: tanvinavik2480@gmail.com,
[3]Computer science and Engineering, Vellore Institute of Technology, Chennai, India
Email: connect.sakshi.ahuja@gmail.com

***Abstract*— The evolving landscape of cybersecurity necessitates innovative approaches to counteract the relentless proliferation of cyber threats. Intrusion detection, a cornerstone of cybersecurity, demands adaptability to effectively identify and thwart emerging attack vectors. This research paper explores the fusion of reinforcement learning and cybersecurity, presenting a case study that showcases the application of reinforcement learning techniques in creating an adaptive intrusion detection system. The case study, presented in this paper, encapsulates the essence of our research. We elucidate the experimental setup, dataset selection, choice of reinforcement learning algorithms, and evaluation metrics used to assess the system's adaptability and performance. Our findings reveal the system's ability to dynamically adapt to evolving attack patterns, offering a compelling demonstration of reinforcement learning's potential in bolstering adaptive cybersecurity mechanisms. This paper's contributions extend beyond the case study. Through a meticulous analysis of the results, we discuss the practical implications, advantages, and limitations of employing reinforcement learning in intrusion detection. By showcasing a practical application of reinforcement learning in a critical cybersecurity domain, this research underscores the viability of leveraging autonomous learning mechanisms to fortify defenses against ever-evolving cyber threats.**

***Index Terms*— Cybersecurity; Deep learning; Reinforcement Learning**

## I. INTRODUCTION

In the rapidly evolving landscape of information technology, cybersecurity stands as an indispensable shield against the relentless tide of malicious cyber activities. As organizations and individuals become increasingly reliant on digital systems for communication, commerce, and critical operations, the risk of cyber threats and intrusions has grown proportionally(Adawadkar and Kulkarni, 2022). Among these threats, intrusion detection plays a pivotal role in safeguarding digital assets and maintaining the integrity of networks and systems(Kolias *et al.*, 2016). As attackers employ novel strategies and techniques, intrusion detection systems must evolve in parallel to effectively detect and mitigate these threats(Klein, 2008).The marriage of machine learning and cybersecurity has emerged as a promising avenue to address these challenges. Particularly, reinforcement learning, a subset of machine learning, offers a paradigm that enables systems to learn from their actions and adapt in dynamic environments. This research paper delves into the realm of using reinforcement learning to enhance adaptive cybersecurity, with a specific focus on the context of intrusion

*Grenze ID: 01.GIJET.10.1.30*

detection(Wazid *et al.*, 2022). In today's digitally interconnected world, the safeguarding of sensitive information, critical infrastructure, and personal privacy has become an imperative of paramount importance. The rapid proliferation of interconnected devices and the ubiquitous nature of the internet have brought unprecedented convenience and efficiency, but they have also introduced new avenues for malicious actors to exploit vulnerabilities and breach security measures(Butun, Österberg and Song, 2020). In this context, cybersecurity stands as a vital defense mechanism against the evolving landscape of cyber threats.

Among the multitude of challenges that cybersecurity professionals face, intrusion detection remains a cornerstone. The ability to promptly identify and respond to unauthorized access attempts, data breaches, and malicious activities within complex network environments is crucial for preventing damage and ensuring the integrity of systems. However, the dynamic nature of cyber threats, characterized by their ability to mutate and adapt, necessitates an equally dynamic approach to intrusion detection. Traditional rule-based and signature-based methods, while effective to a certain extent, often struggle to keep pace with the ever-changing tactics employed by cybercriminals. Machine learning techniques have emerged as a powerful tool to enhance the adaptability and accuracy of intrusion detection systems(Wang *et al.*, 2020). Among these techniques, reinforcement learning a paradigm rooted in decision-making processes has garnered attention for its potential to facilitate autonomous learning and adaptability. This research paper delves into the intersection of reinforcement learning and cybersecurity, focusing specifically on the domain of intrusion detection. We present a case study that showcases the application of reinforcement learning algorithms to create an adaptive intrusion detection system capable of autonomously learning and responding to emerging threats.

In today's interconnected digital landscape, the relentless growth of cyber threats has highlighted the critical need for robust and adaptive cybersecurity measures. Among the primary pillars of safeguarding digital assets and sensitive information is intrusion detection(Magaia *et al.*, 2021), a cornerstone of defense against unauthorized access, data breaches, and malicious activities. As the landscape of cyber threats becomes more complex and dynamic, intrusion detection emerges as a vital mechanism to ensure the integrity, confidentiality, and availability of digital systems.

## II. Understanding Of Intrusion Detection

Intrusion detection refers to the process of identifying and responding to unauthorized or malicious activities within computer networks, systems, and applications. This encompasses a broad spectrum of activities, ranging from unauthorized login attempts and malware propagation to sophisticated zero-day exploits(Khraisat *et al.*, 2019). The goal of intrusion detection is twofold: prompt identification of malicious behaviors and timely response to mitigate potential damage. Traditional approaches to intrusion detection have largely relied on rule-based and signature-based methods. Rule-based systems use predefined rules to detect known attack patterns, while signature-based systems compare incoming data to a database of known attack signatures. (Alazab *et al.*, 2014). Intrusion detection systems must keep pace by evolving their capabilities to recognize both known attack patterns and emerging threats that lack predefined signatures.

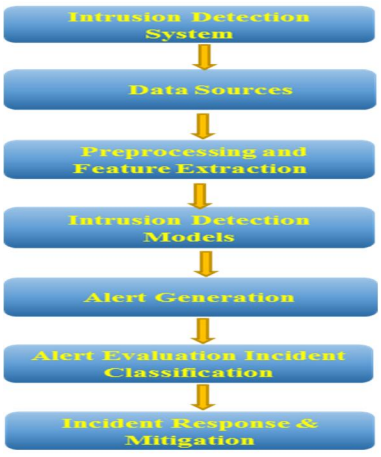


Figure 1: Intrusion detection representation

### *A. An Anomaly-Based Intrusion Detection*

Certainly, here are some equations that capture key aspects of intrusion detection in cybersecurity:

Anomaly detection(Ganeshan *et al.*, 2020) involves comparing incoming data with historical data to identify deviations. One common approach is calculating the anomaly score:

$$\text{Anomaly Score}(x) = | x - \mu | / \sigma$$

Where:
x is the current data point. μ is the mean of historical data. σ is the standard deviation of historical data.

*B. False Positive Rate and True Positive Rate:*

Evaluating the performance of intrusion detection systems often involves false positive rate (FPR) and true positive rate (TPR):

$$FPR = FP / (FP + TN)$$

$$TPR = TP / (TP + FN)$$

Where:
FP is the number of false positives.
TN is the number of true negatives.
TP is the number of true positives.
FN is the number of false negatives.
Precision, Recall, and F1-Score:
Precision, recall, and the F1-score provide a comprehensive view of the detection system's effectiveness:

$$Precision = TP / (TP + FP)$$

$$Recall = TP / (TP + FN)$$

$$F1Score = 2 * (Precision * Recall) / (Precision + Recall)$$

In the context of reinforcement learning, the Bellman equation plays a central role:

$$Q(s, a) = R(s, a) + \gamma * \max(Q(s', a'))$$

Remember that the choice of metrics depends on the specific goals and priorities of your intrusion detection system. Different applications might require different metrics to be emphasized.

TABLE I: PERFORMANCE MATRIC OF INTRUSION DETECTION IN CYBER SECURITY

| **Metric** | **Formula** | **Description** |
|---|---|---|
| True Positive (TP) | - | Instances correctly classified as intrusions. |
| True Negative (TN) | - | Instances correctly classified as normal activities. |
| False Positive (FP) | - | Instances incorrectly classified as intrusions (Type I error). |
| False Negative (FN) | - | Instances incorrectly classified as normal activities (Type II error). |
| Accuracy | (TP + TN) / (TP + TN + FP + FN) | Proportion of correctly classified instances out of the total instances. |
| Precision | TP / (TP + FP) | Proportion of true positive predictions out of the total predicted positive instances. |
| Recall (Sensitivity) | TP / (TP + FN) | Proportion of true positive predictions out of the total actual positive instances. |
| F1-Score | 2 * (Precision * Recall) / (Precision + Recall) | Harmonic mean of precision and recall. |
| Specificity | TN / (TN + FP) | Proportion of true negative predictions out of the total actual negative instances. |
| False Positive Rate (FPR) | FP / (TN + FP) | Proportion of false positive predictions out of the total actual negative instances. |
| False Negative Rate (FNR) | FN / (TP + FN) | Proportion of false negative predictions out of the total actual positive instances. |
| AUC-ROC | - | Area under the Receiver Operating Characteristic curve. Measures discrimination ability at various thresholds. |
| AUC-PR | - | Area under the Precision-Recall curve. Provides insights into performance at different recall and precision levels. |
| Matthews Correlation Coefficient (MCC) | - | Balanced measure that considers true and false positives and negatives. |
| Confusion Matrix | - | Tabular summary of classification model's performance, showing TP, TN, FP, and FN counts. |

It's important to consider the specific context and requirements of your intrusion detection system when selecting and interpreting these metrics(Albdour, Manaseer and Sharieh, 2020). Depending on the application, certain

metrics may be prioritized over others. For instance, in some cases, minimizing false positives might be more critical than achieving high overall accuracy.

## III. Machine Learning

Machine learning plays a pivotal role in revolutionizing the field of cybersecurity, equipping organizations with advanced tools to counter evolving cyber threats(Sarker, 2022). By harnessing the power of algorithms and data analysis, machine learning models can rapidly identify patterns, anomalies, and trends within massive datasets that would be impossible for humans to process manually. Machine learning also enhances malware detection and classification by learning from historical data and adapting to new variants(Das and Morris, 2017). It enables real-time behavioral analysis to distinguish between legitimate user behavior and malicious activities, reducing false positives and improving overall system accuracy. As cyber-attacks become more sophisticated, machine learning empowers security professionals to stay one step ahead in the ongoing battle to safeguard sensitive digital assets and ensure the integrity of critical systems.

### *A. Automated Pattern Recognition*

Machine learning, a subset of artificial intelligence, equips systems with the ability to recognize intricate patterns and relationships within large and complex datasets(Kubassova *et al.*, 2021). In the realm of intrusion detection, machine learning techniques can automatically identify features indicative of cyber-attacks, allowing the system to generalize from historical data and adapt to new attack patterns.

Table II: Result of full data set for different techniques

| S. No. | Technique | Accuracy | Precision | Recall | F1 Score | AUC-ROC |
|---|---|---|---|---|---|---|
| 1. | Logistic Regression | 0.92 | 0.912 | 0.984 | 0.945 | 0.899 |
| 2. | Random Forest | 0.95 | 0.956 | 0.976 | 0.966 | 0.944 |
| 3. | SVM | 0.94 | 0.934 | 0.978 | 0.955 | 0.927 |
| 4. | Neural Network | 0.96 | 0.966 | 0.988 | 0.976 | 0.953 |
| 5. | XGBoost | 0.95 | 0.946 | 0.975 | 0.960 | 0.934 |

### *B. Feature Extraction and Selection*

Machine learning algorithms excel at identifying relevant features from raw data. In the context of cybersecurity, these features could include network packet attributes, traffic behaviors, and system logs(Fatani *et al.*, 2022). Feature extraction and selection are critical in reducing noise and improving the efficiency of the intrusion detection system.

Table III: Feature Extraction Methods

| Feature Extraction Methods | Description |
|---|---|
| Time-based Features | Extract temporal information such as timestamps, day of the week, and time of day. |
| Frequency-based Features | Compute statistics like packet counts, byte counts, and request rates. |
| Protocol-based Features | Extract features based on specific network protocols, including port numbers, IP addresses, etc. |
| Statistical Features | Calculate statistical measures like mean, median, variance, and skewness. |
| Payload Analysis | Analyze payload data, e.g., examining keywords or patterns in packet payloads. |
| Domain-specific Features | Extract features relevant to the specific application or domain, e.g., HTTP headers for web data. |

Table IV: Feature Selection Model

| Feature Selection Methods | Description |
|---|---|
| Correlation Analysis | Identify correlations between features and the target variable; remove highly correlated features. |
| Univariate Selection | Use statistical tests to select features with strong relationships to the target variable. |
| Recursive Feature Elimination | Iteratively remove least important features based on model performance. |
| Embedded Methods | Leverage algorithms that inherently perform feature selection during their training process. |
| Model-Based Selection | Train a model and assess feature importance based on their contributions to model performance. |
| Regularization | Apply techniques like L1 regularization (LASSO) to encourage the use of a subset of features. |
| Dimensionality Reduction | Use techniques like Principal Component Analysis (PCA) to reduce dimensionality while retaining info. |

### *C. Supervised and Unsupervised Learning*

Both supervised and unsupervised machine learning techniques are applicable to adaptive intrusion detection. Supervised learning involves training models on labeled data, enabling them to classify network traffic as normal

or malicious(Talaei Khoei and Kaabouch, 2023). Unsupervised learning, on the other hand, identifies anomalies in network behavior without prior labeling, making it valuable for detecting unknown threats.
Equation for simple linear regression:

$$Y = mx + b$$

where:
y is the predicted output.
x is the input feature.
m is the slope of the line.
b is the y-intercept.
Equation for k-means clustering (for two-dimensional data):

$$\text{Argmin}\sum_{i=0}^{c} \quad n \min_{\mu j} \in C\ (\|x_i - \mu_j\|^2)$$

where:
$n$ is the number of data points.
$x_i$ is the data point.
$\mu_j$ is the centroid of cluster $j$.
$C$ is the set of clusters.
$c$ is the assigned cluster for data poin$x_i$.

*D. Learning From Experience: Reinforcement Learning*

Reinforcement learning, a specialized form of machine learning, is particularly relevant to the adaptive nature of cybersecurity. In reinforcement learning, an agent learns to make decisions through interactions with an environment to maximize cumulative rewards(Sivamayil *et al.*, 2023). In the context of intrusion detection, the agent learns optimal strategies for detecting attacks over time, adapting its behavior to new and emerging threats.

*E. Adaptation and Continuous Learning*

In the realm of cybersecurity, adaptation and continuous learning are paramount. As the threat landscape evolves rapidly, security systems must employ algorithms and strategies that dynamically adapt to emerging threats. Online learning algorithms enable security systems to learn from new attack patterns and adjust their defenses in real-time(Hatzivasilis *et al.*, 2020). Adaptive learning rates ensure that security measures respond effectively to varying levels of threat intensity. Reinforcement learning facilitates the continuous improvement of intrusion detection and prevention systems, enabling them to refine their responses based on the outcomes of previous security incidents(Yang *et al.*, 2023). The concept of concept drift detection becomes crucial in cybersecurity, where models can detect sudden shifts in attack patterns and promptly adjust their defenses. In this landscape, the continuous evolution of threat actors necessitates the use of ensemble methods and transfer learning to incorporate new knowledge while retaining past experience (Xin *et al.*, 2018). This dynamic nature enables the system to respond effectively to evolving tactics employed by cybercriminals.

## IV. Discussion

In this study, we summarized some of the most promising methods used to address various financial problems. We chose the main methodology for our analysis that were primarily based on traditional techniques that are frequently used for time-series forecasting(Ferrag *et al.*, 2020). Many machine-learning methods have been developed recently for the purpose of modeling financial time series. The support vector machine model and random forest classifier belong to this group of algorithms. Support vector machines' core principle is to map data into higher-dimensional spaces where values can be linearly separated from one another in order to find an ideal hyperplane(McCarthy *et al.*, 2022). Before starting training, three key hyperparameters for random forest algorithms must be changed. Some of these are the size of the nodes, the number of trees, and the number of features sampled. These facts have led to a major increase in the usage of several machine learning algorithms, including ANN, LSTM, and RNN(Al-azazi and Ghurab, 2023), for time-series forecasting in recent years. One of the important methods was the artificial neural network (ANN) model. In order to create solutions that are as generalizable as feasible based on the knowledge they already have, ANNs try to find patterns in the data they are given. The financial industry has used ANNs the most, according to the findings that have been presented. The application of RNN and its derivatives, such as LSTM(Sudriani, Ridwansyah and A Rustini, 2019), has been the subject of extensive research in the field of time-series forecasting in recent years. Due to their extraordinary ability

to recognize hidden correlations in data, these models outperformed the typical ANN model in terms of forecasting challenges. The models were able to produce better results thanks to these capabilities. We discussed the subject of developing a successful trading strategy using RL approaches. Because of this, current advancements in this field have integrated DL and RL approaches(Matsuo *et al.*, 2022), utilizing their excellent capacities to produce complex data. The goal of this study was to investigate the reasons why machine learning methods such as deep learning and reinforcement learning (Singh *et al.*, 2022)perform better than approaches based on non-linear algorithms.

Our findings showed that, in the particular security use case of federated intrusion detection, the intrusion detection imposed a modest performance overhead. It is not easy to generalize these conclusions to other applications. On the other hand, some generalizations regarding the characteristics of our methodology can be drawn. Our integration strategy(Preuveneers *et al.*, 2018), in our opinion, is particularly useful for security use cases where inference is carried out directly on raw data. In this scenario, federated learning won't require the expensive transfer of enormous volumes of raw data, which will further minimize the relative performance overhead. Comparable use cases, however, will probably call for the adoption of deeper neural networks with more complex topologies in order to enable automatic feature extraction. In turn, deeper models will have additional performance overhead that is difficult to predict. In order to compute the model changes at each client in the federation, they will first need comparatively more local processing, which could have an impact on the latency of global updates(Chen, Wawrzynski and Lv, 2021). Second, a deeper architecture with more learnable parameters will necessitate storing more data on the blockchain. To validate these hypotheses, a large number of federated learning deployments must be methodically tested in various application situations with varying data types, processing speeds, and network capacities. To illustrate the viability of the proposed method for federated learning and blockchain integration, we employed an intrusion detection security use case in this work. While more sophisticated neural networks have been described in the literature for anomaly and network intrusion detection, the kind of neural network we used in our experiments the auto encoder has a rather straightforward architecture(Gümüşbaş *et al.*, 2021). For deeper or more complicated neural networks, including convolutional neural networks, as well as for other use cases where federated learning could be advantageous, our method is still equally relevant and scalable. A trade-off between the audit frequency of the global model updates and the local rate of convergence on the clients is another effect of the suggested integration technique. Converging faster at the nodes is made possible, on the one hand, by iterating more frequently at each client locally before calculating the federated average. Conversely, fewer local repetitions result in the computation and storage of a greater number of federated averages on the distributed ledger. The machine learning model's auditability is enhanced by more regular blockchain-based model updates.

The main benefit of employing it is that it reduces the amount of time needed to compute while ensuring high-quality work is produced. Currently, there is a growing trend toward the application of deep reinforcement learning-based dynamic trading approaches.(Hu and Lin, 2019) Reinforcement learning can be used to create dynamic trading strategies and solve the problem of sequential decision making. Reinforcement learning, however, excludes the ability to perceive the environment.

## V. CONCLUSION

Reinforcement Learning in Intrusion Detection has emerged as a cutting-edge approach to fortify digital environments against an increasingly sophisticated landscape of cyber threats. This comprehensive investigation into the fusion of reinforcement learning techniques with cybersecurity applications sheds light on the potential of adaptive defense mechanisms that continuously learn and evolve in response to dynamic threats(Oh *et al.*, 2023). As this study delves into the intricacies of the integration, it becomes evident that the marriage of reinforcement learning and cybersecurity heralds a new era of proactive protection and real-time adaptation.

In the realm of cybersecurity, the stakes have never been higher. The proliferation of interconnected systems, the expansion of the attack surface, and the ingenuity of threat actors have collectively underscored the need for innovative defense strategies. Traditional static security measures, while crucial, can be insufficient in a landscape where threats mutate and evolve faster than conventional models can keep pace with. This is where the allure of reinforcement learning comes to the fore(Ahsan *et al.*, 2022). The very essence of reinforcement learning, derived from behavioral psychology, centers on the idea of learning by interacting with an environment to maximize cumulative rewards. This fundamental principle aligns seamlessly with the cybersecurity domain, where security systems need to interact with an ever-changing digital environment to optimize their response and mitigation strategies.

Furthermore, the study delves into the technical aspects that underpin the application of reinforcement learning to intrusion detection. Reinforcement learning algorithms, such as Q-learning(Zhou *et al.*, 2021) and Deep Q-

Networks (DQN)(Mnih *et al.*, 2015), require careful tuning and customization to the specifics of the intrusion detection task. Hyperparameters, network architectures, and training protocols must be tailored to strike a balance between rapid adaptation and convergence to optimal policies. (Chen *et al.*, 2019)The study's findings shed light on the nuances of this process, emphasizing the iterative nature of algorithm development and the significance of rigorous testing and evaluation. Despite the remarkable strides achieved through the case study, challenges and considerations emerge that warrant attention.(Huang, Huang and Zhu, 2022) The application of reinforcement learning in cybersecurity introduces an additional layer of complexity. The vulnerability of the learning process to adversarial attacks, where threat actors manipulate input data to deceive the agent's learning, underscores the need for robustness and resilience(Shaukat *et al.*, 2020). Adversarial training and anomaly detection mechanisms become crucial components of an adaptive defense strategy. Moreover, the computational demands of reinforcement learning, particularly in deep reinforcement learning paradigms, necessitate a careful assessment of resource allocation and scalability in real-world deployment scenarios.

## Future Perspective

Looking ahead, the synergistic relationship between reinforcement learning and cybersecurity holds promise for not only intrusion detection but a myriad of other security applications. From anomaly detection to threat hunting, adaptive defense mechanisms have the potential to revolutionize the cybersecurity landscape. However, this journey is not without challenges – the study sheds light on the need for robustness against adversarial attacks and the optimization of computational resources. As the cyber arms race continues unabated, the fusion of reinforcement learning and cybersecurity offers a beacon of hope – a beacon that illuminates the path towards resilient, proactive, and continuously evolving digital fortifications.

## References


[1] Adawadkar, A. M. K. and Kulkarni, N. (2022) 'Cyber-security and reinforcement learning — A brief survey', Engineering Applications of Artificial Intelligence, 114, p. 105116. doi: https://doi.org/10.1016/j.engappai.2022.105116.

[2] Ahsan, M. et al. (2022) 'Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review', Journal of Cybersecurity and Privacy, pp. 527–555. doi: 10.3390/jcp2030027.

[3] Al-azazi, F. A. and Ghurab, M. (2023) 'ANN-LSTM: A deep learning model for early student performance prediction in MOOC', Heliyon, 9(4), p. e15382. doi: https://doi.org/10.1016/j.heliyon.2023.e15382.

[4] Alazab, A. et al. (2014) 'Using response action with intelligent intrusion detection and prevention system against web application malware', Information Management & Computer Security, 22(5), pp. 431–449. doi: 10.1108/IMCS-02-2013-0007.

[5] Albdour, L., Manaseer, S. and Sharieh, A. (2020) 'IoT Crawler with Behavior Analyzer at Fog layer for Detecting Malicious Nodes', International Journal of Communication Networks and Information Security, 12, pp. 83–94. doi: 10.17762/ijcnis.v12i1.4459.

[6] Butun, I., Österberg, P. and Song, H. (2020) 'Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures', IEEE Communications Surveys & Tutorials, 22(1), pp. 616–644. doi: 10.1109/COMST.2019.2953364.

[7] Chen, D., Wawrzynski, P. and Lv, Z. (2021) 'Cyber security in smart cities: A review of deep learning-based applications and case studies', Sustainable Cities and Society, 66, p. 102655. doi: https://doi.org/10.1016/j.scs.2020.102655.

[8] Chen, T. et al. (2019) 'Adversarial attack and defense in reinforcement learning-from AI security view', Cybersecurity, 2(1), p. 11. doi: 10.1186/s42400-019-0027-x.

[9] Das, R. and Morris, T. (2017) Machine Learning and Cyber Security. doi: 10.1109/ICCECE.2017.8526232.

[10] Fatani, A. et al. (2022) 'Advanced Feature Extraction and Selection Approach Using Deep Learning and Aquila Optimizer for IoT Intrusion Detection System', Sensors. doi: 10.3390/s22010140.

[11] Ferrag, M. A. et al. (2020) 'Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study', Journal of Information Security and Applications, 50, p. 102419. doi: https://doi.org/10.1016/j.jisa.2019.102419.

[12] Ganeshan, R. et al. (2020) 'A Systematic Review on Anomaly Based Intrusion Detection System', IOP Conference Series: Materials Science and Engineering, 981(2), p. 22010. doi: 10.1088/1757-899X/981/2/022010.

[13] Gümüşbaş, D. et al. (2021) 'A Comprehensive Survey of Databases and Deep Learning Methods for Cybersecurity and Intrusion Detection Systems', IEEE Systems Journal, 15(2), pp. 1717–1731. doi: 10.1109/JSYST.2020.2992966.

[14] Hatzivasilis, G. et al. (2020) 'Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees', Applied Sciences, 10, p. 5702. doi: 10.3390/app10165702.

[15] Hu, Y.-J. and Lin, S.-J. (2019) 'Deep Reinforcement Learning for Optimizing Finance Portfolio Management', in 2019 Amity International Conference on Artificial Intelligence (AICAI), pp. 14–20. doi: 10.1109/AICAI.2019.8701368.

[16] Huang, Y., Huang, L. and Zhu, Q. (2022) 'Reinforcement Learning for feedback-enabled cyber resilience', Annual Reviews in Control, 53, pp. 273–295. doi: https://doi.org/10.1016/j.arcontrol.2022.01.001.

[17] Khraisat, A. et al. (2019) ‘Survey of intrusion detection systems: techniques, datasets and challenges’, Cybersecurity, 2(1), p. 20. doi: 10.1186/s42400-019-0038-7.
[18] Klein, A. (2008) ‘Attacks on the RC4 stream cipher’, Designs, Codes and Cryptography, 48(3), pp. 269–286. doi: 10.1007/s10623-008-9206-6.
[19] Kolias, C. et al. (2016) ‘Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset’, IEEE Communications Surveys & Tutorials, 18(1), pp. 184–208. doi: 10.1109/COMST.2015.2402161.
[20] Kubassova, O. et al. (2021) ‘Chapter 1 - History, current status, and future directions of artificial intelligence’, in Mahler, M. B. T.-P. M. and A. I. (ed.). Academic Press, pp. 1–38. doi: https://doi.org/10.1016/B978-0-12-820239-5.00002-4.
[21] Magaia, N. et al. (2021) ‘Industrial Internet-of-Things Security Enhanced With Deep Learning Approaches for Smart Cities’, IEEE Internet of Things Journal, 8(8), pp. 6393–6405. doi: 10.1109/JIOT.2020.3042174.
[22] Matsuo, Y. et al. (2022) ‘Deep learning, reinforcement learning, and world models’, Neural Networks, 152, pp. 267–275. doi: https://doi.org/10.1016/j.neunet.2022.03.037.
[23] McCarthy, A. et al. (2022) ‘Functionality-Preserving Adversarial Machine Learning for Robust Classification in Cybersecurity and Intrusion Detection Domains: A Survey’, Journal of Cybersecurity and Privacy, pp. 154–190. doi: 10.3390/jcp2010010.
[24] Mnih, V. et al. (2015) ‘Human-level control through deep reinforcement learning’, Nature, 518(7540), pp. 529–533. doi: 10.1038/nature14236.
[25] Oh, S. H. et al. (2023) ‘Applying Reinforcement Learning for Enhanced Cybersecurity against Adversarial Simulation’, Sensors. doi: 10.3390/s23063000.
[26] Preuveneers, D. et al. (2018) ‘Chained Anomaly Detection Models for Federated Learning: An Intrusion Detection Case Study’, Applied Sciences. doi: 10.3390/app8122663.
[27] Sarker, I. H. (2022) ‘Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects’, Annals of Data Science. doi: 10.1007/s40745-022-00444-2.
[28] Shaukat, K. et al. (2020) ‘Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cybersecurity’, Energies. doi: 10.3390/en13102509.
[29] Singh, V. et al. (2022) ‘How are reinforcement learning and deep learning algorithms used for big data based decision making in financial industries–A review and research agenda’, International Journal of Information Management Data Insights, 2(2), p. 100094. doi: https://doi.org/10.1016/j.jjimei.2022.100094.
[30] Sivamayil, K. et al. (2023) ‘A Systematic Study on Reinforcement Learning Based Applications’, Energies. doi: 10.3390/en16031512.
[31] Sudriani, Y., Ridwansyah, I. and A Rustini, H. (2019) ‘Long short term memory (LSTM) recurrent neural network (RNN) for discharge level prediction and forecast in Cimandiri river, Indonesia’, IOP Conference Series: Earth and Environmental Science, 299(1), p. 12037. doi: 10.1088/1755-1315/299/1/012037.
[32] Talaei Khoei, T. and Kaabouch, N. (2023) ‘A Comparative Analysis of Supervised and Unsupervised Models for Detecting Attacks on the Intrusion Detection Systems’, Information. doi: 10.3390/info14020103.
[33] Wang, Y. et al. (2020) ‘BSV-PAGS: Blockchain-based special vehicles priority access guarantee scheme’, Computer Communications, 161, pp. 28–40. doi: https://doi.org/10.1016/j.comcom.2020.07.012.
[34] Wazid, M. et al. (2022) ‘Uniting cyber security and machine learning: Advantages, challenges and future research’, ICT Express, 8(3), pp. 313–321. doi: https://doi.org/10.1016/j.icte.2022.04.007.
[35] Xin, Y. et al. (2018) ‘Machine Learning and Deep Learning Methods for Cybersecurity’, IEEE Access, 6, pp. 35365–35381. doi: 10.1109/ACCESS.2018.2836950.
[36] Yang, A. et al. (2023) ‘Application of meta-learning in cyberspace security: a survey’, Digital Communications and Networks, 9(1), pp. 67–78. doi: https://doi.org/10.1016/j.dcan.2022.03.007.
[37] Zhou, S. et al. (2021) ‘Autonomous Penetration Testing Based on Improved Deep Q-Network’, Applied Sciences. doi: 10.3390/app11198823.