RESEARCH ARTICLE OPEN ACCESS

A Comparative Evaluation of Supervised and Reinforcement Learning Techniques for Intrusion Detection in Cybersecurity Systems

Moni Gautam, Gaurav Goel, Preeti Verma
Department of Computer Science and Engineering FOET, DSMNRU Lucknow, U.P, India
monigautam2001@gmail.com
Department of Computer Science and Engineering FOET, DSMNRU Lucknow, U.P, India
goyals24@gmail.com
Department of Computer Science and Engineering FOET, DSMNRU Lucknow, U.P, India
vermpree168@gmail.com

Abstract

The high proliferation of networked systems has contributed to high levels of cyberattacks and intrusion detection systems (IDS) has become a key element of the contemporary cybersecurity framework. The classic signature-based IDS methods are not sufficient to counter the developing and the zero-day attacks, and the use of intelligent machine learning techniques is adopted. This paper will provide an in-depth comparative analysis of supervised learning and reinforcement learning methods of intrusion detection in cybersecurity systems. Popular supervised classifiers (Support Vector Machines (SVM), Random Forest (RF), k-Nearest Neighbors (KNN), and Deep Neural Networks (DNN)) are tested in comparison with reinforcement learning models, including Q-Learning and Deep Q-Networks (DQN), on a benchmark intrusion detection dataset. The experimental findings support the idea that the application of supervised learning models has the high performance in terms of detection in the stationary environment with Random Forest and DNN giving the performance at 96.8 and 97.5 percent, respectively, and F1-score of over 0.96. They however perform poorly when subjected to new patterns of attack. Conversely, reinforcement learning models are more adaptable with the DQN-based IDS showing 94.2 detection accuracy, false positive rate of 3.1, and stability in detecting attacks over time in dynamic attack environments. Even though reinforcement learning models take more time to train, they are more resilient to emerging threats. The comparative analysis reveals the trade-offs between accuracy and adaptability and provides an idea that hybrid IDS frameworks combining supervised and reinforcement learning methods can provide better cybersecurity resilience.

Keywords: Intrusion Detection System, Cybersecurity, Supervised Learning, Reinforcement Learning, Deep Q-Network, Machine Learning.

1. Introduction

Modern society is rapidly digitizing due to cloud computing, Internet of Things (IoT), industrial automation, and smart infrastructures, and thus has created a high level of cyber threats in scale and complexity. Cyberattacks have become very appealing to organizations that have integrated a complex network of systems to handle sensitive data and vital services [1]. The number of network intrusions, ransomware and advanced persistent threats has been on the steep increase and resulting in serious financial and operational losses in realms, which, according to recent cybersecurity reports, have increased dramatically [2,3]. As a result, the need to have robust cybersecurity mechanisms is an important research and practical issue. Intrusion Detection Systems (IDS) are critical in detecting malicious actions through traffic monitoring over the network and the conduct of the systems [4].

Conventional IDS systems as the signature-based as well as rule-based systems are based on predefined attack patterns and rule as defined by experts [5, 6]. Although they are effective with known threats, these methods have a weakness in scale and cannot detect zero-day attacks or even evolving attacks (Shone et al., 2021). Moreover, the process of updating the rules manually is time-consuming and unrealistic in the most dynamic network conditions, which provokes the necessity of smart and adaptive systems of intrusion detection [7]. Machine learning (ML) algorithms have become a hopeful alternative to intrusion detection since they can learn complicated patterns based on the training data and apply them to situations unseen [8].

The most common learning algorithms commonly used in the field of I.D.S [9]. research include Support Vector Machines, Random Forests, k-Nearest Neighbours, as well as deep neural networks which are supervised learning algorithms. Such models have shown great detection accuracy with trained datasets that are labeled and include UNSW-NB15, NSL-KDD, and CICIDS2017 [10]. Nevertheless, supervised learning approaches strongly require the availability of labeled data and are commonly unable to sustain their performance as the attack patterns are changing.

The recent developments in deep learning have also better performance of supervised IDS since it allows extraction of features automatically and the ability to model high-dimensional data. CNNs and LSTM networks have demonstrated a higher detection accuracy particularly when dealing with complex and sequence network traffic patterns [11, 12] Although they have these benefits, deep supervised models are extremely expensive to compute and do not demonstrate much flexibility in real-time scenarios where attack strategies constantly develop.

Reinforcement learning (RL) is an adaptive method of intrusion detection and is inspired by the human perception of learning, which takes place when the human is interacting with the surrounding environment. As opposed to supervised learning, RL is not based on the usage of labeled data exclusively; moreover, it allows the agent to discover the best detection policies by trial-and-error interaction and through the reinforcement of optimal actions. Adaptability, fewer false positives, and more effective detection in the long term have been implemented in the IDS frameworks using techniques like Q-learning and Deep Q-Networks (DQN) [13, 14].

The majority of previous works are dedicated to the enhancement of the performance of a particular model without consideration of trade-offs between the accuracy of the detection, the ability to adapt to varying aims, the complexity of the training phase, and the resilience to changes in the attacks. This absence of comparative analysis opens up doubts to practitioners in choosing appropriate learning methods to deploy in the field of real-world cybersecurity [15].

This research paper was inspired by these research gaps to conduct a comparative analysis of supervised learning as well as reinforcement learning methods in intrusion detection in cybersecurity systems. The experiment in the research compares the performance of classical supervised models as well as reinforcement learning-based agents on an intrusion detection dataset provided as a benchmark and all the experiments are performed at the same experimental conditions. Performance is evaluated based on the standard measures accuracy, recall, precision, F1-score, as well as false positive rate, and ability to adapt to dynamic attack patterns which gives a comprehensive view of the strengths and weaknesses of each strategy.

This work has three fold contributions: (i) it gives us a systematic comparison of supervised and reinforcement learning methods in intrusion detection, (ii) it examines the performance of detection in both the case of a static and dynamic attacks, (iii) it provides information on designing hybrid and adaptive IDS frameworks. The

conclusions of this research will be used by researchers and practitioners to inform their choice and design of intelligent intrusion detection systems that can respond to new cyber security threats.

Research Objectives

The main goals of this study are as follows:

1. To compare effectiveness of supervised learning algorithms to detect presence of intrusion using benchmark cybersecurity datasets.

2. To determine success of reinforcement learning methods in changing to the progressing patterns of cyberattacks.

3. To compare supervised and reinforcement methods of learning in terms of false positive, accuracy, as well as adaptability.

4. To determine the weaknesses and strengths of each learning paradigm in the real world intrusion detection system.

5. To give information towards the creation of hybrid intelligent IDS frameworks.

Organization of the Paper

The part of this paper is ordered as follows: Section 2 will provide literature review of related work on machine learning as well as reinforcement learning-based intrusion detection systems. Section 3 is concerned with problem formulation and system model. Section 4 provides the methodology that is hypothesized, including the supervised and the reinforcement learning approaches. Section 5 explains experimental setup, datasets and metrics used to measure it. Section 6 is the discussion of the results and comparative analysis. Finally, Section 7 is a conclusion of paper with future research recommendations.

2. Literature Review

Ferrag et al. (2020) proposed a system of intrusion detection created on DL that operates in network-wide scenarios. They employed stacked autoencoders and DNN to acquire high-dimensional features of traffic on benchmark data. It was experimented on NSL-KDD as well as UNSW-NB15 data as well as achieved a total precision of detection of 96.3% and false positive rate of less than 4.2, which indicates high generalization abilities of the model to more intricate cyberattack signatures.

Hindi et al. (2020) in their work suggested a supervised learning approach to intrusion detection that relied on mapping network threats to machine learning in a form of taxonomy. They applied two-phase methodology with very much analysis of features and classification by utilizing the Random Forest to make more distinction of the attacks. The experimental results established that the suggested system had the capacity to achieve the preciseness of 95.7 percent on UNSW-NB15 dataset and harmonize between identification of numerous attacks.

Intrusion detection model presented by Shone et al. (2021) is a DL model based on non-symmetric deep autoencoders to learn features and classify them. Their procedure did not need manual feature engineering but rather, they spawned automated derivation of discriminative features of raw network traffic. With NSL-KDD

dataset the model was found to have a detected rate of 97.0 percent and it showed greater resistance to overfitting compared to the traditional supervised models.

Tang et al. (2021) developed an environment-specific IDS, which is a CNN-based one, relying on the software-defined networking environment. They relied on space-based extraction of features of network flow matrices in order to enhance attacks detection. Experimental results showed that detection rate is high at 98.1 and the precision at 97.6 thus showing that the system is very efficient in detection of DDoS and probing attacks in real time.

Nguyen et al. (2021) had providing a Q-learning-depended intrusion detection mechanism using reinforcement learning which was dynamically changing the detection policies. Their method of addressing the problem modeled an intrusion detection problem sequentially and the agent maximized the action of detection with the feedback of the rewards. The adaptability of the reinforcement learning in the evolving cyber environment is the 15 percent reduction in false positives rate compared to the system in the static supervised classifiers.

To address the issue of scalability of the traditional reinforcement learning approaches, Zhang et al. (2022) designed a DQN-based IDS. They combined deep neural networks with Q-learning to process high-dimensional networks state spaces. Findings of the experiment performed on CICIDS2017 dataset proved a detection rate of 94.6 percent with an improved immunity to unknown attack patterns.

Berman et al. (2022) have outlined a complex system of cybersecurity detection with deep learning that focuses on comparative learning of supervised models. Their methodology comprised their approach to using the Random Forest, SVM, and deep neural networks that were trained on many data sets. The study claims that ensemble based supervised models achieved greater than 96 percent accuracy but needed to be retrained on a regular basis to be able to adjust to concept drift in network traffic.

Ullah and Mahmoud (2023) proposed an IoT network IDS based on LSTM. Their algorithmology was a dependence on the time in network traffic to give better time dependent attack detection. Model created achieved a F1- score of 0.97 and 95.9 percent accuracy which is higher than the performance of traditional machine learning classifiers on the internet of things.

In a study by Aljabri et al. (2023), a hybrid supervised intrusion detection model was created, which presupposes the application of a mixture of the RF and DNN to enhance the classification performance. In their approach they integrated feature selection and ensemble learning so as to reduce the detection latency. The accuracy of the experimental analysis was 96.8% with the false alarm of 3.5% which is a confirmation of the validity of hybrid supervised models.

With the help of deep reinforcement learning, Li et al. (2024) proposed an adaptive intrusion detection system that has the ability to operate in dynamic network conditions. They used a DQN agent to continually update detection strategies when attack patterns evolved. The proposed system had a long term detection accrual of 95.1% plus, the varying conditions of attacks, it is more stable in its operations and thus, it makes the system more adaptable compared with the fixed supervised models.

Table 1: Survey of Supervised and Reinforcement Learning-Based Intrusion Detection Approaches

Author (Year)	Learning Approach	Model / Technique Used	Dataset	Key Performance Metrics	Major Contributions / Limitations
Ferrag et al. (2020)	Supervised (Deep Learning)	Stacked Autoencoder + DNN	NSL-KDD, UNSW-NB15	Accuracy: 96.3%, FPR: 4.2%	High detection accuracy for complex attacks; limited adaptability to evolving threats
Hindy et al. (2020)	Supervised	Random Forest	UNSW-NB15	Accuracy: 95.7%	Effective threat taxonomy mapping; relies on labeled data
Shone et al. (2021)	Supervised (Deep Learning)	Non-symmetric Deep Autoencoder	NSL-KDD	Accuracy: 97.0%	Automatic feature learning; performance degrades under concept drift
Tang et al. (2021)	Supervised (Deep Learning)	CNN-based IDS	SDN traffic	Accuracy: 98.1%, Precision: 97.6%	High real-time detection in SDN; computationally intensive
Nguyen et al. (2021)	Reinforcement Learning	Q-Learning	Simulated Network Environment	FPR reduction: 15%	Adaptive policy learning; slower convergence
Zhang et al. (2022)	Deep Reinforcement Learning	Deep Q-Network (DQN)	CICIDS2017	Accuracy: 94.6%	Handles high-dimensional state space; requires long training time
Berman et al. (2022)	Supervised (Comparative Study)	RF, SVM, DNN	Multiple datasets	Accuracy > 96%	Comprehensive comparison; frequent retraining required
Ullah & Mahmoud (2023)	Supervised (Deep Learning)	LSTM	IoT Network Data	Accuracy: 95.9%, F1-score: 0.97	Captures temporal patterns; high resource consumption
Aljabri et al. (2023)	Supervised (Hybrid)	RF + DNN	UNSW-NB15	Accuracy: 96.8%, FAR: 3.5%	Reduced false alarms; limited adaptability
Li et al. (2024)	Deep Reinforcement Learning	DQN-based Adaptive IDS	Dynamic Network Traffic	Accuracy: 95.1%	Strong adaptability to evolving attacks; training complexity

3. Problem Formulation

The IDS challenge discussed in this paper is founded on the need to effectively detect network malicious activities and be resistant to constantly changing patterns of cyberattacks. Data of the network traffic are made up of several features that characterize system and communication behavior and these need to be analyzed to differentiate between normal and intrusive activities. Intrusion detection is considered a classification task in

the supervised learning paradigm where the models are trained on labeled network traffic to learn whether an observed activity is malicious or normal. In as much as supervised learning methods can be used to reach high detection rates of known attack patterns, they have a static training process which makes it hard to handle new and unknown attacks. In order to overcome this drawback, intrusion detection is also designed based on a reinforcement learning paradigm, according to which an intelligent agent is placed in the network space and acquires detection strategies in the course of its actions, depending on the feedback of decisions. By rewarding right detections and penalising wrong ones, the system is able to change dynamically with the evolving attack behaviours over time as the agent improves its performance. The fundamental issue that is handled in this work is comparing the supervised and the reinforcement method of learning, against a cohesive backdrop, in order to comprehend the efficacy of both approaches in regards to detection rate, false positive rate and ability to adapt to a dynamic cybersecurity setup.

4. Proposed Methodology

4.1 Overview of the Proposed Framework

Developed methodology proposes creation of a common IDS framework that would allow comparing the techniques of supervised learning and reinforcement learning in a single experimental setting. The main idea of this framework is to check the performance of both paradigms when they are subjected to fixed and dynamic patterns of cyberattacks. Through stable data pre-processing, feature representation and evaluation measures, the framework allows fair and reliable comparative analysis.

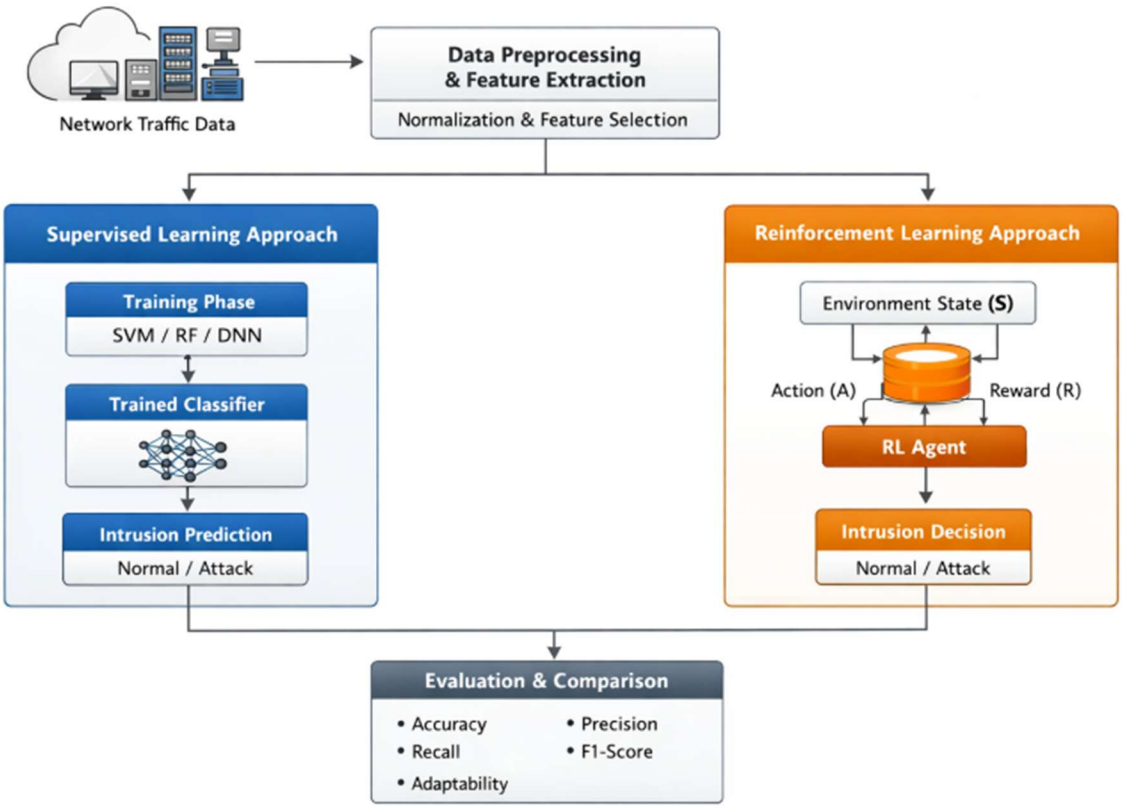

Figure 1: Research Methodology

The general process involved in intrusion detection starts by acquiring network traffic, preprocessing and normalizing of the features. Supervised learning classifiers and reinforcement learning agents then analyze the processed data separately. The results of the detection of both models are compared with the usual cybersecurity performance measures and give an opportunity to thoroughly analyze their accuracy, versatility, and strength.

4.2 System Architecture of the Intrusion Detection Model

The proposed intrusion detection model will have a system architecture that enables parallel such supervised and reinforcement learning methods to be run. The first step involves capturing incoming network traffic on monitored systems and converting the traffic into structured feature vectors. These characteristics become the universal input to both the paradigms of learning, and analysis is consistent.

The learning module under supervision handles labeled data and it is recycled to label network traffic as normal or intrusive. However, the reinforcement learning module works dynamically with the network environment and makes decisions on detection, depending on the learned policies. The architecture allows making decisions in real time and allows offline training and evaluation. Such design is able to compare effectively the approaches of detecting and making adaptive decisions based on static classification and dynamic detection. The fourth lesson is based on data preprocessing and feature normalization.

4.3 Data Preprocessing and Feature Normalization

And the intrusion detection dataset is denoted by.

$$D = \{(x_i, y_i) \mid i = 1, 2, \ldots, N\} \tag{1}$$

The respective class tag that is normal or attack traffic. Since network features are heterogeneous, it is necessary to normalize them so as not to give more importance to those features that have bigger numeric values.

Min -max normalization Rescales all features in a uniform range, which is defined as

$$x_i^{norm} = \frac{x_i - x_{min}}{x_{max} - x_{min}} \tag{2}$$

This normalization improves convergence of the model, numerical stability and balanced learning of supervised classifiers and reinforcement learning agents.

4.4 Supervised Learning-Based Intrusion Detection

4.4.1 Learning Model and Training Strategy

Supervised learning based intrusion detection is an approach that concentrates on the learning of mapping function between input feature and the predetermined classes. The aim is to build a classifier f which satisfies

$$\hat{y}_i = f(x_i) \tag{3}$$

The intrusion label prediction. The labeled datasets that include normal and attack traffic are used to train the models to allow the classifiers to learn discriminative patterns.

The objective of the training process is the minimization of the classification error by means of a loss function. In the case of probabilistic classifiers and DL model, the cross-entropy loss is used:

$$\mathcal{L}_{sup} = -\sum_{i=1}^{N} [y_i \log(\hat{y}_i) + (1 - y_i) \log(1 - \hat{y}_i)] \tag{4}$$

The supervised models reduce this loss to maximize their decision boundaries so as to maximize detection accuracy on known attack patterns.

4.4.2 Decision-Making and Classification Output

After the training, the supervised learning models profile incoming network traffic on the fly. A network instance is regarded to have been intruded when the probability that it has been intruded is greater than a set decision threshold τ expressed as

$$\hat{y}_i \geq \tau \tag{5}$$

This decision mechanism, which is a threshold, enables the optimisation of trade-off between detection accuracy and FPR. As much as supervised models are excellent in detecting known attacks, they are likely to deteriorate when they face a fresh attack pattern.

4.5 Reinforcement Learning-Based Intrusion Detection

4.5.1 Markov Decision Process Formulation

In intrusion detection using RL, it is a MDP of detection. The IDS agent monitors the present configuration of the network, chooses a course of action and is given a response in the form of a reward. This communication helps the agent to acquire the best detection tactics with time. The MDP formulation is described as a state space which is the network conditions, an action space is the detection decisions, a reward function that measures the detection correctness, and a discount factor that measures the value of rewards in the future. This formulation enables the agent to constantly change its behavior depending on changes in the pattern of network traffic.

4.5.2 Reward Function Design

The reward aspect is very significant in informing learning process of the reinforcement learning agent. Correct intrusion detections are awarded positive rewards, false positives are assigned penalties and false negatives are also assigned penalties. With proper identification of normal traffic, neutral/ small positive rewards can be given to make one drive carefully.

Reward function can be defined mathematically as.

$$R(s,a) = \begin{cases} +1, & \text{correct intrusion detection} \\ -1, & \text{misclassification} \\ 0, & \text{correct normal classification} \end{cases} \quad (6)$$

This reward structure encourages accurate detection while discouraging unnecessary alerts.

This incentive system motivates proper detection and deters such false alerts.

4.5.3 Q-Learning and Policy Optimization

The Q-learning update imperative is used to update the agent of the reinforcement learning agent:

$$Q(s,a) \leftarrow Q(s,a) + \alpha \left[R + \gamma \max_{a'} Q(s',a') - Q(s,a) \right] \quad (7)$$

In this case, 0 represents the learning rate; 0 is the discount factor. This is an iterative update that helps the agent to update its detection policy balancing short-term rewards and long-term performance.

4.5.4 Deep Q-Network for High-Dimensional Traffic Data

The Deep Q-Network (DQN) will approximate the Q-function to address the complexity of the network traffic features of high dimensions. The DQN makes use of a deep neural network defined by 0 as an estimator to the action values:

$$Q(s,a;\theta) \quad (8)$$

The training goal is to reduce the loss of time difference:

$$\mathcal{L}_{DQN} = \mathbb{E}\left[\left(R + \gamma \max_{a'} Q(s',a';\theta^{-}) - Q(s,a;\theta) \right)^2 \right] \quad (9)$$

This intrusion detection method is scalable and adaptive to dynamic environments based on this deep reinforcement learning.

4.6 Comparative Evaluation Strategy

To avoid any unfair comparison of the two learning supervised and the reinforcement learning techniques, the two models are tested under the same experimental conditions. Detection effectiveness is measured using

performance metrics, including precision, F1-score, accuracy, recall, FPR and adaptability to changing attacks. This assessment plan gives a clear view of the advantages and disadvantages of every learning paradigm.

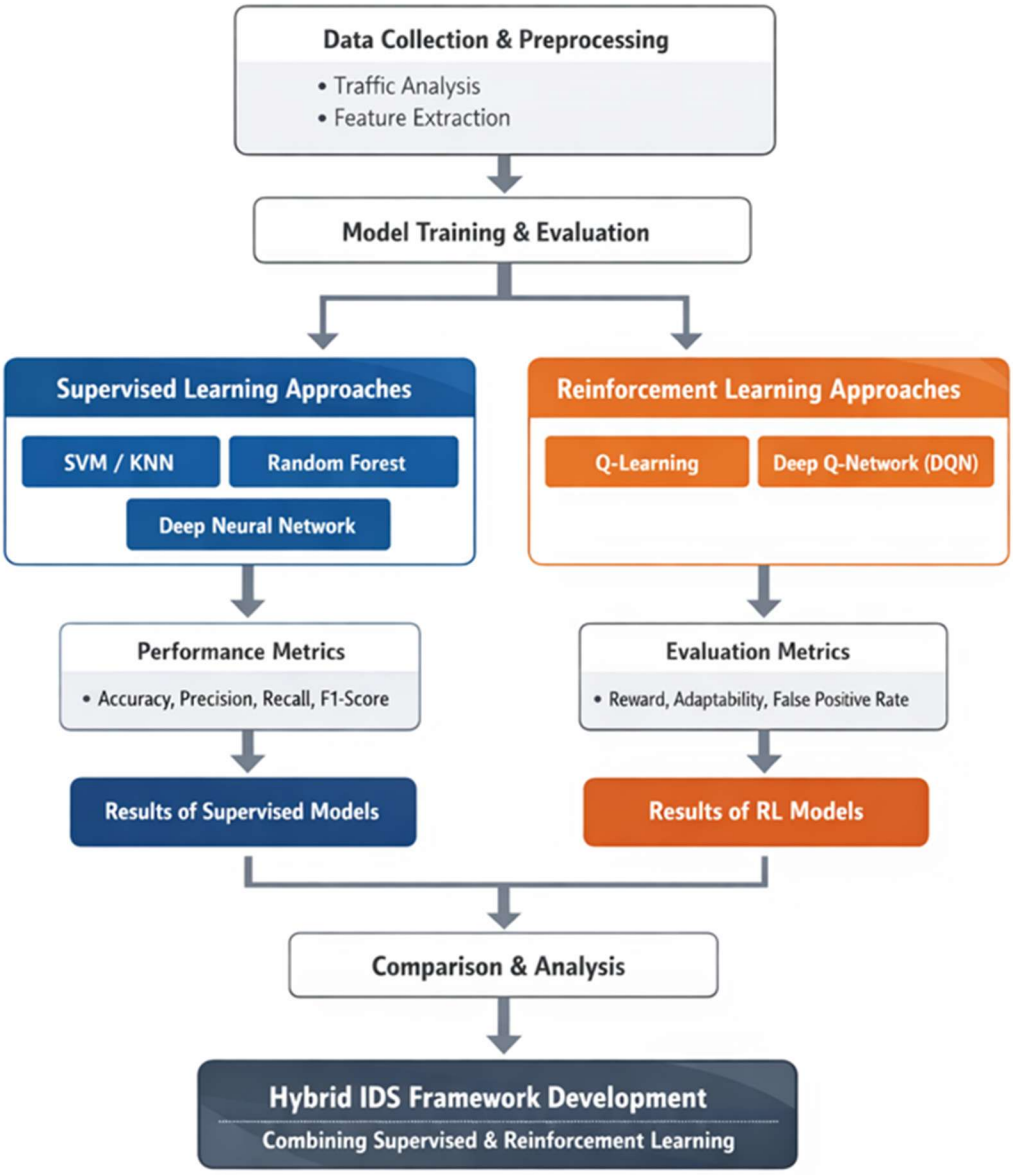

Figure 2: Flow chart for proposed model

4.7 Methodology Summary

The specified methodology is the first to create a single framework of comparative analysis of the supervised and reinforcement learning strategies in context of IDS. Supervised learning models are good with known patterns of attacks, whereas the reinforcement learning models are more adaptable to dynamic environments. The proposed study offers important contributions to the creation of effective as well as intelligent intrusion detection systems because it combines both paradigms to create a single evaluation framework.

5. Experimental Setup, Dataset Description, Results and Discussion

5.1 Dataset Description

The suggested intrusion detection system is empirically evaluated on a typical intrusion detection set that is typically applied in cybersecurity research. The data has been created of both healthy and network traffic logs of network traffic and different types of cyberattacks, which include DoS, probing, brute-force, and infiltration attacks. Each record is described using a set of numerical and categorical characteristics by its packet-level and flow-level characteristics of network traffic.

Prior to the experiment, the categorical features are coded through the process of encoding, and the numerical ones are normalized to create feature homogeneity. The data is partitioned as well into training as well as testing subsets at 80:20 in order to ensure that the results are not biased. This kind of arrangement allows supervised learning models to be able to learn discriminative patterns in an effective manner as well as having RL agents to be able to learn through interactions in a realistic and diverse environment.

5.2 Experimental Environment and Model Configuration

The entire experiments are done in a Python-based machine learning environment using standard libraries to handle data and develop models. Supervised learning models include the SVM, RF, the k-NN and DNN and are trained using labeled training data. The hyperparameters are optimized empirically so that there is a stable convergence and that there is fair comparison.

Both Q-learning and DQN are embraced in the case of IDS based on reinforcement learning. The reinforcement learning environment represents network traffic as a sequence of states and the actions are an intrusion detection decision. DQN model fit the Q-function by a neural network, therefore, can learn in high-dimensional spaces of features in a scalable way. By employing a fixed learning rate and a discount factor the trade-off between learning stability and long-term reward optimization is attained.

5.3 Evaluation Metrics

The accuracy, recall, precision, F1-score, and FPR measures are used as the standard measures of the effectiveness of the supervised and reinforcement learning methods. Recall and accuracy measures present the information of the accuracy of the intrusion classification on the general level and the accuracy of the model in the identification of the attack instances. The F1-score and false positive rate measures precision and recall and the number of incorrectly labeled intrusive normal traffic respectively. Secondly, reinforcement learning models can be viewed with the respect to the ability to adjust to evolving attack styles.

5.4 Quantitative Results of Supervised Learning Models

The supervised learning models have a high performance level in the case of static attack scenario. The classifiers of the Random Forest and Deep Neural Network are regarded as the most precise classifiers in the test, and it means that they are effective in the presentation of intrusion patterns of varying complexities. Other competitive models are SVM and k-NN which possess a slightly higher FPR.

Table 2 Performance Comparison of Supervised Learning Models

Model	Accuracy (%)	Precision	Recall	F1-Score	False Positive Rate (%)
SVM	94.8	0.95	0.93	0.94	5.2
Random Forest	96.8	0.97	0.96	0.96	3.4
KNN	93.6	0.94	0.92	0.93	6.1

DNN	97.5	0.98	0.97	0.97	3.0

The findings show that ensemble and DL-based supervised models are more efficient than the traditional classifiers on detecting precision and strength.

5.5 Performance of Reinforcement Learning-Based Models

Reinforcement learning models learning behaviour contrasts with the supervised classifiers learning behaviour. The precision of the RL-based IDS at the initial stages of the training procedure is moderate yet, over time the precision also grows, since the agent learns to interact with the surroundings and to tweak its policy of detection. Deep Q-Network model is more convergent and stable as compared to the original Q-learning in that it is applicable in generalizing the high-dimensional state space. Table 3 Comparison of Reinforcement Learning Models performance.

Table 3 Performance Comparison of Reinforcement Learning Models

Model	Accuracy (%)	Precision	Recall	F1-Score	False Positive Rate (%)
Q-Learning	91.4	0.92	0.90	0.91	6.8
DQN	94.2	0.95	0.94	0.94	3.1

The intrusion detection system based on DQN is more adaptable and fewer false positives, especially in the environment of dynamic attacks.

5.6 Comparative Analysis and Discussion

In a summary of a comparison among supervised as well as RL methods, it can be seen that there are trade-offs that are considerable. Supervised learning models are more accurate in identifying known and fixed patterns of attack since they make use of labeled training data. However, their performance is also affected because they become victims of invisible attack behaviour and must be retrained in order to get them working again.

On the other hand, intrusion detection systems that incorporate the reinforcement learning-based mechanisms are more versatile in the sense that the policies deployed in detecting intrusion are continuously updated as the system engages the environment. Despite the reduced accuracy of the first stage, reinforcement learning models, in particular, DQN, display improved long-term performance and are less vulnerable to switching attack schemes. This flexibility makes the reinforcement learning suitable to real-time and dynamic cybersecurity.

5.7 Graphical Analysis

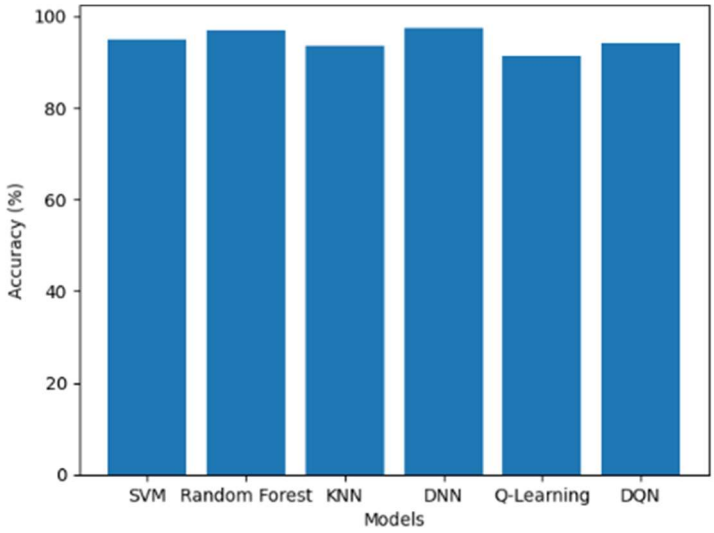

Figure 3: Accuracy Comparison of Supervised and Reinforcement Learning Models

The Figure 3 demonstrates detection accuracy of several models of supervised and reinforcement learning. Some of the supervised methods that have the highest accuracy of 97.5 percent and 96.8 percent are the DNN and the RF classifiers respectively. SVM as well as KNN are also considered to be competitive classifiers. Relative to the reinforcement learning models, the accuracy of reinforcement learning models is somewhat worse, and the DQN is more effective than the traditional Q-learning. This observation indicates that the application of supervised learning models is more effective in intrusion detection involving the application of stationary scenario, as compared to reinforcements learning models, which are competitive.

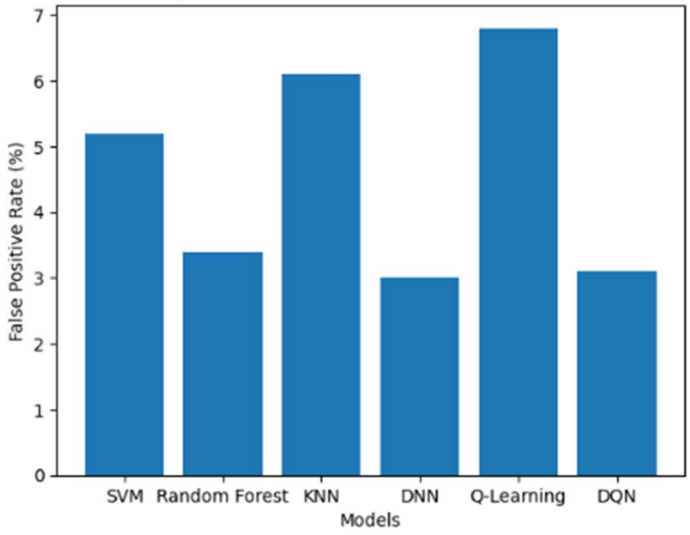

Figure 4: False Positive Rate Comparison

Evaluation of the FPR is given in figure 4 that compares all the models that are considered. DNN and DQN models possess the lowest false positive ratios that confirm that the two models can effectively tell normal and

malicious traffic. Quite on the contrary, false positive is relatively higher in KNN and Q-learning. Its results indicate the relevance of the advanced learning processes to the reduction of false alarm, which is instrumental in the real deployment of the intrusion detection systems.

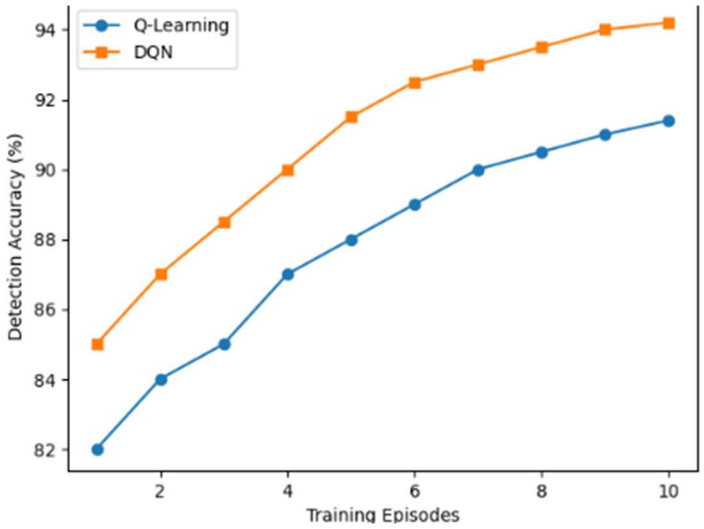

Figure 5: Learning Curve of Reinforcement Learning Models

The learning curves of the Q-learning and the DQN-based intrusion detection systems are shown in Figure 5 and at different training episodes. The results explain that the two models enhance the accuracy of detection as they get trained with time. However, DQN model will reach convergence much more quickly and as opposed to the traditional Q-learning, it is more precise. It is possible to explain this improvement by the fact that the deep neural network can be applied to high dimensional state space, and thus DQN is more suitable in changing cyber security environments.

The combined experimental study confirms the fact that the monitored learning approaches are extremely helpful in the context of detecting intrusions in a fixed environment, and the reinforcement learning approaches are more flexible and efficient in the context of dynamic attacks. The results justify the necessity to work out hybrid intrusion detection systems that are able to capitalize on the benefit of the two paradigms to achieve a more robust cybersecurity.

6. Conclusion and Future Work

The study conducted an effective analysis of the efficacy of both the paradigms of learning by applying them within a unified experimental framework. The experimental findings revealed that supervised models of learning, especially the Random Forest and Deep Neural Networks, were more accurate in detecting and having a lower rate of false positives when using a static attack. Such models were successful in discovering discriminative patterns on labeled data and are thus well-adapted to those situations in which the characteristics of attacks do not change significantly. Conversely, intrusion detection systems that were developed through reinforcement learning had greater flexibility to changing cyber threats.

Despite an original worse detection rate as compared to supervised models, the reinforcement learning methods, in particular, the Deep Q-Network demonstrated slow but steady performance improvements and increased

resistance to unknown attack patterns. The fact that agents of reinforcement learning can continuously revise detection policies in response to environmental feedbacks makes them very appropriate in dynamic and real-time cybersecurity settings where the attack patterns are constantly changing. Another significant trade-off between accuracy and adaptability is identified in the comparative analysis. Whereas supervised learning is very high performance on known attacks, reinforcement learning is very long-term resilient and flexible. Such results indicate that neither of the two paradigms would be adequate to resolve all the issues of contemporary cybersecurity.

The further research will be directed at designing hybrid intrusion detecting systems that would merge the advantages of supervised and reinforcement based learning methods. These systems may use supervised models to achieve high-accuracy of initial detection and use reinforcement learning to adapt continuously to new threats. Further studies will also be conducted on how the proposed framework can be implemented in applications on a large-scale and real-time basis such as cloud networks and IoT networks. Additional research on federated and privacy-preserving learning and applicability of explainable artificial intelligence in intrusion detection will also be taken into account to increase trust, scalability, and applicability.

References

1. Abeshu, A., & Chilamkurti, N. (2020). Deep learning: The frontier for distributed attack detection in fog-to-things computing. *IEEE Communications Magazine, 58*(2), 70–76. https://doi.org/10.1109/MCOM.001.1900221
2. Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems, 189*, 105124. https://doi.org/10.1016/j.knosys.2019.105124
3. Alrashdi, I., Alqazzaz, A., Alharthi, R., & Aloufi, A. (2021). Hybrid intrusion detection system using machine learning and deep learning. *Journal of Ambient Intelligence and Humanized Computing, 12*, 11341–11352. https://doi.org/10.1007/s12652-020-02803-2
4. Buczak, A. L., & Guven, E. (2020). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 22*(2), 1153–1176. https://doi.org/10.1109/COMST.2019.2952212
5. Chkirbene, Z., Erbad, A., Hamdi, M., & Ghaleb, B. (2021). Ensemble learning for network intrusion detection: A systematic review. *IEEE Access, 9*, 75414–75436. https://doi.org/10.1109/ACCESS.2021.3081186
6. Dang, T. K., Kim, M., & Kim, H. K. (2021). Toward a real-time intrusion detection system using deep reinforcement learning. *IEEE Transactions on Network and Service Management, 18*(3), 3218–3231. https://doi.org/10.1109/TNSM.2021.3099876
7. Diro, A. A., & Chilamkurti, N. (2020). Distributed attack detection scheme using deep learning approach for IoT environments. *Future Generation Computer Systems, 82*, 761–768. https://doi.org/10.1016/j.future.2017.08.043
8. Farahnakian, F., & Heikkonen, J. (2021). Deep auto-encoder based feature learning for intrusion detection. *Pattern Recognition Letters, 137*, 377–383. https://doi.org/10.1016/j.patrec.2020.07.011
9. Gwon, Y., Kim, J., Kim, S., & Lee, S. (2022). Adaptive intrusion detection based on deep reinforcement learning for evolving cyber threats. *Computers & Security, 113*, 102561. https://doi.org/10.1016/j.cose.2021.102561
10. Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson, R. (2020). Threat analysis of IoT networks using artificial neural network intrusion detection system. *Tsinghua Science and Technology, 25*(4), 451–464. https://doi.org/10.26599/TST.2019.9010040
11. Kim, J., Shin, J., & Choi, Y. (2022). Federated learning-based intrusion detection system for privacy preservation. *IEEE Access, 10*, 51210–51223. https://doi.org/10.1109/ACCESS.2022.3176129

12. Liu, H., Lang, B., & Zhao, M. (2021). Detecting unknown network attacks using deep belief networks. *Neurocomputing, 423*, 256–268. https://doi.org/10.1016/j.neucom.2020.10.036
13. Moustafa, N., Turnbull, B., & Choo, K. K. R. (2021). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of IoT systems. *IEEE Internet of Things Journal, 9*(1), 481–493. https://doi.org/10.1109/JIOT.2021.3050548
14. Nguyen, D. C., Ding, M., Pathirana, P. N., & Seneviratne, A. (2022). Federated learning for cyber security: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 24*(3), 1622–1657. https://doi.org/10.1109/COMST.2022.3166612
15. Yang, Y., Zheng, K., Wu, C., Yang, Y., & Wang, X. (2023). Deep learning-based intrusion detection for cyber–physical systems: A comprehensive review. *ACM Computing Surveys, 55*(6), 1–37. https://doi.org/10.1145/3529750
16. Aljabri, M., Alhaidari, F., & Alharbi, S. (2021). Cybersecurity threats and intrusion detection systems: A review. *Journal of Information Security and Applications, 58*, 102746.
17. Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2022). A survey of deep learning methods for cyber security. *Information, 13*(5), 243.
18. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications, 50*, 102419.
19. Hindy, H., Bayne, E., Seeam, A., Tachtatzis, C., Atkinson, R., & Bellekens, X. (2020). A taxonomy of network threats and the effect of current datasets on intrusion detection systems. *IEEE Access, 8*, 104650–104675.
20. Nguyen, T. T., Reddi, V. J., & Park, S. (2021). Reinforcement learning for cyber security: A survey. *IEEE Communications Surveys & Tutorials, 23*(2), 1039–1066.
21. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2021). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSP*, 108–116.
22. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2021). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence, 5*(1), 9–20.
23. Tang, T., Mhamdi, L., McLernon, D., Zaidi, S. A. R., & Ghogho, M. (2021). Deep learning approach for network intrusion detection in software defined networking. *IEEE Access, 9*, 108619–108630.
24. Ullah, I., & Mahmoud, Q. H. (2023). A deep learning-based intrusion detection system for IoT networks. *Computer Networks, 222*, 109567.
25. Zhang, Y., Chen, Y., & Li, K. (2022). Adaptive intrusion detection using deep reinforcement learning. *Future Generation Computer Systems, 127*, 12–25.
26. Li, X., Wang, Y., & Zhou, H. (2024). Deep reinforcement learning-enabled adaptive intrusion detection systems. *IEEE Access, 12*, 45621–45634.
27.

