ISSN 2409-2665
Journal of Logistics, Informatics and Service Science
Vol. 11 (2024) No. 3, pp. 1-20
DOI:10.33168/JLISS.2024.0301

Advancements in Machine Learning Techniques for Intrusion Detection Systems: An Overview of Perspectives and Datasets

Mousumi Ahmed Mimi [1, *], Timothy Tzen Vun Yap [2], Hu Ng[1]

[1] Faculty of Computing and Informatics, Multimedia University, Cyberjaya, Malaysia

[2] School of Mathematical & Computer Sciences, Heriot-Watt University, Malaysia

1221404218@student.mmu.edu.my

Abstract. This paper offers a comprehensive study on the topic of intrusion detection systems (IDS) in the context of cyber security, focusing on the application of machine learning (ML). A range of ML methods are explored, including logistic regression (LR), Bayesian logic, support vector machine (SVM), and convolutional neural network (CNN), among others. The study considers various datasets used in IDS and evaluates the advantages and disadvantages of each model. The paper also discusses new approaches that have emerged since 2020. To assess the accuracy of the models, the study compares their performance in supervised and unsupervised classification tasks and ranks them based on key metrics such as detection rate, false alarm, and accuracy. The study identifies the most effective algorithm for IDS in cyber security and explains the rationale behind this choice. Overall, this study provides valuable insights into the application of ML for intrusion detection in cyber security and serves as a practical guide for researchers and practitioners in the field.

Keywords: Intrusion detection system, machine learning, deep learning, supervised learning, unsupervised learning.

1. Introduction

An IDS is a surveillance system that detects and alerts suspicious activity, allowing security teams to investigate and take appropriate action against potential threats. IDS come in various forms, ranging from antivirus software to dedicated tracking systems that monitor entire networks. IDS can be categorized based on their approach, such as signature-based or behavior-based detection. Signature-based detection compares observed activity to known attack patterns, while behavior-based detection analyzes deviations from normal network behavior. While IDS can identify previously detected attacks, they may also produce false positives, flagging legitimate activities as malicious, especially when using advanced techniques that go beyond the current trust model.

Cyber-attacks have become increasingly prevalent in today's world, particularly against financial, credit, and banking institutions due to their substantial capital and sensitive information. Despite this, many establishments remain overconfident in their cyber security strategies, with a 2016 Accenture study showing that 78% of commercial organizations believed they had adequate measures in place. Cyber-attacks can target a broad range of victims, including individuals, businesses, and government agencies, with attackers typically aiming to gain access to sensitive resources such as consumer data, intellectual property, or financial information. Protecting critical infrastructure systems, such as Industrial Control Systems (ICS) and Critical National Infrastructures (CNI), has become crucial for maintaining essential services, including transportation, communication systems, water, and electricity. The recent cyber-attack on the Colonial Pipeline in the United States highlighted the vulnerability of critical infrastructure and the need for robust cyber security measures to protect these assets from cyber threats. An infrastructure has become a matter of utmost importance not only for regulatory bodies but also for national and European security. To address this, European governments have implemented a range of instructions and ordinances aimed at producing a consistent structure for electronic communication, information, and securing networks. However, more needs to be done, including developing separate security measures that address all valid technical angles and viewpoints, as well as establishing the capacity of cyber security. Effective cyber security strategies are crucial for organizations to safeguard their assets and prevent cyber-attacks. This includes investing in cyber-security technologies, educating employees on best practices, and staying with the new threats and vulnerabilities. By doing so, businesses and government agencies can protect themselves against potential threats and ensure the continued operation of critical infrastructure systems. In conclusion, the threat of cyber-attacks is real and growing, particularly against critical infrastructure systems and infrastructures. It is essential for organizations to develop and implement effective cyber security strategies to protect their assets and prevent cyber-attacks. By investing in cyber-security technologies, educating employees, and staying up to date with the latest threats and vulnerabilities, businesses and government agencies can ensure the continued operation of critical infrastructure systems and safeguard national and European security (Zhang et al., 2019).

The increasing frequency and severity of cyber-attacks have underscored the pressing need for robust and comprehensive cyber-security measures. As organizations strive to safeguard their assets and sensitive information, IDS have emerged as a crucial tool in the fight against cyber threats. An IDS serves as a vigilant surveillance system that actively detects suspicious activities within networks, enabling swift responses from security teams to investigate and counter potential threats. The landscape of IDS solutions varies widely, ranging from antivirus software to dedicated monitoring systems capable of overseeing entire network infrastructures. These systems are further classified based on their detection methodologies, with signature-based and behavior-based approaches at the forefront. Signature-based detection involves comparing observed activities against known attack patterns, while behavior-based detection focuses on identifying deviations from established norms of network behavior.

In the context of safeguarding critical infrastructure systems and infrastructures, IDS technologies play a pivotal role. This is particularly pertinent considering the increasing frequency of cyber-attacks targeting critical sectors such as financial institutions, transportation networks, and communication systems. The significance of protecting these essential services was brought to the fore by the Colonial Pipeline cyber-attack in the United States, highlighting the vulnerabilities present in critical infrastructure systems. In response to such threats, governments, particularly in Europe, have taken proactive measures to establish coherent frameworks for electronic communication, information security, and network protection. These initiatives demonstrate a commitment to ensuring the reliability, integrity, and availability of critical infrastructure systems, thus safeguarding both national interests and broader European security concerns.

Nevertheless, a holistic approach to cyber-security demands continued efforts to strengthen defenses against evolving cyber threats. Organizations must proactively address various technical perspectives and dimensions by designing tailored security strategies. Emphasizing both technical innovation and human education is key, as investing in cutting-edge cyber-security technologies while simultaneously imparting best practices to employees creates a multi-faceted defense mechanism. Regular updates on emerging threats and vulnerabilities further bolster an organization's readiness to counter potential attacks. Acknowledging the multifaceted nature of cyber threats, these strategies serve to minimize the risk of In conclusion, the pervasive threat of cyber-attacks necessitates unwavering commitment to cyber-security in critical infrastructure protection. Leveraging the capabilities of IDS technologies alongside comprehensive strategies is essential to thwarting the escalating cyber threats targeting essential services. By adopting a proactive approach that encompasses technological advancements, employee training, and ongoing threat awareness, organizations can fortify their defenses against cyber adversaries. This collaborative effort ensures the resilience and stability of critical infrastructure systems, thereby safeguarding not only organizational assets but also the broader landscape of national and European security in the digital age breaches and disruptions in critical infrastructure systems.

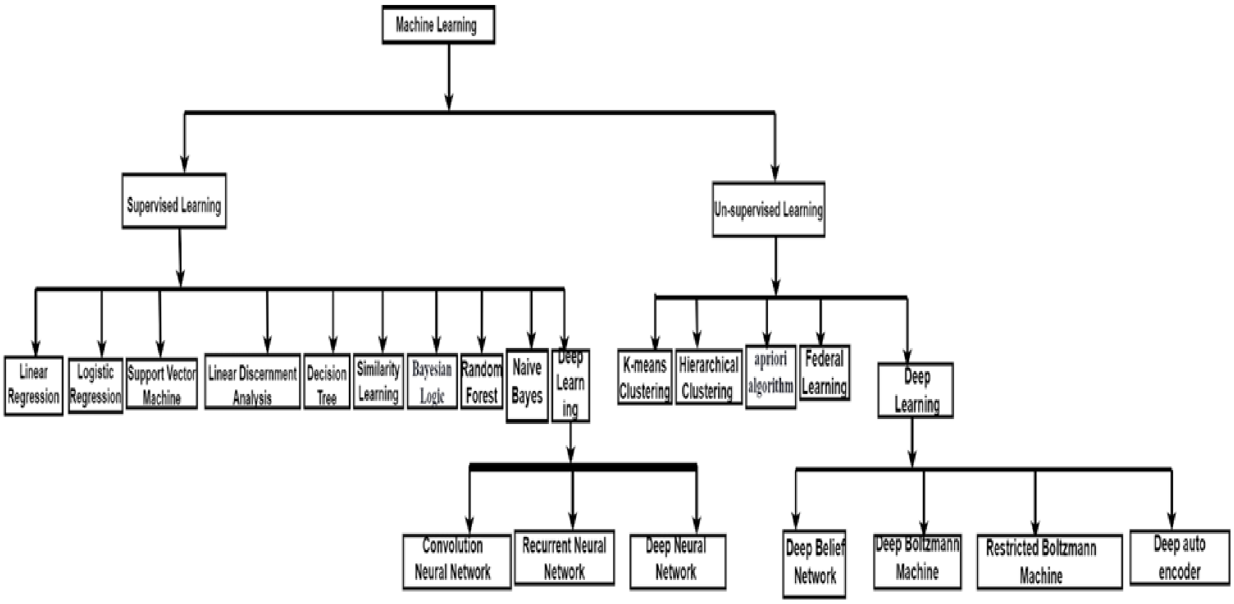

Fig. 1: Machine learning algorithms.

An IDS is designed to detect and alert people to suspicious or malicious activity within a computer system or network. IDS systems come in a variety of forms, including network-based and host-based systems, and can be classified as either signature-based or anomaly-based (Alqahtani et al., 2022).

- Network-based IDS (NIDS) systems monitor network traffic in real-time to detect patterns or anomalies that may indicate an attempted intrusion or attack. These systems typically work by analyzing network packets and comparing them against different datasets. If a match is found, an alert is generated.
- Host-based IDS systems (HIDS) work by monitoring the files and processes on individual computer systems for signs of suspicious or malicious activity. These systems typically rely on system

logs and file integrity monitoring to detect potential attacks or breaches.

- Signature-based IDS systems rely on pre-defined signatures or patterns to detect potential threats. These systems are effective at detecting known threats.
- Anomaly-based IDS systems use ML algorithms to analyze network traffic or system behavior and identify patterns that deviate from normal or expected behavior. These systems are designed to detect unknown or previously unseen attacks but may be more prone to false positives than signature-based systems.

Table 1: Researchers associated with IDS for cyber-security using ML, Deep Learning (DL), analysis deep learning (ADL), and analysis machine learning (AML) techniques.

Study	DL	ML	ADL	AML	Datasets
Agrawal et al., 2022	No	Yes	No	Partially Yes	Not mentioned
Aldhyani et al., 2022	Partially Yes	Partially Yes	Partially Yes	Partially Yes	KDD-CUP-99, UNSW-NB-15, WSN-DS, CIC-IDS-2017
Alqahtani et al., 2020	No	Yes	No	Partially Yes	KDD-CUP-99
Altunay et al., 2023	Partially Yes	Partially Yes	Partially Yes	Partially Yes	UNSW-NB-15
Ayubkhan et al., 2022	Yes	No	Partially Yes	No	CIDDS-01,CIDDS-02, IoTID2020, Bot-IoT, Kyoto 2006, CIC-IDS-2017, ISCX-URL2016, UNSW-NB-15, ISCX-Tor-2016,
Chen et al., 2023	Yes	No	Partially Yes	No	CIC-DDoS-2019
Cui et al., 2023	Partially Yes	Partially Yes	Partially Yes	Partially Yes	NSL-KDD, UNSW-NB-15
Debicha et al., 2022	Yes	No	Partially Yes	No	NSL-KDD, CIC-IDS-2017
Ferrag et al., 2020	Yes	No	Yes	No	DARPA-1998, KDD-Cup-99, NSL-KDD, UNSW-NB-15, DEFCON, CAIDAs, CIC-IDS-2017, CDX, CSE-CIC-IDS-2018, KYOTO, TWENTE, CIC-DoS, ISCX
Figueiredo et al., 2023	Yes	No	Yes	No	CIC-IDS-2017
Imran et al., 2022	Yes	No	Yes	No	KDD-CUP-99
Le et al., 2022	Yes	No	Partially Yes	No	UNSW-NB-15, CIC-IDS-2017
Maesaroh et al., 2022	Yes	Yes	Yes	Yes	DARPA, KDD-CUP- 99
Maesaroh et al., 2023	Yes	No	Yes	No	CIC-IDS-2017,CSE-CIC-IDS-2018,
Mandru et al., 2022	Yes	No	Partially Yes	No	DARPA, KDD-CUP-99
Sarker et al., 2020	No	Yes	No	Partially Yes	Not mentioned
Smys et al., 2020	No	Partially Yes	No	Partially Yes	UNSW-NB-15
Thakkar et al., 2023	Yes	No	Yes	No	NSL-KDD, UNSW-NB-15, CIC-IDS-2017
Wang et al., 2020	Yes	No	Yes	No	NSL-KDD
Yadav et al., 2022	Yes	No	Partially Yes	No	UNSW-2015
Yu et al., 2022	Yes	No	Partially Yes	No	Not mentioned
Zhang et al., 2019	No	Partially Yes	No	Partially Yes	Not mentioned

By detecting and alerting on potential threats in real-time, IDS systems can help organizations respond quickly and effectively to potential security breaches.

In the second part of the paper, we listed 22 ML algorithms that were considered, which are categorized into supervised and unsupervised learning models. The supervised learning models include linear regression, LR, decision trees (DT), and various types of neural networks, while the unsupervised learning models include clustering algorithms and DL models. In the third part of the paper, we will analyze the key characteristics that should be considered when applying ML to IDS, such as the amount and quality of data available, the type of attacks being targeted, and the computational resources required. In the fourth part of the paper, we will compare the accuracy rates of previous research works on IDS from 2019 to 2023, which will help to identify the most effective ML algorithms and approaches for IDS. Finally, in the fifth part of the paper, we will provide a conclusion and discuss future directions for research in this field. This paper will provide valuable insights into the use of ML for IDS and help researchers and practitioners to make informed decisions about which algorithms and approaches to use.

2. Utilizing ML Techniques for Enhanced IDS

IDS play a crucial role in safeguarding computer systems and networks against malicious activities and attacks. ML has emerged as an essential tool for IDS due to its ability to learn from data and identify new and unknown attacks. A total of 22 ML applications in IDS based on supervised and unsupervised learning methods have been identified, as shown in Figure 1. Supervised learning methods involve algorithms that are trained using labeled data, which has already been categorized as normal or anomalous. Examples of supervised learning algorithms that are widely used in IDS include SVM, DT, random forest (RF), Naive Bayes (NB), K-Nearest Neighbors (K-NN), and Artificial Neural Networks (ANN).

DL is a subset of ML that utilizes neural networks with multiple layers to learn hierarchical representations of data. DL algorithms are categorized into two types, supervised and unsupervised, based on the type of training data used. Supervised learning algorithms such as CNN, Recurrent Neural Networks (RNN), and Deep Neural Networks (DNN) have been extensively used in IDS. On the other hand, unsupervised learning methods do not require labeled data for training. Instead, they learn to identify patterns and anomalies in the data by being trained on unlabeled data. Examples of unsupervised learning algorithms used in IDS include Deep Belief Networks (DBN), Deep Boltzmann Machines (DBM), Restricted Boltzmann Machines (RBM), Deep Auto-encoders (DAE), and Deep Embedded Clustering (DEC), with DBN, DBM, RBM, and DAN being representative unsupervised learning tools.

The choice of an algorithm for IDS depends on various factors such as the type of attack, available data, and specific requirements of the IDS. In recent years, ML algorithms including DL have gained popularity in IDS for their ability to detect known and unknown attacks. By leveraging the power of ML algorithms, IDS can identify and mitigate potential threats effectively, enhancing the security and reliability of computer systems and networks.

2.1. Improved IDS through Supervised ML Techniques

In supervised learning, the algorithm is given a set of labeled examples as input, where the label is the correct output for each example. The algorithm then tries to learn a function that maps the input to the correct output by adjusting its internal parameters, or weights, based on the input/output pairs it sees.

The process of adjusting the weights is done through an iterative process called training, where the algorithm is repeatedly presented with input/output pairs and updates its weights to minimize the difference between its predicted output and the correct output. The goal of supervised learning is to learn a function that can accurately predict the correct output for new, unseen input examples. The cross-validation method is a way to evaluate the performance of a supervised learning algorithm by testing it on a separate set of data that was not used for training. This helps to avoid over-fitting, where the algorithm becomes too specialized to the training data and performs poorly on new data. By testing on a separate set of data, we can get a better estimate of how well the algorithm will perform on new, unseen data.

Supervised learning is a powerful tool for solving a wide variety of real-world problems, from image and speech recognition to fraud detection and recommendation systems.

2.1.1. Linear Regression for IDS: Advantages and Limitations

Linear regression is a statistical method used to model the relationship between a dependent variable (Y) and one or more independent variables (X).

$$Y = mX + b \tag{1}$$

The equation (1) represents a linear relationship between X and Y, where m is the slope of the line and b is the y-intercept.

While linear regression is a commonly used ML model, it may not be the best approach for every problem, particularly in the context of IDS and cyber security. There are other algorithms and techniques that are better suited for these applications, such as anomaly detection, clustering, and neural networks. Anomaly detection involves identifying unusual patterns or behavior that may indicate an intrusion or attack. Clustering involves grouping data points into clusters based on their similarity, which can be useful for identifying patterns and anomalies in network traffic. Neural networks are a more complex ML model that can learn to recognize patterns and make predictions based on data.

Overall, the choice of algorithm depends on the specific problem being addressed and the characteristics of the data. It is important to consider a range of ML techniques and select the most appropriate one for the task at hand (Wang et al., 2021).

2.1.2. Enhancing IDS with LR: A Comprehensive Analysis

LR is a type of classification algorithm that applies the sigmoid function to draw probabilities for predicting outcomes. Li et al. (2023) applied LR to data obtained from ECUs in-vehicles, and the results showed an F1 score of 83.5% and an accuracy of 85.4%. However, LR has not been widely used in IDS for cyber security, as mentioned in the survey paper (Thakkar et al., 2021). One approach for improving IDS performance was proposed by Duarte et al. (2021), who used a hybrid method that combined LR with a genetic algorithm (GA) to discover the top feature subdivisions for applying the wrapper-based procedure. This hybrid approach was applied to the UNSW-NB-15 and KDD-CUP-99 datasets.

2.1.3. Improving IDS through Similarity Learning Techniques

Similarity learning is a concept that is closely connected to regression or classification models. Its primary objective is to identify and measure the degree of similarity between two objects. There are four frameworks that are commonly used for metric distance resemblance studies, including regression, classification, ranking, and locality-sensitive hashing similarity learning. While a significant amount of research has been conducted using similarity learning for tasks such as face recognition and visual representation and verification of speakers, it has yet to be widely applied to cyber security in IDS. Despite this, there is significant potential for similarity learning to be used in the field of cyber security to help identify and prevent cyber-attacks (Thakkar et al., 2021).

2.1.4. Enhancing IDS using Linear Discriminant Analysis (LDA)

LDA is a technique used to reduce the number of features in a dataset to make it more manageable for classification purposes. Essentially, LDA creates new dimensions that are linear combinations of pixel values, forming templates that can predict and reduce dimensionality. This method is based on Bayes' theorem, which is used for probability calculations. The formula for the calculation is as follows:

$$P(Y = x|X = x)\ (P|k * fk(x))/sum(P||f(x)) \tag{2}$$

Here, P|k represents the prior probability, f(x) represents the estimated probability, x represents the input class, and k(x) represents the output class. LDA can be used for both multi-class and binary class probability calculations. It is interesting to note that, despite its usefulness in other applications, researchers have not yet applied LDA for IDS to determine the accuracy of attacks and cyber security (Thakkar et al., 2021).

2.1.5. Improving IDS with DT Algorithm

DT is hierarchical structures that represent the cost of resources, outcomes, and utility. They consist of branches and classifiers and are used to make classification decisions (Zhang et al., 2019). The test result is shown by the branch, and the test attribute is shown by an interior node, while the classification decision is represented by the leaf node. In recent research, the D2H-IDS method has been proposed to detect attacks using DT and DBN. DBN is used for data dimensionality reduction, while DT is used to find attacks. The NSL-KDD dataset was used to evaluate the method, and it showed an accuracy of 98.7% (Ferrag et al., 2020).

Other researchers have also applied DT to IDS with promising results. For instance, Ayubkhan et al. (2022) used gain ratio, association-based aspects decision, and IG to select the most relevant features for their model. They applied for the KDD-CUP-99 dataset and achieved an accuracy of 98.7%. Muniyandi et al. (2021) combined ANN, tree classifiers, and clustering ideas to improve the performance of DT. They used K-Means to extract the clusters and built a DT for each cluster to remove the difficulties of obligatory task and class dominion. Aldhyani et al. (2023) investigated discrete and continuous features of IDS datasets and used the Restricted Boltzmann Machine (RBM) model to control continuous network traffic data. Abdullayeva et al. (2019) used Gaussian-Bernoulli RBM, DBN, and Bernoulli-Bernoulli RBM to detect Denial of Service (DoS) attacks and found that Gaussian-Bernoulli RBM performed better than other models. Overall, DT has shown great potential in the field of IDS and can be further optimized with the use of other ML techniques.

2.1.6. Enhancing IDS using Bayesian Logic (BL) Techniques

Bayesian inference, which is a statistical method for updating the probability of a hypothesis based on new evidence. In Bayesian inference, the probability of a hypothesis (B) given some observed evidence (A) is proportional to the product of the prior probability of the hypothesis (P(B)) and the likelihood of the evidence given the hypothesis in equation (3)

$$(P(A|B)) \tag{3}$$

It allows for incorporating prior knowledge and updating beliefs based on new evidence, which can lead to more accurate predictions and decisions. Bayesian networks are a graphical representation of Bayesian inference, where nodes represent variables and edges represent probabilistic relationships between them.

However, it is important to note that Bayesian inference relies on the accuracy and representativeness of the prior probability and the likelihood function. In some cases, the prior probability might be subjective or based on incomplete information, leading to biased or inaccurate results. Additionally, the complexity of Bayesian networks can make them computationally expensive and difficult to interpret. Therefore, it is important to carefully design and validate Bayesian models to ensure their reliability and effectiveness (Kumar et al., 2023).

2.1.7. Utilizing SVM for Improved IDS

SVM is a ML algorithm that can be used for both regression and classification of data into groups. SVM seeks to find the hyper-plane that best separates the data points into different classes (Mighan et al., 2020), (Ravi et al., 2022) and (Thakkar et al., 2021). Incremental Support Vector Machine (ISVM) is an approach that uses candidate support vectors to detect upcoming increases in classification (Ferrag et al., 2020). SAE-SVM is a framework that combines SVM and DT for binary classification (Saranya et al., 2020). In some research papers, SVM is used for shallow learning, while DL is used for automatic and systematic network intrusion detection systems. SVM can work in both cascade and binary classification modes, and the accuracy of SVM can be improved through techniques such as PCA and feature selection. Non-linear data can be made linear or non-linear using kernel functions (Khraisat et al., 2020) and (Thakkar et al., 2021). SVM is a good method for separating data points and is often used in conjunction with other ML approaches. The feasibility and potency of locating intrusions depend on the dataset sample size. SVM can be used as a binary classifier and can also be merged with multiple binary classifiers for multi-class classification (Rajagopal et al., 2021).

2.1.8. Improving IDS with RF

RF is a popular ML algorithm that is used for both classification and regression tasks. The algorithm works by building multiple DT and combining their predictions to improve accuracy and reduce over fitting (Ferrag et al., 2020), (Saranya et al., 2020) and (Thakkar et al., 2021). Nazir et al. (2021) mentioned the effectiveness of RF in detecting various types of cyber-attacks in IDS. Some of these studies have also combined RF with other algorithms or techniques to improve the performance of the system. For example, some studies have used feature selection techniques such as Genetic Algorithm or Tabu Search to identify the most relevant features for detecting cyber-attacks (Abdullah et al., 2021). Others have applied clustering algorithms such as K-Means to group similar network traffic data and improve the accuracy of IDS. Additionally, some studies have proposed hybrid models that combine RF with other algorithms such as CNN or LR to further enhance detection accuracy. The use of regularization techniques in some studies can help to reduce false positives and improve the generalization performance of the system. Its effectiveness can be further improved by combining it with other algorithms or techniques (Khammassi et al., 2020).

2.1.9. Leveraging Naïve Bayes (NB) for Enhanced IDS

NB is one of the classification methods commonly applied in IDS (Le et al., 2022). Some researchers have compared NB with other classification methods such as DT, regression tree, SVM, LR, gradient boost machines, and RF (Ayubkhan et al., 2022). The accuracy gained from these methods varies depending on the dataset and the feature selection method used. In addition, some researchers have applied ensemble methods to improve the accuracy of IDS. The ensemble method combines various models to make a group, which can increase the accuracy of the model (Maesaroh et al., 2022). Bagging is one of the ensemble methods that have been applied with Adaptive Boost, partial DT algorithm (PART), and NB. The research found that the ensemble method has a higher accuracy rate than Adaptive Boost, NB, and PART alone. Hereafter research and experimentation may be required to determine the most effective approach for a particular IDS application.

2.1.10. Improving IDS with K-NN Algorithm

K-NN is a popular algorithm for use in IDS, as it was used for training data in the second defense layer in the IDS proposed by Zhang et al. (2019) and used for comparison with recurrent DNN in the IDS proposed by Ravi et al. (2019). Zhang et al. (2019) proposed a multi-layer data-driven approach for attack detection, with K-NN being used in the first defense layer. Their approach utilized both supervised and unsupervised learning methods for system data and networks and achieved high accuracy rates with low false positive and false negative rates. Ravi et al. (2019) compared the performance of K-NN with that of a recurrent deep neural network for IDS, using various datasets. While their results showed that the neural network outperformed K-NN for accuracy calculation, the specific hyper-parameters used for K-NN (n_neighbors = 5, leaf size = 30) may not have been optimal for the datasets used in their experiment. Overall, K-NN is a relatively simple yet effective algorithm for use in intrusion detection systems, and its performance can be further improved by optimizing its hyper-parameters and incorporating it into a multi-layer defense system.

2.2. Enhancing IDS with Supervised DL Techniques

In the realm of cyber-security, the augmentation of IDS through the integration of Supervised DL techniques holds substantial promise. This fusion seeks to address the escalating challenges posed by sophisticated cyber threats. Supervised DL operates as an advanced analytical tool, leveraging intricate neural networks to scrutinize vast datasets and discern intricate patterns indicative of malicious activities. Unlike traditional IDS approaches, where predefined signatures or rules govern threat detection, supervised DL empowers IDS to autonomously learn from examples, progressively honing its ability to distinguish between normal and anomalous behavior. This paradigm shift introduces a proactive dimension, allowing the IDS to swiftly adapt to emerging threat vectors without constant manual intervention. By training on historical data encompassing diverse attack scenarios, supervised DL-equipped IDS become adept at recognizing subtle deviations from baseline norms, thereby minimizing the risk of false positives and negatives. This precision is pivotal in an era where targeted attacks often bypass conventional signature-based detection methods. The potency of supervised DL extends to its capacity to unravel intricate attack tactics, potentially uncovering hitherto unknown vulnerabilities. Despite its potential, the integration of supervised DL techniques into IDS is not devoid of challenges. The demand for substantial labeled datasets for effective training, coupled with the complexity of configuring and fine-tuning neural networks, requires meticulous planning. Furthermore, the interpretability of DL-driven decisions remains a concern, necessitating ongoing efforts to enhance transparency and facilitate human understanding of detection outcomes. The synergy between Intrusion Detection Systems and supervised Deep Learning techniques ushers in a new era of cyber resilience. The capability of supervised DL to autonomously learn and adapt positions IDS at the forefront of cyber threat mitigation. While challenges persist, the potential gains in accuracy and adaptability signify a pivotal advancement in bolstering digital defenses against an evolving landscape of sophisticated cyber intrusions.

2.2.1. Improving IDS with CNN Algorithm

Le et al. (2022) developed a new method named IMIDS which captures raw network traffic by applying external libraries and then trains the model using 10 layers of CNN. They achieved an accuracy of 96.69%, recall of 98%, precision of 96%, and an F1 score of 97% using UNSW-NB-15 and CIC-IDS-2017 datasets. Cui et al. (2022) developed a novel IDS for an imbalanced dataset using SAE for the feature execution method, GMM-based clustering algorithm for the main class, and WGAN method for lower-level classes. For classification, they used CNN and LSTM and achieved an accuracy of 84.65%, precision of 85%, recall of 84.65%, and an F1 score of 83.95%. Aldhyani et al. (2022) applied CNN and LSTM methods together for finding different attacks in agriculture 4.0 using the CIC-DDoS-2019 dataset, and achieved an accuracy of 100% (Aldhyani et al., 2023). Altunay et al. (2022) developed a hybrid IDS for IoT networks using CNN and LSTM together. For binary classification, they achieved accuracy of 93.48%, and for multi-class classification, they achieved an accuracy of 93.26%. Yu et al. (2019) applied convolution kernel layers and multi-class classification CNN for IDS and achieved an accuracy of 92.64%. Wang et al. (2023) applied CNN for IDS using open-source Bro for data flow analysis and achieved an accuracy of 99.69% using the NSL-KDD dataset. Rizvi et al. (2022) applied DC-CNN (Dual Channel- Convolution Neural Network) for IDS in a simulation environment using CIC-IDS-2017 and 2018 and achieved an accuracy of 95%. Overall, these studies suggest that CNN and LSTM are effective methods for developing IDS.

2.2.2. Enhancing IDS with RNN Techniques

RNNs have been utilized for various applications, including resource selection, intrusion detection, and classification tasks (Thakkar et al., 2021) and (Al-Omari et al., 2021). RNNs are a type of neural network that is particularly suitable for processing sequential data, thanks to their ability to remember past inputs. However, conventional RNNs have faced challenges in training due to the vanishing gradient problem, where the gradients become increasingly smaller as they propagate through time steps, making it difficult for the network to learn. As a result, advanced variants of RNNs, such as Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU), have been developed to tackle the vanishing gradient problem and enable the network to learn long-term dependencies in the input sequence (Xun et al., 2023). Interestingly, several studies have compared RNNs with other neural network architectures. Moreover, bi-directional RNNs, which process the input sequence in both forward and backward directions, have been employed in some studies to improve performance in tasks such as speech recognition and natural language processing. Overall, RNNs and their variants have shown great effectiveness in various applications and continue to be an active area of research in the field of ML (Ravi et al., 2022).

2.2.3. Improving IDS with DNN Techniques

In an initial investigation, a DNN consisting of 5 hidden layers and 41 neurons was utilized to analyze three distinct layers of IDS, including associated, polarization, and prohibition layers, on the KDD-CUP-99 dataset (Mandru et al., 2021). The researchers achieved an accuracy of 92.6%. In a subsequent study, the authors implemented DNN for feature selection in IDS, by computing mean and median values for feature execution, sorting features based on value difference, and ranking them. High-rank features were eliminated, and the dataset was updated before being trained with DNN, resulting in an accuracy of 99.80% (Thakkar et al., 2021). In another investigation, DNN was employed with three fusion rules, including Dempster-Shafer combination, Simple Bayes averaging, and Majority voting, to analyze two types of IDS (serial and parallel) using the NSL-KDD and CIC-IDS-2017 datasets, achieving an accuracy of 83.83% (Debicha et al., 2022). A fourth study examined various features and DNN types, such as multilayer perceptron (MLP), feed-forward artificial neural network (FFANN), RNN, CNN, RBM, de-noising auto-encoder (DAE), deep belief network (DBN), deep metric learning (DML), self-taught learning, and replicator neural network. Additionally, Kasongo et al. (2023) study on FFDNN for filter-based feature selection in wireless networks was also mentioned, demonstrating an accuracy of 99.69% using the NSL-KDD dataset and the KDDTrain+ and KDDTest+ subsets. These investigations provided strong evidence of DNNs' efficacy in IDS and emphasize the importance of feature selection and fusion rules in achieving high accuracy.

2.3. Enhancing IDS with Unsupervised ML Techniques

The enhancement of IDS through the incorporation of Unsupervised ML techniques constitutes a significant advancement in the realm of cyber-security. This integration addresses the evolving challenges posed by intricate and novel cyber threats. Unsupervised ML operates as a pivotal tool by autonomously scrutinizing extensive datasets to uncover hidden patterns and anomalies without the necessity of predefined labels or human guidance. Unlike conventional rule-based approaches, where threat detection relies on predetermined criteria, unsupervised ML empowers IDS to autonomously learn the intricacies of normal network behavior and subsequently identify deviations that may indicate malicious activities. By employing algorithms such as clustering and anomaly detection, unsupervised ML-equipped IDS offer a dynamic approach to threat detection, capable of adapting to emerging attack methodologies. This adaptability is particularly pertinent given the ever-evolving tactics employed by cyber adversaries. Moreover, the application of unsupervised ML techniques holds the potential to detect previously unknown threats, filling gaps in protection that signature-based approaches might overlook. However, while promising, the integration of unsupervised ML into IDS is not devoid of challenges. The complex nature of unsupervised learning algorithms demands substantial computational resources and fine-tuning to achieve optimal performance. Additionally, the interpretation of the outcomes generated by unsupervised ML remains a subject of research, raising questions about the transparency of decision-making processes. the synergy between Intrusion Detection Systems and unsupervised Machine Learning techniques introduces a paradigm shift in cyber threat detection. The capacity of unsupervised ML to autonomously identify anomalies within complex datasets offers a proactive line of defense against evolving cyber threats. As research continues to address challenges and refine methodologies, the application of unsupervised ML to IDS stands poised to enhance the efficacy of cyber-security strategies and fortify digital infrastructure against a spectrum of threats.

2.3.1. Improving IDS with K-Means Clustering Algorithm

K-Means Clustering is a popular unsupervised learning algorithm that is used to divide a dataset into a fixed number of groups or clusters based on the similarity of the data points (Le et al., 2022). It is widely used in various fields, including data mining, pattern recognition, image segmentation, and anomaly detection (Thakkar et al., 2021). One of the limitations of K-Means Clustering is that it assumes the data points to be spherical in shape, which may not be true in all cases. There are other clustering algorithms like DBSCAN and Hierarchical Clustering that can handle non-spherical data points. It is interesting to note that researchers have applied K-Means Clustering in combination with other ML algorithms like DT, artificial neural networks, and NB classifiers to improve the accuracy of their models. They have also used different variations of K-Means Clustering like k-medoids and parallel K-Means Clustering for better results (Chen et al., 2020). Overall, K-Means Clustering has shown promising results in various research studies, and it will continue to be a valuable tool for data analysis in the future. K-medoids is a different algorithm from it but it is still a type of partitioning clustering. K-medoids selects medoids (representative points) from the dataset as the initial centroids and then iteratively updates them to minimize the sum of dissimilarities between the medoids. K-medoids are also known as Partitioning Around Medoids (PAM) clustering (Figueiredo et al., 2020).

2.3.2. Enhancing IDS with Hierarchical Clustering Techniques

Hierarchical Clustering is a versatile and widely used unsupervised ML algorithm that partitions similar objects into clusters based on their distances or similarities (Zeng et al., 2020). As the name suggests, it generates a hierarchical structure of clusters, with each cluster being a subset of a larger cluster (Figueiredo et al., 2020). The two main types of Hierarchical Clustering are agglomerative and divisive, with the former starting with each object as a separate cluster and progressively merging them until all objects belong to a single cluster. The latter, divisive clustering begins with all objects in one cluster and then recursively divides it into smaller, more homogeneous clusters until each object forms its cluster. The practical applications of Hierarchical Clustering are diverse, with computer science, biology, and social sciences being some of the domains where it is extensively used. For instance, Hierarchical Clustering finds applications in person re-identification where it aids in identifying the same individual across multiple cameras by grouping similar images (Lewis et al., 2023). In network intrusion detection, clustering algorithms reduce false alarms triggered by intrusion detection systems. In summary, Hierarchical Clustering is a potent technique that enables grouping of similar objects into clusters and has numerous applications across multiple fields.

2.3.3. Improving IDS with Apriori Algorithm

The Apriori algorithm is a popular method for association rule mining in relational databases. It works by identifying frequent item sets in the database and then generating association rules based on those item sets. The algorithm is based on the idea that if an item set is frequent, then all its subsets must also be frequent. The algorithm works by first identifying all the individual items in the database and counting their frequencies. It then uses these counts to generate candidate item sets of size two, by combining items that appear together frequently enough. It then scans the database again to count the frequencies of these candidate item sets, and discards those that do not appear frequently enough. This process is repeated to generate candidate item sets of increasing size, until no more frequent item sets can be generated. Once the frequent item sets have been identified, the algorithm generates association rules by partitioning the items into antecedents and consequents and calculating their support and confidence values. Apriori algorithm has many applications in ML, including regression, classification, feature selection, visualization, clustering, and data preprocessing. In the context of IDS, the algorithm can be used to identify patterns of attack in network traffic data. Li et al. (2019) used the Apriori algorithm to create a rule-based IDS that could detect a variety of attacks based on their network traffic patterns.

2.4. Enhancing IDS with Unsupervised DL Techniques

The integration of Unsupervised DL techniques to enhance IDS represents a significant leap forward in the realm of cyber-security. This amalgamation addresses the escalating complexity of modern cyber threats. Unsupervised DL, leveraging intricate neural networks, enables IDS to autonomously explore and identify subtle patterns within massive datasets without requiring explicit labels. Unlike traditional rule-based approaches, unsupervised DL empowers IDS to adaptively detect anomalies, even those that elude predefined criteria. This proactive nature equips the system to uncover novel attack vectors and respond effectively to previously unseen threats, thereby reinforcing the resilience of digital networks. However, the implementation of unsupervised DL techniques within IDS is not without challenges, particularly in terms of computational demands and interpretability. Despite these obstacles, the incorporation of unsupervised DL techniques showcases immense potential in fortifying IDS against the dynamic landscape of cyber threats.

2.4.1. Improving IDS with LSTM Algorithm

LSTM is a type of RNN that is designed to address the vanishing gradient problem often encountered in traditional RNNs. LSTM networks can be used in combination with other types of ML algorithms such as CNNs, DNNs, and ANNs. Combining LSTM with other algorithms can further improve the performance of the model. Aldhyani et al. (2023), Cui et al. (2023), Figueiredo et al. (2023), Imran et al. (2022), Ravi et al. (2022), Smys et al. (2020), Thakkar et al. (2021), Yadav et al. (2022) and Yu et al. (2022) and likely discuss the application of LSTM in combination with other algorithms to solve various problems. It is common to see LSTM used in a hierarchical structure with other algorithms to capture different levels of features in the input data.

2.4.2. Enhancing IDS with DBN Techniques

DBN is a multiple layer of RBMs. In DBN, each layer of RBM is trained to learn higher-level abstractions of the input data, with the final layer learning the most abstract representation of the data. This makes DBN a powerful tool for feature extraction and pattern recognition. In the context of cyber security, IDS are used to identify potential attacks or unauthorized access attempts to a computer network. The researchers mentioned that Shone et al. (2020) applied DBN and auto-encoder techniques to the KDD-CUP-99 dataset, which is a well-known dataset for evaluating IDS algorithms. It is interesting to note that the researchers reported a 97.85% accuracy rate for the DBN approach. This suggests that DBN can be a promising technique for IDS. However, it is important to keep in mind that the accuracy of IDS is not the only metric that should be considered, as false positives and false negatives can have serious consequences in a real-world scenario. Therefore, further evaluation and testing of the DBN approach in various settings would be necessary to fully assess its effectiveness.

2.4.3. Improving IDS with DBM

DBMs are a type of generative neural network architecture that consists of multiple layers of stochastic binary units that are interconnected through undirected edges. Each layer of units is fully connected to the layers above and below it. Unlike other DL models, DBMs can capture complex dependencies and interactions between input variables without requiring labeled data. As we mentioned, DBMs consist of hidden layers, which are sometimes called energy states. These hidden layers allow the model to learn increasingly abstract representations of the input data. The model learns by iteratively adjusting the weights and biases of each layer to maximize the likelihood of the input data. Salakhut et al. (2020) applied a DBM with three hidden layers to a variety of tasks. Their experiments demonstrated that DBMs are capable of learning meaningful representations of complex data, and that they can outperform other DL models in certain tasks.

2.4.4. Enhancing IDS with RBM Techniques

RBMs have been widely used in various fields, including image recognition, speech recognition, natural language processing, and anomaly detection. Researchers have used RBMs in the field of IDS and achieved high accuracy rates. The KDD-CUP-99 and NSL-KDD datasets are widely used benchmark datasets for IDS research. RBMs have also been used in DNN by fine-tuning the parameters of the RBM and training the layers of the RBM. It is worth noting that RBMs are just one of many ML techniques that can be used for different applications. Researchers can explore other methods and compare their performance with RBMs (Salakhut et al., 2020).

2.4.5. Improving IDS with Deep Auto-Encoder (DAE) Algorithm

Salakhut et al. (2020) worked on the application of DAE for IDS. It seems that different variations of auto-encoder have been used for IDS, such as non-symmetrical hidden layers, stacked auto-encoder, self-adaptive IDS, and de-noising auto-encoder. The reported accuracy rates vary from 79.99% to 95.7%. While some methods achieved high accuracy rates, some others resulted in relatively poor performance. It is worth noting that the accuracy rate alone does not always reflect the effectiveness of IDS, as other metrics such as false positive rate and false negative rate should also be considered. Overall, the application of DAE for IDS seems to be a promising direction of research, and further studies can explore new variations of auto-encoder and other DL methods for more accurate and efficient IDS.

2.4.6. Enhancing IDS with Federated Learning (FL) Techniques

FL is a decentralized learning method that aims to preserve the privacy of user data by training models locally on user devices and aggregating model updates on a centralized server. This allows the model to be trained without transferring the data to the server, thus reducing privacy risks. There are two types of FL, namely, vertical and horizontal. In vertical FL, different clients have different features, while in horizontal FL, clients have the same features but different samples. FL provides customized predictions for every client based on their experience from the data used and generated by the clients. Li et al. (2021) proposed DeepFed, which uses FL, CNN, and GRU for IDS to detect different attacks on DL methods. Additionally, Li et al. also proposed FL for a 5G network to facilitate transfer learning for better detection methods, using the CIC-IDS-2017 dataset with 91% accuracy.

3. Exploring the Advantages and Drawbacks of ML Algorithms for IDS

Following the discussions in Section 2, Table 2 shows the comparison of key considerations in choosing ML algorithms for IDS. The examination of ML algorithms for IDS offers insights into both their benefits and limitations. ML algorithms bring the advantage of automating the detection process, enabling IDS to learn from data and adapt to evolving threat landscapes. Their ability to recognize intricate patterns and anomalies enhances the system's efficacy in identifying both known and novel attacks. Additionally, ML algorithms exhibit potential in reducing false positives and negatives, leading to improved accuracy in threat detection. However, these advantages come with drawbacks. ML algorithms often demand substantial computational resources, and their success heavily relies on the availability of high-quality training data. The "black box" nature of some ML models can pose challenges in understanding and interpreting their decisions, raising concerns about transparency and accountability. Furthermore, adversaries can potentially exploit vulnerabilities in ML algorithms, leading to adversarial attacks that subvert the system's effectiveness. Thus, while ML algorithms hold promise for enhancing IDS capabilities, a comprehensive evaluation of their advantages and drawbacks is essential for informed implementation and robust cyber-security strategies.

Table 2: Comparison of key considerations for ML algorithms in IDS

Key Considerations for Applying ML in IDS	ML algorithms
Enhances ease of implementation, interpretation, and efficient training.	Linear Regression, LR, LDA, NB, K-NN, Hierarchical Clustering (easy implementation)
Demonstrates high accuracy in classification tasks with well-defined decision boundaries.	Linear Regression, LDA, LR
Provide a different outcome.	Linear Regression, LR, LDA, SVM, NB, K-NN, RF, K-Means Clustering
Reduce the variability in the data and improve the accuracy of the predictions.	Linear Regression, LR, LDA
Use both classification and regression class.	K-NN, similarity learning, RF
Require feature scaling.	DT, RF, adaptive boost, XGBoost, Gradient Boost, K-NN
Maximize the class distance.	LDA, K-NN, K-Means Clustering
Interpretability.	DT, Linear Regression, LR, BL
Less data preparation.	Linear Regression, LR, DT, RF, NB, Apriori algorithm
Non-linearity.	DT, RF
Combining previous information with data, a convenient setting.	BL
Prevent overfitting, small data, noise-free, improve accuracy.	BL, RF, XGBoost, K-NN, SVM, LSTM
Don't work without a large dataset.	CNN, RNN, DNN, FL
More efficient in high dimension, (higher dimension>number of spaces=good performance), memory efficient.	SVM
Works well both categorical and continuous value.	RF, DT, K-Means Clustering
Handle both continuous and discrete data, make a real-time prediction.	NB
Efficiency for image processing.	CNN, ANN
High accuracy rate.	CNN, RF, SVM, Linear Regression, K-NN
Quickest training time.	NB, DT, K-NN (quick calculation time)
Each pattern depends on the previous pattern, do tree-like structure, and only memorizes short-term memory.	RNN
Learning more complex features, intensive computational tasks.	DNN
Don’t need to pre-specify the number of clusters.	Hierarchical Clustering
Large datasets.	CNN, RNN, DNN, K-Means Clustering (pre-specify the number of a cluster), DBN, DBM, DAE, LSTM
Huge duration for development, complex data models, weight adjustment problem.	DBN (black box), DBM, RBM
Reduce the noise of input data, eliminate dataset complexity.	DAE
High cost for implementation.	DNN, CNN, RNN, FL, DBM, RBM, DBN
Prevent the vanishing gradient problem.	LSTM

4. Comparison of Achieved Accuracies and Corresponding Datasets

Various ML algorithms, notably SVM, RF, and DT, are applied in network security classification. Their effectiveness is highlighted when paired with datasets like NSL-KDD and KDD-CUP-99, yielding accuracy from 83.24% to 99.65%. Algorithm choice hinges on task context and data. Feature selection, key to accuracy, often involves a subset rather than all features. NSL-KDD features numeric, nominal, and binary attributes, demanding fitting selections. KDD-CUP-99, relevant since 1999, remains a respected malicious attack identifier. Comparative accuracies, detailed in Table 3, underscore the interplay of algorithms, feature selection, and dataset specifics in shaping network security efficacy.

Table 3: Comparison of achieved accuracies and their corresponding datasets of research work reviewed in this paper.

Study	ML algorithm	Accuracy	Dataset
Adel et al., 2020	Genetic algorithm+RF (binary classification)	86.7%	UNSW-NB-15
Agrawal et al., 2021	Fl+CNN+Gated recurrent unit	91%	CIC-IDS-2017
Agrawal et al., 2022	DT	98.7%	KDD-CUP-99
Alazab et al., 2022	SVM+DT	83.24%	AFDA & NSL-KDD
Aldhyani et al., 2023	CNN+LSTM attacks in agriculture 4.0)	100%	CIC-DDoS-2019
Aldhyani et al., 2020	DT	71%	NSL-KDD
Alharbi et al., 2020	DAE	90.95%	KDD-CUP-99 and NSL-KDD
Alqahtani et al., 2023	DC-CNN (dual channel-convolution neural network)	95%	CIC-IDS-2017
Altunay et al., 2023	NB+Adaptive boost	84.76%	UNSW-NB-15
Altunay et al., 2023	2-stage Tabu search+RF	85.78%	UNSW-NB-15
Altunay et al., 2021	CNN+LSTM	93.26%	CIC-IDS-2017
Chandra et al., 2021	SMO+K-Means Clustering	82.4%	KDD-CUP-99
Chen et al., 2020	K-Means Clustering+XGBoost	98%	KDD-CUP- 99
Cui et al., 2023	CNN+LSTM	84.65%	CIC-IDS-2017
Elsayed et al., 2022	RF+CNN	97%	NSL-KDD
Ferrag et al., 2020	RBM+DNN	82.4%	KDD-CUP-99
Ferrag et al., 2020	Feed-forward DNN, RNN, CNN	99.69%	NSL-KDD
Ferrag et al., 2020	DNN	92.6%	KDD-CUP-99
Ferrag et al., 2020	DT+DBN (D2H-IDS)	95.65%	NSL-KDD
Ferrag et al., 2020	RF+LR+K-NN	96%	KDD-CUP-99
Ferrag et al., 2020	Hierarchical Clustering	97.85%	KDD-CUP-99 and NSL-KDD
Gharib et al., 2021	RF regression method	90.33%	NSL-KDD
Hareesha et al., 2021	SVM+LR+K-NN+RF (Stacked Classifier)	94%	UGR-16 and UNSW-NB-15
Huang et al.,2021	K-Means Clustering+NB	92.33%	NSL-KDD
Imran et al., 2022	Tabu search algorithm+RF	83.12%	UNSW-NB-15
Kapralov et al., 2023	Hierarchical Clustering	91.90%	UNSW-NB-15
Kasongo et al., 2023	Genetic algorithm (RF)+NB+LR	87.61%	UNSW-NB-15
Khammassi et al., 2020	LR+RF (Multi-class classification)	84.23%	KDD-CUP-99
Le et al., 2022	NB+ DT+Regression tree+SVM	72.72%	UNSW-NB-15 and ISOT
Le et al., 2022	CNN	96.69%	CIC-IDS-2017 and UNSW-NB-15
Lewis et al., 2023	DAE+DNN	95%	KDD-CUP-99
Li et al., 2023	LR	85.4%	NSL-KDD
Lohiya et al., 2022	NB+K-NN+RF	75.67%	UNSW-NB-15
Mighan et al., 2020	SVM+DT (SAE-SVM)	99%	NSL-KDD
Mandru et al., 2021	RF	85%	KDD-CUP-99

Muda et al., 2021	K-Means Clustering+ANN	99.98%	KDD-CUP-99
Papamartz et al., 2020	DAE	79.99%	KDD-CUP-99
Ravi et al., 2022	SVM+RBMS (gradient descent algorithm)	80%	NSL-KDD
Ravi et al., 2022	K-NN	89%	KDD-CUP-99, UNSW-NB-15, WSN-DS and CIC-IDS-2017
Ravi et al., 2022	RNN+GRU+LSTM	92%	CIC-IDS-2017
Saranya et al., 2020	RF	99.65%	KDD-CUP-99
Saranya et al., 2020	K-Means Clustering (multiple layers)	95.94%	NSL-KDD
Sarker et al., 2020	K-NN	83.23%	UNSW-NB-15
Soheily et al., 2021	RF+ K-Means Clustering	88.97%	ISCX
Sydne et al., 2021	NB+RF+LR+DT	87.61%	UNSW-NB-15
Thakkar et al., 2021	RF	94.7%	NSL-KDD
Thakkar et al., 2021	LR+GA	87.82%	UNSW-NB-15
Thakkar et al., 2021	DNN	99.80%	KDD-CUP-99
Thakkar et al., 2021	SVM (minimal square)	85.65%	KDD-CUP-99
Thakkar et al., 2021	DT+ANN+K-Means Clustering	83.5%	KDD-CUP-99
Thakkar et al., 2021	LSTM	82.5%	KDD-CUP-99
Thakkar et al., 2021	RNN+FFNN	89.99%	KDD-CUP-99
Wang et al., 2021	CNN	99.64%	CIC-IDS-2017
Yassin et al., 2021	K-Means Clustering	99.0%	ISCX dataset
Yu et al., 2022	CNN (multi-class classification)	92.64%	CIC-IDS-2017
Zhang et al., 2021	RF	94.7%	NSL-KDD
Zhang et al., 2019	DT	92.5%	KDD-CUP-99
Zhang et al., 2019	K-NN+Bag+RF	89.84%	KDD-CUP-99

5. Conclusion and Future Directions for IDS Research

In today's complex digital landscape, the role of IDS emerges as indispensable in ensuring the integrity and security of computer networks and systems. These systems act as vigilant gatekeepers, actively safeguarding against unauthorized access, cyber-attacks, and various malicious activities. Leveraging a blend of ML and DL techniques, researchers have delved into the realm of IDS to unearth challenges and viable solutions. The deployment of DL, despite its need for extensive datasets, has shown promise, with some researchers effectively implementing it within the confines of IDS. In contrast, conventional ML algorithms such as linear regression, LDA, and apriori algorithm have encountered limitations in this context. As a countermeasure, hybrid methodologies that fuse diverse ML algorithms, including SVM, RF, or DT, have taken center stage in the pursuit of enhanced IDS efficacy. Among the obstacles confronted by researchers, the prevalence of noise in data stands as a significant hurdle. Counteracting this, innovative techniques like auto-encoders, stacked auto-encoders, and Gaussian noise reduction have been employed to mitigate data noise. Envisioning the road ahead, researchers are poised to extend their investigations, pairing auto-encoder methodology with other ML algorithms like SVM or RF, aiming to further elevate the accuracy of IDS predictions. Categorically, IDS span diverse types, encompassing network-based IDS, host-based IDS, and hybrid IDS, each showcasing its own strengths and vulnerabilities. Selecting the optimal IDS type mandates a thorough assessment of an organization's security requisites and available resources. Beyond the choice of IDS, the caliber of data sources and the efficacy of rules or signatures utilized to discern anomalous behavior wield significant influence over IDS performance. The dynamic nature of cyber threats underscores the vital importance of consistent updates and maintenance to sustain the IDS's efficacy against evolving attack vectors. In a holistic cyber-security strategy, IDS finds synergy with other protective layers such as firewalls, antivirus software, and employee training. Cumulatively, these elements form a comprehensive defense mechanism against multifaceted cyber threats. In summation, Intrusion Detection Systems confront a spectrum of challenges, yet research strides have unveiled pathways to bolster their effectiveness. By harnessing the potential of ML and DL techniques and devising innovative strategies to surmount obstacles like data noise, researchers and practitioners are on a trajectory to amplify the capabilities of these vital security systems. In an era where digital threats persistently evolve, IDS emerge as a linchpin in fortifying cyber landscapes, necessitating their integration into a cohesive cyber-security framework. Using both ML and DL techniques, researchers have identified some challenges and potential solutions in the area of IDS. Although DL requires a large dataset, some researchers have been able to apply DL successfully in IDS despite this limitation. However, traditional ML algorithms like linear regression, LDA, and a priori algorithm are not as effective in this context, and hybrid approaches combining different ML algorithms, such as SVM, RF, or DT, have been explored instead. One common issue that researchers have encountered is the presence of noise in the data, which can be reduced by techniques such as auto-encoder, stacked auto-encoder, and Gaussian noise. Going forward, researchers plan to continue exploring the use of auto-encoder with other ML algorithms such as SVM or RF to enhance the accuracy of IDS. There are various types of IDS available, including network-based IDS, host-based IDS, and hybrid IDS, each with its own strengths and weaknesses. Organizations should evaluate their security needs and resources to determine the most appropriate type of IDS for their environment. In addition to the type of IDS used, the quality of data sources and rules or signatures used to identify suspicious behavior are critical factors that impact the effectiveness of the IDS. Regular updates and maintenance are also essential to ensure that the IDS remain effective against evolving threats. Overall, IDS should be implemented as part of a comprehensive cyber-security strategy and should work in tandem with other security. At the end, while IDS face challenges, research has provided potential solutions that will continue to enhance the effectiveness of these security systems.

Acknowledgements

This research is supported by Fundamental Research Grant Scheme (FRGS), FRGS/1/2022/ICT06/MMU/03/3, and TM Research & Development Grant (TM R&D), MMUE/220028.

References

Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Alazab, M., & Gadekallu, T. R. (2022). Federated learning for intrusion detection system: Concepts, challenges and future directions. *Computer Communications.*

Aldhyani, T. H., & Alkahtani, H. (2023). Cyber security for detecting distributed denial of service attacks in agriculture 4.0: deep learning model. *Mathematics*, 11(1), 233.

Alharbi, A., Seh, A. H., Alosaimi, W., Alyami, H., Agrawal, A., Kumar, R., & Khan, R. A. (2021). Analyzing the impact of cyber security related attributes for intrusion detection systems. *Sustainability*, 13(22), 12337.

Alqahtani, H., Sarker, I. H., Kalim, A., Minhaz Hossain, S. M., Ikhlaq, S., & Hossain, S. (2020). Cyber intrusion detection using machine learning classification techniques. *In Computing Science, Communication and Security: First International Conference, COMS2 2020, Gujarat, India,* March 26–27, 2020, Revised Selected Papers 1 (pp. 121-131). Springer Singapore.

Altunay, H. C., & Albayrak, Z. (2023). A hybrid CNN+LSTM based intrusion detection system for industrial IoT networks. *Engineering Science and Technology, an International Journal*, 38, 101322.

Al-Omari, M., Rawashdeh, M., Qutaishat, F., Alshira'H, M., & Ababneh, N. (2021). An intelligent tree-based intrusion detection model for cyber security. *Journal of Network and Systems Management*, 29, 1-18.

Apruzzese, G., Andreolini, M., Colajanni, M., & Marchetti, M. (2020). Hardening random forest cyber detectors against adversarial attacks. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 4(4), 427-439.

Assiri, A. (2021). Anomaly classification using genetic algorithm-based random forest model for network attack detection. *Comput. Mater. Continua*, 66(1), 767-778.

Ayubkhan, S. A. H., Yap, W. S., Morris, E., & Rawthar, M. B. K. (2022). A practical intrusion detection system based on denoising autoencoder and LightGBM classifier with improved detection performance. *Journal of Ambient Intelligence and Humanized Computing*, 1-26.

Bueno, A. M., da Luz, I. M., Niza, I. L., & Broday, E. E. (2023). Hierarchical and K-Means Clustering to assess thermal dissatisfaction and productivity in university classrooms. *Building and Environment*, 233, 110097.

Chen, J., Qi, X., Chen, L., Chen, F., & Cheng, G. (2020). Quantum-inspired ant lion optimized hybrid K-Means for cluster analysis and intrusion detection. *Knowledge-Based Systems*, 203, 106167.

Cui, J., Zong, L., Xie, J., & Tang, M. (2023). A novel multi-module integrated intrusion detection system for high-dimensional imbalanced data. *Applied Intelligence,* 53(1), 272-288.

Debicha, I., Bauwens, R., Debatty, T., Dricot, J. M., Kenaza, T., & Mees, W. (2023). TAD: Transfer learning-based multi-adversarial detection of evasion attacks against network intrusion detection systems. *Future Generation Computer Systems*, 138, 185-197.

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.

Figueiredo, J., Serrão, C., & de Almeida, A. M. (2023). Deep learning model transposition for network intrusion detection systems. *Electronics*, 12(2), 293.

Henriques, J., Caldeira, F., Cruz, T., & Simões, P. (2020). Combining K-Means and XGBoost models for anomaly detection using log datasets. *Electronics*, 9(7), 1164.

Imran, M., Haider, N., Shoaib, M., & Razzak, I. (2022). An intelligent and efficient network intrusion detection system using deep learning. *Computers and Electrical Engineering*, 99, 107764.

Kapralov, M., Kumar, A., Lattanzi, S., & Mousavifar, A. (2023). Learning hierarchical cluster structure of graphs in sublinear time. In Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA) (pp. 925-939). *Society for Industrial and Applied Mathematics*.

Karimzadeh, S., & Olafsson, S. (2019). Data clustering using proximity matrices with missing values. *Expert Systems with Applications*, 126, 265-276.

Kasongo, S. M. (2021). An advanced intrusion detection system for IIoT based on GA and tree-based algorithms. *IEEE Access,* 9, 113199-113212.

Khammassi, C., & Krichen, S. (2020). A NSGA2-LR wrapper approach for feature selection in network intrusion detection. *Computer Networks*, 172, 107183.

Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., & Alazab, A. (2020). Hybrid intrusion detection system based on the stacking ensemble of c5 decision tree classifier and one class support vector machine. *Electronics*, 9(1), 173.

Kumar, C. S. (2023). Design of acceptance sampling-based network intrusion detection system using deep learning techniques. *Journal of Survey in Fisheries Sciences*, 10(1S), 3817-3821.

Le, K. H., Nguyen, M. H., Tran, T. D., & Tran, N. D. (2022). IMIDS: An intelligent intrusion detection system against cyber threats in IoT. *Electronics*, 11(4), 524.

Lewis, S. C., McMillan, S. L., Mac Low, M. M., Cournoyer-Cloutier, C., Polak, B., Wilhelm, M. J., & Wall, J. E. (2023). Early-forming massive stars suppress star formation and hierarchical cluster assembly. *The Astrophysical Journal*, 944(2), 211.

Li, W., Tian, Y., & Yuan, R. (2023). Statistical analysis of a linear regression model with restrictions and superfluous variables. *Journal of Industrial and Management Optimization*, 19(5), 3107-3127.

Louk, M. H. L., & Tama, B. A. (2023). Dual-IDS: A bagging-based gradient boosting decision tree model for network anomaly intrusion detection system. *Expert Systems with Applications*, 213, 119030.

Maesaroh, S., Kusumaningrum, L., Sintawana, N., Lazirkha, D. P., & Dinda, R. (2022). Wireless network security design and analysis using wireless intrusion detection system. *International Journal of Cyber and IT Service Management*, 2(1), 30-39.

Mandru, D. B., Aruna Safali, M., Raghavendra Sai, N., & Sai Chaitanya Kumar, G. (2022). Assessing deep neural network and shallow for network intrusion detection systems in cyber security. *In Computer Networks and Inventive Communication Technologies: Proceedings of Fourth ICCNCT 2021* (pp. 703-713). Springer Singapore.

Mighan, S. N., & Kahani, M. (2021). A novel scalable intrusion detection system based on deep learning. *International Journal of Information Security*, 20, 387-403.

Nazir, A., & Khan, R. A. (2021). A novel combinatorial optimization-based feature selection method for network intrusion detection. *Computers & Security*, 102, 102164.

Poo, Z. Y., Ting, C. Y., Loh, Y. P., & Ghauth, K. I. (2023). Multi-Label Classification with Deep Learning for Retail Recommendation. Journal of Informatics and Web Engineering, 2(2), 218-232.

Rajagopal, S., Kundapur, P. P., & Hareesha, K. S. (2020). A stacking ensemble for network intrusion detection using heterogeneous datasets. *Security and Communication Networks*, 2020, 1-9.

Ravi, V., Chaganti, R., & Alazab, M. (2022). Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system. *Computers and Electrical Engineering*, 102, 108156.

Rizvi, S., Scanlon, M., McGibney, J., & Sheppard, J. (2023). Deep learning-based network intrusion detection system for resource-constrained environments. *In Springer* (pp. 1-7).

Saranya, T., Sridevi, S., Deisy, C., Chung, T. D., & Khan, M. A. (2020). Performance analysis of machine learning algorithms in intrusion detection system: A review. *Procedia Computer Science*, 171, 1251-1260.

Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). Intrudtree: a machine learning based cyber security intrusion detection model. *Symmetry*, 12(5), 754.

Smys, S., Basar, A., & Wang, H. (2020). Hybrid intrusion detection system for internet of things (IoT). *Journal of ISMAC*, 2(04), 190-199.

Thakkar, A., & Lohiya, R. (2021). Attack classification using feature selection techniques: a comparative study. *Journal of Ambient Intelligence and Humanized Computing*, 12, 1249-1266.

Thakkar, A., & Lohiya, R. (2022). A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. *Artificial Intelligence Review*, 55(1), 453-563.

Thakkar, A., & Lohiya, R. (2023). Fusion of statistical importance for feature selection in deep neural network-based intrusion detection system. *Information Fusion*, 90, 353-363.

Wang, H., Cao, Z., & Hong, B. (2020). A network intrusion detection system based on convolutional neural network. *Journal of Intelligent & Fuzzy Systems*, 38(6), 7623-7637.

Wang, L., Gu, L., & Tang, Y. (2021). Research on alarm reduction of intrusion detection system based on clustering and whale optimization algorithm. *Applied Sciences*, 11(23), 11200.

Xun, Y., Deng, Z., Liu, J., & Zhao, Y. (2023). Side channel analysis: a novel intrusion detection system based on vehicle voltage signals. *IEEE Transactions on Vehicular Technology*.

Yadav, N., Pande, S., Khamparia, A., & Gupta, D. (2022). Intrusion detection system on IoT with 5G network using deep learning. *Wireless Communications and Mobile Computing*, 2022, 1-13.

Yu, J., Ye, X., & Li, H. (2022). A high precision intrusion detection system for network security communication based on multi-scale convolutional neural network. *Future Generation Computer Systems*, 129, 399-406.

Zeng, K., Ning, M., Wang, Y., & Guo, Y. (2020). Hierarchical Clustering with hard-batch triplet loss for person re-identification. *In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 13657-13665).

Zhang, F., Kodituwakku, H. A. D. E., Hines, J. W., & Coble, J. (2019). Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data. *IEEE Transactions on Industrial Informatics*, 15(7), 4362-4369.