A Comprehensive Survey on Various Machine Learning Models for Anomaly-Based Intrusion Detection System

Hidangmayum Satyajeet Sharma, Khundrakpam Johnson Singh

National Institute of Technology, Manipur, India

Corresponding author: Hidangmayum Satyajeet Sharma, Email: satya4hidang@gmail.com

As a result of the current global pandemic, there has been a surge in the use of various online platforms and services available via the internet. This results in the increase of exposure to different cyber-attacks on the network infrastructures. Cyber threats in the form of malicious software or also known as "malwares" have posed a serious threat to the smooth running of both government and business sectors. To cope with such issues, researchers have come up with various methods of machine learning based techniques in order to detect malicious activity on the network. But the major issue remains with the presence of vast diversity of features that leads to lengthy training processes and the need to deal with the prediction accuracy. This paper presents a literary review of various works on different machine learning-based intrusion detection system presented in different research papers over the last five years. Also, the results obtained from the various works such as evaluated metrics, datasets, and accuracy are discussed and compared. The scope of our review study is to provide a brief idea of intrusion detection as well as a reference to other research works done in the field of machine learning based intrusion detection system. Finally, the issues and future development are discussed by evaluating typical studies from recent years.

Keywords: Malware, Intrusion Detection System, DDoS attack, Machine Learning, Feature selection, Ensemble, Hybrid.

2023. In Saroj Hiranwal & Garima Mathur (eds.), *Artificial Intelligence and Communication Technologies*, 393–408. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-955020-5-9-38

1 Introduction

Intrusion is a term that can be defined as a form of anomaly which tries to compromise the CIA (Confidentiality, Integrity and Availability) triad [16]. An Intrusion Detection System (IDS) is used to observe and detectany form of anomalies in the incoming networks [16]. An intruder may gain access to a network through an unauthorised manner to gain access to the resource and thereby manipulating the data to make it unreliable and corrupted. The intruder takes the control of the vulnerabilities in the network like software bugs or weak security policies which can be utilize to gain access through the network which results in the network security violations. With the gradual advancement of the malicious attacks or also known as "Malware Attacks" it has become a challenge to detect such activities by an IDS. Therefore, a number of attacks such asDDoS (Distributed Denial of Service) attacks, Ransomware attacks have increased in the last few years.

An IDS may be a software or a hardware system or may sometimes comprises both software and hardware components in order to recognise any malicious or abnormality in the network [15]. However, the primary goal of an IDS is to identify various sorts of malicious network activity that would otherwise go undetected by a traditional firewall.This is essential for an IDS system to protect against the activity that compromises the CIA triad. IDS can be divided into the following categories based on the method used to detect intrusions as: Anomaly-based intrusion detection system (AIDS) and Signature-based intrusion detection system (SIDS) [15].

Signature based intrusion detection system or simply SIDS are based on Knowledge-based detection or misuse detection. A pattern matching technique is utilised to define an intrusion in the Signature based intrusion detection system. It simply means that when the intrusion signatures are samewith a known signature that are already in the database of the IDS a distress signal is alerted. However, in the case of Anomaly based intrusion detection system (AIDS) a normal behaviour model of the network is created using machine learning. Any slight variance between the detected behaviour and the model is considered as an intrusion or an anomaly in the network. The AIDS consist of training phase where the normal behaviour is learned and in the testing phase a dataset is used to detect the unseen intrusions.

IDS can be classed as either host-based IDS (HIDS) or network-based IDS (NIDS), depending on the sources of input data [15]. HIDS monitors the host system and inspects any strange activity inside the host from any sources such as the firewalls, operating system, application systems to name a few. HIDS doesn't require any network traffic. It can also scrutinize end-to-end encrypted information and can also detect intrusions by checking the files, network events and system calls inside the host. Network based IDS (NIDS) can monitor a network traffic by checking the network packets which are extracted from a network traffic over different network data source. NIDS can monitor different computers over the network and check for any malicious or anomaly activities to prevent before the threats spread to other systems. At the same time, NIDS have difficulty in analysing a wide range of broadcast in a high bandwidth network.

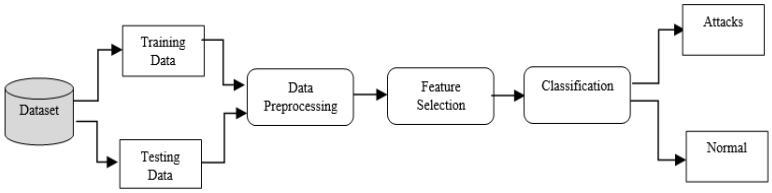

Fig. 1. Intrusion Detection System

In the last few years, a lot of AIDS approaches have been created using numerous machine learning algorithms which are applied in the Host-based IDS (HIDS) and Network-based IDS (NIDS) to improve the rate of detection and decrease in false alarm rate. Several machine learning techniques have come up to create IDS with the motivation to increase the accuracy and higher detection rate. Our literature review presents how different hybrid, single, ensemble, autoencoder and machine learning methods helps in the selection of features on different dataset. The study is organized in five sections. The first section of the paper provides a brief introduction. In Section 2, an overview of the research works is discussed and mentions about the type of attacks and various machine learning algorithms. In section 3, a review of the research works is studied and analysed based on their accuracy, algorithms and datasets used. Finally, in section 4, a brief set of conclusion and future research works in intrusion detection system have been discussed.

2 Overview of the Research Paper

2.1. Preprocessing

Data preprocessing in machine learning plays a pivotal role to enhance and promote the extraction of relevant insights of the data. A dataset may contain different formats like nominal, binary and numeric types. It is hard for the process of classification to handle different formats of data. As a result, null values and duplicate data are deleted during the preprocessing step, and categorical data is transformed into numeric data.[2]. The data processor calculates statistical values which includes the sum, mean, median and standard deviation which are used to record unique values contained in each feature [4]. In A.E. Cil et al [3], the preprocessing consists of three steps: preparing data like dropping rows and columns with misleading values, normalization where dataset is scaled as either '0' or '1' based on the type of attack and finally splitting the dataset into training and testing sets. Chaofei Tang et al [27] uses one-hot-encoding technology to convert 3 types of non-numeric categorical features: protocol type (tcp, udp,icmp), flag and servic*e* into binary vectors.

2.2 Feature Extraction

Feature selection (FS) or feature extraction is the procedure to select those features which are best fit for our prediction variable or output in order to improve the detection precision, remove redundant data and to decrease the computational complexity [1]. FS can be classified as filter, embedded and wrapper model from the strategy approach [5]. Filter approach evaluates the significance of the features obtained from the dataset and the selection of features is based on statisticswhile in wrapper model the classification capability is used to evaluate the feature subsets and selection process [17]. Whereas, embedded models are less intensive in terms of computational power as they assimilate both feature selection and learning process. Intrusion detection datasets involve a large amount of irrelevant and redundant data, which hampers the effectiveness of data mining algorithms and causes unaccountable results. As a result, the initial step in every IDS is to decrease the number of redundancies by choosing the best feature subset from the provided dataset. In this article, we listed some methods of feature selection and some of this feature observe are used in examining DDoS attacks and Botnets. Some of the feature selection algorithms used are meta-heuristics, rank search, ensemble methods, autoencoders, deep neural networks and hybrid models.

2.3 Distributed Denial-of-Service (DDoS)

A Distributed Denial-of-Service (DDoS) attack is an automated malicious program that obstructs normal traffic by overwhelming the target victim server, service or network. It tries to block the

computing system from working normally in order to disrupt the victim server.A DDoS attack utilize a large number of compromised systems which are located in different geographical areas in order to accomplish the attack on an intended victim [14].These infected systems are referred to as bots, and collections of these bots are called botnets.[14]. There are two types of DDoS attacks: application layer DDoS attacksand network layer DDoS attacks. For flooding the server, the first one employs OSI layer 7 protocols such as Domain name service (DNS), hypertext transfer protocol (HTTP) etc. In the case of network layer DDoS attack, it uses layer 3 or layer 4 of the Internet Control Message Protocol (ICMP) to overload the target server. The aim of this attack is to hamper the accessing of resources from the server by any legitimate client.

2.4 Hybrid Models

To improve the performance of the IDS, many hybrid models combining feature selection and ensemble models have been developed [17]. A conventional IDS has the constraints to adapt, to detect or identify new malicious attacks with poor accuracy and higher false alarm rate. A hybrid model is a collection of machine learning algorithms that work together to improve the performance of the resultant aggregated features [11]. The main reason for applying hybrid models in IDS is to boost the performance of the feature section phase and thereby increasing the performance metrics of the IDS.

2.5 Ensemble Method

An ensemble system multiplies a number of classifier systems which have been shown to be efficacious and flexible in a variety of Machine Learning problems and different applications [15, 14]. Ensemble systems have been effectively utilized to solve a range of machine learning challenges, including feature selection, feature missing, confidence estimate and error correction. As a result, a variety of models using ensemble techniques demonstrate a high level of accuracy and predictive performance. Adaptive boosting, gradient boosting, stacking generalizations, and bagging are some of the approaches for setting up ensembles.

2.6 Autoencoder

Autoencoders are part of unsupervised artificial neural network use for training unlabelled and compressed representation of raw data [4]. An autoencoder comprise of two parts, an encoder and a decoder. The encoder learns to reduce the size and compress the input data in the form an encoded representation. In the decoder model, the encoded representation of the input data is decoded to reconstruct back into its original input. Typically, autoencoders are employed for feature reduction, which is achieved by reducing the number of neurons in the hidden layer. AE-IDS can discover unknown atypical network behaviour by comparing usual traffic within coming traffic[7].

2.7 Deep Neural Network

Deep learning also known as Deep Neural Network (DNN) model [3], can work faster with higher accuracy values because it can perform both feature extraction and classification processes simultaneously. The primary component of a DNN is a neuron [9].Table 1 shows thedifferent types of deep learning methods used.

Table 1. Different methods of deep learning models and comparison [36]

Algorithms	Data types	Supervised/unsupervised	Functions
DNN	Feature Vectors	Supervised	Feature extraction and classification
CNN	Feature vectors; Raw data; matrices	Supervised	Feature extraction and classification
RNN	Feature vectors; Raw data; matrices	Supervised	Feature extraction and classification
Autoencoder	Raw data; Feature Vectors	Unsupervised	Feature extraction, Feature Reduction and Denoising
DBN	Feature Vectors	Supervised	Feature extraction and classification

2.8 Performance metrics of an IDS

Machine learning models are evaluated using a variety of classification metrics.These metrics are used to assess the performance of the feature selection model. Table 2 shows the confusion matrix which is used to evaluate the performance of an IDS. Each row and column represent an instance or attribute in the actual class and the predicted class respectively.

Table 2: Confusion matrix for measuring performance of IDS

		Predicted class	
		Normal	Anomaly
Actual Class	Normal	True Positive	False Negative
	Anomaly	False Positive	False Negative

The elements in the confusion matrix can be expressed as: True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). The standard performance measure of IDS can be described as follows:

- **Accuracy:** It can be represented as the ratio of all the outcomes which are correctly predicted to the total number of outcomes. The formula of accuracy can be given as:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

- **Precision (P):** It shows how much of the positive outcomes are predicted correctly. It is given by the ratio of the true positive outcomes to the total positive outcomes.

$$P = \frac{TP}{TP+FP} \quad (2)$$

- **Recall (R):** The recall rate, also known as the detection rate, demonstrates the model's capacity to detect and recognise attacks, and is given by the formula:

$$R = \frac{TP}{TP+FN} \quad (3)$$

- **F-measure (F):** It shows the classifier's robustness and precision.

$$F = \frac{2*P*R}{P+R} \quad (4)$$

- **False negative rate (FNR):** Also known as missed alarm rate, it is calculated as the proportion of false negative results to the total positive samples.

$$FNR = \frac{FN}{FN+TP} \quad (5)$$

- **False Positive Rate (FPR):** FPR or also called as false alarm rate can be defined as the ratio of the false positive predictions to the total number of positive samples.

$$FPR = \frac{FP}{FP+TN} \quad (6)$$

3 Review of Related Works

This section will go over the various related works that have been done by several researchers in recent years.Table 3 shows some of the work done on various datasets.The main objective of each of the works is mostly related with feature selections and classifications.

In the work of Mauro et al [1], a review of different experimental-based feature selection algorithms is analyzed. The different algorithms considered in the work ranges from rank-guided, Meta-heuristic and to nature-inspired algorithms and modern technologies and uses more recent dataset in contrast to the KDD99 dataset. The experiment considers five types of datasets DDoS, Portscan, Web attack and TOR which are group as single class datasets and another MultiAndroid dataset. The results of the experiments reveal that the Feature Selection (FS) algorithm retains more features on MultiAndroid datasets than single class datasets.

Theja et al [2] proposes a metaheuristic algorithm to select the best features for detecting the DoS attacks in cloud computing. The model employs the Opposition Based Crow Search Algorithm (OCSA), which combines Opposition Based Learning (OBL) and Crow Search Algorithm(CSA).The OCSA is used for feature selection and after that detection is done using Recurrent Neural Network (RNN). It extracts 41 different features and detects 8 different types of DoS attacks. The findings of the experiment reveal thatthe proposed method has high performance on precision, accuracy, recall and F-measure by a percentage of 98.18%, 94.12%, 95.13% and 93.56% respectively.

A feed forward Deep Neural Network (DNN) algorithm was proposed by Abdullah Emir Cil et al [3] to detect DDoS attacks. The approach uses DNN for feature extraction and classification process on the CICDDoS2019 dataset. The proposed model converted the datasets into two different models, one is composed of both normal and attack network traffic, while the other is composed of simply normal traffic. The first dataset only detects the existence of DDoS attacks whereas the second set of data is used to categorize all types of DDoS attacks. The result obtained shows that the first dataset has high accuracy rate in determining the DDoS attack as compare to the second dataset. Overall, the result shows 99.99% rate of success in detecting attacks on the network traffic and classification accuracy of 94.5% was observed for different attack types.

An adaptable feature selecting Complete Autoencoder (CA) was proposed by Ili Ko et al [4]. The method uses the Complete Autoencoder to create a Dynamic Learning System (DLS), which is an unsupervised model. The DLS has four different types of modules: Attack Detector, IP finder, Data Processor and an Ensemble Critical Module. The DLS was trained using a TCP-ICMP flood attack, and it was tested using UDP-TCP and UDP-TCP-ICMP flood attack datasets. On comparing the experimental results with few other unsupervised models, it is revealed that the DLS outperforms other existing algorithms like Single SOM, Dual- SOM and K-means. The average score of precision, recall and F1 measure are above 97%.

Wang et al [5] proposed a multilayer perceptron (MLP) based model for DDoS attack detection which works on NSL-KDD dataset. The method comprises of three modules: knowledge base where it preprocessed the dataset into training and feedback dataset, detection model which uses a sequential backward selection (SBS) to adopt the optimal feature, and a feedback mechanism to recognize the occurrence of errors based on the feedback datasets. After calculating the method's efficacy and comparing it to other similar works, the result shows that it could yield better detection performance and can detect more errors. The SBS-MLP has a performance of 97.66% Acc, 94.88% DR and 0.62% FR.

Wu et al [6] proposed a novel Semantic Re-encoding and Deep Learning Model (SRDLM).Through Deep learning, the model re-encodes the semantics of network traffic, improves traffic detectability, and aids in boosting the algorithm's generalization ability. The semantic re-encoding method converts the raw data into character stream and a sequence of word segmentation, reordering, remapping and reprojection is done, thereby increasing the classification accuracy. Resnet is used as a deep learning framework for classification. The experiment is done on two different datasets, Hduxss_data1.0 and NSL-KDD. The method effectively improves the generalization ability of the anomaly detection of the network traffic.

In Li et al [7], AE-IDS (Auto-Encoder Intrusion Detection System) using Random Forest (RF) algorithm was proposed. The auto-encoder deep neural network is used in this IDS approach to detect anomalies in network traffic. For feature selection of the datasets Random Forest algorithm is applied which helps in selecting the most optimal features from the data. Using the AP clustering algorithm feature grouping is implemented on the selected features. After feature grouping, the anomaly detection operation is performed using AE neural network. The experimental result shows that when compared with KitNet algorithm, the AE-IDS takes lesser time and can detect attacks more accurately. Though the experiment works more efficiently as compare to KitNet, the recall value in some of the attacks needs to be addressed further in upcoming research.

A deep learning method based on Wrapper Based Feature Extraction Unit (WFEU) was proposed by Kasongo and Sun [8], for wireless IDS. The experiment is carried on UNSW-NB15 and AWID datasets which includes both binary and multiclass types of attacks. In the case of UNSW-NB15 dataset, the WFEU model produced 22 feature vectors and in the instance of AWID the model generated 26 features. In the AWID dataset the method obtained a highest accuracy of 99.67% and 99.77% in binary and multiclass classification respectively.

Another work done by Kasongo and Sun [9], employs a deep learning method alongside a filter based Feature Extraction Unit (FEU) to generate the optimal feature subsets with less redundancy. Using the Filter-based algorithms, the FEU generates the optimal features and helps remove irrelevant and redundant data. To investigate the performance of the FEU, the Filter based Feed Forward Deep Neural Network (FFDNN) is introduced. After applying the model in a wireless intrusion detection utilizing the NSL-KDD dataset, the result shows that FEU-FFDNN outperforms other methods like the SVM, KNN, RF, Naïve Bayes and Decision tree models.

A work done by Yu et al [10] uses a novel Deep Learning method known as Few-Shot Learning (FSL) that has become approachable in the last few years. The FSL algorithm works effectively in solving a small amount of less than 1% of labelled dataset. It needs a balanced dataset to detect the abnormal behavior and hence it uses a balance resampling method. The essential features are extracted using CNN and DNN algorithms which is also used as embedding functions. The work was conducted on two independent datasets: UNSW-NB15 and NSL-KDD datasets. The results reveals that the model has higher accuracy and detection rate in multiclass classification on KDDTest+ and KDDTest-21 dataset with a rate of 92.33% and 86.23% respectively.

Hosseini et al [11] proposes a hybrid strategy for detecting DDoS attacks that is based on data stream techniques and splits the computing load between the client and proxy sides. The client side performs three steps: data collecting, feature extraction and divergence test. Naïve Bayes, decision tree, Random Forest, MLP and KNN algorithms are used on the proxy side and the results are processed in an algorithm determiner to provide the better result. Upon implementing the model on an analytics platform KNIME, it is found that the model has higher accuracy while using a number of classifications in which random forest gives better results than other algorithms.

A novel approach of voting based Deep Neural Network also known as VNN was introduced by Hashem et al [12]. The VNN model consist of different deep learning techniques like DNN, CNN, LSTM, SAE and GRU which are merged and after which it selects a best model in a prediction phase which performs a heuristic function. The chosen model performs a voting procedure to predict the test label. To make the voting mechanism more obvious and clearer, the procedure is implemented on two separate datasets: KDDCUP'99 and CTU-13.On applying the test in KDDCUP'99 on both binary as well as five-class classifiers it is found that the result have higher accuracy compare to other deep learning method. Similarly in the case of CTU-13 datasets the result predicts higher accuracy.

An ensemble-based approach that combine MLP, SVM (Support Vector Machine), KNN (K-Nearest Neighbor) and decision tree was proposed by Das et al [13]. The four classifiers work in parallel, and their outputs are integrated using the majority voting method to get the final output. The experimental result of the ensemble model reveals that the IDS model accurately classifies 99.7% of data instances and is effective for DDoS IDS in terms of accuracy, FPR, and TPR. The model has an excellent detection accuracy rate of 99.1% and a very less false positive rate of 0.088%.

An ensemble feature selection approach described by Singh et al [14] uses MLP, Naïve Bayes, Random Forest and RBF network. The MLP classifier was used against the other classifier models, as it predicts higher precision when compared to other classical machine learning classification models. The work was carried out on CAIDA2017 dataset and the model show a high accuracy of 98.3% with low RMSE value of 0.089.

Zhou et al [17] introduces a model that combines feature extraction with ensemble learning techniques. To minimize dimensionality and choose feature subsets, a hybrid model integrating Correlation-based feature selection (CFS) and Bat algorithm (BA) is presented. The CFS selects the subsets of the best features using correlation base evaluation function and to remove the redundancy and minimize dimensionality, BA is used. An ensemble classifier using C4.5, Forest by Penalizing Attributes (Forest PA) and Random Forest (RF)was proposed and finally, a voting algorithm was used to carry out the decision-making process by combination rules. The experimental result reveals that the CFS-BA-ensemble model outperforms other feature selection models when it comes to accuracy, F-measure and efficiency.

The work in Oluwaseun et al [18] presents IDS that utilizes Particle Swarm Optimization (PSO) algorithm. The PSO was used to reduce the number of features and for the classification procedure two classifiers used are PSO with Decision Tree (DT) and PSO with K-Nearest Neighbor (KNN). The results

were assessed using KDD-CUP 99 dataset and the model shows that PSO + KNN classifiers works with better performance than PSO + DT classifier algorithm with a detection accuracy of 96.2% to 89.6%.

In Halim et al [19] the author proposed an enhanced Genetic Algorithm (GA) - based Feature Selection (GbFS) model in order to increase the accuracy of the classifier. The GbFS learning module enables to select a set of best features from the data for executing classification instead of using the whole attributes or features of the data. The classification is done using three different classifiers, KNN, SVM and XgBoost (eXtreme Gradient Boosting). Experiments performed on three different datasets:UNSW-NB15, CIRA-CIC-DOHBrw-2020 and BOT-IOT shows that the classifier is able to enhanced the performance when using the feature extraction method rather than using the complete feature set. The average accuracy of all the three classifiers increases by 5.5% from 90.98% when using the GbFS module.

Sayed et al [20] proposed a novel hybrid approach which works on the SDN environment based on CNN and a regularization method, the SD-Reg, which works by applying the Standard Deviation of the weighted matrix. The SD-Reg improves the overfitting problem which helps in reducing the model generalization error. The proposed method combines the CNN with various algorithms like RF, SVM and KNN. The outcomes of the experiment shows that the CNN based on the SD-Reg method has a high detection accuracy, while the CNN-RF model has the best precision, F-score and recall value.

3.1 Datasets Considered for the Research Works

One of the major challenging issues while tackling with the supervised FS models is obtaining training datasets that are both recent and labeled [1]. Each dataset is collection of instances which is made up of numerous features called attributes of the dataset. One of the most common datasets used in most of the works is the NSL-KDD datasets.

Altogether, a total of seven datasets have been used in our review works: NSL-KDD, KDD Cup'99, CSE-CIC-IDS2018, UNSW-NB15, AWID, CICDDoS2019, UDP flood attack dataset. The most used dataset is the KDD Cup'99 (Knowledge Discovery and Data Mining) dataset is a subgroup of the DARPA-98 dataset. The KDD-99 contains five different classes of patterns: normal, DoS (Denial of Service), U2R (User to Root), R2L (Remote to Local) and probing attacks. The main issue with the KDD-99 dataset is the presence of large number of duplicate instances that creates a biased towards the normal packets and. To sort out the issues of KDD-99 Cup dataset, a new dataset, NSL-KDD was introduced. Many algorithms have utilized the NSL-KDD dataset as a benchmark. It has 41 features and 24 attack types in the training set with 125973 data points. A recent dataset is the CIC-IDS, set up by the Canadian Institute of Cyber security. It has 2,830,743 data points and allocated on 8 different files with each record containing 78 labelled features [17]. It contains the most up-to-date common attacks such as DDoS, XSS, SQL injection, Brute Force, Port Scan and Botnets. AWID which stands for Aegian Wi-Fi intrusion Dataset, is a Wi-Fi network data obtained from a wireless Local Area Network (WLAN) environment [8]. Each record in the dataset contains a collection of 155 attributes, and each attribute has a numeric or nominal values [17]. The UNSW-NB15 contains nine different attack types: Shellcode, Worms, Generic, DoS, Fuzzers, Reconnaissance, Backdoor, Analysis and Exploits [8]. It contains 42 input features in which 3 inputs are nominal and the remaining 39 are numeric features.

4 Comparison of various Machine Learning Algorithms used for IDS

In this review article, different machine learning-based intrusion detection algorithms are given and discussed. Here Table 3 gives a brief comparison of the survey from different works done by researcher. Different models which are used in each of these experiments are discussed.

Table 3: Comparison of various ML algorithms used in different research work

TITLE	MODEL	TYPES	ACCURACY	REMARKS
M. Di Mauro et al [1]	Rank, Tabu Search, Particle Swarm, Linear Forward Selection, Ant Search, Cuckoo Search, Genetic Search, Scatter, Multi-Objective Evolutionary	Binary class/Multiclass	Average accuracy for all models > 95.5%	The result of the paper shows that different feature extraction models based on heuristic algorithms leads to an effective reduction in feature subsets and improvement in computational time.
Reddy SaiSindhuTheja et al[2]	1. Oppositional Crow Search Algorithm (OCSA) for feature selection. 2. RNN for classification.	Multiclass	94.12%	The OCSA-RNN has better performance in optimal feature selection and outperforms other techniques in all factors of precision, recall and F-measure.
Abdullah Emir Cil et al[3]	Deep Neural Network (DNN)	Multiclass	94.57%	DNN has the advantage of performing both feature extraction and classification and hence It can detect the presence of a DDoS attack in small databases with a high degree of accuracy.
Ili Ko et al [4]	Complete Autoencoder (CA)	Binary Class	Average Recall > 97%	The method works well on the ISP domain. The DLS model outperforms other unsupervised model like K-means, single SOM, dual SOM model.
Meng Wang et al [5]	1. Sequential Backward selection (SBS) for feature selection and	Multiclass	97.66%	The SBS-MLP model could find the optimal feature subset and has better accuracy as compared to other

	2. Multi Layer Perceptron (MLP) for classification			MLP models. The feedback mechanism able to retract the detection error although it does not have any impact on the detection performance.
Zhendong Wu et al [6]	1. Semantic re-encoding and 2. Multi space projection algorithm based on Convolution Neural Network (CNN)	Multiclass	94.03%	The SRDLM method uses the several semantic dimensions of the network to re-encode which improves the generalization ability of the algorithm.
XuKui Li et al [7]	Auto-Encoder	Multiclass	Average AUC = 95%	The experimental results reveal that the model predicts with greater accuracy than other unsupervised models in a shorter amount of time.
S.M. Kasongo and Y.Sun[8]	1. Wrapper based Feature Extraction unit (WFEU) 2. Feed-Forward Deep Neural Network (FFDNN)	Binary class/Multiclass	1. UNSW-NB15 using multiclass classification= 77.16%, binary classification = 87.10% 2. AWID using multiclass classification= 99.77%, binary class= 99.66%	The result of the proposed model shows that FEU-FFDNN algorithm perform better than other ML models.
S.M. Kasongo and Y.Sun[9]	Filter-based Feed Forward Deep Neural Network (FEU-FFDNN)	Binaryclass/Multiclass	Binary classification = 87.74% Multiclass classification = 86.19%	The proposed method shows that the WFEU model generates a reduced feature subsets of 21 attribute. The result achieves high accuracy as compared to classical ML model.
Yingwei Yu et al [10]	Few-Shot Learning (FSL)	Binaryclass/Multiclass	1. On NSL-KDD = 92.33% 2. On UNSW-NB15 = 92%	The FSL method achieves remarkable performance on small size sample data like U2R and R2L which takes only 2% of the data.

Soodeh Hosseini et al[11]	1. Naïve Bayes 2. Decision tree 3. Random Forest 4. KNN and 5. MLP	Binary class	1. NSL-KDD Naïve Bayes= 98.4% Random Forest= 98.02% MLP= 98.80% 2. SIDDOS-HTTP flood attack dataset Naïve Bayes= 96.91% Random Forest= 98.70% MLP= 98.63%	The result of the proposed model shows that RF algorithm yields better result than the other classifiers used in the model.
Mohammad Hashem et al[12]	Voting-Based Neural Network (VNN) based on DNN, CNN, LSTM, GRU	Binary class/Multiclass	1. KDDCup99 using binary classification = 99.86%, Five-class classification = 95.63% 2. CTU-13 = 99.95%	When compared to other deep learning models, VNN outperforms them and decreased false alarm rate significantly.The proposed model needs to be applied to other new datasets.
Saikat Das et al [13]	1.MLP 2. SVM 3.KNN 4. Decision tree	Binary class	MLP = 96.5% SMO (SVM) = 95.73% IBK (KNN) = 97.83% J48 (DT) = 97.89%	The proposed model is capable of detecting and classifying 99.77% of the data with a low false rate and outperforming every other single classifier.
K.J. Singh et al [14]	1. Ensemble technique of information gain, SVM,Gain ratio, Correlation ranking, Chi square, ReliefF, Symmetrical uncertainty ranking filter 2. MLP	Binary class	98.3%	The ensemble method uses a collection of seven feature selection algorithms to calculate the average threshold value.More recent datasets should be used to test the approach.
Yuyang Zhou et al [17]	1. Correlationbased feature selection method and Bat-algorithm (CFS-BA) 2. Ensemble classifier.	Multiclass	1. NSL-KDD = 99.81% 2. AWID = 99.52% 3. CIC-IDS2017 = 99.89%	The CFS-BA selects the subsets of the best features using correlation base evaluation function and to remove the redundancy and reduce dimensionality

Roseline Oluwaseun et al [18]	1. Particle Swarm Optimization 2. KNN 3. Decision Tree	Binary class	1. PSO + DT = 98.6% 2. PSO + KNN = 99.6%	The proposed model demonstrates that the algorithm has a high level of accuracy and a low rate of false alarms. The model needs to be implemented on recent intrusion datasets.
Zahid Halim et al [19]	1. Genetic Algorithm based Feature Selection (GbFS) 2. SVM 3. KNN 4. extreme Gradient Boosting (XgBoost)	Multiclass	Average Accuracy = 98.11%	The novel GbFS module performs better when compared to other currentadvanced methods for feature selection.
Mahmoud Said El Sayed et al [20]	1. SD-Reg regularizer 2. CNN- SD-Reg 3. CNN- SVM 4. CNN- KNN 5. CNN- RF	Multiclass	Average accuracy on InSDN = 98.4% Average accuracy on UNSW-NB15= 99.31% Average accuracy on CSE-CIC-IDS2018 = 99.6%	The CNN based with a new technique of regularization the SD-Reg outperforms other hybrid models when implemented in a NIDS environment.

From the above table, most of the proposed models done by researchers are compared with Heuristic models for the feature selection. M. Di Mauro et al [1], Reddy SaiSindhuTheja et al[2], Roseline Oluwaseun et al [18], Zahid Halim et al [19] proved that using metaheuristic models such as PSO, OCSA and GbFs can give better feature reduction ability. In the case of Abdullah Emir Cil et al[3]and Sunanda Gamage et al [37],DNN model is used for both feature extraction and classification processes. The DNN model can classify different attack types with high accuracy rate. However, the work done by Saikat Das et al [13] and K.J. Singh et al [14] proved that the ensemble model gives better accuracy than other models.

5 Results and Discussion

From the given figure2, it can be observe that ensemble classifier and hybrid classifier have higher accuracy value and better detection rate as compare to other single ML classifiers. Most of the research works are done on NSL-KDD datasets except only a few are done on more recent datasets. Some of the informations we can deduce from our work are as follows: (i) Single classifiers work better when they are combined in an ensemble or hybrid model. And so, the hybrid model or ensemble models needs to be used in the later research works. (ii) In the case of unsupervised learning models autoencoders and complete autoencoders (CA) can learn the data more efficiently with low False Positive Rate (FPR). (iii) Some classifier models perform better on specific datasets and must be tested on multiple datasets to determine their efficacy. (iv) Feature selection techniques like the meta-heuristic, rank guided

algorithm can reduce features effectively in very less time. Furthermore, deep learning models are playing a remarkable role in machine learning and have a significant advantage over large datasets.

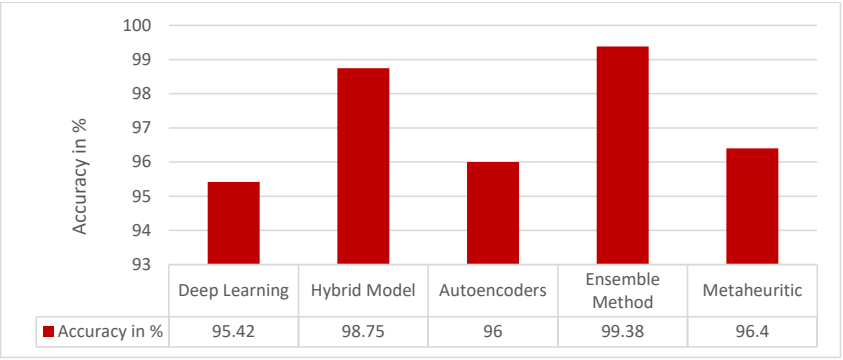

Fig. 2. Accuracy of different ML models

This article presented a literature review related to IDS research using machine learning FS and classification methods published from 2017 to 2021. We conclude that among the various techniques of IDS analyzed in our reviewed papers, models like the hybrid or ensemble manifested better accuracy and detection rates. Our long-term goal is to do additional experimental analysis on feature extraction models in order to reduce features to an appropriate subset and thereby increasing the rate of detection and accuracy of the IDS.

6 Conclusion

The Intrusion Detection System (IDS) plays a critical role for the security of computer systems and incoming network traffics by analyzing the data packets that passes through the system to check either being normal or malicious. But the problem remains with the dimensionality of the vast datasets which creates a challenge for the IDS to achieve high detection rates. To improve the performance of the IDS, multiple Machine Learning algorithms were usedto decrease the dimensionality of the enormous datasets which is a crucial step to influence the detection accuracy of the classifiers used.

This paper's main contribution is to present a survey of several IDS methodologies, types of feature selection and classification models thereby additional datasets and improvements can be made in the later research works.

References

[1] Mauro, M. et al. (2021). Supervised feature selection techniques in network intrusion detection: A critical review. *Engineering Applications of Artificial Intelligence*, 101: 104216.

[2] Theja, R. S. S. and Shyam, G. K. (2021). An efficient metaheuristic algorithm based feature selection and recurrent neural network for DoS attack detection in cloud computing environment. *Applied Soft Computing Journal*, 100: 106997.

[3] Cil, A. E., Yildiz, K. and Buldu, A. (2021). Detection of DDoS attacks with feed forward based deep neural network model. *Expert Systems with Applications,* 169: 114520.

[4] Ko, I., Chambers, D. and Barrett, E. (2020). Adaptable feature-selecting and threshold-moving complete autoencoder for DDoS flood attack mitigation. *Journal of Information Security and Applications*, 55: 102647.

[5] Wang, M., Lu, Y. and Qin, J. (2020). A dynamic MLP-based DDoS attack detection method using feature selection and feedback. *Computers & Security*, 88: 101645.

[6] Wu, Z. et al. (2020). A network intrusion detection method based on semantic Re-encoding and deep learning. *Journal of Network and Computer Applications*, 164: 102688.

[7] Li, X. K. et al. (2020). Building Auto-Encoder Intrusion Detection System based on random forest feature selection. *Computers and Security*, 95: 101851.

[8] Kasongo, S. M. and Sun, Y. (2020). A deep learning method with wrapper based feature extraction for wireless intrusion detection system. *Computers and Security*, 92: 101752.

[9] Kasongo, S. M. and Sun, Y. (2019). A deep learning method with filter based feature engineering for wireless intrusion detection system. *IEEE Access*, 7: 38597-38607.

[10] Yu, Y. and Bian, N. (2020). An intrusion detection method using few-shot learning. *IEEE Access*, 8: 49730-49740.

[11] Hosseini, S. and Azizi, M. (2019). The hybrid technique for DDoS detection with supervised learning algorithms. *Computer Networks*, 158: 35-45.

[12] Haghighat, M. H. and Li, J. (2021). Intrusion detection using voting-based neural network. *Tsinghua Science and Technology*, 26(4): 484-495.

[13] Das, S. et al. (2019). DDoS Intrusion Detection through Machine Learning Ensemble. In *IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*.

[14] Singh, K. T. and De, T. (2017). Efficient Classification of DDoS Attacks Using an Ensemble Feature Selection Algorithm. *Journal of Intelligent Systems*, 29(1).

[15] Khraisat, A. et al. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, 2: 20.

[16] Ravipati, Devi, R. and Munther, A. (2019). Intrusion Detection System Classification Using Different Machine Learning Algorithms on KDD-99 and NSL-KDD Datasets - A Review Paper. *International Journal of Computer Science & Information Technology*, 11(3).

[17] Zhou, Y. et al. (2020). Building an efficient intrusion detection system based on feature selection and ensemble classifier. *Computer Networks*, 174: 107247.

[18] Ogundokun, R. O. et al. (2021). An enhanced Intrusion Detection System using particle swarm optimization feature extraction technique. *Procedia Computer science*, 193: 504-512.

[19] Halim, Z. et al. (2021). An effective genetic algorithm-based feature selection method for intrusion detection systems. *Computers & Security*, 110: 102448,

[20] ElSayed, M. S. et al. (2021). A novel hybrid model for intrusion detection systems in SDNs based on CNN and a new regularization technique. *Journal of Network and Computer Applications*, 191: 103160.

[21] Lee, S. N. et al. (2021). Towards secure intrusion detection systems using deep learning techniques: Comprehensive analysis and review. *Journal of Network and Computer Applications*, 187: 103111.

[22] Saranya, T. et al. (2020). Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review. *Procedia Computer Science*, 171: 1251-1260.

[23] Yerriswami, T. and Murtugudde, G. (2021). An efficient algorithm for anomaly intrusion detection in a network. *Global Transitions Proceedings*, 2(2): 255-260.

[24] Ji, S. et al. (2020). A Network Intrusion Detection Approach Based on Asymmetric Convolutional Autoencoder. In *Zhang Q., Wang Y., Zhang LJ. (eds) Cloud Computing – CLOUD 2020*.

[25] Asharf, J. et al. (2020). A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions. *Electronics,* 9: *1177*.

[26] Aldweesh, A. et al. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, 189: 105124.

[27] Tang, C., Luktarhan, N. and Zhao, Y. (2020). An Efficient Intrusion Detection Method Based on Light GBM and Autoencoder. *Symmetry*, 12: 1458.

[28] Sharma, N. V. and Yadav, N. S. (2021). An optimal intrusion detection system using recursive feature elimination and ensemble of classifiers. *Microprocessors and Microsystems*, 85: 104293.

[29] Zavrak, S. and İskefiyeli, M. (2020). Anomaly-Based Intrusion Detection from Network Flow Features Using Variational Autoencoder. *IEEE Access*, 8: 108346-108358.

[30] Zhang, H. et al. (2018). An Effective Deep Learning Based Scheme for Network Intrusion Detection. In *24th International Conference on Pattern Recognition (ICPR),* 682-687.

[31] Zhang, Y. et al. (2020). A network intrusion detection method based on deep learning with higher accuracy. *Procedia Computer Science*, 174: 50-54.

[32] Hande, Y. and Muddana, A. (2020). A Survey on Intrusion Detection System for Software Defined Networks (SDN). *International Journal of Business Data Communications and Networking*, 16(1): 28-47.

[33] Idrissi, I., Azizi, M. and Moussaoui, O. (2020). IoT security with Deep Learning-based Intrusion Detection Systems: A systematic literature review. In *Fourth International Conference on Intelligent Computing in Data Sciences (ICDS),* 1-10.

[34] Khalaf, B. A. et al. (2019). Comprehensive Review of Artificial Intelligence and Statistical Approaches in Distributed Denial of Service Attack and Defense Methods. *IEEE Access*, 7: 51691-51713.

[35] Qatf, M. A. et al. (2018). Deep Learning Approach Combining Sparse Autoencoder with SVM for Network Intrusion Detection. *IEEE Access*, 6: 52843-52856.

[36] Liu, H. and Lang, B. (2019). Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. *Applied Sciences*, 9: 4396.

[37] Gamage, S. and Samarabandu, J. (2020). Deep learning methods in network intrusion detection: A survey and an objective comparison. *Journal of Network and Computer Applications*, 169: 102767.

[38] Ahmad, R. and Alsmadi, I. (2021). Machine learning approaches to IoT security: A systematic literature review. *Internet of Things*, 14: 100365.

[39] Pitropakis, N. et al. (2019). A taxonomy and survey of attacks against machine learning. *Computer Science Review*, 340: 100199.

[40] Gao, X. et al. (2019). An Adaptive Ensemble Machine Learning Model for Intrusion Detection. *IEEE Access*, 7: 82512-82521.

[41] Bhati, B. S. et al. (2020). An intrusion detection scheme based on the ensemble of discriminant classifiers. *Computers & Electrical Engineering*, 86: 106742.

[42] Alazzam, H., Sharieh, A. and Sabri, K. E. (2020). A feature selection algorithm for intrusion detection system based on Pigeon Inspired Optimizer. *Expert Systems with Applications*, 148: 113249.