Machine and Deep Learning Based Comparative Analysis Using Hybrid Approaches for Intrusion Detection System

Azam Rashid
Computer Department.
Board of Intermediate and Secondary Education, Lahore.
Lahore, Pakistan.
azamrashid@gmail.com

Muhammad Jawaid Siddique
Faculty of Information Technology.
Pakistan Institute of Management.
Lahore, Pakistan.
jawaid@imforhelp.org

Shahid Munir Ahmed
Network Administrator
Institute of Business Administration
University of Punjab
Lahore, Pakistan
shahidmunir49@yahoo.com

***Abstract*— Intrusion detection is one of the most prominent and challenging problem faced by cybersecurity organizations. Intrusion Detection System (IDS) plays a vital role in identifying network security threats. It protects the network for vulnerable source code, viruses, worms and unauthorized intruders for many intranet/internet applications. Despite many open source APIs and tools for intrusion detection, there are still many network security problems exist. These problems are handled through the proper pre-processing, normalization, feature selection and ranking on benchmark dataset attributes prior to the enforcement of self-learning-based classification algorithms. In this paper, we have performed a comprehensive comparative analysis of the benchmark datasets NSL-KDD and CIDDS-001. For getting optimal results, we have used the hybrid feature selection and ranking methods before applying self-learning (Machine / Deep Learning) classification algorithmic approaches such as SVM, Naïve Bayes, k-NN, Neural Networks, DNN and DAE. We have analyzed the performance of IDS through some prominent performance indicator metrics such as Accuracy, Precision, Recall and F1-Score. The experimental results show that k-NN, SVM, NN and DNN classifiers perform approx. 100% accuracy regarding performance evaluation metrics on the NSL-KDD dataset whereas k-NN and Naïve Bayes classifiers perform approx. 99% accuracy on the CIDDS-001 dataset.**

***Index Terms*— Deep Learning, Machine Learning, Intrusion Detection, Intrusion Detection System (IDS), Cyber Security**

I. Introduction

In recent days, it's too difficult to find out the intrusion in local and global networks by conventional techniques, like encryption and firewall; because of the intrusion is wrapped with malicious source code in the form of viruses, Trojan horse and worms. Although significant development has done in network security field but the existing systems are not fully capable to defend network security threats. The unauthorized users are trying to enter in large-scale networks.

Intrusion detection system (IDS) [1] plays a vital role to solve the security threats. It is used to achieve two major purposes. 1) to identify the behavior of network activities and known attacks over networks 2) to identify the unknown attacks that breach the security policies in networks. Intrusion detection based on two techniques: anomaly based intrusion and signature based intrusion. Anomaly based intrusion detection is further investigated through self-learning based methods.

In this paper, we perform statistical comparative analysis on benchmark datasets NSL-KDD and CIDDS-001. We apply hybrid feature selection and ranking methods on dataset attributes, then applying different self-learning (machine/deep learning) classification approaches for detecting intrusion. Conventional IDS do not apply proper implementation of pre-processing, normalization, feature selection and machine learning classification on raw data or data mining datasets. But our proposed methodological work produces highest performance on cutting-edge classifiers.

We divide this paper into multiple sections that briefly highlight the intrusion detection system, machine and deep learning classification approaches, benchmark datasets, experimental criteria, future research work and finally the concluding synopsis. In section II, we discuss some related research works. In section III, we explain the general definition, historical prospective, types and operations of IDS for intrusion detection. Similarly, section IV & V describe the benchmark datasets, experimental criteria, methodology, and comparative analysis of multiple self-learning approaches on benchmark datasets. In the last section, we briefly focus on future research work and concluded our paper.

II. Related Work

Machine and Deep Learning approaches play a vital role for the detail analysis of anomaly based intrusion detection by deploying supervised, semi-supervised and unsupervised learning algorithms such as support vector machine, k- nearest neighbor, neural networks, deep neural networks, recurrent neural networks, convolutional neural networks, deep belief

978-1-7281-4235-7/20/$31.00 ©2020 IEEE

networks, restricted boltzmann machines, deep boltzmann machines and deep auto encoders. Many researchers have applied these machine learning techniques on benchmark publically available datasets for analyzing the best performance indicator metrics such as accuracy, precision, recall and positive / false alert rate. Some important previous research work done as follows.

Zhou, Liang et al. [2] proposed a system that uses a deep neural network model for the classification of cyberattacks. The system is based on three phases: 1) Data acquisition 2) Data pre-processing. 3) Deep neural network classification. They used global optical parameters to achieve high performance accuracy approx. 96.30% on SVM model with a learning rate 0.01, training epochs 10, and input units 86. The results show that SVM model performs better than other traditional machine learning algorithms: random forest, linear regression, and k-nearest neighbourhood.

S. Naseer et al. [3] investigated the anomaly based intrusion detection system. They built a model that uses various machine and deep learning algorithms for anomaly based intrusion detection on NSL-KDD dataset. They compared the conventional machine learning classification algorithms k-nearest neighbour, SVM, Random Forest and Decision Tree to deep convolutional neural network (DCNN) and LSTM models and claimed approx. 85-89% accuracy on NSL-KDD test dataset.

Jiang et al. [4] proposed a multi-channel intrusion detection system that uses long short term memory recurrent neural networks (LSTM-RNNs). They integrated the data pre-processing, feature abstraction, multi-channel training and detection in the intrusion detection algorithm. The performance of the proposed system analysed on NSL-KDD dataset. The system reported approx. 98.94% accuracy and 99.23% detection rate.

M. Tavallee [5] proposed the multi-layered hybrid network intrusion detection system. They compared the performance of the NSL-KDD dataset on different machine learning classification algorithms including Naive-Bayes, Support Vector Machines, and Decision-Trees. The hybrid detector reported approx. 91% accuracy.

Shone et al. [6] proposed a model that combines the deep and shallow learning, capable of correctly analyzing a wide-range of network traffic named as non-symmetric deep autoencoder (NDAE) for unsupervised feature learning. They implemented the classifier in graphics processing unit (GPU)-enabled Tensor Flow and evaluated on the benchmark KDD Cup '99 and NSL-KDD datasets.

Salama et al. [7] proposed a model that combines the restricted boltzmann machine and support vector machine classifiers for intrusion detection on NSL-KDD dataset. They selected 22 attack types in training set and 17 attack types in testing set. The model produced the highest performance as compared to traditional support vector machine.

Biswas et al. [8] investigated various feature selection methods and classification techniques to minimize the redundancy in data attributes through the combination of CFS, PCA and IGR feature selection methods prior to apply the classification algorithms like SVM, k-NN, NN, DT and NB. The experimental results on NSL-KDD dataset show that the performance of k-NN classifier is better than other classifiers and also the Information Gain Ratio (IGR) feature selection method produces highest performance than other feature selection methods.

Zhao et al. [9] proposed the intrusion detection technique using the combination of Deep Belief Network (DBN) and Probabilistic Neural Network (PNN). In this technique, they convert the raw data into low-dimensional data by using non-linear learning model to classify the low-dimensional data. The experiments performed on KDD Cup99 dataset. The results show that the performance of proposed model is comparatively better than traditional techniques PNN, PCA-PNN and DBN-PNN.

III. Intrusion Detection System and How it Works

Intrusion Detection System (IDS) is a system that monitors network and host-based traffic for vulnerable malicious threats in manual or automatic manner and also generates false positive alerts. In between 1984 to 1986, Dorothy Denning and Peter Neumann developed a first model of real-time intrusion detection system named as Intrusion Detection Expert System (IDES).

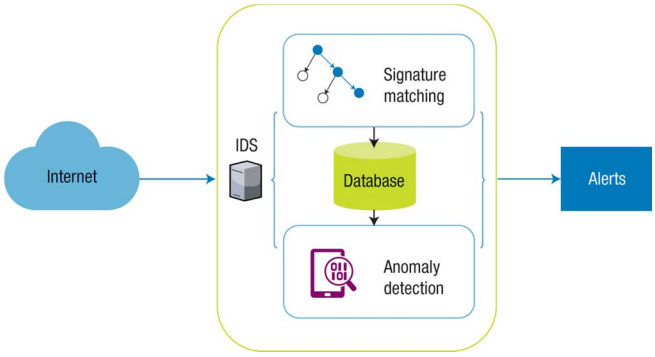

Fig. 1. Intrusion Detection System (IDS)

In early 2000, Network Intrusion Detection Systems (NIDS) became the best practice of network security and replaced firewalls that encountered multiple threats of network traffic. There are four eras or generations for the evolution of IDS in monitoring network traffic. Firstly, the concept of intrusion detection has introduced in 2000 for some small scale networks in parallel to firewalls because it bypass the cross site scripting threats and SQL malicious queries. The second

era started in 2005 when the IPS began to grow and more vendors supported the intrusion detection technology models. In between 2011 to 2015, Next Generation Intrusion Prevention Systems (NGIPS) came into the market along with application and user control features. A traditional IPS investigates network traffic looking for known attack signatures. It generates alerts on traffic or shutdown network traffic activities.

Since 2016 onwards the next generation firewalls are introduced by many vendors such as Cisco, Symantec, IBM, etc. Security vendors are focusing on high-fidelity machine learning, which uses algorithms to analyze files, and uses noise cancellation techniques like census and whitelist checking. As machine-learning grows, attackers are discovering different ways to breach network security policies. IPS vendors are still working to create the upcoming network security threats antidote.

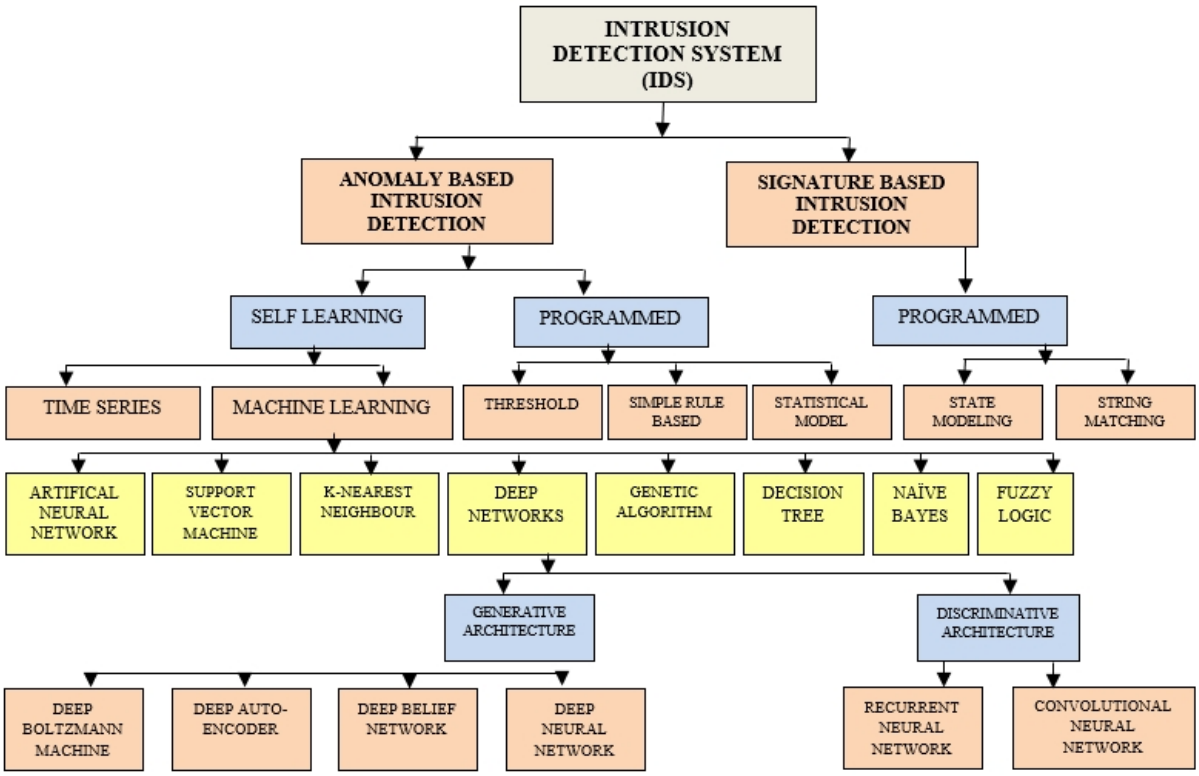

Fig. 2. Hierarchical Classification of Intrusion Detection System (IDS).

III-A. Types of Intrusion Detection Systems

A. Network Intrusion Detection Systems (NIDS)

NIDS [13] are used for statistical measures and the computation of thresholds on feature vectors such as time stamps, traffic flow size and other hyper parameters related to network traffic within a specified time interval. Network based intrusion analyzes during the sharing of data packets over the network. The whole network monitors during the sharing of data packets from source to destination address location.

The performance of NIDS is measured by false negative and false positive alerts rate. High false negative alerts indicate that the NIDS could fail to detect known or unknown attacks. Similarly high false positive alerts indicate that NIDS could unnecessarily generate alerts when no attack is actually happened in network traffic. It is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts.

B. Host Based Intrusion Detection Systems (HIDS)

HIDS [13] operates the host-level by monitoring and analyzing all network traffic activities on the system application log files, system log files or system calls and operating system log files. Such network traffic activities are called audit trails. System calls are used for the communication of application software to the operating system resources and also distinguish the known and unknown applications. HIDS based on three major components named as data source, the sensors and the decision engine. The sensor monitor changes in data source and the decision engine uses machine learning modules to implement the intrusion detection mechanism.

C. Hybrid Intrusion Detection Systems

Anomaly based intrusion detection systems [5] have a great capability for detecting unknown or zero-day vulnerabilities. To overcome current and future challenges and getting benefits of misuse or signature-based anomaly detection, some researcher provides the idea of hybrid intrusion detection systems. They divide into two categories. 1) Sequence based detection, in which either anomaly detection or misuse detection applied first. 2) Parallel based detection, in which multiple intrusion detectors are applied in a parallel way and the final decision based on multiple output sources.

Conventional Hybrid IDS detects intrusion with the combination of anomaly and signature or misuse detection altogether. In such systems, the anomaly detection detects the unknown attacks and the signature detection detects the known attacks.

III-B. Intrusion Detection Techniques

Intrusion detection is used to detect the network and host based traffic vulnerabilities. Normally, there are two types of techniques used for intrusion detection: Anomaly based intrusion detection and signature or misuse based intrusion detection. Nowadays, another progressive technique is used for intrusion detection is stateful protocol analysis.

A. Anomaly Based Intrusion Detection

Anomaly based intrusion detection refers to the classification problem in supervised learning in which we build a model of legitimate activities based on normal data. Any deviation that occurs in normal model is considered an attack or anomaly. The training and testing of model is done through the machine learning classification techniques. It is used to detect unknown intrusion for both network and host based on feature vectors.

B. Signature Based Intrusion Detection

Signature or misuse based intrusion detection refers to unsupervised learning classification models that do not require the labelled training data.

C. Stateful Protocol Analysis

Stateful protocol analysis acts better than Anomaly and Signature based detection methods. Stateful protocol analysis acts on the network layer, application layer, and transport layer. It uses the predefined vendor's specification settings to detect the deviations of appropriate protocols and applications.

IV. BENCHMARK DATASETS

The intrusion detection methods (supervised or unsupervised) determine the properties of datasets. Some benchmark or well-known datasets are as follows.

A. KDD Cup99

Knowledge Discovery and Dissemination (KDD) Cup99 is a benchmark dataset most widely used for anomaly based intrusion detection. The dataset created in KDD Cup challenge since 1999. It contains over 4 million network traffic records and 42 attributes or features about protocols (tcp, icmp, udp) connections. The dataset includes 5 million data records that encompass over 21 different types of attacks (e.g. DoS, Guess_passwd, buffer overflow) and comes along with an explicit test subset.

B. NSL-KDD

NSL-KDD is a refined version of KDD Cup99. It contains essential records and all attributes of KDD dataset. It removed duplicates from the KDD CUP 99 dataset and created more sophisticated subsets. The resulting dataset contains about 130,000 data points and divided into pre-defined training and test subsets for intrusion detection methods. The dataset is publicly available.

C. CIC-IDS 2017

The dataset contains eight different files containing five days normal and attacks traffic data of Canadian Institute of Cybersecurity. It contains benign and the most up-to-date common attacks such as Brute Force FTP, Brute Force SSH, DoS, DDoS, Heartbleed, Web Attack, Infiltration, and Botnet. It resembles the true real-world data (PCAPs). It also includes the results of the network traffic analysis using CICFlowMeter. The data label flow based on the time stamp, source, and destination IPs, source and destination ports, protocols and attack.

D. CSE-CIC-IDS 2018

The dataset is collected from Amazon´s AWS LAN network (CIC-AWS-2018) by the Canadian Institute of Cybersecurity (CIC). It includes seven different attack classes, named as Brute-force, Heartbleed, Botnet, DoS, DDoS, Web attacks, and infiltration of the network. The attacking infrastructure includes 50 machines and the victim organization has 5 departments includes 420 PCs and 30 servers. The dataset includes network traffic and log files of each machine from the victim side, along with 80 network traffic features extracted from captured traffic using CICFlowMeter-V3.

E. UNSW-NB15

The dataset is created with the help of IXIA Perfect Storm tool in a small emulated environment over 31 hours. It contains one normal class and nine attack classes such as backdoors, DoS, exploits, fuzzers, or worms. The dataset is available in flow-based format with additional attributes. It comes along with predefined splits for training and test. The dataset includes 45 distinct IP addresses and is publicly available.

F. CIDDS-001 / CIDDS-002

Ring M et at [10] created a CIDDS-001 (Coburg Intrusion Detection dataset). It's a labelled flow-based dataset used for the evaluation of anomaly-based intrusion detection. They captured approx. 32 million data flow from two sources: Open Stack Servers and External Servers. It includes 92 attacks. 70

attacks executed within the OpenStack environment and 22 attacks targeted the external server. They use Week 3 External Server traffic data file for analysis. It contains 159373 records having 12 feature vectors. Every traffic record instance is labelled as normal, suspicious, unknown, attacker and victim classes.

CIDDS-002 [10] is a port scan dataset which is created through the scripts of CIDDS-001. It contains two weeks of unidirectional flow-based network traffic within an emulated small business environment. CIDDS-002 contains normal user behavior and a wide range of different port scan attacks. The dataset is publicly available.

V-A. EXPERIMENTAL CRITERIA AND METHODOLOGY

A. Experiment Setup

There are many open source and licensed tools (WEKA, Rapid Miner, etc.), available to perform data mining processes such as data pre-processing, normalization, feature selection, clustering, regression, and classification. We used open source machine learning, visualization and automated data mining toolkit "Orange 3.23.1" along with Python 3.6 scripting, Keras on the top of Tensor flow libraries to perform hybrid feature selection and classification approaches to get optimal results on benchmark datasets NSL-KDD and CIDDS-001. In NSL-KDD 24 attacks are grouped into four classes: DoS, Probe, R2L, U2R. CIDDS-001 dataset based on 80 attacks are also grouped into four major classes: DoS, BruteForce PortScan and PingScan.

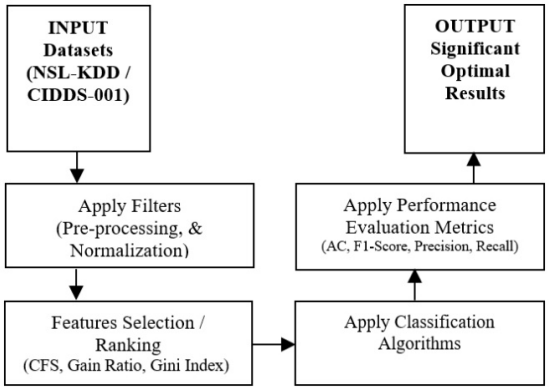

Fig.3. Proposed Methodology for Experimental Analysis.

B. Source Datasets

The experimental results based on two benchmark datasets. (1) NSL-KDD (2) CIDDS-001. NSL-KDD is a refined version of KDD Cup99. It contains essential records of KDD dataset. Each record contains 41 attributes unfolding different features and 1 label attribute based on one normal class and four attack classes. The attack classes are divided into four groups named as DoS (Denial of Service Attack), Probe (Scan and Detected Vulnerability), U2R (without permission granted by local users), R2L (unauthorized remote access attack). The attribute 1~9 is the basic characteristics of each network connection, 10~22 is the content-related features of each network connection, 23~31 is the time-related traffic characteristic of each network connection, and 32~41 is the host-based traffic features of each network connection and the last attribute label marks attack type or whether for normal data. Table no I, shows the details of normal and attack classes and their types of data in training and test datasets.

TABLE I
DETAIL OF NORMAL AND ATTACK CLASSES / TYPES DATA IN NSL-KDD TRAIN / TEST DATA SETS

Attack / Normal Class	Attack Type	Records In KDD Train+	Records In KDD Test+
Normal	Normal	67343	9711
DoS	Teardrop, Back, Land, Pod, Smurf, Neptune, Apache2, Worm, Udpstorm, Processtable,	45927	7458
Probe	Saint, Satan, Ipsweep, Portsweep, Mscan, Nmap	11656	2421
R2L	Named, Guess_passwd, Imap, Phf, Multihop, Warezmaster, Warexclent, Ftp_write, Spy, Snmpguess, Snmpgetattack, Xlock, Xsnoop, Httptunnel, Sendmail	995	2754
U2R	Rootkit, Buffer_overflow, Loadmodule, Sqlattack, Perl, Xterm, Ps	52	200
Total		125973	22544

Table II shows the distribution of CIDDS-001 dataset records. It's a labelled flow-based dataset used for the evaluation of anomaly-based intrusion detection. It includes 1 normal and 92 attack classes. It contains 159373 records having 12 feature vectors. Every traffic record instance is labelled as normal, suspicious, unknown, attacker and victim classes.

TABLE II
DETAIL OF NORMAL AND ATTACK CLASSES DATA IN CIDDS-001 DATASET

Attack / Normal Class	Attack Description	Records In CIDDS-001
Normal	Normal connections records	28426
Attacker	Portscan, Pingscan, Bruteforce, Dos	2389
Suspicious	---	116588
Unknown	---	9571
Victim	Portscan, Pingscan, Bruteforce, Dos	2389
Total		159373

C. Data Pre-processing

NSL-KDD dataset has 41 attributes per data, including 3 symbol attributes and 38 numerical attributes. In order to be recognized by the algorithm, data is needed to pre-processing before detection.

1) Character data conversion

In NSL-KDD dataset, three attributes name as "Flag_type, Protocol and Service) are in nominal format that can be converted into numerical form (0, 1,2, etc). The flag type data can be converted to rej-0, rsto-2, ..., other-7, etc. Protocol type data can be converted into values: tcp-1, icmp-2, udp-3. The

same criteria apply to the service attribute. The whole process is being done by 1-hot-encoding

2) Data normalization
Data normalization is a basic work of data mining. Because the dimensions and units used in data collection are different, the value range of data often varies, and it is prone to large data eat the small. In order to avoid such a situation, this paper mainly adopts the maximum and minimum algorithm to normalize the data, and its calculation formula is as follows:

$$y = \frac{x-min}{max-min} \quad (1)$$

D. Feature Selection & Ranking
The network data always contains many features that are irrelevant or contain little information. These features have little effect on the classification results. The feature selection algorithm mainly eliminates these redundant features and reduces the impact of redundant features on the classification algorithm.
There are many feature selection & ranking methods and algorithms are available for removing redundancy in dataset attributes to achieve better classification results such as Correlation Feature Selection Algorithm (CFS), Random Forest Feature Selection Algorithm (RFFS), Information Gain Ratio, Gini Index, etc. We applied hybrid feature selection methods (CFS, IGR, Gini Index) on 42 features of NSL-KDD dataset and get top ranked 11 features for classification. Similarly, hybrid feature selection methods applied on 12 attributes of CIDDS-001 dataset and get top ranked 11 features for classification.

1) Correlation Based Feature Selection (CFS)
CFS [9] algorithm mainly searches for feature subsets based on the redundancy between features. The purpose is to find feature subsets with high correlation and low correlation between features. The algorithm overcomes the single variable screening and fully considers the interdependence of feature scan effectively eliminate features that are not related. The feature subset evaluation function of CFS is as follows:

$$Merit_s = kr_{cf} / k+(k-1)r_{ff} \quad (2)$$

Where $Merit_s$ is a heuristic 'merit' containing a feature subset S of k features, r_{cf} is a feature class average correlation, and r_{ff} is a feature-feature average correlation. r is the Pearson correlation coefficient and all variables need to be normalized.

2) Information Gain Ratio (IGR)
The Information Gain method is biased towards the high-branch attributes having more values. Information Gain Ratio (IGR) removes the biasness of high-branch attributes. It corrects the information gain by taking the intrinsic information of a split account patterns. Gain Ratio of attribute decreases as value of intrinsic information increases.

$$IGR(Class, Attributes) = \frac{H(Class) - H(Class \mid Attribute))}{H(Attribute)} \quad (3)$$

3) Gini Index
Corrado Gini, an Italian statistician and sociologist since 1912 developed the Gini index. It measures the statistical dispersion of income distribution across different population sectors. Recently, it widely used for data mining. The Gini Index is calculated by subtracting the sum of the squared probabilities of each class attributes to one. It favors the high-branch attributes. A high decrease in Gini index indicates a high importance of the feature for a correct classification.

$$Gini = 1 - \sum_{i=1}^{C} (p_i)^2 \quad (4)$$

E. Classification Algorithms
There are many machine learning algorithms are used for the classification of intrusion detection. We selected some of them that are as follows.

1) Naive Bayes classifier is one of the classic models in the classification field because of its simplicity and high computational performance. It based on Bayes' theorem, it is assumed that the influence of each feature parameter on a given type is independent of each other, and the classification result is identified by known prior probability and conditional probability. The advantage is that it is insensitive to missing data and can quickly and efficiently get classification results.

2) Support Vector Machine (SVM) [12] is based on the principle of structural risk minimization, looking for an optimal interval to divide the instance into two categories.

3) k-Nearest Neighbour (k-NN) [11] is a simple and effective method for target classification based on the most recent training samples into feature space. When the prior knowledge about the data distribution is little or no prior knowledge, the KNN classifier transforms the samples into metric space and classifies new points based on the majority of votes obtained from the K nearest points in the training data. Usually, the Euclidean distance is often used as a distance metric to measure the similarity between two vectors.

4) Neural Networks (NN) is based on the principle of structural risk minimization, looking for an optimal interval to divide the instance into two categories.

5) Deep Neural Networks (DNN) is a refined form of Artificial Neural Network (ANN) having more than one hidden layer between input and output layers. DNN based on multilayer perceptron's (MLP) with a number of layers superior to three. MLP is a class of feed forward artificial neural network, which is defined by the *n* layers that compose it and succeed each other.

6) Deep Auto-encoders (DAE) is a popular technique used for deep learning. An auto-encoder is an unsupervised neural network-based feature extraction algorithm, which learns the best parameters required to reconstruct its output as close to its input as possible. An auto-encoder typically has an input layer, output layer (with the same dimension as the input layer) and a hidden layer. This hidden layer normally has a smaller dimension than that of the input (known as an under complete or sparse auto-encoder).

F. Evaluation Metrics

Evaluation or Performance Metrics are used to evaluate the performance of Intrusion detection systems (IDS) by using machine learning classification algorithms. The predicted outcomes are between the range 0 to 1. The confusion matrix shows the statistical results on the basis of actual or predicted records in a dataset. The most commonly used evaluation metrics are as follows.

1) Accuracy: It is the estimated ratio of correctly recognized data records to the total number of data records in a given data set. The higher rate of accuracy shows that the machine learning model is performed better. (Accuracy [0,1]) is defined as follows.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (5)$$

2) Precision: It is the estimated ratio of correctly identified attack data records to the total number of all identified data records in a given dataset. The higher rate of precision shows that the machine learning model is performed better. (Precision [0,1]) is defined as follows.

$$\text{Precision} = \frac{TP}{TP+FP} \quad (6)$$

3) Recall: It is the estimated ratio of correctly classified attack data records to the total number of attack data records in a given dataset. The higher rate of recall shows that the machine learning model is performed better (Recall [0,1]) is defined as follows.

$$\text{Recall} = \frac{TP}{TP+FN} \quad (7)$$

4) F1-Score / F1-Measure: It is the harmonic mean of Precision and Recall. The higher rate of F1-Score shows that the machine learning model is performed better. (F1-Score [0,1]) is defined as follows.

$$\text{F1-Score} = 2 \text{ x } \left[\frac{Precision\ x\ Recall}{Precision+Recall}\right] \quad (8)$$

In above Equations, the term TP, TN, FP and FN are used for describing the classification of Normal and Attack records in a dataset. TP (True Positive) defines that the number of connection records correctly classified or identified into Normal class of dataset similarly TN (True Negative) defines that the number of connection records correctly classified or identified into an attack class of dataset. FP (False Positive) defines that the number of normal class connection records are wrongly classified or identified into attack class similarly FN (False Negative) defines that the number of attack class connection records are wrongly classified or identified into normal class connection records.

V-B. EXPERIMENTAL RESULTS AND ANALYSIS

In all experiments, we tuned our datasets NSL-KDD and CIDDS-001 on 10-fold cross-validation. In k-NN classification, we set the parameter values Neighbours= 5, Metric= Euclidean and Weight: Uniform. In Neural Networks classification, we set the parameter values Activation= Relu, Hidden Layers= 10. In SVM classification, we set the parameter values Cost (C)= 1.00, Kernel= RBF, Regression Loss Epsilon= 0.10. In DNN classification, we set the parameter values Activation= Relu, Hidden Layers=10.

Table III & Table IV shows the performance of six classifiers (k-NN, Naïve Bayes, SVM, NN, DNN, DAE) on NSL-KDD & CIDDS-001 datasets.

TABLE III
PERFORMANCE COMPARISON OF STATE-OF-THE-ART CLASSIFIERS ON NSL-KDD DATASET

Attack Type	Algorithm	Accuracy	F1 Score	Precision	Recall
Normal	k-NN	0.996	0.996	0.997	0.995
	Naïve Bayes	0.975	0.977	0.979	0.995
	SVM	1.000	1.000	0.999	1.000
	NN	1.000	1.000	1.000	1.000
	DNN	1.000	1.000	1.000	1.000
	Autoencoder	0.999	0.997	1.000	0.998
DOS	k-NN	0.997	0.996	0.994	0.998
	Naïve Bayes	0.979	0.971	1.000	0.943
	SVM	1.000	1.000	1.000	1.000
	NN	1.000	1.000	1.000	1.000
	DNN	1.000	1.000	1.000	1.000
	Autoencoder	0.998	0.997	0.999	0.999
Probe	k-NN	0.996	0.977	0.981	0.974
	Naïve Bayes	0.991	0.954	0.916	0.996
	SVM	1.000	0.999	1.000	0.998
	NN	0.999	1.000	1.000	0.999
	DNN	1.000	1.000	1.000	1.000
	Autoencoder	0.994	0.992	0.994	0.995
R2L	k-NN	0.999	0.951	0.954	0.948
	Naïve Bayes	0.995	0.743	0.603	0.966
	SVM	1.000	0.993	1.000	0.987
	NN	0.998	0.995	0.997	0.994
	DNN	1.000	0.998	1.000	0.997
	Autoencoder	0.987	0.982	0.980	0.979
U2R	k-NN	1.000	0.480	0.783	0.346
	Naïve Bayes	0.990	0.073	0.038	0.962
	SVM	1.000	0.928	1.000	0.865
	NN	0.997	0.951	0.962	0.971
	DNN	1.000	0.975	0.972	0.981
	Autoencoder	0.950	0.921	0.957	0.948

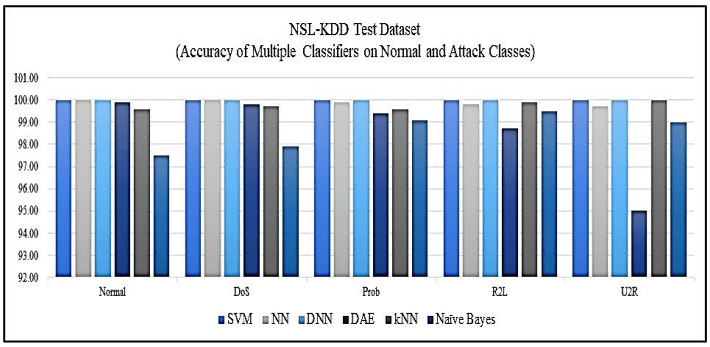

Fig.4. Graphical representation for the accuracy of multiple Classifiers on NSL-KDD Dataset

TABLE IV
PERFORMANCE COMPARISON OF STATE-OF-THE-ART CLASSIFIERS ON CIDDS-001 DATASET

Attack Type	Algorithm	Accuracy	F1 Score	Precision	Recall
Normal	SVM	0.515	0.272	0.186	0.509
	k-NN	0.994	0.985	0.973	0.997
	Naïve Bayes	0.994	0.983	0.991	0.975
	NN	0.822	0.000	0.000	0.000
	DNN	0.850	0.000	0.000	0.000
	Autoencoder	0.822	0.795	0.810	0.805
Attacker	SVM	0.888	0.039	0.022	0.150
	k-NN	1.000	0.988	0.979	0.997
	Naïve Bayes	1.000	0.999	0.999	0.999
	NN	0.985	0.000	0.000	0.000
	DNN	0.989	0.000	0.000	0.000
	Autoencoder	0.985	0.000	0.000	0.000
Suspicious	SVM	0.318	0.177	0.754	0.100
	k-NN	0.972	0.981	0.982	0.980
	Naïve Bayes	0.954	0.968	0.985	0.952
	NN	0.732	0.845	0.732	1.000
	DNN	0.710	0.885	0.752	1.000
	Autoencoder	0.732	0.845	0.732	1.000
Unknown	SVM	0.689	0.106	0.064	0.307
	k-NN	0.978	0.808	0.834	0.784
	Naïve Bayes	0.958	0.715	0.603	0.880
	NN	0.940	0.000	0.00	0.000
	DNN	0.967	0.000	0.00	0.000
	Autoencoder	0.940	0.000	0.00	0.000
Victim	SVM	0.985	0.627	0.496	0.854
	k-NN	1.000	0.988	0.981	0.996
	Naïve Bayes	0.999	0.999	0.999	0.999
	NN	0.985	0.000	0.00	0.000
	DNN	0.985	0.000	0.00	0.000
	Autoencoder	0.985	0.000	0.00	0.000

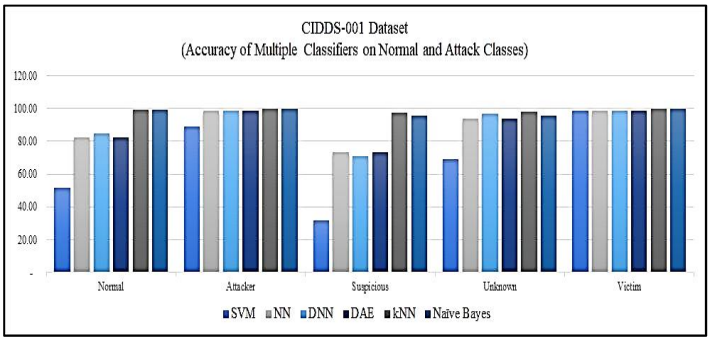

Fig.5. Graphical representation for the accuracy of multiple Classifiers on CIDDS-001 Dataset.

TABLE V
COMPARATIVE PERFORMANCE ANALYSIS FOR MULTIPLE CLASSIFIERS TO PROPOSED METHODOLOGY WORK ON NSL-KDD DATASET

Classification Algorithm	Feature Selection Methods	Ref No / Year	Accuracy
k-NN	IGR & PCA	[8] 2018	99.80
Naïve Bayes			90.29
SVM			94.78
NN			94.70
J48	Hybrid (CFS,IG & DT)	[14] 2017	99.93
Bayes Net (NN)			96.26
SVM			99.83
MLP (NN)			99.36
DNN	Normalization(Min-Max)	[15] 2018	66.60
RNN			79.20
Autoencoder			98.90
Intrusion-Miner	PCA & FDR	[16] 2019	96.10
k-NN	Hybrid (CFS, IGR, Gini Index)	This Work 2020	99.80
Naïve Bayes			98.60
SVM			100
NN			99.90
DNN			99.90
Autoencoder			98.60

The experimental results show that in Table III, SVM & DNN classifiers with hybrid feature selection methods (CFS, IGR & Gini Index) produce the highest performance on normal and attack classes (DoS, Probe, R2L, U2R) among all the classifiers but Naïve Bayes produces the lowest performance on NSL-KDD dataset. Similarly, in Table IV, k-NN & Naïve Bayes produce the highest accuracy on normal and attack classes on CIDDS-001 dataset.

Table V results show that our proposed methodology work based on six classifiers (k-NN, Naïve Bayes, SVM, NN, DNN & Autoencoder) produce the highest performance accuracy approx. 99.90% on benchmark NSL-KDD dataset. Whereas in Biswas et al [8], k-NN with IGR feature selection method produces the highest performance 99.80% among all the feature selection combinations. In Jamal et al [14], SVM, Bayes Net & MLP (NN) produce 99.83, 96.26 & 99.36% accuracy. In Zafar et al [16], Intrusion-Miner classifier produces 96.10 accuracy. So, our proposed work shows the highest performance on state-of-the-art classifiers.

VI. CONCLUSION AND FUTURE WORK

In this paper, we have investigated a comparative analysis on benchmark datasets NSL-KDD and CIDDS-001 by using multiple machine and deep learning classification algorithms. Six classification algorithms have been used to measure the performance and accuracy of datasets. On the basis of evaluation metrics results, we have concluded that our proposed work based on k-NN, SVM, NN and DNN classifiers perform approx. 100% in terms of performance evaluation metrics on NSL-KDD dataset, whereas k-NN and Naïve Bayes classifiers perform approx. 99% accuracy on CIDDS-001 dataset. Hence, the comparative study results

have promoted the hybrid feature selection methods for better performance of cutting-edge classifiers.

In future, we have planned to perform detailed comparative study of some progressive Deep Learning approaches CNN, RNN, DBN etc. on up-to date datasets such as CIDDS-002, CIC-IDS 2017, CIC-IDS 2018 etc. and utilize feature learning on raw data of network traffics headers instead of derived features, so that deep neural networks can automatically learn data features and stimulate the maximum potential of neural networks.

REFERENCES

[1] Debar, H., Dacier, M., & Wespi, A. (1999). Towards a taxonomy of intrusion-detection systems. Computer Networks, 31(8), 805-822

[2] Zhou, Liang, et al. "Cyber-Attack Classification in Smart Grid via Deep Neural Network." *Proceedings of the 2nd International Conference on Computer Science and Application Engineering*. ACM, 2018.

[3] S. Naseer et al., ''Enhanced network anomaly detection based on deep neural networks,'' IEEE Access, vol. 6, pp. 48231–48246, 2018.

[4] Jiang, F., Y. Fu, B. B. Gupta, F. Lou, S. Rho, F. Meng, and Z. Tian (2018). Deep learning based multi-channel intelligent attack detection for data security. *IEEE Transactions on Sustainable Computing*.

[5] M. Tavallaee, "An adaptive hybrid intrusion detection system," Ph.D. dissertation, University of New Brunswick, 2011.

[6] Shone, N., T. N. Ngoc, V. D. Phai, and Q. Shi (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topic in Computational Intelligence 2*(1), 41–50.

[7] Salama, M. A., H. F. Eid, R. A. Ramadan, A. Darwish, and A. E. Hassanien (2011). Hybrid intelligent intrusion detection scheme. In *Soft computing in industrial applications*, pp. 293–303. Springer.

[8] Biswas, S. "Intrusion detection using machine learning: A comparison study." *International Journal of Pure and Applied Mathematics* 118.19 (2018): 101-114.

[9] Ma H. Correlation-based feature selection for machine learning [D]. Hamilton: The University of Waikato,2000.

[10] Ring, M., Wunderlich, S., Gru¨dl, D., Landes, D., Hotho, A.: Flow-based benchmark data sets for intrusion detection. In: Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS), to appear. ACPI (2017)

[11] Y. Liao and V. Vemuri, "Use of K-Nearest Neighbor classifier for intrusion detection," Computers & Security, vol. 21, no. 5, pp. 439–448, Oct. 2002. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S016740480200514X

[12] S. Mukkamala, G. Janoski, and A. Sung, "Intrusion detection using neural networks and support vector machines." IEEE, 2002, pp. 1702– 1707. [Online]. Available: http://ieeexplore.ieee.org/document/1007774/

[13] Vinayakumar, R., et al. "Deep Learning Approach for Intelligent Intrusion Detection System." *IEEE Access* 7 (2019): 41525-41550.

[14] Assi, Jamal H., and Ahmed T. Sadiq. "NSL-KDD dataset Classification Using Five Classification Methods and Three Feature Selection Strategies." *Journal of Advanced Computer Science and Technology Research* 7.1 (2017): 15-28.

[15] Lee, Brian, et al. "Comparative study of deep learning models for network intrusion detection." *SMU Data Science Review* 1.1 (2018): 8.

[16] Zafar, Samra, Muhammad Kamran, and Xiaopeng Hu. "Intrusion-Miner: A Hybrid Classifier for Intrusion Detection using Data Mining."