Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 171 (2020) 1251–1260

Procedia Computer Science

www.elsevier.com/locate/procedia

Third International Conference on Computing and Network Communications (CoCoNet'19)

Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review

T.Saranya[a], S.Sridevi[b,*], C.Deisy[c], Tran Duc Chung[d], M.K.A.Ahamed Khan[e]

[a,b,c]*Department of Information Technology, Thiagarajar College of Engineering, Madurai, India*
[d]*Computing Fundamental Department, FPT University, Hanoi, Vietnam*
[e]*Faculty of Engineering, UCSI University, KualaLumpur,Malaysia.*

Abstract

The rapid growth of technologies not only formulates life easier but also exposes a lot of security issues. With the advancement of the Internet over years, the number of attacks over the Internet has been increased. Intrusion Detection System (IDS) is one of the supportive layers applicable to information security. IDS provide a salubrious environment for business and keeps away from suspicious network activities. Recently, Machine Learning (ML) algorithms are applied in IDS in order to identify and classify the security threats. This paper explores the comparative study of various ML algorithms used in IDS for several applications such as fog computing, Internet of Things (IoT), big data, smart city, and 5G network. In addition, this work also aims for classifying the intrusions using ML algorithms like Linear Discriminant Analysis (LDA), Classification and Regression Trees (CART) and Random Forest. The work was tested with the KDD-CUP dataset and their efficiency was measured and also compared along with the latest researches.

Keywords:Intrusion Detection System(IDS); Machine Learning(ML) Algorithm; Classification; Random Forest;Support Vector Machine; Accuracy

*Corresponding author.Tel.:+91-452-2482240-613
E-mail address:[b,*]sridevi@tce.edu, [a]saranshakthi09@gmail.com,[c]cdcse@tce.edu,[d]chungtd6@fe.edu.vn,[e]mohamedkhan@ucsiuniversity.edu.my

1877-0509
10.1016/j.procs.2020.04.133

1. Introduction

The world Internet statistics report informs that, the Internet growth (2000-2019) reached 1,114%, since more than 2 quintillion bytes of data are generated every day. This shows that, the rate of data growth from various sources are extremely very fast, and at the same time the development of hacking tools and methodologies also growing in the faster manner. Therefore, there is a need for information security and data analysis for protecting the data from the intrusion. Due to the huge volume and high speed of data, the traditional detection system is not able to detect intrusion in the faster manner. In order to handle intrusion efficiently, the big data techniques are employed. The big data is defined under 7v's such as (i) volume: size of the data, (ii) velocity: speed at which the data are generated, (iii) variety: different types of data, (iv) value: the worth of data, (v) veracity: trustworthiness of data, (vi) variability: constant change of data meaning, and (vii) visualization: easy accessible or readable of data. The exponential rate of data growth makes the traditional data handling system as complex due to consuming more time and resources. Big data are very complex in nature to handle such kind of data and they need powerful technologies and advanced intelligent algorithms.IDS plays an important role in detecting the attacks. The IDS is a system that will monitor the network traffic in the intent to find out any suspicious activity and known threats. It may also issue the alerts to the admin when such activity is discovered. To handle and classify the attacks in the efficient manner, various ML algorithms can be used. This section focuses on various techniques that are used for identifying the intrusion.

IDS can be a hardware system or software system that automatically monitors, identify the attack or intrusion, and alert the computer or network. This alert report helps the administrator or user to find and resolve the vulnerability present in the system or network. Some common ways of intrusion detections are: Anomaly-based detection, Signature-based detection and Hybrid-based detection.

The anomaly-based intrusion detection is also known as behaviour-based detection, because this method models the behaviour of the users, network, and host systems and thus generates alarm or alert the admin whenever the behaviour is deviated from the usual behaviour. The signature-based IDSs also called as knowledge-based detection. This method is relying on the database which contains previous known attack signature and known system vulnerabilities. Hybrid based detection system is the combination of anomaly-based intrusion detection and signature-based intrusion detection. Most of the IDSs use any one of the intrusion detections namely anomaly or signature. Since both intrusion detections have their own drawbacks, hybrid IDS can be used.

Based on their action, intrusion detection is classified into two types namely:

- Active IDS: These types of IDS will just like passive IDS and also take prevention against the attack, by blocking the suspicious traffic.
- Passive IDS: These types of IDS will simply monitor and analyse the traffic and alert the administrator about the attacks and their vulnerability.

There are several types of intrusion detection techniques such as: Host based detection and Network based detection. Host based intrusion detection is deployed in an individual host and employed to monitor the drive, incoming and outgoing traffic and compare the result with pre-created image of the host flow activity. This usually consists of software agent who detects the intrusion by analysing the host systems, system call, application logs, system directories and other host user activities. Network based intrusion detection will examine network traffic and monitor multiple host on the network to detects for any suspicious activity. This attempts to identify suspicious activity by analysing the network, transport, application and hardware layer protocols within the captured network traffic. This research work focuses classification of various attacks using intelligent ML algorithms. ML can be explained as improving the learning process of computers based on their experiences without being actually programmed. The work compares the performance of various ML algorithms such as Modified K- Means, J.48, Support Vector Machine (SVM), decision table, Principle Component Analysis (PCA), Logistic regression, decision tree and Artificial Neural Network (ANN) for IDS. In addition to the above machine learning algorithms, this research work implements algorithms like Linear Discriminant Analysis (LDA), Classification and Regression Trees

(CART) and Random Forest (RF) algorithms for classifying the intrusion detection. The performance of the algorithms was compared using the metrics like accuracy, precision, recall and F-Score.

The remaining of this paper is organized as follows: Section 2 discusses ML algorithms for intrusion detection, Section 3 conveys some applications of intrusion detection, Section 4 outlines the metrics used for performance evaluation, Section 5 covers the survey of ML used for intrusion detection, Section 6 discusses some simple study done on data set using ML and Section 7 ends the paper with conclusions and recommendation for future works.

2. ML Algorithm for Intrusion Detection

ML is a subset of Artificial Intelligence (AI). ML makes the system to learn and improve their automatic ability from the experience without being explicitly programmed. For Intrusion Detection System (IDS), ML algorithm works more accurately in detecting the attacks for huge amount of data under less time. Typically, ML algorithms can be classified into three categories:

- Supervised
- Unsupervised
- Semi-supervised.

2.1. Supervised ML Algorithm

The supervised algorithm deals with fully class labelled data, and finds the relationship between data and its class. This can be done by either classification or regression. The classification has two steps such as training and testing. The training data is done with the help of response variable. The common algorithms under classification category are Support Vector Machine (SVM), Discriminant Analysis, Naïve Bayes, Nearest Neighbour, Neural Network, and Logistic Regression. While some algorithms under regression category are Linear Regression, Support Vector Regression (SVR), Ensemble Methods, Decision Tree, and Random Forest. In this paper, Support Vector Machine, Logistic Regression, Linear Discriminant Analysis (LDA), Classification and Regression Tree (CART), Random Forest (RF) and Ensemble methods are discussed.

2.1.1 Support Vector Machine (SVM)

SVM is one of the mostly used supervised ML algorithm. SVM can be used for both classification and regression. The algorithm can be trained with the labelled data, and it can output the separation of data into classes by the hyper plane that maximizes the margin among all attack classes. Mehmood et al. [14] stated that SVM as a binary classifier, it will also perform multi-class classification by using cascade manner. SVM is mainly depends on the types of kernel used and parameters.

2.1.2 Logistic Regression (LR)

LR is a supervised ML classification algorithm used to observe the discrete set of classes. The logistic function makes use of cost function which is called as sigmoid function. This function maps predictions to probabilities. Belavagi et al. [5] mentioned that by fitting data to the logistic function the probability of occurrence of event can be predicted. The formula of sigmoid function is:

$$F(x) = \frac{1}{1+e^{-(x)}} \tag{1}$$

Where F(x) is an output between 0 and 1, x is an input to the function, and e is a base of natural log.

2.1.3 Linear Discriminant Analysis (LDA)

LDA is a simple linear supervised ML algorithm used for dimensionality reduction and prediction. Based on Bayes theorem, LDA estimates the probability that a new inputs belongs [8] to which class.

$$P(Y = x \mid X = x) = \frac{(P|k * fk(x))}{sum\ (P|| * f(x))} \quad (2)$$

Where k(x) is the output class, x is the input class, f(x) is the estimated probability and $P|k$ is the prior probability.When LDA is used as a classification problem, the output variable should be categorical and supports binary as well as multi-class class.

2.1.4 Classification and Regression Tree (CART)

CART is a simple nonlinear supervised ML algorithm used for classification and regression. In CART, the target variable should be categorical, whereas in regression tree the target variable should be continuous. In CART, Gini index is a metric used for classification [8].

$$Gini\ index\ = 1 - \sum_{i=1}^{c} P_i \quad (3)$$

Where, c is the number of classes and P_i is the probability of each class in the dataset.

2.1.5 Random Forest (RF)

RF is a complex nonlinear supervised algorithm used for classification and regression. This will construct many decision trees at training the model and the outcomes of predictions from all trees are pooled to make a result so, it is mentioned as Ensemble techniques. The RF classifiers works as follows: the higher the number of trees in the model will result in the higher accuracy and not over-fit the model.

2.1.6 Ensemble Methods

In order to produce the optimal predictive model, this ML technique combines several models. The main idea behind ensemble method is to grouping of all weak learners to form a strong learner; thereby the accuracy of the model is increased. Some common types of ensemble methods are Bagging, Boosting, and Stacking. Gautam et al. [9] approached the bagging ensemble method and works out the trail with Naive Bayes, partial decision tree algorithm (PART) and Adaptive Boost. They showed that ensemble approach has the higher rate than PART, Naive Bayes and Adaptive Boost.

2.2. Unsupervised ML Algorithm

For intrusion detection, the unsupervised learning algorithm will try to find out the hidden structure in unlabelled data. There is no training data for unsupervised learning. This can be done by clustering or association analysis or dimensionality reduction. The clustering algorithms such as K-Means, K- Mediods, and C-Means can be used. The dimensionality reductions algorithms such as Singular Value Decomposition (SVD), Principle Component Analysis (PCA) can be used.

2.2.1. K-means

K-means is one of the unsupervised ML algorithms. This algorithm works based on the finding groups in the data, and the number of groups can be represented by the variable. K-means algorithm is highly used in time series data for pattern matching. Sridevi et al. [17] proposed clustering based pattern matching algorithms for predicting the time series data. Varuna et al. [18] proposed K-means clustering, with the cluster of five types such as four types of attack and one normal traffic. These five features are then classified by using Naive Bayes classifier. The drawback

of K-Means algorithm is it is not applicable for non-spherical form of data.

2.2.2. Principle Component Analysis (PCA)

PCA is a technique which is used for dimensionality reduction. PCA provides new set of variables called principle components and can also be used as an input to any supervised ML algorithm. Aburomman et al. [1] proposed ensemble PCA-LDA method. The PCA is able to remove only linear feature information and LDA will remove the non-linear feature information.

2.3. Semi-Supervised ML algorithm

The semi supervised ML algorithm lies between unsupervised learning and supervised learning. These learning techniques make use of unlabelled data for training and also a small amount of labelled data for large set of unlabelled data. Jarrah et al.[2] proposed semi-supervised multi layered clustering model for network intrusion detection. This algorithm provides a multiple layers of randomized K-Means clustering algorithm, which improves the diversity among classifier and result in accurate intrusion detection.

3. Applications of Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS) is very essential technology to keep the people away from cyber-attack. Every transaction and information processing is take place through Internet which is very prone to more different types of malicious activity. Therefore, there is a need to provide more concentration for the information security. The application areas covered in this paper are:

- IDS for Internet of Things
- IDS for Smart City
- IDS for Big Data Environment
- IDS for Fog
- IDS for Mobile.

3.1. IDS for Internet of Things (IoT)

Internet of Things (IoT) is a network of object or device with unique identification, which can sense, accumulate and transfer data over Internet without any human to human or human to computer intervention. IoT devices are powered with low power and it is developed with lightweight protocols. It is lightweight also. Ghasempouret al. [10] discussed the purpose of IoT device in smart grid. It can be highly vulnerable and even attackers can modify the sensors data. The major attack that take place in IoT devices are physical attack, side channel attack, environmental attack, cryptanalysis attacks, Black hole attack, Sybil attack and so on. Jan et al. [16] proposed lightweight intrusion detection by using supervised learning strategy. They developed SVM classifier to detect the attacks (target DDoS). Hasan et al. [11] discussed anomaly and attack detection. They implemented their work using ML algorithm such as LR, SVM, Decision Tree, RF and Artificial Neural Network.

3.2. IDS for Smart City

Elsaeidyet al. [7] discussed Intrusion detection on smart cities. The author used the data set collected from smart water distribution plant. The work is to detect the DDoS attack in smart city applications. The proposed method of this paper consists of two parts: Restricted Boltzmann Machines (RBM) model and classifier model. This RBM model is applied to learn high level features in an unsupervised manner. The classification is used to differentiate the normal and variety of DDOS attack. They used four types of classifiers such as Feed Forward Neural Network (FFNN), Automated FFNN, RF, and SVM. For the high level of features, K-Means algorithm is processed by RBM model and they developed up to 5 layers which provide 5 sub versions of each from clustering algorithm with different k value. For each 5 data set generated from the clustering, 4 types of classifiers are applied and totally 20 experiments have done.

3.3. IDS for Big Data Environment

Big data consists of very large amount of structured, unstructured, and semi structured data in heterogeneous format. For such a huge amount of data, traditional intrusion handling system is not capable to solve the issues. IDS for big data environment can be only possible by employing ML algorithm. Othman et al. [15] used an Apache Spark big data platform for feature selection and SVM to find intrusion detection. Pre-processed model is standardized to unit variance in spark Mllib. Chisqselector and SVM are used for feature selection and the feature selection model is based on the method of numTopFeatures. In order to reduce the effect of misclassification error, the soft SVM margin is used. The user defined variable called slack variable is used to trade between margin and misclassification error. Their result shows that the intrusion detection on big data is achieved with higher performance and speed.

3.4. IDS for Fog Computing

Fog computing is a new technology of computing paradigm, which bring analytic service to the edge and improving the performance by placing the resources closer to where they are needed. The fog computing has three types of layers such as cloud service layer, fog service layer, and user layer. The fog service layer has a geographically distributed fog node which composed of routers, gateway, server at the edge and offers a unique layer in fog computing. Fog nodes support heterogeneous computing which makes the fog node more vulnerable to attack such as DDoS, Remote-to-Local (R2L), User-to-Root (U2R), PROBE and so on. An et al. [4] contributes the attack process of DDOS in fog computing, and explore the relationship between the fog node and DDOS based on hyper graph. The state of the fog node is computed by the load factor. To determine the state of the fog node, it is compared with the threshold load level of node. Their model is used to analyse the association of fog nodes suffering from DDoS attack.

3.5. IDS for Mobile

Mobiles are becoming more predominant tool among the people for communication and for storing more sensitive information. The mobile vulnerabilities are application vulnerability, device vulnerability, networks vulnerability, web and content vulnerability. To resolve these vulnerability and threats, the device should have IDS. Maimo et al. [12] proposed a 5G-oriented cyber defence architecture to identify cyber threats in 5G mobile networks by using self-adaptive deep learning based system. They design their architecture for classifying the intrusion by arranging the anomaly detection in two levels: ASD module (anomaly symptom detection) and NAD module (network anomaly detection). The NAD is implemented by a supervised way of LSTM (long short term memory recurrent networks) and ASD module is implemented by a two level supervised or semi-supervised way of DBN (deep belief network) and SAE (stacked auto-encoders).

4. Performance Evaluation Metrics

The efficiency of the ML algorithms can be measured using metrics like accuracy, precision, recall and F-Score etc. Some of the metrics are discussed below:

4.1. Basic Terms and Formula

- True positive (TP): Both the original data points and the predicted data points are true.
- True Negative (TN): Both the original data points and the predicted data points are false.
- False Positive (FP): Original data points are false, but the predicted data points are true.
- False Negative (FN): Original data points are true but the predicted data points are false.

$$Accuracy = \frac{TN+TP}{TP+TN+FP+FN} \tag{4}$$

$$Precision = \frac{TP}{TP+FP} \tag{5}$$

$$Recall = \frac{TP}{TP+FN} \quad (6)$$

The F-Measure is also called as F-Score [11], which defines the weighted average of Recall and Precision. It is measured by the formula:

$$F - Score = \frac{2(R*P)}{R+P} \quad (7)$$

Where, R is recall and P is a precision.ROC curve [11] is a receiver operating characteristic curve which shows the performance of a classifier at various thresholds level. This ROC graph plots two parameters such as TP vs FP. AUC-ROC will measures the two dimensions' area underneath the ROC curve. Othman et al. [15] used the formula to find AUROC is as follows:

$$AUROC = \int_0^1 \left(\frac{TP}{P}\right) d\left(\frac{FP}{N}\right) \quad (8)$$

Area Under Precision-Recall Curve explains the trade-off between recall and precision at various threshold.

$$AUPR = \int_0^1 \left(\frac{TP}{TP+FP}\right) d\left(\frac{TP}{P}\right) \quad (9)$$

The intelligence and efficiency of the intrusion detection is measured by the above metrics, moreover for intrusion detection most of the researcher used the metrics called Detection rate and false positive rate. The good IDS should have very high detection rate and very low false positive rate [1]. It is calculated by the formula:

$$Detection\ rate = \frac{TP}{TP+FN} \quad (10)$$

$$False\ Positive\ rate = \frac{FP}{FP+TP} \quad (11)$$

5 Comparison of various MLA used for IDS

In this paper, the survey of intrusion detection using ML algorithm has been presented and discussed. Various applications of IDS are thrown out and the performance evaluation is also done. Table 1 gives the summary of the survey.

Table 1. Summary.

Paper	Dataset	Detection	Infrastructure	Algorithm used	Evaluation	Outcomes
Othman (et al, 2018)	KDDCUP99	Intrusion detection	Scala programming using MLlib in apache spark.	Chisqselector and SVM.	AUROC and AUPR.	The result of the paper achieves high performance and low false positive rate for IDS.
Elsaeidy (et al, 2019)	Smart water distribution	DDoS attack	Java SDK 1.8, weka libraries, matlab 9.1.	K-means, deep RBM, FFNN, automated FFNN, RF, SVM.	F-measures	The result of the paper shows that automated FFNN outperforms all other algorithm.
Mehmood (et al, 2016)	KDD99	Intrusion detection like DoS, R2L, U2R.	-	SVM, j.48, Naive Bayes, decision tables.	True positive rate, false positive rate, precision.	The result of the paper shows that j.48 algorithm achieve better performance even under the redundant features among all other algorithm.

Gautam (et al, 2018)	KDD-99	Intrusion detection	R- Programming language and Weka tool.	Naive Bayes, PART, Adaptive Boost and ensemble methods.	Precision, Recall, Accuracy.	The result of the paper shows that the ensemble approach by bootstrapping achieves better performance than the other classifier.
Aburomman (et al, 2016)	KDD-99	Intrusion detection	-	PCA-LDA Ensemble classification.	Overall-accuracy, False-positive, False-negative.	The result of the paper show that ensemble approach LDA-PCA feature extraction is better than a single feature extraction algorithm, by having less false positive rate (0.0196).
Jan (et al, 2018)	Simulated dataset	DoS/DDoS attack	Matlab version 2018b simulation tool.	SVM	Accuracy, True positive rate, False positive rate, False detection rate.	The result of the paper achieves the light weight IDS for IoT. Experiments show that packet arrival rate and SVM classifier is enough to detect intrusions on IoT.
Hasan (et al, 2019)	Kaggle	Attack and Anomaly detection	Framework used pandas, numpy, matplotlib, seaborn, scikit-learn, keras.	DF, ANN, Logistic Regression, SVM.	Accuracy, precision, recall, f1 score, ROC.	The experiment shows, DF is the good technique to use in IoT for IDS with the accuracy of 99.4%.
Maimo (et al, 2018)	Botnet data set.	Anomaly detection	Caffe2, PyTorch	Deep belief network, Stacked Auto-Encoder, and L	Precision, Recall and F1 Score.	The result achieves accuracy of anomaly detection in 5G network by using two –level deep learning algorithm.

From the above literature survey, most of the researcher compared their proposed model with SVM. Yaseen et al. [3], Jan et al. [16] used SVM and modified SVM in their research work. Elrawy et al. [7], Maleh et al. [13] proved that their proposed model gives better accuracy than SVM. Zhang et al. [19] stated that SVM identifies the intrusion with less probability than that of RF. The classification done by RF has high true positive rate and low false positive rate, whereas the SVM classifies at high false positive rate (39%) and low true positive rate (75%), this is all because of using too many feature from the data set and SVM's linear kernel. Thus Implementing ML algorithms yield different result for different applications.

6. Result and Discussions

In order to evaluate the above literature work, this research work implements Linear Discriminant Analysis (LDA), Classification and Regression Tree (CART) and Random Forest (RF) algorithms for testing purpose. It is implemented on standard KDD'99 Cup data set. The data set has 42 features and 494021 instances with 25 predictors which was mapped to 5 types of classes such as DoS, probes, user to remote attack (U2R), remote to local (R2L), and normal. The work has three step processes such as Data pre-processing, Classifications and Evaluation.

```
Models: lda, cart
Number of resamples: 10

Accuracy
          Min.   1st Qu.    Median      Mean   3rd Qu.      Max. NA's
lda  0.9818334 0.9825095 0.9835408 0.9833409 0.9841676 0.9845652    0
cart 0.9805162 0.9807505 0.9842619 0.9830170 0.9845534 0.9849194    0

Kappa
          Min.   1st Qu.    Median      Mean   3rd Qu.      Max. NA's
lda  0.9462902 0.9483059 0.9513086 0.9507276 0.9531384 0.9543379    0
cart 0.9410264 0.9418288 0.9520842 0.9484624 0.9530112 0.9540817    0
```

Fig. 1. Classification result of LDA and CART algorithms

pred	dos	normal	probe	r2l	u2r
dos	352262	31	24	2	0
normal	49	87485	42	73	30
probe	1	15	3630	3	0
r2l	0	18	0	935	4
u2r	0	1	0	0	12

Fig. 2. Confusion Matrix Result of Random Forest Algorithm

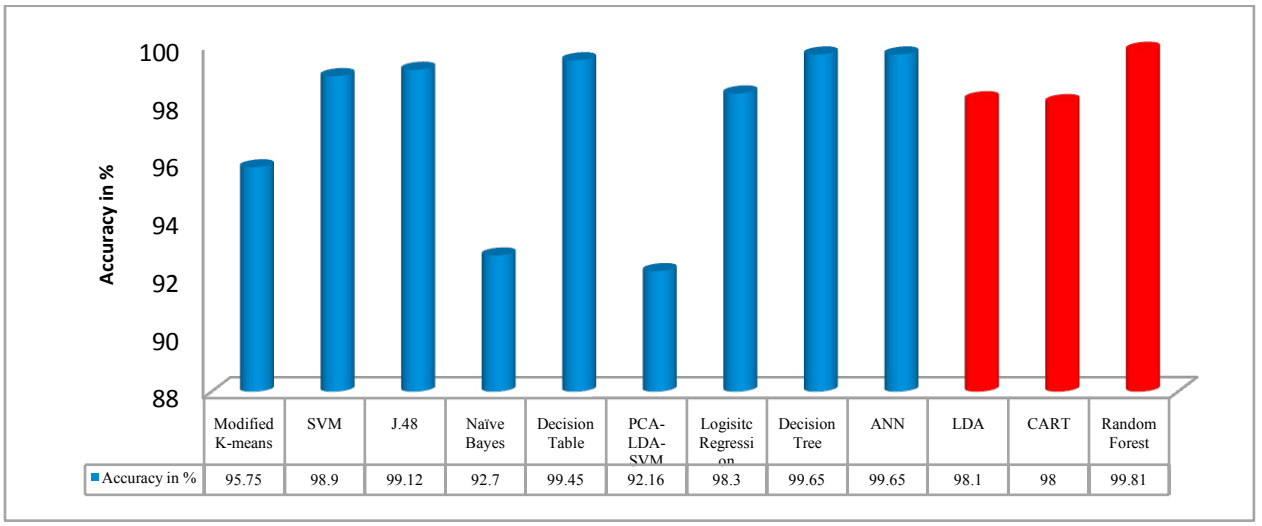

Fig. 3.Performane Comparisons of various ML algorithms in IDS

In data pre-processing steps, the features are mapped to their appropriate functions and features are selected based on filter method. From 42 variables, 20 variables where selected based on correlation attribute evaluation by choosing ranker search method. In classification phase, LDA algorithm, CART algorithm and Random Forest are used.The data set is divided into training set and testing set based on 80 – 20 rule. In evaluation phase, the metrics like accuracy and kappa were used to measure the performance of LDA, RF and CART algorithms. The experimental result shows that the RF algorithm yields better accuracy (99.65 %) than LDA (98.1%) and CART (98%) algorithms. The work was implemented using R Studio. The classification results of KDD cup dataset using LDA, CART an RF are shown in Fig.1 and Fig.2.The different ML algorithms such as LDA, CART and RF used in this work as well as in above survey is compared in terms of accuracy is shown in Fig. 3. The graph shows that, the RF algorithm used in this research work also yields better accuracy among other algorithms. In general, the algorithms like RF, ANN and decision tree give better results for classifying the attacks. From the above comparisons, it is observed that the performance of the algorithms also depends on the size of the dataset and applications employed.

7. Conclusion and Future Work

The rapid growth of Internet usage and generation of enormous amount of valuable digital data attracts the attacker to illegally attain economic benefits and so on. This paper explores the ML algorithms used for IDS on various environments and also done some experiment on KDD'99 Cup data set using MLA and the results are also compared. This study will convey that the detection rate, false positive rate, and accuracy are not only depends on the algorithm but also depends on the application area. In future, we will conduct an extensive study of ML algorithms to provide better solution for the IDS by taking real-time dataset.

References

[1] Aburomman, A. A., &Reaz, M. B. I. (2016) "Ensemble of binary SVM classifiers based on PCA and LDA feature extraction for intrusion detection."*Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)* : 636-640.
[2] Al-Jarrah, O. Y., Al-Hammdi, Y., Yoo, P. D., Muhaidat, S., & Al-Qutayri, M. (2018) "Semi-supervised multi-layered clustering model for intrusion detection." *Digital Communications and Networks* **4(4)**: 277-286.
[3] Al-Yaseen, W. L., Othman, Z. A., &Nazri, M. Z. A. (2017) "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system." *Expert Systems with Applications* **67(1)**: 296-303.
[4] An, X., Su, J., Lü, X., & Lin, F. (2018) "Hypergraph clustering model-based association analysis of DDOS attacks in fog computing intrusion detection system." *EURASIP Journal on Wireless Communications and Networking* **249 (1)**: 1-9.
[5] Belavagi, M. C., &Muniyal, B. (2016) "Performance evaluation of supervised machine learning algorithms for intrusion detection." *Procedia Computer Science* **89(1)**: 117-123.
[6] Elrawy, M. F., Awad, A. I., &Hamed, H. F. (2018) "Intrusion detection systems for IoT-based smart environments: a survey." *Journal of Cloud Computing* **7 (1)**: 21
[7] Elsaeidy, A., Munasinghe, K. S., Sharma, D., &Jamalipour, A. (2019) "Intrusion detection in smart cities using Restricted Boltzmann Machines." *Journal of Network and Computer Applications* **135 (1)**: 76-83.
[8] Ganapathy, S., Kulothungan, K., Muthurajkumar, S., Vijayalakshmi, M., Yogesh, P., &Kannan, A. (2013) "Intelligent feature selection and classification techniques for intrusion detection in networks: a survey." *EURASIP Journal on Wireless Communications and Networking* **(1)**: 271.
[9] Gautam, R. K. S., &Doegar, E. A. (2018) "An Ensemble Approach for Intrusion Detection System Using Machine Learning Algorithms." *International Conference on Cloud Computing, Data Science & Engineering (Confluence)* : 14-15.
[10] Ghasempour, A. (2019). Internet of Things in Smart Grid: Architecture, Applications, Services, Key Technologies, and Challenges. *Inventions* ***4*****(1)**: 22.
[11] Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019) "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches." *Internet of Things* ***7(1)***:100059.
[12] Maimó, L. F., Gómez, Á. L. P., Clemente, F. J. G., Pérez, M. G., & Pérez, G. M. (2018) "A self-adaptive deep learning-based system for anomaly detection in 5G networks." *IEEE Access* **6 (1)**:7700- 7712.
[13] Maleh, Y., Ezzati, A., Qasmaoui, Y., &Mbida, M. (2015) "A global hybrid intrusion detection system for wireless sensor networks." *Procedia Computer Science* 52 **(1)***:* 1047-1052.
[14] Mehmood, T., &Rais, H. B. M. (2016) "Machine learning algorithms in context of intrusion detection." *International Conference on Computer and Information Sciences (ICCOINS)*: 369-373.
[15] Othman, S. M., Ba-Alwi, F. M., Alsohybe, N. T., & Al-Hashida, A. Y. (2018) "Intrusion detection model using machine learning algorithm on Big Data environment."*Journal of Big Data* ***5*****(1)**: 34.
[16] Sana Ullah Jan, Saeed Ahmed, Vladimir Shakhov, and Insookoo. (2019) "Towards a Lightweight Intrusion Detection System for the Internet of Things." IEEE Access **7 (1)**:42450-42471.
[17] Sridevi, S., Parthasarathy, S., & Rajaram, S. (2018). "An Effective Prediction System for Time Series Data Using Pattern Matching Algorithms." *International Journal of Industrial Engineering* ***25*****(2)**: 123-136.
[18] Varuna, S., &Natesan, P. (2015) "An integration of k-means clustering and naïve bayes classifier for Intrusion Detection." In *2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN)* : 1-5.
[19] Zhang, J., Gardner, R., &Vukotic, I. (2019) "Anomaly detection in wide area network meshes using two machine learning algorithms." *Future Generation Computer Systems* **93 (1)**:418-426.