© Universiti Tun Hussein Onn Malaysia Publisher's Office

JSCDM

Journal homepage: http://penerbit.uthm.edu.my/ojs/index.php/jscdm
e-ISSN : 2716-621X

Journal of Soft Computing and Data Mining

Application of Machine Learning Approaches in Intrusion Detection System

Zena Abdulmunim Aziz[1*], Adnan Mohsin Abdulazeez[2]

[1]IT Department Technical College of Informatics Akre,
Duhok Polytechnic University, Duhok, Kurdistan Region, IRAQ

[2]Presidency of Duhok Polytechnic University, Duhok, Kurdistan Region, IRAQ

*Corresponding Author

DOI: https://doi.org/10.30880/jscdm.2021.02.02.001
Received 26 April 2021; Accepted 20 September 2021; Available online 15 October 2021

Abstract: The rapid development of technology reveals several safety concerns for making life more straightforward. The advance of the Internet over the years has increased the number of attacks on the Internet. The IDS is one supporting layer for data protection. Intrusion Detection Systems (IDS) offer a healthy market climate and prevent misgivings in the network. Recently, IDS has been used to recognize and distinguish safety risks using Machine Learning (ML). This paper proposed a comparative analysis of the different ML algorithms used in IDS and aimed to identify intrusions with SVM, J48, and Naive Bayes. Intrusion is also classified. Work with the KDD-CUP data set, and their performance has been checked with the WEKA software. A comparison of techniques such as J48, SVM, and Naïve Bayes showed that the accuracy of j48 is the higher one which was (99.96%).

Keywords: IDS, attacks, machine learning, support vector machine, Naïve Bayes, J48, KDD dataset

1. Introduction

Machine learning (ML) is a subset of artificial intelligence in which computers are more adept at learning without human direction. ML's ability to embrace newer software that can adapt when not secure. Fig. 1 depicts the three ways ML algorithms are graded as supervised, unsupervised, and reinforcement learning [1], [2], [3].

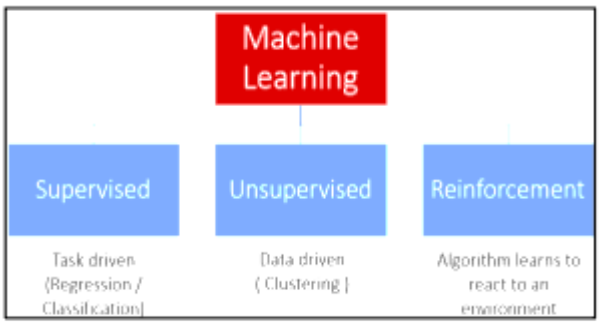

Fig. 1 - The different types of machine learning [4]

Supervised learning aims to produce a training example for each of the meanings to be identified. For supervised learning, every example is a pillar with an input object (usually a vector amount) and an enforced output value (may also

* *Corresponding Author: zena.aziz@dpu.edu.krd*

be referred to as a supervisory signal). A monitored algorithm for learning performs the task of analyzing the data and builds a contingent feature to draw up new examples. The maximum configuration would likely allow the algorithm to courageously mark the class for the covered cases [5],[6]. The supervised learning algorithm needs to be used to "rationally" reduce data from training data to covered circumstances. These regulated methods can be used in different applications, including marketing, security of the network, prediction about attacks, finance, manufacturing, research, stock market forecasting,[7],[8], etc.

The computers on the Internet have given rise to a lot of social and economic progress. In recent years, the impact of global trade, healthcare, and healthcare systems in both developed and developing countries has expanded significantly. This has brought about an ever-increasing focus on network security by business and academic entities alike. Networks can be breached from both inside and outside; IDS is essential to detect attacks. “The value of Intrusion Detection Systems (IDS) is considerable because they can be attacked from both the inside and the outside” [9],[10],[11].

The solution to those problems has been established with human-independent IDS incorporating machine learning techniques. Machine training IDS is learned by training on a dataset from regular traffic and abnormal transport to prevent an assassination attack [12]. A number of machine learning techniques have been applied successfully, but they have multiple faults, such as low throughput and a high rate of erroneous detection [13],[14].

The Denial-of-service attack (DOS) is considered one of the most frequently reported harmful attacks. DOS attacks aim to deny multiple end-user services temporarily. In general, network resources are created, and the system is overloaded with unwanted demands. That is why the DOS serves as an excellent guide for all forms of attacks to consume computers and network resources [15],[16]. Yahoo was the first DOS attack victim in 2000, and DOS published the first attack on the same day [17].

From another aspect, Remote Attacks to Local (R2L) attacks are another umbrella for all kinds of attacks that have local rights because specific network resources are only available to local users, e.g., file servers. Some forms of R2L attacks exist, e.g., SPY and PHF, which are aimed at preparing unauthorized access to network resources [18].

Regarding unauthorized access to the network and computing services, the User's attacks to Root (U2R) seek to transfer the attacker's license to the root user, who has complete computer and network access privileges[19]. Regarding the literature [20],[21] Detection of attacks is called a Classification challenge because it aims to explain whether the packet is a common one or a packet attack. Thus, based on significant learning algorithms, the agreed intrusion detection device model can be applied. This paper has been used to test and precisely the model intrusion detection scheme, based on a database dataset based on information Discovery in databases (KDD), which contains the following forms of assault,

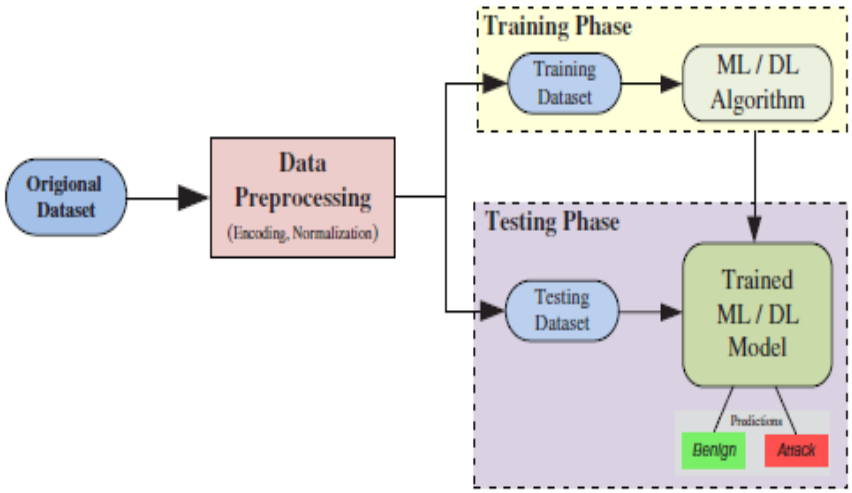

Fig. 2 - ML in intrusion detection system [22]

The structure of this paper is organized: Section 2 shows related work. Section 3 presents the materials and methods used in the studies and provides a brief overview of selected ML classifier types. The results are shown in Section 4. The paper is finally closed in Section 5.

2. Related Work

Computer training methods have been a widely researched field of study in recent years in intrusion detection systems. Many different methods have been developed with many publicly accessible datasets to tackle the network attack detection issue. Currently, classification models are standard methods used for the field of intrusion detection.

Since they typically perform better than conventional machine learning models, the methods in this field became popular. Here you can find some of the analysis.

In [23], the author has suggested hybrid approaches that combine J48, the Vector Support, and Bayesian Naïve to detect various attack types, including different algorithm precision types. All of these experiments were performed on NSL-KDD.

In [24] The proposed computer teaching methods, such as SVM and Extreme Learning Machine (ELM), are designed to create a hybrid model. Modified K-means was used to construct a data set of high quality. It produces small datasets that display original datasets overall. This move reduces the classifier's training time. For implementation, KDDCUP 1999 was used. It is accurate at approximately 95.75%.

Wang et al. [25] Proposed a system for intrusion detection focused on SVM and validated NSL–KDD data set methodology. They argued that their method, which has an efficacy rate of 99.92 %, was higher than other methods; however, results, training numbers, and test samples were not mentioned. When much data is involved, the SVM output declines and is not the optimal option for analyzing massive intrusion traffic in the network.

Teng et al. [26] Significant analysis has been carried out, and They built a model focused on decision-making bodies and SVMs and validated their model using a dataset of KDD CUP 1999. The findings showed a precision of 89.02%. However, for the high calculation cost and low efficiency, SVMs are not favored for rich datasets.

Lia et al. [27] Used GA pre-processed data set KDD Cup 99 in a data reduction pre-processing module as data processing with all 41 features was difficult. For selecting 10 of the 41 features in the KDD Cup 99 dataset and using the SVM for classification, GA was used. The experiment was conducted with 100 datasets, of which 95% were used as training data and 10% as test data. The classification process continued until ten times the results were reviewed. Four separate SVM attacks were classified (DOS, probe, U2R, R2L attacks). Accuracy of up to 92.02%.

Bhavani et al. [28] Introduced An intrusion detection method focused on the classification of a single computer, using random KDD-NSL data set forest and tree decision techniques. The random classifier gives an improved result accuracy of 95,323 %. The proposed work did not address low detection and false-positive rates.

In paper [29], the standard and PCA-based algorithm Naive Bayes was used with the KDD data set without an accuracy comparison library. The Naive Bayesian Classification has the advantage that missing values are handled by simply omitting probabilities of members of each group are likely. The results showed that the PCA-based algorithm is more precise than conventional Naive Bayes, reducing the runtime for ten key components. However, the precision decreases by increasing the number of features.

In a study of [30], the author proposed a new algorithm to select the function using the data set KDD CUP 99. They have chosen the relevant features for network intrusion detection from the total number of features (41). C4.5 function selection is made possible using several feature selection methods based upon Mutual Information (MI) and Bayesian network wrapper. Instead of an existing approach for feature selection, they are proposed selection technique produces better results, the precision of 99.93%.

In a study of [31], the proposed NIDS is trained and evaluated on the NSL-KDD data set. The results of the evaluation showed its effectiveness in acknowledging normal behavior and detecting attacks with a high degree of detection accuracy and a low probability of false alarms. In addition, the comparison with the other IDSs involved is carried out, and the outcome of our proposed system is 99.11 %.

3. Materials and Methodology

WEKA (Waikato Environment for Knowledge Analysis) used the popular open-source data mining method (version 3.8.5) for this research. Data sets of KDDs Cup99 have been used, and numerous significant algorithmic classification (classifiers) have been tested. The research was conducted with an Intel® Core TM i5 CPU fitted with an HP Windows 10 Enterprise unit and 4 GB of RAM. Fig. 3 illustrates the research methodology.

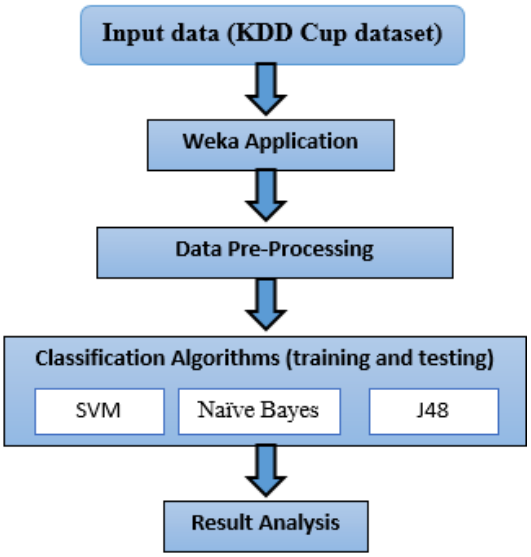

Fig. 3 - Research methodology

3.1 Data Sets

The KDD Cup-99 data set has been developed by the 1998 DARPA IDS validation data set processing of the TCP-dump segment. This data set is prepared by Stolfo et al. Of Lincoln Labs, U.S.A [32], [33]. DARPA-98 consists of approximately 4 gigabytes of compressed raw (binary) TCP-dump data from 7 weeks of network traffic, converted into approximately 5 million link logs, each containing about 100 bytes. There are approximately 2 million link records in the two weeks of test results. The data collection for the KDD Cup-99, The Fifth World Congress on Knowledge Discovery and Data Mining served as the foundation for the Third International Knowledge Discovery Conference. Data Mining Tools contest. KDD Cup-99 has been the most widely used data collection for evaluating anomaly detection methods since 1999 [34], [35].

The training dataset of KDD Cup- 99 comprises approximately 4,900,000 individual link vectors, each with 41 features and labeled as regular or as an attack, with precisely one particular form of attack[36]. The data collection includes 24 attack forms (connections) falling into one of the four main categories: denial of service (DOS), sample/scanning, root user (U2R), and user remote (R2L). A complete listing of features given for the link vectors in the KDD cup 99 datasets is provided [37], [38]. Taxonomy of the target attribute in the KDD 99 dataset is shown in Fig. 4.

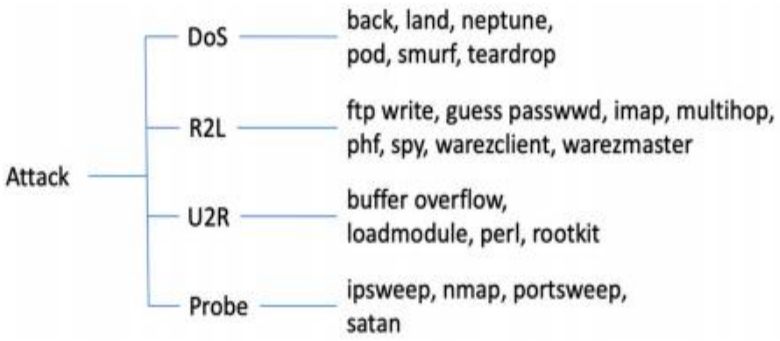

Fig. 4 - The target attribute's taxonomy in the KDD 99 dataset [39]

3.2 WEKA (Waikato Environment for Knowledge Analysis)

Weka is a library of machine learning techniques for performing data mining tasks. Alternatively, the techniques can be applied directly to a dataset [40]. Weka includes tools for pre-processing data, classifying it, performing regression, clustering, defining association rules, and visualizing it. Additionally, it is well-suited for the development of novel machine learning schemes. WEKA is comprised of the following components: Explorer, Experimenter, Knowledge Flow, Simplified Command Line Interface, and Java interface [41]. The WEKA tool incorporates the following steps [42],[43]:

- Analyze and pre-process the database's features, as well as evaluate the data's accuracy.

- Definition of the class attributes that categorize the set of instances.
- Extraction of potential classifier features.
- A subset of features is selected to be used in the learning process.
- Investigate a potential imbalance in the given data set and devise a strategy for resolving it.
- Selection of a subset of examples, i.e. the records on which to base learning.
- The learning process is aided by using a classification algorithm.
- I was deciding on a method for estimating the performance of the chosen algorithm.

3.3 Architecture of Intrusion Detection System

Intrusion detection systems are positioned strategically in a network for threats and packet monitoring. The IDS gathers data and reviews data against potential risks from various networks and network resources [46], [47]. The IDS features were expected to have included gathering information on risks, making corrections when it notices them, and gathering and recording all relevant events. [13]. Fig. 5 illustrates an intrusion detection system model.

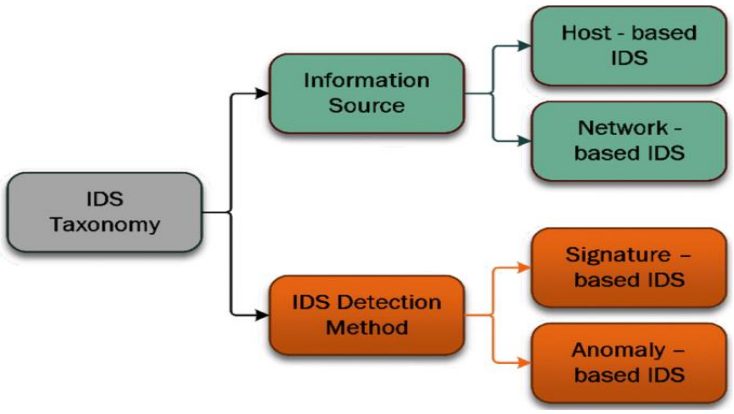

Fig. 5 - Intrusion detection system [48]

3.3.1 Host-Based IDS (HIDS) Vs. Network-Based IDS (NIDS)

The Host-Based is the first type of IDS to be developed [49][50]. Host-based (HIDS) are software items mounted on the host machine to analyze and track all traffic events in device application files and operating systems [51]. Network-Based IDS are located at strategic points on the network to catch and analyze the stream of packets passing through network links, in contrast to the HIDS, which analyzes each host individually [52][53]. The difference between HIDS and NIDS is shown in Table 1.

Table 1 - Difference between HIDS and NIDS [30]

NIDS	HIDS
Well for sensing attacks from outside	Well for sensing attacks from inside that NIDS cannot examine.
Examiner pocket header &entire packet	Does not understand the packet header.
Host independent	Hos dependent
Bandwidth in need	Bandwidth free
Reduce the speed of networks with IDS clients installed	Reduce the speed of hosts that have an IDS client installed
Sense network attack, as the payload is analyzed	Sense local attacks before they hit the network.

3.3.2 Anomaly Intrusion Detection Systems and Signature-Based Intrusion

Table 2 shows the difference between Anomaly and Signature-Based—systems for detecting anomalous intrusions. Signature-based intrusion detection relies on comparisons to known attacks' signatures stored in a database, but it is incapable of detecting unknown attacks [54]. However, anomaly-based IDS use a statistical approach to identify

behaviors that deviate from the normal resource use and behavior parameters. The rate of false positives and negatives remains high when using anomaly-based detection.

Table 2 - Difference between anomaly and signature-based

	Signature detection	Anomaly detection
Definition	Matching the sequence of " signature action" of know intrusion scenario	Using statistical measure on system feature.
Shortcoming	- Must hand-coded know pattern. -Unable to detect any future intrusion.	- Rely on while deciding on a system feature -Has to study the sequential interrelation between transactions.
Example	STAT [HLMS90]	IDES [LTG+92]

Centered on an anomaly Detection method should be established to detect abnormal behaviors and achieve optimal accuracy. Machine learning techniques are based on mathematical algorithms that are used to train models from datasets. If sufficient training data is available and appropriate algorithms are implemented, an IDS can also predict zero-day attacks [55], [56]. Cyber security administrators may use these strategies to ensure the effectiveness of security initiatives.

3.4.Machine Learning Methods for Intrusion Detection System

This section contains a comprehensive classification of machine learning techniques. Each technique is explained in detail and how they were implemented as Intrusion detection system IDS [57].

Support Vector Machine (SVM) is a decision-making algorithm that is based on the concept of decision planes referred to as decision boundaries. These decision planes aid SVM in categorizing data. SVM's primary goal is to determine the optimum decision boundary. These boundaries are built-in multidimensional spaces to obtain the best result possible when dealing with non-linear data. This is a significant advantage of SVMs over straightforward linear classifiers. Margin is critical to the classification accuracy of a new data point. The margin is the distance between the nearest data point, alternatively referred to as the 'Support Vector,' and the decision boundary. SVM mathematical representation [58] is given in Fig. 6:

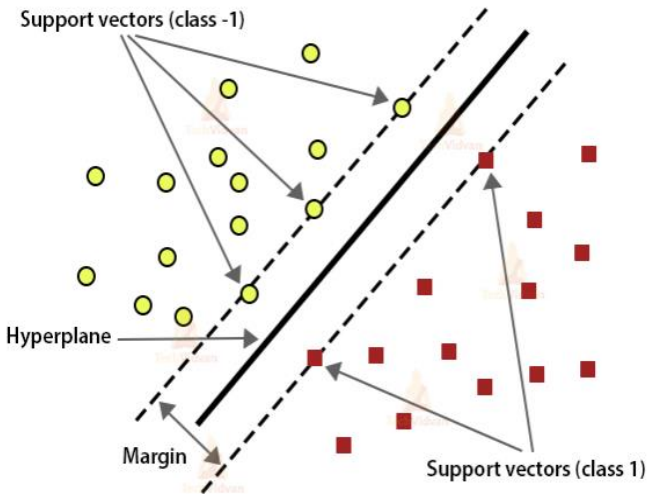

Fig. 6 - SVM architecture

The naïve Bayes algorithm is based on the attribute independence hypothesis and conditional probability. The Naive Bayes classifier calculates the conditional probabilities for each sample. The sample is allocated to the class with the highest probability [59], [60]. Fig. 7 shows the architecture of the Naive Bayes classifier.

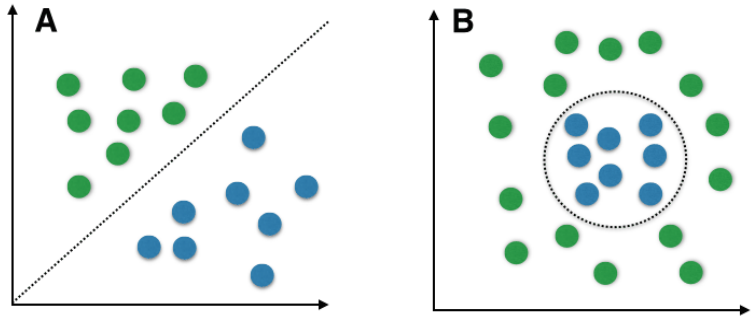

Fig. 7 - Naïve Bayes architecture

When the naive Bayes algorithm has reached its optimum state, then the attribute independence hypothesis is satisfied. Unfortunately, it does not hold up in reality; so, it cannot be said that the Naïve Bayes model is the ideal algorithm for dealing with attribute data.

The decision tree algorithm classifies data using several rules. The model is like a tree and can be interpreted. The algorithm of the decision tree will remove obsolete and redundant features automatically [61]. The process of learning involves the selection of functions, the development of the tree, and tree cutting. The algorithm selects the most appropriate features individually when a decision tree model is formed and creates child nodes from the root node [62], [63]. The tree of judgment is a fundamental classifier. There are some advanced algorithms, such as random forest and extreme gradient boosting (JGBoost). The J48 is a C4.5 application that, like ID3, uses the Information Entropy theory to construct decision-making trees from training data collection [37]. The data training set S = s1, s2,... consists of previously classified samples. Each sample SI = x1, x2... is represented as a vector in which x1, x2... are sample attributes or features. DT's are simple to use and extremely accurate when dealing with massive amounts of data. C4.5 selects one data characteristic at each node of the tree that efficiently divides the set of samples into subsets enriched in one or the other class. [64] [65][66]. The advantages and disadvantages of various classifiers are summarized in Table 3.

Table 3 - Advantages and disadvantages between classifiers

Algorithms	Advantages	Disadvantages	Improvement Measures
SVM	Learn valuable knowledge from the small data package;	Perform poorly on tasks involving large amounts of data or multiple classifications; Kernel function parameters are taken into account.	Parameters optimized via particle swarm optimization (PSO) [8]
Naïve Bayes	Sensitive to noise; Capable of gradual learning	Perform poorly when it comes to attribute-related data	Latent variables were imported in order to relax the independent presumption [11].
J48	Pick features automatically; Highly interpreted	Classification result trends toward the dominant class; data correlations are ignored.	SMOTE was used to balance datasets; latent variables were introduced.

4. Performance Evaluation

Many techniques of machine learning are used to test the accuracy and value of algorithms. These measures are used to select the most effective models. In IDS research, many metrics are also used simultaneously to fully quantify the detection effect [44], [45].

- Accuracy: is defined as the percentage of correctly labeled samples in relation to the total number of items. Accuracy A is a useful statistic for determining whether a dataset is balanced. However, standard samples are far more plentiful than irregular samples in real-world network environments; consequently, accuracy may not be the appropriate metric. Accuracy has been calculated based on Equation 1.

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

- Precision (P) is defined as the ratio between true positive and predicted positive samples, the trust in attack detection. Precision has been calculated based on Equation 2.

$$P = \frac{TP}{TP + FP} \tag{2}$$

- The Recall (R) is the percentage of true positive to total positive samples, also known as the detection rate, is defined. The identification rate represents the capacity of the model to identify threats, a significant component of IDS. Recall has been calculated based on Equation 3.

$$R = \frac{TP}{TP + FN} \tag{3}$$

- The F-measure (F) is the harmonic average of the precision and recall. F-measure has been calculated based on Equation 4.

$$F = \frac{2 * P * R}{P + R} \tag{4}$$

- The False Negative Rate (FNR) is calculated as the ratio of false-negative to total positive samples. The FNR is also known as the missing warning rate. In assault detection. The missed alarm rates. FNR has been calculated based on Equation 5.

$$FNR = \frac{FN}{FN\ +\ TP} \tag{5}$$

- The False Positive Rate (FPR): is the percentage of false-negative to total test data is determined. In assault detection. FPR has been calculated based on Equation 6.

$$FPR = \frac{FP}{FP\ +\ TN} \tag{6}$$

Where TP is the true positive, FP is the false positive, the true negatives are TN, and the false ones are FN. An IDS aims to detect threats, so anomalies are typically considered positive, and average samples are usually considered negative. The most commonly used measurements include precision, reminder or detection time, FNR (or missing warning rate), and FPR in attack detection (or false alarm rate) [67]. Table 4 shows the confusion matrix.

Table 4 - Confusion matrix

	Predicted Class	
Actual Class	Attack	Normal
Attack	True Positive	False Negative
Normal	False Positive	True Negative

According to the methodology as we mentioned in section 3. We used machine learning algorithms Such as (SVM, J48, and Naïve Bayes) with the KDD Cup99 dataset by using Weka Application; we got different results in each algorithm, as shown in the following tables (Tables 5-8).

Table 5 - Comparison of accuracy using different ML algorithms on KDD CUP 99 dataset

Class	**Accuracy**	**Time in Sec**
Naive Bayes	92.16%	56.32
SVM	99.89%	718.02
J48	99.96%	134.56

Table 6 - Result of all evaluation metrics by using Naïve Bayes

Naive Bayes					
Class	**F-Measure**	**Recall**	**Precision**	**FP Rate**	**TP Rate**
normal	0.911	0.862	0.965	0.008	0.862
U2R	0.015	0.904	0.008	0.013	0.904
Dos	0.967	0.939	0.997	0.01	0.939
R2L	0.387	0.343	0.443	0.001	0.343

Proble	0.202	0.877	0.114	0.057	0.877
weighted Avg.	0.948	0.922	0.982	0.01	0.922

Table 7 - Result of all evaluation metrics by using SVM

Support Vector Machine					
Class	**F-Measure**	**Recall**	**Precision**	**FP Rate**	**TP Rate**
Normal	0.997	0.998	0.996	0.001	0.998
U2R	0.568	0.442	0.793	0.000	0.442
Dos	1.000	1.000	1.000	0.001	1.000
R2L	0.906	0.898	0.915	0.000	0.898
Proble	0.986	0.976	0.995	0.000	0.976
Weighted Avg.	0.999	0.999	0.999	0.001	0.999

Table 8 - Result of all evaluation metrics by using J48

J48					
Class	**F-Measure**	**Recall**	**Precision**	**FP Rate**	**TP Rate**
Normal	0.999	1.00	0.999	0.000	1.000
U2R	0.518	0.423	0.667	0.000	0.423
Dos	1.000	1.000	1.000	0.000	1.000
R2L	0.970	0.958	0.982	0.000	0.958
Probe	0.994	0.992	0.995	0.000	0.992
weighted Avg.	1.000	1.000	1.000	0.000	1.000

Based on the classification (support vector machine, Naive Bayes, and j48) results, in IDS dataset KDD Cup99, using the Weka application, the accuracy was different in each algorithm since each algorithm spent a different period of time, as it's shown in Table 7. The proposed J48 scored a mean classification accuracy of 99.96%, with the best accuracy. Meanwhile, SVM recorded the second-highest accuracy performance, scoring classification accuracy of 99.89%, and in comparison, Naïve Bayes with the other two algorithms gives the lowest accuracy. Fig. 8 shows the accuracy analysis of all algorithms, and Fig. 9 shows the time.

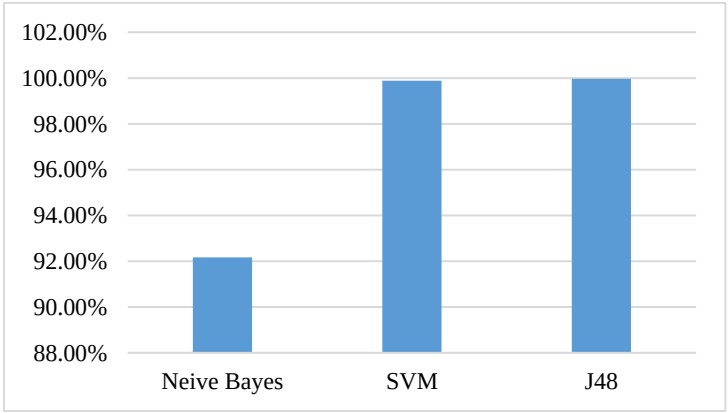

Fig. 8 - Accuracy analysis of all algorithms

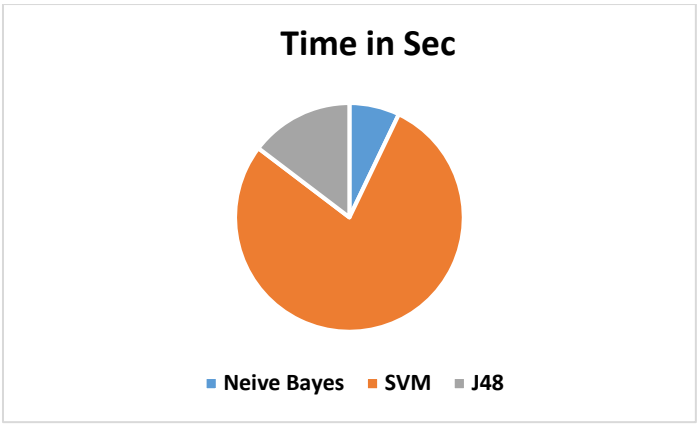

Fig. 9 - Time analysis of all algorithms

5. Conclusion

In this paper, various experiments have been carried out and tested to assess J48, Naive Bayes, and SVM's efficiency and output. Every test was based on the data set for KDD intrusion detection. Approximately 79 percent of DOS, 19 percent of usual packets, and 2 percent of others are attacks of a different kind inside the KDD dataset (R2L, U2R, and PROBE). Several measurements of success are calculated (accuracy rate, precision, false positive, true positive). The experiments have shown that no single learning machine algorithm can manage all forms of attacks effectively. The decision table (Bayes naïve) had the lowest precision, but the (j48) algorithm was far from the highest actual rate.

References

[1] Abdulazeez, A. M., Zeebaree, D. Q., Zebari, D. A., & Hameed, T. H. (2021). Leaf Identification Based on Shape, Color, Texture and Vines Using Probabilistic Neural Network. Computación y Sistemas, 25(3)

[2] Sulaiman, M. A. (2020). Evaluating Data Mining Classification Methods Performance in Internet of Things Applications. Journal of Soft Computing and Data Mining, 1(2), 11-25

[3] Al-Yaseen, A. P. D. W., Othman, Z., & Ahmad Nazri, M. Z. (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. https://doi.org/10.1016/j.eswa.2016.09.041

[4] Alamiedy, T. A., Anbar, M., Alqattan, Z. N. M., & Alzubi, Q. M. (2020). Anomaly-based intrusion detection system using multi-objective grey wolf optimisation algorithm. Journal of Ambient Intelligence and Humanized Computing, 11(9), 3735–3756. https://doi.org/10.1007/s12652-019-01569-8

[5] Jahwar, A. F., Abdulazeez, A. M., Zeebaree, D. Q., Zebari, D. A., & Ahmed, F. Y. (2021, July). An Integrated Gapso Approach for Solving Problem of an Examination Timetabiking System. In 2021 IEEE Symposium on Industrial Electronics & Applications (ISIEA) (pp. 1-6). IEEE

[6] Amudha, P., Karthik, S., & Sivakumari, S. (2013). Classification Techniques for Intrusion Detection An Overview. International Journal of Computer Applications, 76(16), 33–40. https://doi.org/10.5120/13334-0928

[7] Amanoul, S. V., Abdulazeez, A. M., Zeebare, D. Q., & Ahmed, F. Y. (2021, June). Intrusion Detection Systems Based on Machine Learning Algorithms. In 2021 IEEE International Conference on Automatic Control & Intelligent Systems (I2CACIS) (pp. 282-287). IEEE

[8] Sadeeq, H. T., Abdulazeez, A. M., Kako, N. A., Zebari, D. A., & Zeebaree, D. Q. (2021, February). A New Hybrid Method for Global Optimization Based on the Bird Mating Optimizer and the Differential Evolution. In 2021 7th International Engineering Conference “Research & Innovation amid Global Pandemic"(IEC) (pp. 54-60). IEEE

[9] Bhuiyan Akhi, A. (2019). Network Intrusion Classification Employing Machine Learning: A Survey. January

[10] Maseer, Z. K., Yusof, R., Mostafa, S. A., Bahaman, N., Musa, O., & Al-rimy, B. A. S. (2021). DeepIoT. IDS: Hybrid Deep Learning for Enhancing IoT Network Intrusion Detection. *CMC-Computers Materials & Continua*, *69*(3), 3945-3966

[11] Chand, N., Mishra, P., Krishna, C. R., Pilli, E. S., & Govil, M. C. (2016). A comparative analysis of SVM and its stacking with other classification algorithm for intrusion detection. Proceedings - 2016 International Conference on Advances in Computing, Communication and Automation, ICACCA 2016, April. https://doi.org/10.1109/ICACCA.2016.7578859

[12] Dathar, H., & Abdulazeez, A. M. (2020). A Modified Convolutional Neural Networks Model for Medical Image Segmentation. Learning, 20(July), 20

[13] Dey, S. K., & Rahman, M. M. (2020). Effects of machine learning approach in flow-based anomaly detection on software-defined networking. Symmetry, 12(1). https://doi.org/10.3390/SYM12010007
[14] Zeebaree, D. Q., Haron, H., Abdulazeez, A. M., & Zebari, D. A. (2019, April). Trainable model based on new uniform LBP feature to identify the risk of the breast cancer. In 2019 International Conference on Advanced Science and Engineering (ICOASE) (pp. 106-111). IEEE
[15] Farhat, S., Abdelkader, M., Meddeb-Makhlouf, A., & Zarai, F. (2020). Comparative Study of Classification Algorithms for Cloud IDS using NSL-KDD Dataset in WEKA. 2020 International Wireless Communications and Mobile Computing, IWCMC 2020, 445–450. https://doi.org/10.1109/IWCMC48107.2020.9148311
[16] Fukami, K., Fukagata, K., & Taira, K. (2020). Assessment of supervised machine learning methods for fluid flows. Theoretical and Computational Fluid Dynamics, 34(4), 497–519. https://doi.org/10.1007/s00162-020-00518-y
[17] Geurts, P., El Khayat, I., & Leduc, G. (2004). A machine learning approach to improve congestion control over wireless computer networks. Proceedings - Fourth IEEE International Conference on Data Mining, ICDM 2004, 383–386. https://doi.org/10.1109/ICDM.2004.10063
[18] Haddadi, F., Khanchi, S., Shetabi, M., & Derhami, V. (2010). Intrusion detection and attack classification using feed-forward neural network. 2nd International Conference on Computer and Network Technology, ICCNT 2010, 262–266. https://doi.org/10.1109/ICCNT.2010.28
[19] Abdulkareem, N. M., Abdulazeez, A. M., Zeebaree, D. Q., & Hasan, D. A. (2021). COVID-19 World Vaccination Progress Using Machine Learning Classification Algorithms. Qubahan Academic Journal, 1(2), 100-105
[20] Muhammad, M., Zeebaree, D., Abdulazeez, A. M., Saeed, J., & Zebari, D. A. (2020). A Review on Region of Interest Segmentation Based on Clustering Techniques for Breast Cancer Ultrasound Images. J. Appl. Sci. Technol. Trends, 1(3), 78-91
[21] Jijo, B. T., & Abdulazeez, A. M. (2021). Classification Based on Decision Tree Algorithm for Machine Learning. 02(01), 20–28. https://doi.org/10.38094/jastt20165
[22] Kessler, G. C. (2000). Defenses Against Distributed Denial of Service Attacks A Short History of DDoS. February. http://webtorials.net/main/resource/papers/kessler/paper1/ddos.pdf
[23] Khraisat, A., & Alazab, A. (2021). A critical review of intrusion detection systems in the Internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity, 4(1). https://doi.org/10.1186/s42400-021-00077-7
[24] Kulkarni, E. G., & Kulkarni, R. B. (2016). WEKA Powerful Tool in Data Mining General Terms. International Journal of Computer Applications, 5(Rtdm), 975–8887
[25] Li, J., Qu, Y., Chao, F., Shum, H. P. H., Ho, E. S. L., & Yang, L. (2019). Machine learning algorithms for network intrusion detection. Intelligent Systems Reference Library, 151, 151–179. https://doi.org/10.1007/978-3-319-98842-9_6
[26] Lian, W., Nie, G., Jia, B., Shi, D., Fan, Q., & Liang, Y. (2020). An intrusion detection method based on decision tree-recursive feature elimination in ensemble learning. Mathematical Problems in Engineering, 2020. https://doi.org/10.1155/2020/2835023
[27] Lin, S.-W., Ying, K.-C., Lee, C.-Y., & Lee, Z.-J. (2012). An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection. Applied Soft Computing, 12, 3285–3290. https://doi.org/10.1016/j.asoc.2012.05.004
[28] M. Sakr, M., A. Tawfeeq, M., & B. El-Sisi, A. (2019). Network Intrusion Detection System based PSO-SVM for Cloud Computing. International Journal of Computer Network and Information Security, 11(3), 22–29. https://doi.org/10.5815/ijcnis.2019.03.04
[29] Ma, Z., Liu, Y., Wang, Z., Ge, H., & Zhao, M. (2020). A machine learning-based scheme for the security analysis of authentication and key agreement protocols. Neural Computing and Applications, 32(22), 16819–16831. https://doi.org/10.1007/s00521-018-3929-8
[30] Madhusudhanarao, C., & Naidu, M. M. (2017). Acceptance sampling for network intrusion detection. Journal of Theoretical and Applied Information Technology, 95(24), 6707–6718
[31] Maniriho, P., Mahoro, L. J., Niyigaba, E., Bizimana, Z., & Ahmad, T. (2020). Detecting intrusions in computer network traffic with machine learning approaches. International Journal of Intelligent Engineering and Systems, 13(3), 433–445. https://doi.org/10.22266/IJIES2020.0630.39
[32] Masduki, B. W., Ramli, K., Saputra, F. A., & Sugiarto, D. (2016). Study on implementation of machine learning methods combination for improving attacks detection accuracy on Intrusion Detection System (IDS). 14th International Conference on QiR (Quality in Research), QiR 2015 - In Conjunction with 4th Asian Symposium on Material Processing, ASMP 2015 and International Conference in Saving Energy in Refrigeration and Air Conditioning, ICSERA 2015, 56–64. https://doi.org/10.1109/QiR.2015.7374895
[33] Maulud, D., & Abdulazeez, A. M. (2020). A Review on Linear Regression Comprehensive in Machine Learning. Journal of Applied Science and Technology Trends, 1(4), 140–147. https://doi.org/10.38094/jastt1457
[34] Meena, G. (2017). 2017 International Conference on Computer, Communications and Electronics, COMPTELIX 2017. 2017 International Conference on Computer, Communications and Electronics, COMPTELIX 2017, 553–558

[35] Mohammad, M. N., Sulaiman, N., & Muhsin, O. A. (2011). A novel Intrusion Detection System by using intelligent data mining in WEKA environment. Procedia Computer Science, 3, 1237–1242. https://doi.org/10.1016/j.procs.2010.12.198
[36] Mohammadpour, L., Hussain, M., Aryanfar, A., Maleki Raee, V., & Sattar, F. (2015). Evaluating Performance of Intrusion Detection System using Support Vector Machines: Review. International Journal of Security and Its Applications, l.9, No.9, 10. https://doi.org/10.14257/ijsia.2015.9.9.20
[37] Mohsin, A., Brifcani, A., & Sabry Issa, A. (2011). Intrusion Detection and Attack Classifier Based on Three Techniques: A Comparative Study. Eng. & Tech. Journal, 29(2)
[38] Mr. Kamlesh Lahre Suresh Kumar Kashyap, Pooja Agrawal, M. T. dhar D. (2013). Analyze Different approaches for IDS using KDD 99 Data Set. International Journal on Recent and Innovation Trends in Computing and Communication, 1(8), 7. http://www.ijritcc.org
[39] Mukherrjee, B., Heberlein, T., & Levitt, K. (1994). Network Instrusion Detection.Pdf. In IEEE Network (Vols. 26–41, Issue May/June)
[40] Nguyen, H. A., & Choi, D. (2008). Application of data mining to network intrusion detection: Classifier selection model. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 5297 LNCS, 399–408. https://doi.org/10.1007/978-3-540-88623-5_41
[41] Nie, L., Ning, Z., Wang, X., Hu, X., Cheng, J., & Li, Y. (2020). Data-Driven Intrusion Detection for Intelligent Internet of Vehicles: A Deep Convolutional Neural Network-Based Method. IEEE Transactions on Network Science and Engineering, 7(4), 2219–2230. https://doi.org/10.1109/TNSE.2020.2990984
[42] Omar, N., Abdulazeez, A. M., Sengur, A., & Al-Ali, S. G. S. (2020). Fused faster RCNNs for efficient detection of the license plates. Indonesian Journal of Electrical Engineering and Computer Science, 19(2), 974–982. https://doi.org/10.11591/ijeecs.v19.i2.pp974-982
[43] Paliwal, S., & Gupta, R. (2012). Denial-of-Service, Probing & Remote to User (R2L) Attack Detection using Genetic Algorithm. International Journal of Computer Applications, 60(19), 57–62
[44] Zebari, D. A., Abdulazeez, A. M., Zeebaree, D. Q., & Salih, M. S. (2020, December). A Fusion Scheme of Texture Features for COVID-19 Detection of CT Scan Images. In 2020 International Conference on Advanced Science and Engineering (ICOASE) (pp. 1-6). IEEE
[45] Mostafa, S. A., Mustapha, A., Mohammed, M. A., Ahmad, M. S., & Mahmoud, M. A. (2018). A fuzzy logic control in adjustable autonomy of a multi-agent system for an automated elderly movement monitoring application. *International journal of medical informatics*, *112*, 173-184
[46] Qureshi, A. U. H., Larijani, H., Ahmad, J., & Mtetwa, N. (2019). A Novel Random Neural Network Based Approach for Intrusion Detection Systems. 2018 10th Computer Science and Electronic Engineering Conference, CEEC 2018 - Proceedings, 50–55. https://doi.org/10.1109/CEEC.2018.8674228
[47] Sahu, S., & Mehtre, B. M. (2015). Network intrusion detection system using J48 Decision Tree. 2015 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2015, 2023–2026. https://doi.org/10.1109/ICACCI.2015.7275914
[48] Salih, A. A., & Abdulrazaq, M. B. (2019). Combining Best Features Selection Using Three Classifiers in Intrusion Detection System. 2019 International Conference on Advanced Science and Engineering, ICOASE 2019, April, 94–99. https://doi.org/10.1109/ICOASE.2019.8723671
[49] Saranya, T., Sridevi, S., Deisy, C., Chung, T. D., & Khan, M. K. A. A. (2020). Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review. Procedia Computer Science, 171(2019), 1251–1260. https://doi.org/10.1016/j.procs.2020.04.133
[50] Sarnovsky, M., & Paralic, J. (2020). Hierarchical intrusion detection using machine learning and knowledge model. Symmetry, 12(2), 1–14. https://doi.org/10.3390/sym12020203
[51] Selvakumar, B., & Muneeswaran, K. (2019). Firefly algorithm based feature selection for network intrusion detection. Computers and Security, 81, 148–155. https://doi.org/10.1016/j.cose.2018.11.005
[52] Senthilnayaki, B., Venkatalakshmi, K., & Kannan, A. (2015). Intrusion detection using optimal genetic feature selection and SVM based classifier. 2015 3rd International Conference on Signal Processing, Communication and Networking, ICSCN 2015, 1–4. https://doi.org/10.1109/ICSCN.2015.7219890
[53] Sharmila, B. S., & Nagapadma, R. (2019). Intrusion detection system using naive bayes algorithm. 2019 5th IEEE International WIE Conference on Electrical and Computer Engineering, WIECON-ECE 2019 - Proceedings, 8–11. https://doi.org/10.1109/WIECON-ECE48653.2019.9019921
[54] Solanki, S., Gupta, C., & Rai, K. (2020). A Survey on Machine Learning based Intrusion Detection System on NSL-KDD Dataset. International Journal of Computer Applications, 176(30), 36–39. https://doi.org/10.5120/ijca2020920343
[55] Sulaiman, D. M., Abdulazeez, A. M., Haron, H., & Sadiq, S. S. (2019). Unsupervised Learning Approach-Based New Optimization K-Means Clustering for Finger Vein Image Localization. 2019 International Conference on Advanced Science and Engineering, ICOASE 2019, 82–87. https://doi.org/10.1109/ICOASE.2019.8723749

[56] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set in Computational Intelligence for Security and Defense Applications. Computational Intelligence in Security and Defense Applications (CISDA), Cisda, 1–6

[57] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2015). 2015 IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA 2015 - Proceedings. 2015 IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA 2015 - Proceedings, Cisda, 1–6

[58] Tran, N. N., Sarker, R., & Hu, J. (2018). An approach for host-based intrusion detection system design using convolutional neural network. In Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST (Vol. 235). Springer International Publishing. https://doi.org/10.1007/978-3-319-90775-8_10

[59] Wang, H., Gu, J., & Wang, S. (2017). An effective intrusion detection framework based on SVM with feature augmentation. Knowledge-Based Systems, 136(September), 130–139. https://doi.org/10.1016/j.knosys.2017.09.014

[60] Yao, H., Gao, P., Zhang, P., Wang, J., Jiang, C., & Lu, L. (2019). Hybrid intrusion detection system for edge-based IIoT relying on machine-learning-aided detection. IEEE Network, 33(5), 75–81. https://doi.org/10.1109/MNET.001.1800479

[61] Yılmaz Gündüz, S., & ÇETER, M. N. (2018). Feature Selection and Comparison of Classification Algorithms for Intrusion Detection. ANADOLU UNIVERSITY JOURNAL OF SCIENCE AND TECHNOLOGY A - Applied Sciences and Engineering, 19(1), 206–218. https://doi.org/10.18038/aubtda.356705

[62] Zeebaree, D. Q., Abdulazeez, A. M., Zebari, D. A., Haron, H., & Hamed, H. N. A. (2020). Multi-level fusion in ultrasound for cancer detection based on uniform LBP features. Computers, Materials and Continua, 66(3), 3363–3382. https://doi.org/10.32604/cmc.2021.013314

[63] Zeebaree, D. Q., Haron, H., & Abdulazeez, A. M. (2018). Gene Selection and Classification of Microarray Data Using Convolutional Neural Network. ICOASE 2018 - International Conference on Advanced Science and Engineering, December 2018, 145–150. https://doi.org/10.1109/ICOASE.2018.8548836

[64] Zeebaree, D. Q., Haron, H., Abdulazeez, A. M., & Zebari, D. A. (2019a). Machine learning and Region Growing for Breast Cancer Segmentation. 2019 International Conference on Advanced Science and Engineering, ICOASE 2019, April, 88–93. https://doi.org/10.1109/ICOASE.2019.8723832

[65] Mohammed, M. A., Zeebaree, D. Q., Abdulazeez, A. M., Zebari, D. A., Fadhil, Z. D., Ahmed, F. Y., & Rashed, E. M. (2021, July). Machine Learning Algorithm for Developing Classroom Attendance Management System Based on Haar Cascade Frontal Face. In 2021 IEEE Symposium on Industrial Electronics & Applications (ISIEA) (pp. 1-6). IEEE

[66] Zong, W., Chow, Y. W., & Susilo, W. (2020). Interactive three-dimensional visualization of network intrusion detection data for machine learning. Future Generation Computer Systems, 102(October 2020), 292–306. https://doi.org/10.1016/j.future.2019.07.045

[67] Zebari, D. A., Zeebaree, D. Q., Abdulazeez, A. M., Haron, H., & Hamed, H. N. A. (2020). Improved Threshold Based and Trainable Fully Automated Segmentation for Breast Cancer Boundary and Pectoral Muscle in Mammogram Images. IEEE Access, 8, 203097-203116