BALTIC JOURNAL OF LAW & POLITICS
A Journal of Vytautas Magnus University
VOLUME 15, NUMBER 4 (2022)
ISSN 2029-0454

Cite: *Baltic Journal of Law & Politics* 15:4 (2022): 21-29
DOI: 10.2478/bjlp-2022-004003

Detection of Denial of Service Attacks Using J48 Algorithm Compared with Naive Bayes Algorithm to Improve Positive Detection Rate

S.Yuga Sai Sekhar
Research Scholar, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical And Technical Sciences, Saveetha University, Chennai, Tamilnadu, India. Pincode: 602105

P.Sriramya
Project Guide, Corresponding Author, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical And Technical Sciences, Saveetha University, Chennai, Tamilnadu, India. Pincode: 602105

Received: August 8, 2022; reviews: 2; accepted: November 29, 2022.

Abstract

Aim: The goal of this study is to compare accuracy to evaluate the efficiency of two machine learning methods for detecting Denial of Service (DOS) assaults.**Materials and Methods:** To diagnose DoS assaults and obtain a prediction rate to compare algorithms, several Novel J48 algorithms were used as group 1 and Naive bayes algorithms as group 2. The algorithm should be capable of detecting the specific type of DoS attack. For each of the groups studied, a sample size of N=20 was evaluated for implementation. SPSS was used to calculate the sample size. The pre-test analysis was maintained at 80%. G-power is used to calculate sample size. **Results:** Based on statistical analysis, the significance value for calculating accuracy was found to be 0.046. The significant values for calculating Flow Duration and Idle Std were found to be 0.945 and 0.266, respectively, based on statistical analysis. With a mean Flow Duration percentage of 91.14 percent, the Novel J48 Method is somewhat more accurate than the Naive Bayes algorithm, which has a mean Flow Duration percentage of 86.48 percent. **Conclusion**: The Novel J48 method provides a slightly better prediction rate value than the Naive Bayes technique when it comes to detecting DoS assaults.

Keywords

Novel J48 Algorithm, Naive bayes Algorithm, detection rate, Machine Learning, Detection of DOS attacks

INTRODUCTION

The goal of this study is to examine the Novel J48 and Naive Bayes algorithms for predicting DoS attacks using machine learning algorithms. The most important aspect of this research is the prediction of DoS attacks and their types. This allows us to detect DoS attacks more quickly and determine the nature of DoS attacks (Wang, Gao, and Wu 2021).

Nowadays, data security is critical in almost everyone's life. Organizations with sensitive data, such as NASA should protect their files from hackers. As a result, detecting the attacks is critical.DoS attacks are used to compromise devices and slow down services. As a result, detecting DoS attacks is critical. It's used by a lot of firms to find out how vulnerable their systems are. Many businesses engage hackers to find security flaws. This research is utilized in cyber security to identify a device's weaknesses.

Over 30 papers are published every year. This is a hot topic right now, with a slew of articles citing it. There are about 120 papers published in Google scholar in this domain. Scholars are focused on improving data security and lowering data breaches. About 50 paper are published in IEEE Detection of DoS attack. Detecting DoS attacks has thus far relied on a variety of techniques. There are about 120 papers published in Google scholar in this domain. However, all of the techniques have a low accuracy rate when it comes to detecting the sort of DoS attack (Yu, Liu, and Hu 2022). There are various vulnerabilities/loopholes identified in existing research that can produce erroneous results, resulting in low detection accuracy for DoS assaults (Yan and Yang 2021).The outcomes of these methods were poor. The goal of this study is to use several methods to detect DoS assaults. We developed the Novel J48 algorithm by comparing them and finding that it produces accurate results. This is capable of accurately predicting the sort of DoS attack. We can easily handle the threat and protect the device from data leak by doing so. Novel J48 has been used for emotion recognition through facial expression and psychological signals. The algorithm has also been used for pathology of skeletal system classification. (Hidayah, Adhistya, and Kristy 2014)

Previously our team has a rich experience in working on various research projects across multiple disciplines (Venu and Appavu 2021; Gudipaneni et al. 2020; Sivasamy, Venugopal, and Espinoza-González 2020; Sathish et al. 2020; Reddy et al. 2020; Sathish and Karthick 2020; Benin et al. 2020; Nalini, Selvaraj, and Kumar 2020)(Venu and Appavu 2021; Gudipaneni et al. 2020; Sivasamy, Venugopal, and Espinoza-González 2020; Sathish et al. 2020; Reddy et al. 2020; Sathish and Karthick 2020; Benin et al. 2020; Nalini, Selvaraj, and Kumar 2020)(Venu and Appavu 2021; Gudipaneni et al. 2020; Sivasamy, Venugopal, and Espinoza-González 2020; Sathish et al. 2020; Reddy et al. 2020; Sathish and Karthick 2020; Benin et al. 2020; Nalini, Selvaraj, and Kumar 2020)enu and Appavu 202. Till now various techniques are used to detect DoS attacks.(Zhang et al. 2017) But all the techniques give the poor accuracy of detecting the type of DoS attacks. In existing research there are different Vulnerabilities/ loopholes which can give false results which leads to the low accuracy of detecting DoS attacks. (Djanie et al. 2019) These techniques gave bad results. The aim of this research is to detect DoS attacks using different algorithms. By comparing them we came up with the Novel J48 algorithm which gives accurate results. This can predict the type of DoS attacks with good accuracy. By this we can easily handle the attack and save the device from data breach.

MATERIALS AND METHODS

The study was carried out in the Saveetha School of Engineering's Data Analytic lab. This study necessitates server workflow data samples. During a DoS assault on a system, the data set of a server workflow should be taken. This study compares two algorithms, with group 1 being the Novel J48 method and group 2 being the Naive Bayes algorithm. To acquire reliable findings, we took 20 samples of each algorithm. The data came from a gadget that iterated ten times to achieve the requisite accuracy with a 80 percent G power.(Bakhtiar, Pramukantoro, and Nihri 2019)

Naive Bayes Algorithm

Naive Bayesian Classification is both a supervised learning method and a statistical classification method.(Yoshikawa 2022) It assumes an underlying probabilistic model and allows us to capture uncertainty about the model in a logical manner by calculating probabilities of outcomes. It has the ability to tackle diagnostic and predictive issues. The Bayes Theorem was proposed by Thomas Bayes (1702-1761), and this classification is named after him (Cinelli et al. 2017).

Prior knowledge and observed data can be merged in Bayesian classification, which enables practical learning techniques. Many learning algorithms benefit from a Bayesian classification approach for understanding and evaluating them (Kumar et al. 2021). It calculates explicit hypothesis probabilities and is resistant to noise in the input data.

From the standing point of acquiring a general tool kit, the Naive Bayes Classifier is more suitable for general classification expectations. There has been a good variety of successful real-life applications that are based on Naive Bayes classifier, such as weather prediction services, customer credit evaluations, health condition categorizations and so on (Albon 2018). As long as the format of a data set within the problem domain is preprocessed into a tabular format. This mathematical classifier can go on to compute the validities of fitting a piece of new data into each possible classification (He et al. 2017). In this manner, the classification with highest fitness value can be chosen to be the best-fitted classification of this piece of data.

J48 Algorithm

The J48 algorithm is one of the best machine learning algorithms to examine the data categorically and continuously. When it is used, for instance, it occupies more memory space and depletes the performance and accuracy in classifying medical data (Hilal et al. 2021).It is based on a top-down strategy, a recursive divide and conquer strategy. You select which attribute to split on at the root node, and then you create a branch for each possible attribute value, and that splits the instances into subsets, one for each branch that extends from the root node.(anaN et al. 2018). To begin, we must obtain the data set for a server workflow of a DoS attack and filter it using the appropriate parameters. Take the necessary data and save it in a data frame. This data frame should be subjected to exploratory analysis (Daud et al. 2018). Using a Naive Bayes technique, we should be able to determine the positive detection rate. Fig. 1 represents the pseudo code for the J48 algorithm.

We should use the same data set of server workflow of device attacks for the second sample and filter it with the needed criteria. Fill a data frame with the needed quantity of information. on the data set, conduct exploratory analysis Using the J48 algorithm, calculate the positive detection rate. For research, Google co lab (version 2.1 x) is utilized. Mount the drive after opening the colab. To use the colab workspace, you must first upload the relevant dataset.

The dataset should be saved in the required variables. Create a programme to detect expressions using the Naive Bayes and J48 methods. run the programme In the output space, the output accuracy and detection rate will be displayed. Now, take a look at some different samples and see what you can come up with. Using SPSS, determine the positive detection rate. The data set was acquired from the source code of kaggle.com's article "DoS Detection." The Naive Bayes and j48 algorithms for stimulation were performed using colab software. There are twenty samples in each algorithm. SPSS software is used to calculate the detection rate. Using SPSS software, we can obtain precise results. Data packets and data flow at various rates are the independent variables in this study. The accuracy and detection rate are the dependent variables. With sample outputs, the detection rate was computed.

Statistical Analysis

In this examination the functioning Statistical instrument called International Business Machines (IBM)Statistical Package for Social Sciences (SPSS) V22.0. The precision values are resolved utilizing engaging and bunch insights given by this product. The huge upsides of autonomous example still up in the air. As per the correlation of Novel J48 Algorithm and Naive bayes Algorithm on all stages, Novel J48 Algorithm hopes to beat Naive bayes Algorithm. In this dataset Packet_length and FTA_flow are autonomous factors that stay consistent when different boundaries are changed. Thus, this SPSS instrument figures out the qualities and gives the diagram and the expectation rate

RESULTS

According to the data, the J48 algorithm has a 96.67 percent accuracy, whereas the Naive Bayes algorithm has a 94.09 percent accuracy. The correctness of the outputs is measured in terms of the stated inputs. The IBM SPSS application was used to obtain the results. According to the statistics, there is statistical significance between the Predictive algorithm and has an accuracy of $p = 0.046$ ($p<0.005$, 2-tailed), which is more accurate than the value.

Table 1 shows a summary of the collection of Accuracies for both Algorithms using various sample photos. In Table 2, the Accuracy for both algorithms is determined for each sample size and entered into the appropriate columns. The accuracy of both algorithms was found to improve as sample numbers were increased. Finally, the Average Accuracy is computed and saved. The J48 Algorithm has an average accuracy of 93.67 percent, whereas Naive Bayes has an accuracy of 94.09 percent. In a statistical examination of five samples, the Novel J48 model had a standard deviation of 0.7094 and a standard error of 0.2244, while Naive Bayes had a standard deviation of 0.8178 and a standard error of 0.2586.
Table 3 shows the results of independent t-tests performed to assess the accuracy of two algorithms, revealing a statistically significant difference. Fig. 2 shows the graph of J48 method has an accuracy of 96.67 percent, whereas the Naive Bayes Algorithm has an accuracy of 94.09 percent, with a statistical significant difference of $p = 0.046$ ($p<0.05$, 2-tailed). For a dataset, SPSS is used with a confidence interval of 95% and a level of significance of 0.05. For two algorithms, the mean difference and standard error difference are tabulated. In this suggested paper, the accuracy of our J48 method is 96.67 percent. Because we develop our Naive Bayes using a well-balanced and constrained dataset, it has a greater accuracy than the other methodologies.

DISCUSSION

When compared to the Naive Bayes algorithm, which has an accuracy rate of 94.06 percent, the Novel J48 method has the best performance with an accuracy rate of 96.67 percent. The performance of the Novel J48 method and the Naive Bayes algorithm for detecting DOS attacks has been examined using a dataset from GitHub and a database from the Kaggle repository. We discovered that using the parameters "Avg packets " and "Flow Packets Sec " as parameters improves the prediction rate. Furthermore, when compared to the Naive Bayes method, the Novel J48 approach performs better.

The study's trials exhibit cost analysis and categorization accuracy. In a dataset with two values, Yes and No, J48 provides better classification accuracy for the class. Though the cost analysis for both the classifiers is equal in this case, we can show that J48 is more cost effective than the Naive Bayes classifier by using the gender attribute. (Saritas and Yasar 2019) The authors used different data sets that consisted of 1000 malware data analysis with various attributes whereas in this experimental research fewer data set values were used and achieved a mean accuracy of 78.82% for Naive Bayes Algorithm which is lesser than the referred paper. In the Naive Bayes algorithm the output graph fluctuates when the input differs, whereas the Novel J48 algorithm gives the perfect and stable graph. (Zhang et al. 2017) This demonstrates that J48 is a basic decision tree classification approach. Weka technology was used to extract efficient results from this dataset experiment. (Hermawan et al. 2021) Also visible is the Naive Bayes classifier good outcomes. The Novel J48 algorithm gives the perfect prediction rate in many of the cases, except when the packet attack rate is more than 1000 at a single attempt. (Sahu and Mehtre 2015)

Because of the increased complexity and time required, the novel J48 algorithm is relatively costly. When compared to other algorithms, some calculations can be quite complex. The project's future goals include lowering the cost and time complexity of the Novel J48 algorithm. The major goal is to change the pseudo code and data techniques to boost speed and reduce complexity.

CONCLUSION

In this survey, Detection of DOS attacks using Novel J48 computation gives favored precision over Naive Bayes estimation. Novel J48 computation performed better contrasted with the Naive Bayes estimation and certain various techniques in making theories from the testing stage to the endorsement set. The Novel J48 Algorithm showed a higher precision rate (96.67%) and accomplished better at a more exact level than that of the Naive bayes estimation (94.09%).

DECLARATION

Conflict of Interests

No conflict of interests in this manuscript

Authors Contribution

Author S.Yuga Sai Sekhar was involved in data collection, data analysis, and manuscript writing. Author S.Yuga Sai Sekhar,P.Sriramya was involved in conceptualization, data validation, and critical review of manuscript.

Acknowledgement

The authors would like to express their gratitude towards Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (Formerly known as Saveetha University) for providing the necessary Infrastructure to carry out this work successfully.

Funding: We thank the following organizations for providing financial support that enabled us to complete the study.

1. Inoaura Technologies, Chennai.
2. Saveetha University.
3. Saveetha Institute of Medical And Technical Sciences.
4. Saveetha School of Engineering

REFERENCES

Albon, Chris. 2018. *Machine Learning with Python Cookbook: Practical Solutions from Preprocessing to Deep Learning*. "O'Reilly Media, Inc."

anaN, N. Sarav, N. Sarav anaN, Periyar University, and V. Gaya thri. 2018. "Performance and Classification Evaluation of J48 Algorithm and Kendall's Based J48 Algorithm (KNJ48)." *International Journal of Computer Trends and Technology*. https://doi.org/10.14445/22312803/ijctt-v59p112.

Bakhtiar, Fariz Andri, Eko Sakti Pramukantoro, and Hilman Nihri. 2019. "A Lightweight IDS Based on J48 Algorithm for Detecting DoS Attacks on IoT Middleware." *2019 IEEE 1st Global Conference on Life Sciences and Technologies (LifeTech)*. https://doi.org/10.1109/lifetech.2019.8884057.

Benin, S. R., S. Kannan, Renjin J. Bright, and A. Jacob Moses. 2020. "A Review on Mechanical Characterization of Polymer Matrix Composites & Its Effects Reinforced with Various Natural Fibres." *Materials Today: Proceedings* 33 (January): 798–805.

Cinelli, Mattia, Yuxin Sun, Katharine Best, James M. Heather, Shlomit Reich-Zeliger, Eric Shifrut, Nir Friedman, John Shawe-Taylor, and Benny Chain. 2017. "Feature Selection Using a One Dimensional Naïve Bayes' Classifier Increases the Accuracy of Support Vector Machine Classification of CDR3 Repertoires." *Bioinformatics* 33 (7): 951–55.

Djanie, Djanie, Tutu, and Dzisi. 2019. "A Proposed DoS Detection Scheme for Mitigating DoS Attack Using Data Mining Techniques." *Computers*. https://doi.org/10.3390/computers8040085.

Gudipaneni, Ravi Kumar, Mohammad Khursheed Alam, Santosh R. Patil, and Mohmed Isaqali Karobari. 2020. "Measurement of the Maximum Occlusal Bite Force and Its Relation to the Caries Spectrum of First Permanent Molars in Early Permanent Dentition." *The Journal of Clinical Pediatric Dentistry* 44 (6): 423–28.

He, Baoji, S. M. Mortuza, Yanting Wang, Hong-Bin Shen, and Yang Zhang. 2017. "NeBcon: Protein Contact Map Prediction Using Neural Network Training Coupled with Naïve Bayes Classifiers." *Bioinformatics* 33 (15): 2296–2306.

Hermawan, Dicky Rahma, Mohamad Fahrio Ghanial Fatihah, Linda Kurniawati, and Afrida Helen. 2021. "Comparative Study of J48 Decision Tree Classification Algorithm, Random Tree, and Random Forest on In-Vehicle CouponRecommendation Data." *2021 International Conference on Artificial Intelligence and Big Data Analytics*. https://doi.org/10.1109/icaibda53487.2021.9689701.

Hidayah, Indriana, Erna P. Adhistya, and Monica Agustami Kristy. 2014. "Application of J48 and Bagging for Classification of Vertebral Column Pathologies." *Proceedings of the 6th International Conference on Information Technology and Multimedia*. https://doi.org/10.1109/icimu.2014.7066651.

Hilal, Anwer Mustafa, Fahd N. Al-Wesabi, Masoud Alajmi, Majdy M. Eltahir, Mohammad Medani, Mesfer Al Duhayyim, Manar Ahmed Hamza, and Abu Sarwar Zamani. 2021. "Machine Learning Based Decision Tree J48 with Grey Wolf Optimizer for Environmental Pollution Control." *Environmental Technology*, December, 1–23.

Kumar, Mukesh, Karan Bajaj, Bhisham Sharma, and Sushil Narang. 2021. "A Comparative Performance Assessment of Optimized Multilevel Ensemble Learning Model with Existing Classifier Models." *Big Data*, December. https://doi.org/10.1089/big.2021.0257.

Nalini, Devarajan, Jayaraman Selvaraj, and Ganesan Senthil Kumar. 2020. "Herbal Nutraceuticals: Safe and Potent Therapeutics to Battle Tumor Hypoxia." *Journal of Cancer Research and Clinical Oncology* 146 (1): 1–18.

Reddy, Poornima, Jogikalmat Krithikadatta, Valarmathi Srinivasan, Sandhya Raghu, and Natanasabapathy Velumurugan. 2020. "Dental Caries Profile and Associated Risk Factors Among Adolescent School Children in an Urban South-Indian City." *Oral Health & Preventive Dentistry* 18 (1): 379–86.

Sahu, Shailendra, and B. M. Mehtre. 2015. "Network Intrusion Detection System Using J48 Decision Tree." *2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. https://doi.org/10.1109/icacci.2015.7275914.

Saritas, Mucahid Mustafa, and Ali Yasar. 2019. "Performance Analysis of ANN and Naive Bayes Classification Algorithm for Data Classification." *International Journal of Intelligent Systems and Applications in Engineering*. https://doi.org/10.18201/ijisae.2019252786.

Sathish, T., and S. Karthick. 2020. "Gravity Die Casting Based Analysis of Aluminum Alloy with AC4B Nano-Composite." *Materials Today: Proceedings* 33 (January): 2555–58.

Sathish, T., D. Bala Subramanian, R. Saravanan, and V. Dhinakaran. 2020. "Experimental Investigation of Temperature Variation on Flat Plate Collector by Using Silicon Carbide as a Nanofluid." In *PROCEEDINGS OF INTERNATIONAL CONFERENCE ON RECENT TRENDS IN MECHANICAL AND MATERIALS ENGINEERING: ICRTMME 2019*. AIP Publishing. https://doi.org/10.1063/5.0024965.

Sivasamy, Ramesh, Potu Venugopal, and Rodrigo Espinoza-González. 2020. "Structure, Electronic Structure, Optical and Magnetic Studies of Double Perovskite Gd2MnFeO6 Nanoparticles: First Principle and Experimental Studies." *Materials Today Communications* 25 (December): 101603.

Venu, Harish, and Prabhu Appavu. 2021. "Experimental Studies on the Influence of Zirconium Nanoparticle on Biodiesel–diesel Fuel Blend in CI Engine." *International Journal of Ambient Energy* 42 (14): 1588–94.

Wang, Jiaqi, Jinfeng Gao, and Ping Wu. 2021. "Attack-Resilient Event-Triggered Formation Control of Multi-Agent Systems under Periodic DoS Attacks Using Complex Laplacian." *ISA Transactions*, November. https://doi.org/10.1016/j.isatra.2021.10.030.

Yan, Jing-Jing, and Guang-Hong Yang. 2021. "Secure State Estimation of Nonlinear Cyber-Physical Systems Against DoS Attacks: A Multiobserver Approach." *IEEE Transactions on Cybernetics* PP (September). https://doi.org/10.1109/TCYB.2021.3100303.

Yasin, Waheed, Hamidah Ibrahim, Nur Izura Udzir, and Nor Asilah Wati Hamid. 2014. "Intelligent Cooperative Least Recently Used Web Caching Policy Based on J48

Classifier." *Proceedings of the 16th International Conference on Information Integration and Web-Based Applications & Services*. https://doi.org/10.1145/2684200.2684299.

Yoshikawa, Hideo. 2022. "Can Naive Bayes Classifier Predict Infection in a Close Contact of COVID-19? A Comparative Test for Predictability of the Predictive Model and Healthcare Workers in Japan." *Journal of Infection and Chemotherapy: Official Journal of the Japan Society of Chemotherapy*, February. https://doi.org/10.1016/j.jiac.2022.02.017.

Yu, Yi, Guo-Ping Liu, and Wenshan Hu. 2022. "Security Tracking Control for Discrete-Time Stochastic Systems Subject to Cyber Attacks." *ISA Transactions*, February. https://doi.org/10.1016/j.isatra.2022.02.001.

Zhang, Heng, Yifei Qi, Huan Zhou, Jian Zhang, and Jing Sun. 2017. "Testing and Defending Methods Against DOS Attack in State Estimation." *Asian Journal of Control*. https://doi.org/10.1002/asjc.1441.

Dietterich, T. [1998] An Experimental Comparison of Three Methods for Constructing Ensembles of Decision Trees: Bagging, Boosting and Randomization, Machine Learning 1-22

Freund, Y. and Schapire, R. [1996] Experiments with a new boosting algorithm, Machine Learning: Proceedings of the Thirteenth International Conference, pp. 148-156

Grove, A. and Schuurmans, D. [1998]. Boosting in the limit: Maximizing the margin of learned ensembles. In Proceedings of the Fifteenth National Conference on Artificial Intelligence (AAAI-98).

TABLES AND FIGURES

Table 1. The below table shows the 10 iterations of the Naive Bayes algorithm and J48 algorithm with different iterations and their extracted accuracies.

S.NO	**J48**	**NAIVE BAYES**
1	98.3	94.7
2	94.5	93.1
3	97.9	90.4
4	99.7	89.2
5	95.9	92.3
6	90.4	87.6
7	97.9	94.9
8	94.7	91.4
9	98.5	89.2

10	90.4	90.2

Table 2. Independent Variable:The statistical calculations for independent samples T test between Novel J48 Algorithm and Navie Bayes Algorithm(NBA). This independent sample test consists of significance as 0.046, significance.

Accuracy	Levene's test for equality of variances		t-test for Equality of Means						
	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error difference	95% Confidence Interval of the Difference	
								Lower	Upper
Equal variances assumed	2.910	0.046	10.508	38	.000	8.76597	.83422	7.07719	10.45476
Equal variances not assumed			10.508	33.379	.000	8.76597	.83422	7.06948	10.46247

Table 3. Group Statistics:Novel J48 Algorithm and Naive Bayes are the two machine learning algorithms used in this statistics.Sample size N = 20. Mean for Novel J48 Algorithm is 94.972 and Naive Bayes is 86.206. Std. Deviation for Novel J48 Algorithm is 2.09041 and Naive Bayes is 3.09008. Std Error Mean for J48 is 0.46743 and Naive Bayes is 0.69096.

	Algorithm	**N**	**Mean**	**Std. Deviation**	**Std. Error Mean**
Accuracy	J48	20	94.972	2.09041	0.46743
	Naive Bayes	20	86.206	3.09008	0.69096

```
Algorithm of J48 (D)
Input: a dataset D
begin
   Tree = {}
   If (D is "pure") ||( other stopping criteria met)then terminate;
   For all attribute a a ∈ D D do
      Compute criteria of impurity function if we split on a;
   a_best = Best attribute according to above computed criteria
   Tree = Create a decision node that tests a_best in the root
   D_v = Induced sub-datasets from D based on a_best
    For all D_v do
      begin
        Tree_v = J48(D_v)
         Attach Tree_v to the corresponding branch of Tree
       end
     return Tree
end
```

Fig. 1. Pseudo Code for J48 Algorithm(Yasin et al. 2014)

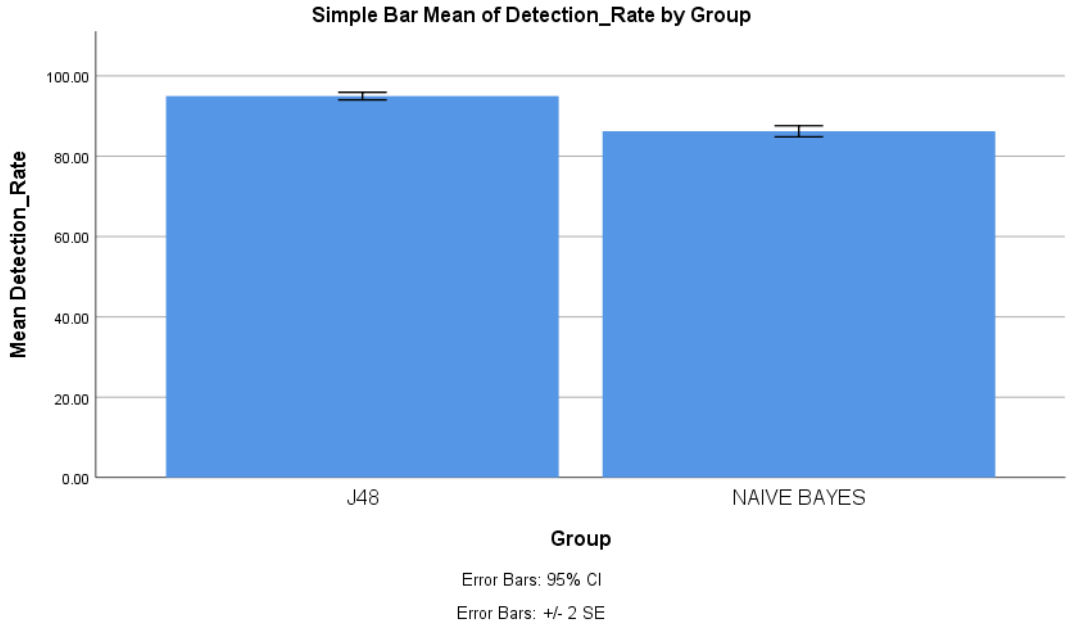

Fig. 2. Bar Graph showing the Mean of Accuracy by J48 Algorithm and Naive Bayes Algorithm(NBA), the bar chart representing the comparison of mean accuracy of J48 Algorithm is 94.972 and Naive Bayes Algorithm is 86.206. X-Axis: J48 Algorithm vs Naive Bayes Algorithm. Y-Axis: Mean accuracy. The error bars are 95% for both algorithms. The Standard Deviation Error Bars are +/- 1 SD.