Original Article

Accurate Deauthentication Attack Detection using SVM Classifier in Comparison with Decision Tree Classifier

B Janardhan[1], Karthikeyan.P. R[2]

[1]Research Scholar, Department of Electronics and Communication Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamilnadu, India, Pincode: 602105
[2]Project Guide, Corresponding Author, Department of Electronics and Communication Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamilnadu, India, Pincode: 602105

Abstract

Aim: This study aims to compare the accuracy of Support Vector Machine Classifier to Decision Tree Classifier in detecting deauthentication attacks.
Materials and Methods: The dataset used in this study consists of 61,000 records. For testing, 9,604 records calculated using G power are used to achieve a 95 % confidence level in accuracy with 1% margin error. Each record consists of 42 attributes/features. In order to detect deauthentication attacks, SVM and Decision Tree are used.
Results: The accuracy of SVM was 87.02%, P<0.05, whereas the accuracy of the Decision Tree Classifier was 71.81%, P<0.05.
Conclusion: Comparing SVM to Decision Tree Classifier, the present study found that SVM performed significantly better in detecting deauthentication attacks.

Keywords: Deauthentication attack, SVM, Novel Features Selection, Decision Tree Classifier, Machine Learning, Entropy

DOI: 10.47750/pnr.2022.13.S04.091

INTRODUCTION

Deauthentication attack is a type of denial of service attack. The primary target of the Deauthentication attack is the wifi connection between the client and the access point. During this attack, the attacker can send a deauthentication frame spoofing the MAC address that seems to be the same as the legitimate data frame. The reason why the attack exists is due to the unencrypted Deauthentication frames (Gast 2005). The Deauth-DoS detection is performed here with the aid of a machine learning-based intrusion detection system (IDS) (Agarwal, Biswas, and Nandi 2015). Detection of deauthentication attacks helps in getting rid of all other attacks that use the deauthentication attack as the base for the advanced attacks. Thus detection of Deauth-DoS attacks and protecting the network from it can be the efficient way to get rid of other attacks that use Deauth-DoS as the primary attack.
In total, there are 35 conference papers in IEEE Xplore and 3 journal papers. ("Improvement of Approach to Detect Sinkhole Attacks in Wireless Sensor Networks" 2014)(Y. Zhang, Zheng, and Hu 2008; Cheema, Bansal, and Sofat 2011)("Improvement of Approach to Detect Sinkhole Attacks in Wireless Sensor Networks" 2014) concludes that Deauth-DoS attack can cause serious damage if performed against ad-hoc sensitive solely Wi-Fi-based devices like health care lab machines. (Kristiyanto and Ernastuti 2020) performed an attack using Arduino ESP8266 NodeMCU WiFi with Lua programming to know the level of security of WiFi connectivity against deauthentication. (Cheema, Bansal, and Sofat 2011) implemented a real deauth-DOS attack on the wifi network and concluded that the attack reduces the bandwidth and throughput of the connection. This is due to unencrypted management frames in WPA2. (Nguyen et al. 2008) implemented a one-way hard function to verify the deauthentication attack is legitimate or not. Implementation of this may contradict to the Wi-Fi standards which introduces a change in the protocol of the WPA2. DOS is an attack that consumes all the resources of the network, therefore halting the communication (Y. Zhang, Zheng, and Hu 2008; Cheema, Bansal, and Sofat 2011). Data frames are authenticated and encrypted, while control and management frames are not. As a result, the attacker can easily spoof them and undertake various types of dos attacks such as impersonation attacks, resource reduction assaults, and media access attacks (Kaur 2016).

Our team has extensive knowledge and research experience that has translate into high quality publications (Bhansali et al. 2021; Jayanth et al. 2021; Sudhakar, Ravel, and Perumal 2021; Sathiyamoorthi et al. 2021; Deepanraj et al. 2021; Raju et al. 2021; Arun Prakash et al. 2020; Kamath et al. 2020; Shanmugam et al. 2021; Rajasekaran et al. 2020; Adhinarayanan et al. 2020; Rajesh et al. 2020; Aurtherson et al. 2021). Most of the existing works use protocol modification to prevent deauthentication attack but modifying protocol may contradict the already implemented systems that use a specific standard. In this proposed method IDS is implemented using machine learning models to detect the Deauth-DOS. SVM and Decision Tree Classifier are compared and the performances are compared to determine the accurate one to detect Deauth-DOS.

MATERIALS AND METHODS

The proposed research is conducted in the Signal and Image Processing Lab at Saveetha School of Engineering. For the study setting two groups were identified namely Normal and attack groups (Agarwal, Biswas, and Nandi 2015; Agarwal et al. 2016). With calculator.net, a sample size of 9604 is calculated with a confidence level of 95% on the accuracy value and a margin of error of 1%. The data sets were taken from the University of New Brunswick, Canada. The NSL-KDD dataset used in this project consists of 50,000 samples. Each sample consists of 42 attributes/features as shown in the table1.

NSL-KDD dataset collected from the University of New Brunswick, Canada needs to be processed before applying it to the machine learning model. The processed dataset is given for training and testing. In the action of Data processing initially, the data is loaded into the environment and missing data removal, replacement of null values are done. As the next step descriptive statistics is done on the features available in the data set. The process of novel features selection involves manually or automatically selecting the features that contribute the most to prediction variable or output of interest here accuracy. Novel Features selection is done by using Randomforest classifier and the significance of all the attributes in distinguishing the attack are plotted. As the next step in the process of novel features selection, 10 most significant features are selected for the classification of data as normal and attack class. The preprocessed dataset with features are given as input to SVM and Decision Tree Classifier. From the total sample size 80% of the data is given for training and the remaining 20% is given for testing. Finally the models are trained and tested against the data sets and the accuracy of the models in detection of deauthentication attack is obtained. The learning process of SVM and Decision Tree Classifier was given below.

SVM stands for Support Vector Machine. It is a supervised machine learning model that searches for the boundary that classified the groups efficiently. SVM constructs a hyperplane in high dimensional space which can be used for classification, regression, or other tasks like outliers detection. Support Vectors are simply the coordinates of individual observation. The best hyperplane that fits our model is selected based on the distance between the support vectors and the hyperplane this distance is called Margin. The hyperplane with maximum margin is considered the best one for the classification. The C parameter tells the SVM optimization how much do one want to avoid misclassifying each training. For large values of C, the optimization will choose a smaller-margin hyperplane if that hyperplane does a better job of getting all the training points classified correctly. Conversely, a very small value of C will cause the optimizer to look for a larger-margin separating hyperplane, even if that hyperplane misclassifies more points. Higher c value leads to overfitting and lower c value leads to under fitting.

The Decision Tree algorithm belongs to the family of supervised machine learning algorithm. It is a tree-structured classifier, where internal nodes represent the features of a dataset, branches represent the decision rules and each leaf node represents the outcome. The features for conclusion of the results are taken based on the increasing levels of entropy. Entropy is a measure of the randomness in the information being processed. The higher the entropy, the harder it is to draw any conclusions from that information. Entropy always lies between 0 to 1. In the given set the src_bytes have lower entropy therefore it lies at the initial root node followed by the features with their entropy levels in ascending order.

Our team has extensive knowledge and research experience that has translate into high quality publications(Bhansali et al. 2021; Jayanth et al. 2021; Sudhakar, Ravel, and Perumal 2021; Sathiyamoorthi et al. 2021; Deepanraj et al. 2021; Raju et al. 2021; Arun Prakash et al. 2020; Kamath et al. 2020; Shanmugam et al. 2021; Rajasekaran et al. 2020; Adhinarayanan et al. 2020; Rajesh et al. 2020; Aurtherson et al. 2021). The proposed work uses the google colab cloud platform with 12.67GB RAM and 107.27 Disk space for testing the SVM and Decision Tree Classifier. The Python programming tool is used for the execution of the algorithm.

SPSS Analysis

All analyses are conducted using Python and SPSS tools (IBM-SPSS v21) (Aldrich 2018). The independent sample T-test is done using SPSS and group statistics are calculated using python. SPSS is used to measure the mean, std deviation, and significant difference between the two groups. The simulated mean values and standard deviation are shown in the tabulation. In this study, independent variables are the input features such as src_bytes, dst_bytes, etc. The dependent variable accuracy is the output parameters.

RESULTS

Accuracy is used as an independent variable in comparing SVM and Decision Tree Classifier in deauthentication attack detection. Table 1 consists of number of features and classes present in the data set. Table 2 is the statistical analysis of the data set and consists of minimum, maximum, mean and standard deviation of all the features available. Using the same data set, each model was trailed ten times and the results are presented in Table 3. T-test analysis is done using statistical packages of social sciences (IBM-SPSS v21) and the results are tabulated in Table 4. From the mean accuracy graph in Fig 2, it can be observed that SVM detects deauthentication attacks accurately compared to Decision Tree Classifier.

From Table 3, it can be observed that the accuracy of SVM is greater than the Decision Tree Classifier. The accuracy values of SVM have not much deviation compared to Decision Tree Classifier.

Figure. 1 shows the output of the RandomForest algorithm used in the novel features selection process . The most important features in the data sets for detecting deauthentication attacks are src bytes, followed by flags, same srv rate, diff srv rate, and dst host same srv rate. Novel Features selection helps in identifying the features that contribute the most in detection of the attack class. From Fig. 2, it can be observed that accuracy of SVM for the first iteration is 85.81% . During the third iteration the accuracy value increases to 87.91% and continues at the same values till the fifth iteration. During the sixth iteration the accuracy drops to 85.82% and for the seventh iteration increases to 87.90%. This oscillation of accuracy values continues till the tenth iteration. Accuracy of Decision Tree Classifier in detection of deauthentication attack is shown in Fig. 3. For the first iteration the accuracy of the Decision Tree classifier is 58.26% , for the second iteration the accuracy increases to 85% and stays till the third iteration. For the fourth iteration the accuracy drops to 58.26% and increases to 84.64% for the fifth iteration. It continues at 84.64% till seventh iteration. For the eighth iteration the accuracy value decreases and settles at 60% for further iterations. From Fig 4, it can be observed that the SVM has higher accuracy compared to Decision Tree Classifier. The standard deviation in accuracy for SVM is lesser compared to Decision Tree Classifier. Therefore, SVM is better compared to Decision Tree Classifier in detection of deauthentication attacks.

DISCUSSION

In this study it is observed that the accuracy of SVM is greater than that of Decision Tree Classifier. The mean accuracy of SVM obtained is 87.02% and Decision Tree is 71.81%. SVM and Decision Tree algorithms are trained and tested with NSL-KDD dataset obtained from the University of New Brunswick, Canada. The data set consists of 42 features. The importance of each attribute in distinguishing the datapoint of normal class or attack class is plotted in Fig 1. From all the features available 10 most significant features are taken for training the model. On training and testing the model against the data set it can be concluded that SVM detects the attack more accurately compared to Decision Tree Classifier.

(B. Zhang et al. 2018) detects attacks using a Gaussian Naive Bayes algorithm and achieves an accuracy of 83.28. The proposed work archives an accuracy value of 87.07 which is better compared to the existing. (Agarwal, Biswas, and Nandi 2015) implements SVM algorithm in the detection of deauthentication attack and achieves an accuracy value of 82.9 %. The proposed model detects deauthentication attacks with an accuracy of 87.02% which is greater than the previously proposed model. (Agarwal, Biswas, and Nandi 2015; Agarwal et al. 2016) carried out the study of detection of flooded DoS attacks using SVM and obtained an accuracy of 98.7% which is far greater than the accuracy obtained in the proposed work. The higher accuracy in the previous work is due to lesser dataset used for the analysis and different novel features selection process employed for selection of most significant features.

The dataset used in the proposed work is finite thus the confidence in accuracy obtained is limited. If the datasets are increased the confidence in the accuracy can be increased. SVM algorithm do not perform well if the target classes overlap with each other. For future work, a combination of multiple Machine Learning models is used to increase the accuracy of the model using larger data sets and hybrid multi-level models. The future model could categorize attacks more effectively by developing well-organized classifiers.

CONCLUSION

Detecting a deauthentication attack accurately lowers the risk of communication bandwidth being reduced. SVM produced an accuracy of 87.02%, $P < 0.05$ compared to the Decision Tree Classifier whose accuracy is 71.81%, $P < 0.05$. Comparing SVM to Decision Tree Classifier, the present study found that SVM performed significantly better in detecting deauthentication attacks.

Declarations

Conflict of interests

No conflict of interest in this manuscript.

Author Contribution

Author BJ was involved in data collection, data analysis, manuscript writing. Author KG was involved in the conceptualization, guidance, and critical review of the manuscript.

Acknowledgment

The authors would like to thank Saveetha School of Engineering and Saveetha Institute of Medical and Technical Sciences (Formerly Known as Saveetha University) for providing the infrastructure required to complete this study effectively.

Funding We would like to express our gratitude to the following organizations for giving financial support that helped us to finish the study.

1. Manac Infotech Pvt.Ltd.
2. Saveetha Institute of Medical and Technical Sciences.
3. Saveetha School of Engineering.
4. Saveetha University.

REFERENCE

1. Adhinarayanan, Rajesh, Aravindh Ramakrishnan, Gopal Kaliyaperumal, Melvinvíctor De Poures, Rajesh Kumar Babu, and Damodharan Dillikannan. 2020. "Comparative Analysis on the Effect of 1-Decanol and Di-N-Butyl Ether as Additive with diesel/LDPE Blends in Compression Ignition Engine." Energy Sources, Part A: Recovery, Utilization, and Environmental Effects, June, 1–18.
2. Agarwal, Mayank, Santosh Biswas, and Sukumar Nandi. 2015. "Detection of De-Authentication DoS Attacks in Wi-Fi Networks: A Machine Learning Approach." 2015 IEEE International Conference on Systems, Man, and Cybernetics. https://doi.org/10.1109/smc.2015.55.
3. Agarwal, Mayank, Dileep Pasumarthi, Santosh Biswas, and Sukumar Nandi. 2016. "Machine Learning Approach for Detection of Flooding DoS Attacks in 802.11 Networks and Attacker Localization." International Journal of Machine Learning and Cybernetics. https://doi.org/10.1007/s13042-014-0309-2.
4. Aldrich, James O. 2018. Using IBM SPSS Statistics: An Interactive Hands-On Approach. SAGE Publications.
5. Arun Prakash, V. R., J. Francis Xavier, G. Ramesh, T. Maridurai, K. Siva Kumar, and R. Blessing Sam Raj. 2020. "Mechanical, Thermal and Fatigue Behaviour of Surface-Treated Novel Caryota Urens Fibre–reinforced Epoxy Composite." Biomass Conversion and Biorefinery, August. https://doi.org/10.1007/s13399-020-00938-0.
6. Aurtherson, P. Babu, Bhanu Teja Nalla, Karthikeyan Srinivasan, Kulmani Mehar, and Yuvarajan Devarajan. 2021. "Biofuel Production from Novel Prunus Domestica Kernel Oil: Process Optimization Technique." Biomass Conversion and Biorefinery, May. https://doi.org/10.1007/s13399-021-01551-5.
7. Bhansali, Karan J., Kamlesh R. Balinge, Subodh U. Raut, Shubham A. Deshmukh, M. Senthil Kumar, C. Ramesh Kumar, and Pundlik R. Bhagat. 2021. "Visible Light Assisted Sulfonic Acid-Functionalized Porphyrin Comprising Benzimidazolium Moiety for Photocatalytic Transesterification of Castor Oil." Fuel 304 (November): 121490.
8. Cheema, Rupinder, Divya Bansal, and Sanjeev Sofat. 2011. "Deauthentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks." International Journal of Computer Applications. https://doi.org/10.5120/2901-3801.
9. Deepanraj, B., N. Senthilkumar, D. Mala, and A. Sathiamourthy. 2021. "Cashew Nut Shell Liquid as Alternate Fuel for CI Engine—optimization Approach for Performance Improvement." Biomass Conversion and Biorefinery, February. https://doi.org/10.1007/s13399-021-01312-4.
10. Gast, Matthew S. 2005. 802.11 Wireless Networks: The Definitive Guide: The Definitive Guide. "O'Reilly Media, Inc."
11. "Improvement of Approach to Detect Sinkhole Attacks in Wireless Sensor Networks." 2014. Computer, Intelligent Computing and Education Technology. https://doi.org/10.1201/9781315760827-152.
12. Jayanth, Bellappu Venkat, Melvin Victor Depoures, Gopal Kaliyaperumal, Damodharan Dillikannan, Dilipsingh Jawahar, Kumaran Palani, and Ganesha Prasad Meravanigee Shivappa. 2021. "A Comprehensive Study on the Effects of Multiple Injection Strategies and Exhaust Gas Recirculation on Diesel Engine Characteristics That Utilize Waste High Density Polyethylene Oil." Energy Sources, Part A: Recovery, Utilization, and Environmental Effects, June, 1–18.
13. Kamath, Manjunath, Subha Krishna Rao, Jaison, Sridhar, Kasthuri, Gopinath, Sivaperumal, and Shantanu Patil. 2020. "Melatonin Delivery from PCL Scaffold Enhances Glycosaminoglycans Deposition in Human Chondrocytes – Bioactive Scaffold Model for Cartilage Regeneration." Process Biochemistry 99 (December): 36–47.
14. Kaur, Jaspreet. 2016. "Mac Layer Management Frame Denial of Service Attacks." 2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE). https://doi.org/10.1109/icmete.2016.83.
15. Kristiyanto, Yogi, and E. Ernastuti. 2020. "Analysis of Deauthentication Attack on IEEE 802.11 Connectivity Based on IoT Technology Using External Penetration Test." CommIT (Communication and Information Technology) Journal. https://doi.org/10.21512/commit.v14i1.6337.
16. Nguyen, T. D., D. Nguyen, B. N. Tran, H. Vu, and N. Mittal. 2008. "A Lightweight Solution for Defending Against Deauthentication/Disassociation Attacks on 802.11 Networks." 2008 Proceedings of 17th International Conference on Computer Communications and Networks. https://doi.org/10.1109/icccn.2008.ecp.51.
17. Rajasekaran, S., D. Damodharan, K. Gopal, B. Rajesh Kumar, and Melvin Victor De Poures. 2020. "Collective Influence of 1-Decanol Addition, Injection Pressure and EGR on Diesel Engine Characteristics Fueled with diesel/LDPE Oil Blends." Fuel 277 (October): 118166.
18. Rajesh, A., K. Gopal, De Poures Melvin Victor, B. Rajesh Kumar, A. P. Sathiyagnanam, and D. Damodharan. 2020. "Effect of Anisole Addition to Waste Cooking Oil Methyl Ester on Combustion, Emission and Performance Characteristics of a DI Diesel Engine without Any Modifications." Fuel 278 (October): 118315.
19. Raju, P., K. Raja, K. Lingadurai, T. Maridurai, and S. C. Prasanna. 2021. "Glass/Caryota Urens Hybridized Fibre-Reinforced nanoclay/SiC Toughened Epoxy Hybrid Composite: Mechanical, Drop Load Impact, Hydrophobicity and Fatigue Behaviour." Biomass Conversion and Biorefinery, March. https://doi.org/10.1007/s13399-021-01427-8.
20. Sathiyamoorthi, Ramalingam, Gomathinayakam Sankaranarayanan, Dinesh Babu Munuswamy, and Yuvarajan Devarajan. 2021. "Experimental Study of Spray Analysis for Palmarosa Biodiesel-diesel Blends in a Constant Volume Chamber." Environmental Progress

& Sustainable Energy 40 (6). https://doi.org/10.1002/ep.13696.
21. Shanmugam, Rajasekaran, Damodharan Dillikannan, Gopal Kaliyaperumal, Melvin Victor De Poures, and Rajesh Kumar Babu. 2021. "A Comprehensive Study on the Effects of 1-Decanol, Compression Ratio and Exhaust Gas Recirculation on Diesel Engine Characteristics Powered with Low Density Polyethylene Oil." Energy Sources, Part A: Recovery, Utilization, and Environmental Effects 43 (23): 3064–81.
22. Sudhakar, M. P., Merlyn Ravel, and K. Perumal. 2021. "Pretreatment and Process Optimization of Bioethanol Production from Spent Biomass of Ganoderma Lucidum Using Saccharomyces Cerevisiae." Fuel 306 (December): 121680.
23. Zhang, Bing, Zhiyang Liu, Yanguo Jia, Jiadong Ren, and Xiaolin Zhao. 2018. "Network Intrusion Detection Method Based on PCA and Bayes Algorithm." Security and Communication Networks. https://doi.org/10.1155/2018/1914980.
24. Zhang, Yan, Jun Zheng, and Honglin Hu. 2008. Security in Wireless Mesh Networks. CRC Press.

Tables and Figures

Table 1. Samples, features, and classes from Datasets - The data sets consist of two classes attack class and normal class with 42 features.

Data Sets	Features	Classes
Test Dataset	42	2
Train Dataset	42	2

Table 2. Statistical features of the NSL-KDD dataset - The mean, standard deviation, minimum and maximum values are tabulated.

	count	mean	std	min	25%	50%	75%	max
duration	50000	86.9285	927.6287847	0	0	0	0	29053
src_bytes	50000	6515.08484	142678.4508	0	0	0	244	18828976
dst_bytes	50000	2309.65104	43058.86775	0	0	0	478	5131424
land	50000	0.0004	0.0199962	0	0	0	0	1
urgent	50000	6.00E-05	0.013416408	0	0	0	0	3
hot	50000	0.1452	1.633122868	0	0	0	0	77
num_failed_logins	50000	0.00074	0.038203162	0	0	0	0	4
logged_in	50000	0.37382	0.483821547	0	0	0	1	1
num_compromised	50000	0.19534	9.873936002	0	0	0	0	884
root_shell	50000	0.00102	0.031921466	0	0	0	0	1
su_attempted	50000	0.001	0.042415044	0	0	0	0	2
num_root	50000	0.20306	10.92727847	0	0	0	0	975
num_file_creations	50000	0.01268	0.501362389	0	0	0	0	40
num_shells	50000	0.00026	0.01612258	0	0	0	0	1
num_access_files	50000	0.00372	0.091358243	0	0	0	0	8
is_guest_login	50000	0.00612	0.077991456	0	0	0	0	1
count	50000	94.4	101.5810589	0	4	39	185	511
srv_count	50000	19.27404	43.67500993	0	3	8	17	502

serror_rate	50000	0.4076464	0.488829594	0	0	0	1	1
srv_serror_rate	50000	0.4065064	0.488561702	0	0	0	1	1
rerror_rate	50000	0.103159	0.301654323	0	0	0	0	1
srv_rerror_rate	50000	0.104535	0.302062167	0	0	0	0	1
same_srv_rate	50000	0.5528708	0.456239461	0	0.07	0.99	1	1
diff_srv_rate	50000	0.0494412	0.114967439	0	0	0.03	0.06	1
srv_diff_host_rate	50000	0.0661986	0.205012136	0	0	0	0	1
dst_host_count	50000	196.03142	91.55295447	0	128	255	255	255
dst_host_srv_count	50000	104.53792	110.3305853	0	10	25	255	255
dst_host_same_srv_rate	50000	0.454722	0.446524815	0	0.04	0.17	1	1
dst_host_diff_srv_rate	50000	0.0521972	0.094205699	0	0	0.05	0.07	1
dst_host_same_src_port_rate	50000	0.0628646	0.192257523	0	0	0	0.01	1
dst_host_srv_diff_host_rate	50000	0.0133572	0.051442688	0	0	0	0.01	1
dst_host_serror_rate	50000	0.4070912	0.487968758	0	0	0	1	1
dst_host_srv_serror_rate	50000	0.4022024	0.488018533	0	0	0	1	1
dst_host_rerror_rate	50000	0.103876	0.298456104	0	0	0	0	1
dst_host_srv_rerror_rate	50000	0.1028422	0.297259306	0	0	0	0	1

Table 3. Accuracy of SVM and Decision Tree classifier in the detection of deauthentication attack over 10 iterations - The accuracy of both SVM and Decision Tree Classifier is not constant. Accuracy of Decision Tree Classifier deviates more compared to SVM in detection

Trail	SVM	Decision Tree Classifier
1	0.8581	0.5826
2	0.8534	0.8500
3	0.8791	0.8499
4	0.8790	0.5826
5	0.8790	0.8464
6	0.8582	0.8464
7	0.8790	0.8464
8	0.8790	0.5969
9	0.8582	0.5827
10	0.8790	0.5969

Table 4. Independent sample test: Independent sample T- test is performed for the dataset with a 95% confidence interval and a significance level P < 0.05 (SVM appears to perform significantly better than Decision Tree Classifier)

		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
Accuracy	Equal variances assumed	3955.476	.000	3.503	18	.003	.15212	.04343	.06087	.24337
	Equal variances not assumed			3.503	9.126	.007	.15212	.04343	.05408	.25016

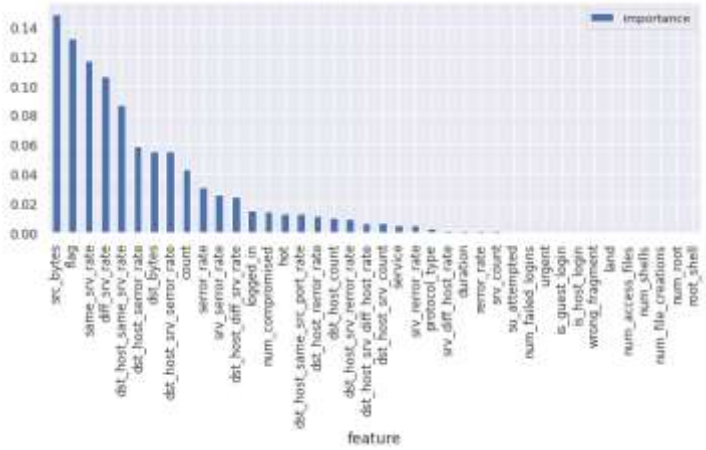

Fig. 1. Features selection - The features are plotted based on their significance in detecting the attack.

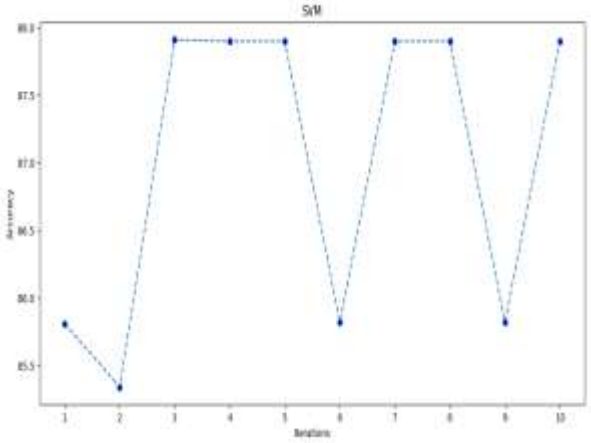

Fig. 2. Accuracy of SVM over 10 iterations - Accuracy of SVM in detection of attack oscillates between 85% and 88% as the iterations increase.

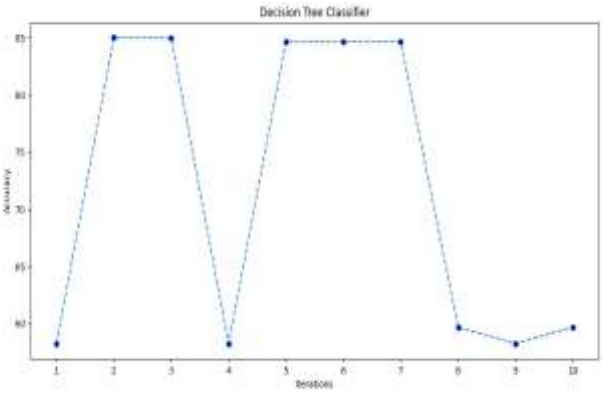

Fig. 3. Accuracy of Decision Tree Classifier over 10 iterations - Accuracy of Decision Tree classifier is oscillating between 85% and 60% till seventh iteration. After 8 the iteration it starts to settle at 60%.

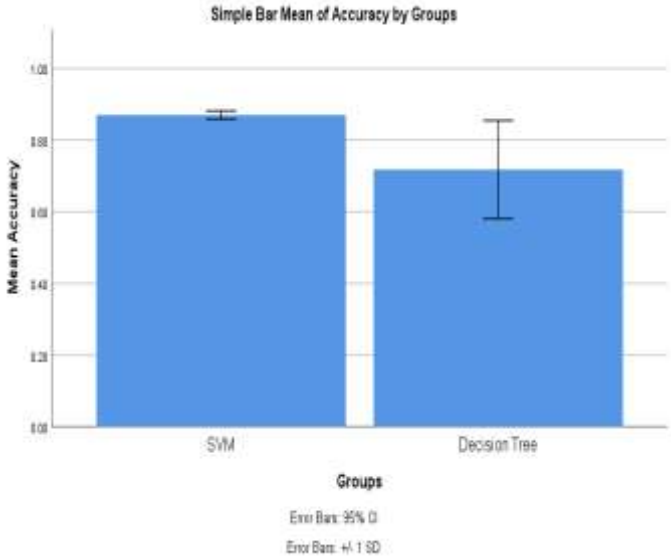

Fig. 4. Mean accuracy graph of SVM and Decision Tree - Accuracy of SVM is high compared to Decision Tree in detection of deauthentication attack. Standard Deviation (SD) of Decision Tree classifier is high compared to Standard Deviation (SD) of SVM. X Axis: SVM vs Decision Tree,Y Axis: Mean accuracy of detection ± 1 SD.