iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** IV **Month of publication:** April 2017

DOI: http://doi.org/10.22214/ijraset.2017.4113

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Intrusion Detection System by using K-Means Clustering, C 4.5, FNN, SVM Classifier

Akshay Takke[1], Ravikumar Gujjul[2], Mikhil Ghag[3] , Vivek Pawar[4], Vivek Pandey[5]
[1 2 3 4] *UG Student, IT Engineering Department of Information Technology,* [5] *Professor*

Abstract: ***Security of Information is one of the keystones of Information Society. Past few year, many attacks are increased, intrusion detection system(IDS) is important component and to protect the network. In present-days, many researchers are using data mining techniques for building IDS. One of the main challenges in the security management of large-scale high speed networks is to detect of inconsistency in network traffic patterns due to Distributed Denial of Service (DDoS) attacks or worm propagation. Intrusion detection methods started appearing in the last few years. Here, so we present a Intrusion detection method using K-means clustering, neuro-fuzzy models, Support vector machine (SVM) and C4.5 algorithm. We are using a four level framework for Intrusion detection in which first step related to generate different training datasets by using k-means clustering, second step based on the training datasets different neuro-fuzzy models are trained, third step a vector for SVM classification and radial SVM classification is perform. Finally we build the decision tree using C4.5 decision tree algorithm and we build graph on the basis of SVM classification and C4.5 decision tress algorithm.***

I. INTRODUCTION

Nowadays network is very important for the communication. We can do lots of things on the internet like searching, images, videos, etc. this is main advantages of the internet .we are using the internet for our personal work or commercial work. But we cannot sure about, our data is secure. now days we transfer the data from source to destination. While transferring from source to destination we cannot sure about that data correctly transfer to the destination, because nowadays attacks are increases so if we want to transfer the data securely so we have to make some security. So that you can transfer your data securely. Important thing is it will use in anywhere like home, company, colleges, etc. to secure your data from attacker so you have to use security. security is very important thing in our life.

II. LITERATURE SURVEY

We found that there are many advantages of C4.5 algorithm for different attacks occurs in your dataset and C4.5 will detect the R2L and U2R attacks and neural network is using for detecting the DOS and Probe attacks and many more. In this we are using four algorithms. The first one is k-means clustering and the second steps is fuzzy logic third steps is SVM and the last and final step is C4.5. The advantages of all this algorithm is to detect the attacks from the datasets. After that it will compare it with the SVM and C4.5 classifiers to find out how many attacks are occurred in dataset while transferring the dataset from source to destination.

III. PROPOSED SYSTEM

To overcome the problem in previous intrusion detection system, so that we create the new intrusion detection systems we are using the four level in intrusion detection system, first we have to apply the k-means clustering then the second steps is to apply the fuzzy logic, after that third steps is SVM(support vector system) and finally we have apply the C4.5 algorithm.

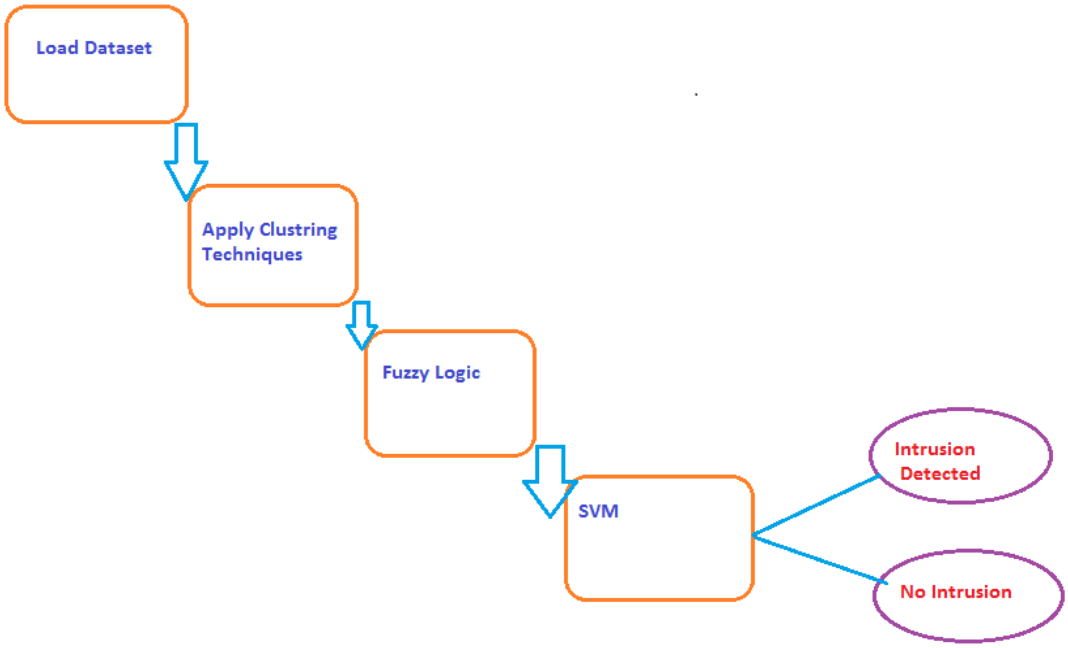
A. Advantages

In intrusion detection system, we can use large amount of dataset and this huge amount of dataset can handle by using mining technology

B. DIAGRAM

1) Process Model:

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)



IV. WORKING

A. System Requirement Specification

1) *Clustering Techniques:* In cluster techniques, we are using k-means clustering and fuzzy logic and SVM (support vector system) and C4.5.

2) *K-Means Clustering :* In k-means clustering, you have the set of objects and then you have to choose the centroid from the sets of objects. Then using that centroid you have to apply the distance matrix. After that iteration of the clusters are updated on the basis of optimization of objectives. K-means clustering is the one of the popular technique, which is used from long time, and it is very efficient and time saving technique. k-means clustering working is to separate the normal and malicious attacks and that acting like similarly in several partition that is known as k-th centroid.

3) *Fuzzy Logic:* In fuzyy logic there are multiple truth of degree to certain value to true or false and in Boolean algebra only two values are to choose that is 0 and 1. So that fuzzy can active in hardware, software, and on both. It is problem solving control structure so it will give for implementation in the system of multichannel PC.

4) *SVM (Support Vector System):* SVM (support vector system), this algorithm is used in the classification. And the classifiers are viewed in the rank of separating classes in feature space. Before we have to perform he svm we used the fuzzy logic output and using that output we perform the svm and the svm will detect all the attacks that are in the datasets and svm will separate that threats from the datasets.

V. FUNCTIONAL REQUIREMENTS

A. System Requirements

1) *Hardware Requirements:*

a)	System	:	Pentium IV 2.4 GHz.
b)	Hard Disk	:	40 GB.
c)	Floppy Drive	:	1.44 Mb.
d)	Monitor	:	15 VGA Colour.
e)	Mouse	:	Logitech.
f)	Ram	:	512 Mb.

B. Software Requirements

1) Operating system : Windows XP/7/8.

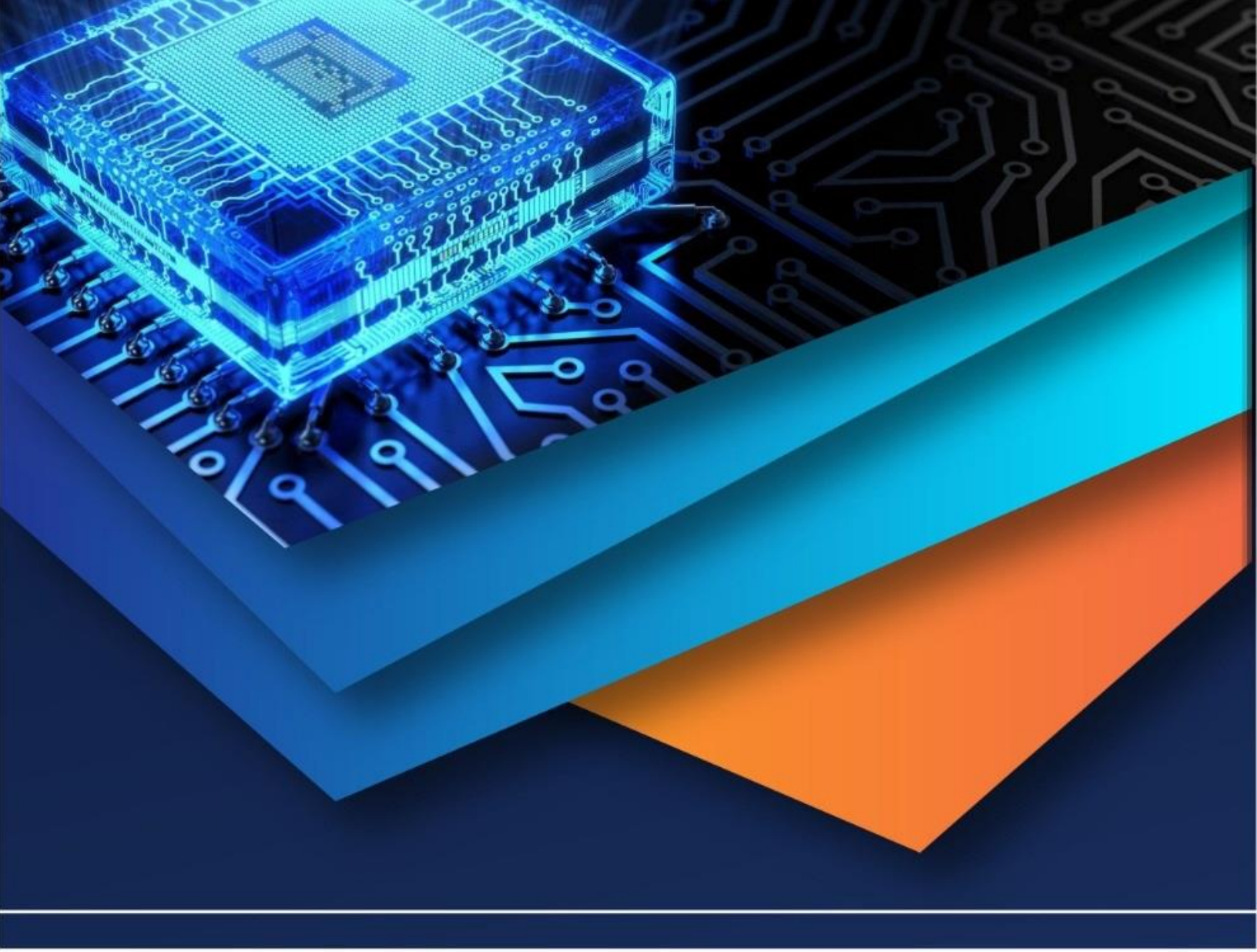
2) Programming Language : Java
3) Data Base : MYSQL/Oracle

VI. CONCLUSION

Protecting the data from attackers. intrusion detection system plays a important role in day to day life. IDS provides reliable and security effectively to the IDS users. IDS users are depends on IDS because IDS protecting their computers, data and networks. now a day intrusion detection creates the FP (false positive), FN (false negative), TP (true positive), TN (true negative). In this paper we present a algorithm of k-means clustering and fuzzy logic, svm , and c4.5 algorithm. It gives the effective protection to the datasets and it gives accuracy

REFERENCES

[1] Y. Li, J. Xia, S. Zhang, J. Yan, X. Ai, K. Dai, "Anefficient intrusion detection system based on support vector machines and gradually feature removal method", Expert Systems with Applications,2011,39: p. 424 430.
[2] M. Panda and M.R. Patra. 2007. Network intrusion detection using naive bayes. IJCSNS International Journal of Computer Science and Network Security, 7, 258-263.
[3] A.M. Chandrasekhar, "Intrusion Detection Technique By Using K-Means, Fuzzy Neural And Svm Classifier ",2013 International Conference on Computer Communication and Informatics (ICCCI - 2013), Jan 04-06, 2013 Coimbatore, India.
[4] Hesham Altwaijry, "Bayesian Based Intrusion Detection System ", Journal of King Saud University–Computer and Information Sciences (2012) 24,1–6.
[5] Ammar Boulaiche, "A Quantitative Approach For Intrusions Detection And Prevention Based On Statistical N-Gram Models ", Procedia Computer Science 10 (2012) 450 – 457.
[6] Muamer N.Mohammed, "Intrusion Detection System Based On Svm For Wlan ",Procedia Technology 1 (2012) 313 – 317.
[7] E.Biermann, E. Cloeteand L.M.Venter,"A comparison of intrusion detection Systems", Computer and Security, vol.20, pp.676-683, 2001.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY