International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-3, February 2013

Mingle Intrusion Detection System Using Fuzzy Logic

Prabhdeep Kaur, Sheveta Vashisht

Abstract-Intrusion detection system must be proficient of known and unknown vulner-abilities.In order to obtain superior accuracy an appropriate dataset should be there to detect the known and unknown attacks. In this research work new approach will be proposed which will utilize fuzzy if-then rules to detect known and unknown attacks i.e. sequential multilevel misuse along fuzzy if-then rules. In order to evaluate the performance of proposed algorithm and KDD'99 data set will be used. As fuzzy if-then rules comes up with overheads so overhead will be evaluated in this research work.

Keywords: KDD'99 dataset, Known and Unknown attacks, Misuse and Anomaly Detection.

I. INTRODUCTION

With the enlargement of technology in the computer networks, the necessitate of security is also grow. Computer security is Significant in almost any technology, Industry which operates on computer systems. Now a day's no any area is there where the security is not applied. Security is useful in the Banks, in Data mining, for cloud computing or other significant areas. So the One aspect is make use of data mining to get better security e.g. for intrusion detection. Data mining is widely used in business indemnity, banking, retail, science research astronomy, medication, and government security detection of criminals and terrorists which is the paramount equipment for finding the well-informed patterns.[11] Data Mining involves six widespread modules of responsibilities:

1) Anomalies and Attacks Detection.
2) Association and Combination Rules.
3) Clustering Task.
4) Classification principle.
5) Regression
6) Summarization

The effectuality of an Intrusion detection system is measured using its probability of giving a signal upon an intrusion i.e. attack detection rate and the ratio of false alarms in them. The great concern in relevance of data mining techniques for attack detection and identification purposes has been evaluated. The dilemma of attack detection can be reduced to a data mining task of classifying data. Precisely, given a set of data points belonging to dissimilar classes normal activity and attacks of different types one has to separate them as accurately as possible by means of a model. There are two different approaches used to recognize attacks-

Manuscript published on 30 February 2013.
* Correspondence Author (s)
Prabhdeep Kaur, Research Scholar, Done M.Sc (CS) from GNDU, Amritsar. Now doing M.Tech(CSE) from Lovely Professional University, Phagwara, Punjab, India,
Sheveta Vashisht, Assistant Professor in Department Of CSE, Lovely Professional University, Phagwara, Punjab, India.

1) Misuse detection
2) Anomaly Detection

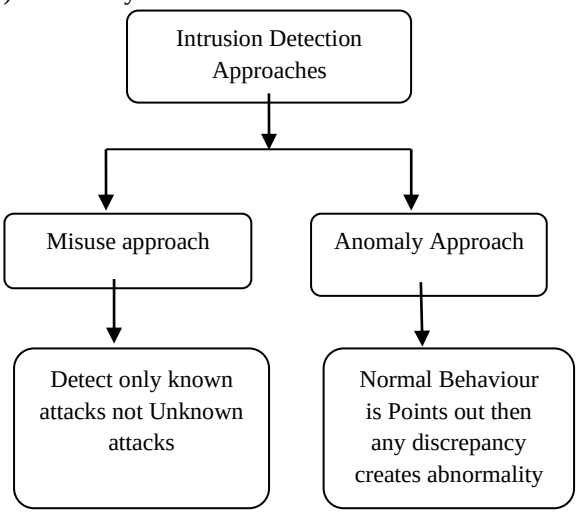

Fig. 1

Misuse detection where attacks are detected by means of their known signatures but do not detect the unknown attacks. In Anomaly detection, firstly normal system behaviour is created and any variation from that as defined profile marked as anomaly.
In this paper new approach will be proposed a sequential multilevel misuse detection model along fuzzy if-then rules for misuse attack known as well as unknown detection using data mining techniques based on decision tree.
Decision Tree for Misuse Detection Model and Anomaly Detection Model:

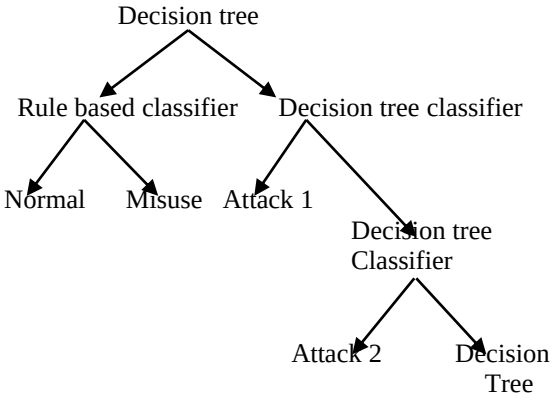

Fig. 2

A model with binary decision tree classifier at each level is proposed. This approach break up one attack at a time. This technique defines the exceptional features of one attack and at the similar time brings as regards the general features of rest of the other attacks which differentiate the rest from that

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

attack. So the proposed work also will be followed the decision tree criteria.

II. RELATED WORK

This section discusses the related works on IDS, Existing Pre-processing and Classifiers techniques applied on the IDS data. There are many research papers published regarding the pre-processing as well as classifiers in order to detect the intrusions in the dataset. The majority of them suffering with false positive type of errors while classifying the attacks and redundancy in the datasets. The following are the some of the related works suffering with low accuracy and false positive errors.

Mahbod Tavallaee *et.al* (2009) Anomaly detection has attracted the attention of many researchers to overcome the weakness of signature based IDSs in detecting novel attacks, and KDDCUP'99 is the mostly widely used dataset for the evolution of these systems. [1] Having conducted a statistical analysis on this data set, they found two important issues which highly affect the performance of evaluated system, and results in a very poor evaluation of anomaly detection approaches. To solve these issues, they proposed a new dataset, NSL-KDD, which consists of selected records of the complete KDD dataset and does not suffer from any of the mentioned shortcomings.

Lei, De-Zhan get *et.al* (2010) Network security is becoming an increasingly important issue, since the rapid Development of internet. Network intrusion detection systems, as the main security defending techniques, is widely used against such malicious attacks. [2] Data mining and machine learning technology has been extensively applied in network intrusion detection and prevention system by discovering user behaviour patterns from the network traffic data. Association rules and sequence rules are the main techniques of data mining for intrusion detection. Radhika Goel *et.al* (2012) in this paper a novel hybrid model is being proposed for Misuse and anomaly detection. C4.5 based binary decision trees are used for misuse and CBA based classifier is used for anomaly detection. Firstly, the C4.5 based decision tree separates the network traffic into normal and attack categories. The normal traffic is sent to anomaly detector and parallel attacks are sent to a decision trees based classifier for labelling with specific attack type. [3] The CBA based anomaly detection is a single level classifier where as the decision trees based misuse detector is a sequential multilevel classifier which labels one attack at a time in a step by step manner. Results show that 99.995% misuse detection rate with an anomaly detection rate of 99.298% is achievable. The overall attack detection rate is 99.911% and false alarm ratio of the integrated model is 3.229%. To overcome the deficiencies in KDD 99 dataset, a new improved dataset is also proposed. The overall accuracy of integrated model trained on new dataset is 97.495% compared to 97.24% of the old dataset. Kristopher Kendall (1999) the standard corpus was designed to evaluate both false alarm rates and detection rates of intrusion detection systems using many types of both known and new attacks embedded in a large amount of normal background traffic. [4] The focus of this thesis is the attacks that were developed for use in the 1998 DARPA intrusion detection evaluation. In all, over 300 attacks were included in the 9 weeks of data collected for the evaluation. These 300 attacks were drawn from 32 different attack types and 7 different attack scenarios. The attack types covered the different classes of computer attacks and included older, well-known attacks, newer attacks that have recently been released to publicly available forums, and some novel attacks developed specifically for this evaluation. Some attacks occur in a single session with all actions occurring in the clear, while others are broken up into several sessions spread out over a long period of time with the attacker taking deliberate steps to minimize the chances of detection by a human administrator or an intrusion detection system. Mrudula gudade *et.al* (2010) Since Many current intrusion detection systems are constructed by manual encoding of an expert knowledge, changes to them are expensive and slow.[5] In data mining based intrusion detection system, they propose new ensemble boosted decision tree approach for intrusion detection system. Experimental results shows better results for detecting intrusions as compared to others existing methods. Duanyang Zhao *et.al* (2012) A truly effective intrusion detection system will employ both technologies. They discusses the differences in host and network-based intrusion detection techniques to demonstrate how the two can work together to provide additionally effective intrusion detection and protection.[6] They propose a hybrid IDS, which combines network and host IDS, with anomaly and misuse detection mode, utilizes auditing programs to extract an extensive set of features that describe each network connection or host session, and applies data mining programs to learn rules that accurately capture the behaviour of intrusions and normal. K.Nageswara rao *et.al* (2012) it has become essential to evaluate machine learning techniques for web based intrusion detection on the KDD Cup 99 data set.[7] This data set has served well to identify attacks using data mining. Furthermore, selecting the relevant set of attributes for data classification is one of the most significant problems in designing a reliable classifier. Existing C4.5 decision tree technology has a problem in their learning phase to detect automatic relevant attribute selection, while some statistical classification algorithms require the feature subset to be selected in a preprocessing phase. Also, C4.5 algorithm needs strong preprocessing algorithm for numerical attributes in order to improve classifier accuracy in terms of Mean root square error. In this paper, evaluated the influence of attribute pre-selection using Statistical techniques on real-world kddcup99 data set. Experimental result shows that accuracy of the C4.5 classifier could be improved with the robust pre-selection approach when compare to traditional feature selection techniques.

III. PROPOSED WORK

Proposed work is designed as the techniques Sequential multilevel misuse detection along fuzzy if-then rules, which will detect the both attacks either known and unknown attacks. Also this technique uses the algorithm that is the Mingle intrusion detection system using fuzzy logic algorithm which is based on decision tree.

Mingle Intrusion detection system using fuzzy logic:

Proposed Algorithm introduces an original framework for as revealed in figure 3. for intrusion detection system. In this framework KDD'99 CUP dataset is prearranged as an input which includes sequential multilevel misuse detection along fuzzy if-then rules to identify known and unknown attacks.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

IV. DESCRIPTION OF PROPOSED ALGORITHM

KDD'99 has been the most widely used data set for the evaluations of anomaly detection methods. In the first step the KDD dataset will taken as an input. In the next step dataset be refined. The KDD attacks fall in one of the following four categories:

1) Denial of Service Attack (DoS): is an attack, in which the attacker makes several computing or memory resource too demanding or too bursting to handle legitimate requirements.
2) User to Root Attack (U2R): is a class of exploit in which the attacker starts out with right to use to a normal user account on the system, and is able to exploit some vulnerabilities to achieve root access to the system.
3) Remote to Local Attack (R2L): occurs when an attacker who has the capability to transmit packets to a machine over a network but who does not have an account on that machine exploits some vulnerability to achieve local access as a consumer of that machine.
4) Probing Attack: is an effort to gather information about a network of computers for the perceptible purpose of circumventing its security controls.

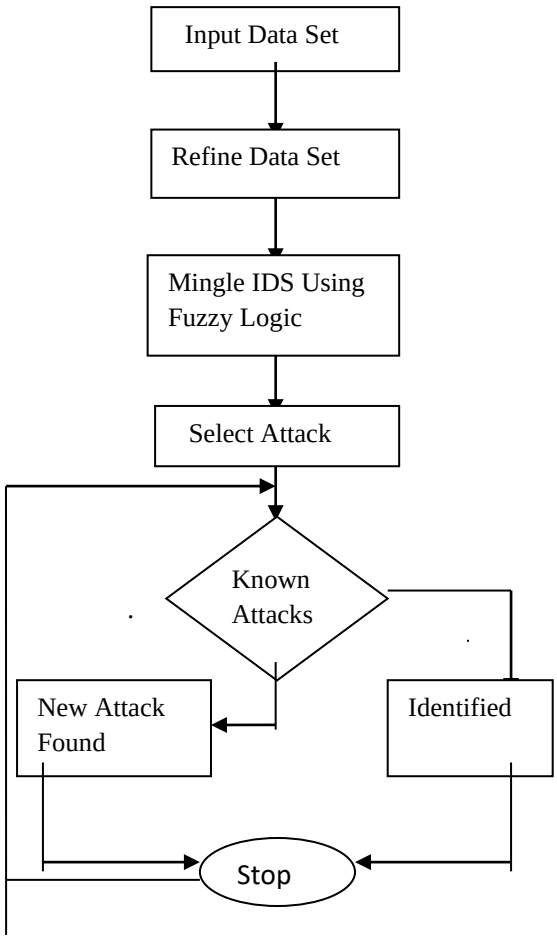

Fig 3.Flowchart

Fig 3. Proposed Algorithm for sequential multilevel misuse detection along fuzzy if-then rules.

Steps involved in Proposed Algorithm

1. First input dataset in string file not in binary file.
2. Fuzzy if-then Rules will be then come in action.
3. Categorization will be drawn either known and unknown attacks.
4. Now come for metrics which will be selected like.
   a. Time vs. No of lines in file.
   b. Degree of Different attacks.
   c. Unknown attacks Vs Known attacks.
   d. Unknown attacks Vs No of lines in file.
   e. Overheads of proposed technique in terms of time.

V. CONCLUSION AND FUTURE WORK

In this paper new technique for attack detection using fuzzy if-then Rules is proposed which is based on sequential multilevel Misuse and also proposed a new algorithm for identification of known and unknown attacks. Model's performance is evaluated on KDD'99 CUP dataset. So in future work it should be consider that how to remove the problems of detection of known and unknown attacks and implementation of new proposed technique and algorithm for detection of known and unknown attacks. The overall accuracy of the proposed model is which will be strong, increase as compared to the old model and the overheads will be evaluated.

REFERENCES

[1] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani "*A Detailed Analysis of the KDD CUP 99 Data Set proceeding on 2009"*
[2] Lei Li, De-Zhang Yang, Fang-Cheng Shen," *A Novel Rule-based Intrusion detection System Using Data Mining* "international conference 2010.
[3] Radhika Goel, Anjali Sardana, and Ramesh C. Joshi" *Parallel Misuse and Anomaly Detection Model*" *International Journal of Network Security, Vol.14, No.4, PP.211-222, July 2012*
[4] K. Kendall "*A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems*, M. Eng.Thesis" Massachusetts Institute of Technology, Massachusetts, United States, June 1999.
[5] Mrudula Gudadhe, Prakash Prasad" *A New Data Mining Based Network Intrusion Detection Model"* International conference on computer and communication technology, |ICCCT'10|
[6] Duanyang Zhao," *Analysis of an intrusion detection system"*" in second international conference on security and management 2012(3):127-13ISSN.
[7] K.Nageswara Rao, D.Rajya Lakshmi, T.Venkateswara Rao" *Robust Statistical Outlier based Feature Selection Technique for Network Intrusion Detection"* International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012
[8] A.A.Olusola, A.S.Oladele and D.O.Abosede, *"Analysis of KDD '99 Intrusion Detection Dataset for Selection of Relevance Features".* Proceedings of the World Engineering and Computer Science, vol. 1, Oct-2010.
[9] Vipin Das, Vijaya Pathak" *Network intrusion detection system on machine learning algorithm* "International Journal of Computer Science & Information Technology (IJCSIT), Vol 2, No 6, December 2010.
[10] A. S. Ashoor and S. Gore, "*Importance of Intrusion Detection system (IDS)".* International Journal of Scientific and Engineering Research, vol. 2, no. 1, pp.1-4 Jan-2011.
[11] http://www.britannica.com/EBchecked/topic/10 56150/data-mining.

Prabhdeep Kaur, Research Scholar , Done M.Sc (CS) from GNDU, Amritsar. Now doing M.Tech(CSE) from Lovely Professional University, Phagwara, Punjab, India, Research area is Security in Data Mining.

Sheveta Vashisht, Assistant Professor in Department Of CSE, Lovely Professional University, Phagwara, Punjab, India, have done BTech, M.Tech from lovely professional university, Research area is Networking, Security, Data Mining,.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)