Intrusion Detection System using fuzzy clustering algorithm

[1]Bhujbal Harishchandra J., [2] Shinde Nandkumar P.[3] Walkunde Kiran B.

Student
Computer, GCOEARA, Pune, India
[1]hari.bhujbal007@gmail.com, [2]shindenandu499@gmail.com, [3]kwalkunde@gmail.com

***Abstract*- Nowadays Intrusion Detection System (IDS) which is increasingly a key element of system security is used to identify the malicious activities in a computer system and network. There are different approaches being employed in intrusion detection systems, but unluckily each of the technique so far is not entirely ideal. The prediction process may produce false alarms in many anomaly based intrusion detection systems. To achieve that, this paper proposes IDS model based on Fuzzy Logic. Proposed model consists of three parts Client side model which include simple bank application, IDS model in which previously defined testing set and training set are defined with fuzzy algorithm,apriori algorithm and Admin model which are define some rule for user and show system result. Also IDS model contain Artificial Neural Network algorithm which is useful for self intrusion detection system.**

Keywords: Intrusion detection, self Intrusion Detection System, Fuzzy algorithm, Artificial neural network.

I. INTRODUCTION

Intrusion detection is a critical component in securing information systems. Traditional methods for intrusion detection are based on extensive knowledge of signatures of known attacks Monitored events are matched against the signatures to detect intrusions. These methods extract features from various audit streams, and detect intrusions by comparing the feature values to a set of attack signatures provided by human experts. The signature database has to be manually revised for each new type of intrusion that is discovered. A significant limitation of signature-based methods is that they cannot detect emerging cyber threats, since by their very nature these threats are launched using previously unknown attacks. In addition, even if a new attack is discovered and its signature developed, often there is a substantial latency in its deployment across networks. To overcome this manually update database we discover self detection and updating technique by using artificial neural network algorithm. Intrusion Detection System, can detect, prevent and react to the attacks. Intrusion Detection has become an integral part of the information security process. But, it is not technically feasible to build a system with no vulnerabilities; as such intrusion detection continues to be an important area of research.

The remaining part of this paper is organized as follows: Section 2 gives an overview of current Intrusion Detection Systems and also about the usage of fuzzy and apriori algorithm in Section 3 explains the overview of our proposed architecture. Section 4 briefs about the Trace back framework and Section 5 summarizes the work and points out what we will be doing in future.

II. LITERATURE SURVEY

A. Existing System

An intrusion is defined as any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource. An Intrusion Detection System (IDS) monitors and restricts user access to the computer system by applying certain rules. These rules are based on expert knowledge extracted from skilled administrators, who construct attack scenarios and apply them to find system exploits. The system identifies all intrusions by users and takes or recommends necessary action to stop an attack on the database. Two approaches to intrusion detection are currently used. The first one, called misuse detection, is based on attack signatures, i.e., on a detailed description of the sequence of actions performed by the attacker. This approach allows the detection of intrusions matching perfectly the signatures, so that new attacks performed by slight modification of known attacks cannot be detected. The second approach is based on statistical knowledge about the normal activity of the computer system, i.e., a statistical profile of what constitutes the legitimate traffic in the network. In this case, intrusions correspond to anomalous network activity, i.e. to traffic whose statistical profile deviates significantly from the normal one.

B. Proposed System

To overcome this drawback we are developing new model of Intrusion Detection System which has capacity of self detecting or updating attacks. In proposed IDS model we are develop Artificial Neural Network algorithm with fuzzy logic to detect and update database for newly attacks. in proposed model we define two separate set of data. 1] Training set 2] Testing set. In training set every user query checked using apriori algorithm and fuzzy algorithm .In training set we use apriori, artificial neural network, clustering algorithm for train the user query and database. In testing set we compare every user query with exiting database. We use KDD CUP dataset as exiting database which is developed in 1999 by Sun Microsystems computers.

III. AIMS AND OBJECTIVE

Main aim of developing this model is self detecting and updating database without admin interface.

1. To provide the better prevention against intrusion.
2. To overcome the difficulties found in the signature based systems.
3. It can also support us to analyses the network traffics.
4. Identifying problems with security policies.
5. Documenting existing threats.

IV. MODULAR APPROCH

A variety of attacks incorporated in the dataset fall into following four major categories:1] Denial of Service Attacks (DOS): A denial of service attack is an attack where the attacker constructs some computing or memory resource fully occupied or unavailable to manage legitimate requirements, or reject legitimate users right to use a machine. 2]User to Root Attacks(U2R): User to Root exploits are a category of exploits where the attacker initiate by accessing a normal user account on the system (possibly achieved by tracking down the passwords, a dictionary attack, or social engineering) and take advantage of some susceptibility to achieve root access to the system.3] Remote to User Attacks (R2L): A Remote to User attack takes place when an attacker who has the capability to send packets to a machine over a network but does not have an account on that machine, makes use of some vulnerability to achieve local access as a user of that machine. 4]Probes (PRB): Probing is a category of attacks where an attacker examines a network to collect information or discover well-known vulnerabilities. These network investigations are reasonably valuable for an attacker who is staging an attack in future. An attacker who has a record, of which machines and services are accessible on a given network, can make use of this information to look for fragile points.

V. IMPLEMENTATION

We are developing a banking application. Using this client send their queries to server and each of the query is inspected at the server through IDS . In IDM we using two algorithm mainly 1] apriori algorithm 2]fuzzy clustering algorithm. admin define some rule foe user and checked client system. get result about attack.
Implementing flow show in following diagram:-

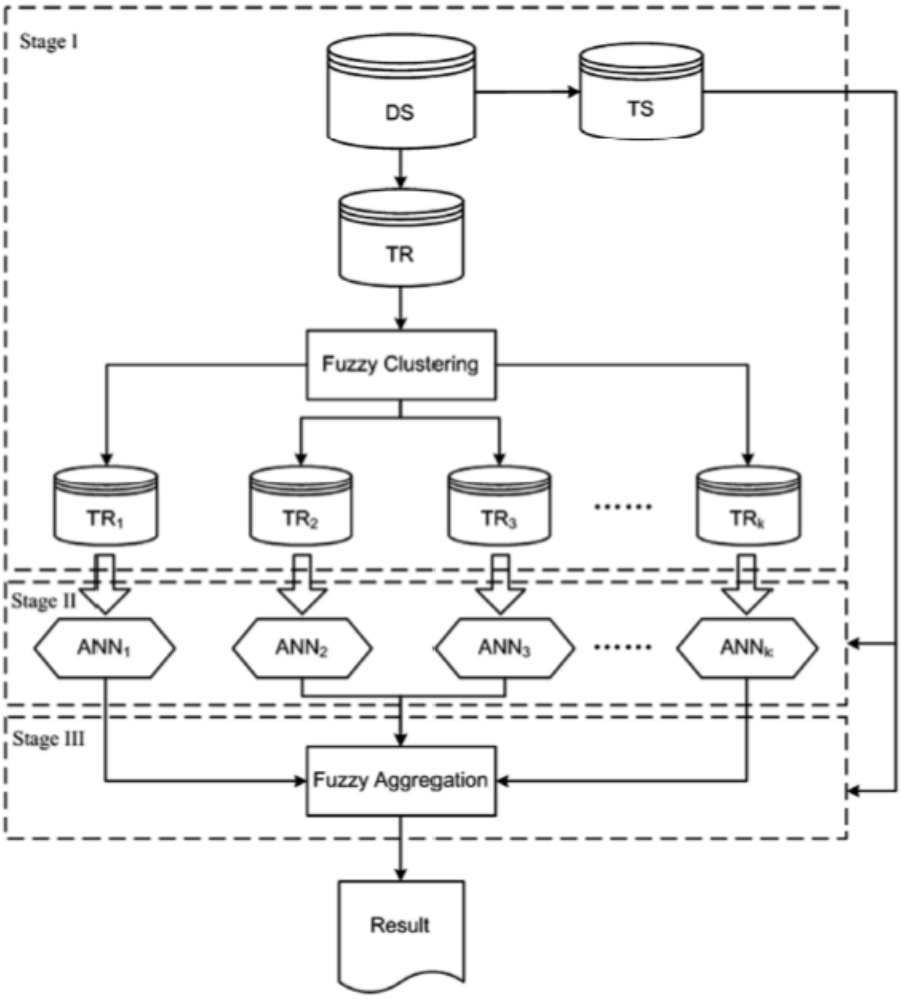

Fig: 1 Framework of FC-ANN for IDS

VI. ALGORITHMS USED

There are several algorithms used as follows,

1. ***Apriori algorithm***
   It is the algorithm for the frequent item set mining and association rule learning over transactional database. It proceeds by identifying the frequent individual item in database and extending them to larger and larger item set as long as those items sets appear sufficiently often in the database.
2. ***Fuzzy clustering algorithm***
   Fuzzy is in between state of 0 and 1.using fuzzy algorithm we can guess one maximum probability condition. that condition can be compare with another logic and checked with result.

VII. CONCLUSION

In this paper, we focused on intrusion detection in computer networks by combination of fuzzy systems and artificial neural network algorithm. The proposed method performs the classification task and extracts required knowledge using fuzzy rule based systems which consists of fuzzy if-then rules. The proposed system has two main features of data mining techniques which are high reliability and adequate interpretability, and is comparable with several well-known algorithms. Results on intrusion detection data set from KDD cup-99 repository show that the proposed approach would be capable of classifying intrusion instances with high accuracy rate in addition to adequate interpretability of extracted rules.

REFERENCES

[1] Infort technology pvt Ltd pune.
[2] Global Journal of Computer Science and Technology Neural & Artificial Intelligence Volume 12 Issue 11 Version 1.0 Year 2012 Global Journals Inc. (USA)
[3] Yager RR, Zadeh LA. Fuzzy Sets, Neural Networks, and Soft Computing. New York: Van Nostrand Reinhold, 1994.