ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

Various Approaches for Intrusion Detection System: An Overview

Priya U. Kadam[1], Prof.Manjusha Deshmukh[2].

PG Student, Department of Computer Engineering, Mumbai, MH, India[1].

Assistant Professor, Department of Computer Engineering, Mumbai, MH, India[2].

ABSTRACT: Nowadays it is very important to maintain a high level security to ensure safe and trusted announcement of information between various organizations. But secured data communication over internet and any other network is always under threat of intrusions and misuses. So Intrusion Detection Systems have become a needful component in terms of computer and network security. There are various approaches being utilized in intrusion detections, but unfortunately any of the systems so far is not completely flawless. So, the quest of betterment continues. In this progression, here we present an Intrusion Detection System (IDS) various approaches to efficiently detect various types of network intrusions. Parameters and evolution processes for IDS are discussed in details and implemented. This approach uses evolution theory to information evolution in order to filter the traffic data and thus reduce the complexity. To implement and measure the performance of our system we used the Real time benchmark dataset and obtained reasonable detection rate.

I. INTRODUCTION

In 1987 Dorothy E. Denning proposed intrusion detection as is an approach to counter the computer and networking attacks and misuses. Intrusion detection is implemented by an intrusion detection system and today there are many commercial intrusion detection systems available.

Generally an intruder is defined as a system, program or person who tries to and may become successful to break into an information system or perform an action not legally allowed. We refer intrusion as any set of actions that attempt to compromise the integrity, confidentiality, or availability of a computer resource. The act of detecting actions that attempt to compromise the integrity, confidentiality, or availability of a computer resource can be referred as intrusion detection. An intrusion detection system is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.

Basic concepts of IDS:

The below sections give a short overview of networking attacks, classifications and variouscomponents of Intrusion Detection System.

Networking Attacks: This section is an overview of the four major categories of networking attacks. Every attack on a network can comfortably be placed into one of these groupings.

Denial of Service (DoS): A DoS attack is a type of attack in which the hacker makes a computing or memory resources too busy or too full to serve legitimate networking requests and hence denying users access to a machine e.g. apache, smurf, neptune, ping of death, back, mail bomb, UDP storm etc. are all DoS attacks.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

Remote to User Attacks (R2L): A remote to user attack is an attack in which a user sends packets to a machine over the internet, which s/he does not have access to in order to expose the machines vulnerabilities and exploit privileges which a local user would have on the computer e.g. xlock, guest, xnsnoop, phf, sendmail dictionary etc.

User to Root Attacks (U2R): These attacks are exploitations in which the hacker starts off on the system with a normal user account and attempts to abuse vulnerabilities in the system in order to gain super user privileges e.g. perl, xterm.

Probing: Probing is an attack in which the hacker scans a machine or a networking device in order to determine weaknesses or vulnerabilities that may later be exploited so as to compromise the system. This technique is commonly used in data mining e.g. saint, portsweep, mscan, nmap etc.

Classification of Intrusion Detection:
Intrusions Detection can be classified into two main categories. They are as follow:

Host Based Intrusion Detection: HIDSs evaluate information found on a single or multiple host systems, including contents of operating systems, system and application files.

Network Based Intrusion Detection:
NIDSs evaluate information captured from Network communications, analyzing the stream of packets which travel across the network.

Components of Intrusion Detection System:

An intrusion detection system normally consists of three functional components. The first component of an intrusion detection system, also known as the event generator, is a data source. Data sources can be categorized into four categories namely Host-based monitors, Network-based monitors, Application-based monitors and Target-based monitors.The second component of an intrusion detection system is known as the analysis engine. This component takes information from the data source and examines the data for symptoms of attacks or other policy violations. The analysis engine can use one or both of the following analysis approaches:

Misuse/Signature-Based Detection: This type of detection engine detects intrusions that follow well-known patterns of attacks (or signatures) that exploit known software vulnerabilities. The main limitation of this approach is that it only looks for the known weaknesses and may not care about detecting unknown future intrusions.

Anomaly/Statistical Detection: An anomaly based detection engine will search for something rare or unusual. They analyses system event streams, using statistical techniques to find patterns of activity that appear to be abnormal. The primary disadvantages of this system are that they are highly expensive and they can recognize an intrusive behavior as normal behavior because of insufficient data.

The third component of an intrusion detection system is the response manager. In basic terms, the response manager will only act when inaccuracies (possible intrusion attacks) are found on the system, by informing someone or something in the form of a response.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

Architecture of IDS

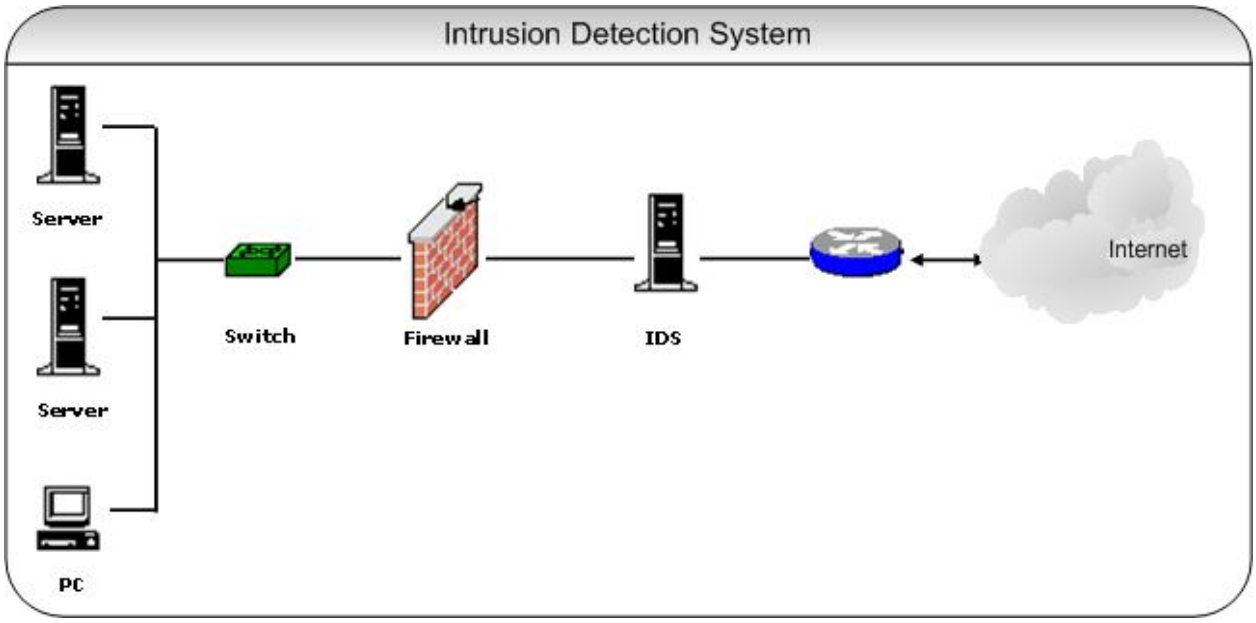


Figure1:Architecture of Intrusion detection System

II. LITERATURE REVIEW

Several Genetic Algorithms (GAs) and Genetic Programming (GP) has been used for detecting intrusion detection of different kinds in different scenarios. Some uses GA for deriving classification rules. GAs used to select required features and to determine the optimal and minimal parameters of some core functions in which different AI methods were used to derive acquisition of rules. There are several papers related to IDS which has certain level of impact in network security.

Wenke Lee[6] described a method using data mining to address three types of issues:accuracy,efficiency and usability,also implemented feature extraction and construction algorithms for labeled audit data and algorithms for unlabeled data.

Wei Li[7] described a method using GA to detect anomalous network intrusion. The approach includes both quantitative and categorical features of network data for deriving classification rules. However, the inclusion of quantitative feature can increase detection rate but no experimental results are available.

P.Jongsuebsuk[8] proposed a fuzzy genetic algorithm for real time intrusion detection system to classify behavior of intrusion and network attack data also evaluated intrusion detection system in terms of detection rate,detection speed and false alarm rate.

Tao Peng, WanliZuo [9] presents adata mining-based network intrusion detection framework in realtime (NIDS). This framework is a distributed architectureconsisting of sensor, data preprocessor, extractors of features anddetectors. To improve efficiency, our approach adopts a novelFP-tree structure and FP-growth mining method to extractfeatures based on FP-tree without candidate generation.FP-growth is just accord with the system of real-time andupdating data frequently as NIDS. Heemploy DARPA intrusiondetection evaluation data set to train and test the feasibility of his proposed method. Experimental results show that thePerformance is efficient and satisfactory level.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

RistoVaarandi [10] propose a data miningbased real-time technique for distinguishing importantnetwork IDS alerts from frequently occurring falsepositives and events of low importance. Unlikeconventional data mining based approaches, ourmethod is fully automated and able to adjust toenvironment changes without a human intervention.

Sr. No.	Title of the paper	Author and year of publication	Observations/Remarks
1	Data Mining for Network Intrusion Detection System in Real Time	Tao Peng, WanliZuo IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.2B, February 2006[6].	In this paper,outlined and implemented the architecture of the data mining-based network intrusion detection system in real-time (NIDS). analyze a frequent patterns mining algorithm that integrate Apriori candidate generation into FP-growth method.Experimentson DARPA show the performance of the NIDS is satisfied.
2	Real-time Classification of IDS Alerts with Data Mining Techniques	RistoVaarandi 2009 IEEE MILCOM Conference. [7]	In this paper, they have presented a novel datamining based IDS alert classification method.Although given approach's preliminary results are promising, one issue remains open major changes in the arrivalrate of routine alerts might be symptoms of largescale attacks, but are hard to detect.
3	Real Time Data Mining-based Intrusion Detection	WenkeLee, Salvatore J. Stolfo and Philip K. ChanIEEE 2010[8]	In this paper successfully completed a prototype implementation of a data mining and CIDF (Common Intrusion Detection Framework CIDF, funded by DARPA) based IDS. There can be several (or multiple layers of) detectors monitoring the same system. For example, workloads can be distributed to different detectors to analyze events in parallel
4	Real Time Intrusion Detection System Using Genetic Algorithm	Wei Li IEEE Transaction on parallel and distributed system, vol.23,no.3,Marach 2012[9]	Wei Li describe the using genetic algorithm for intrusion detection system different detection techniques.He is also working on TCP/IP layer for detection.The proposed system is genetic algorithm rule base system which including crossover, mutation, fitness and selection process and finally generate the rules for test data.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

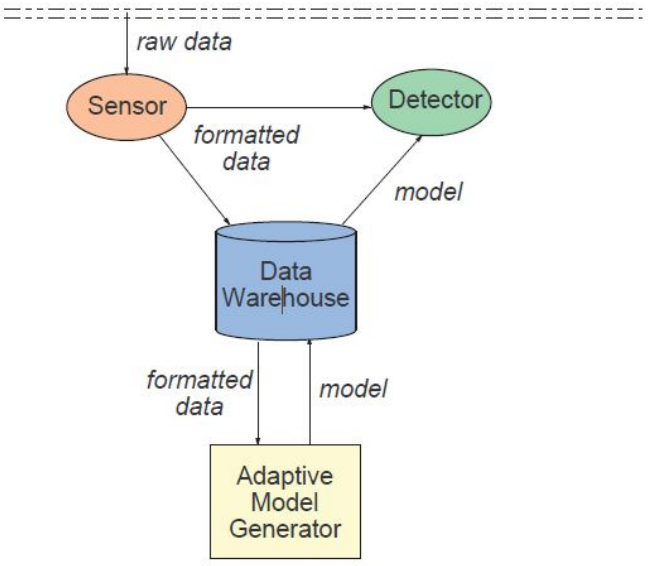
5	Real-Time Intrusion Detection with Fuzzy Genetic Algorithm	P. Jongsuebsuk and N. attanapongsakorn. IEEE 2013[10]	This paper describe, Fuzzy rule is a machine learning algorithm that can classify network attack data, while a genetic algorithm is an optimization algorithm that can help finding appropriate fuzzy rule and give the best/optimal solution. Given experimental results show that our fuzzy GA can efficiently detect online network dataset within 2-3 seconds

Table 1: Summary of Literature Survey

III. VARIOUS APPROACHES OF IDS

- Wenke Lee, Salvatore J. Stolfo and Philip K. Chan[6] described research in real time data mining-based intrusion detection system. They implemented the system for feature extraction and construction algorithms for labeled audit data.In this paper successfully completed a prototype implementation of a data mining and CIDF (Common Intrusion Detection Framework CIDF, funded by DARPA) based IDS.There can be several (or multiple layers of) detectors monitoring the same system. For example, workloads can be distributed to different detectors to analyze events in parallel. Below is the architecture of given syste.

System Architecture



The Architecture of Data Mining-based IDS

Figure 2: Architecture Data Mining base IDS

Algorithm

- **Level 1** features can be computed from the first packet, e.g., the service.
- **Level 2** features can be computed at any point during the life of the connection, e.g., the connection state (SYN WAIT, CONNECTED, FIN WAIT, etc.).
- **Level 3** features can be computed at the end of the connection, sing only information about the connection being examined, e.g., the total number of bytes sent from source to destination.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

- **Level 4** features can be computed at the end of the connection, but require access to data of potentially many other prior connections. These are the temporal and statistical features and are the most costly to compute.

- if $(H_1(\mathbf{x}) = normal) \vee (H_1(\mathbf{x}) = anomaly)$ then
  - if $H_2(\mathbf{x}) = normal$ then $output \leftarrow H_1(\mathbf{x})$ ($normal$ or $anomaly$)
  - else $output \leftarrow new\_intrusion$
- else $output \leftarrow H_1(\mathbf{x})$

Ensemble-based Adaptive Learning Configuration

Figure 3: Rule creation Data Mining base IDS

- Wei Li[7] describe the using genetic algorithm for intrusion detection system different detection techniques. He is also working on TCP/IP layer for detection.He also working on TCP/IP layer for detection.In the proposed system is genetic algorithm rule base system which including crossover, mutation, fitness and selection process and finally generate the rules for test data.

System Architecture

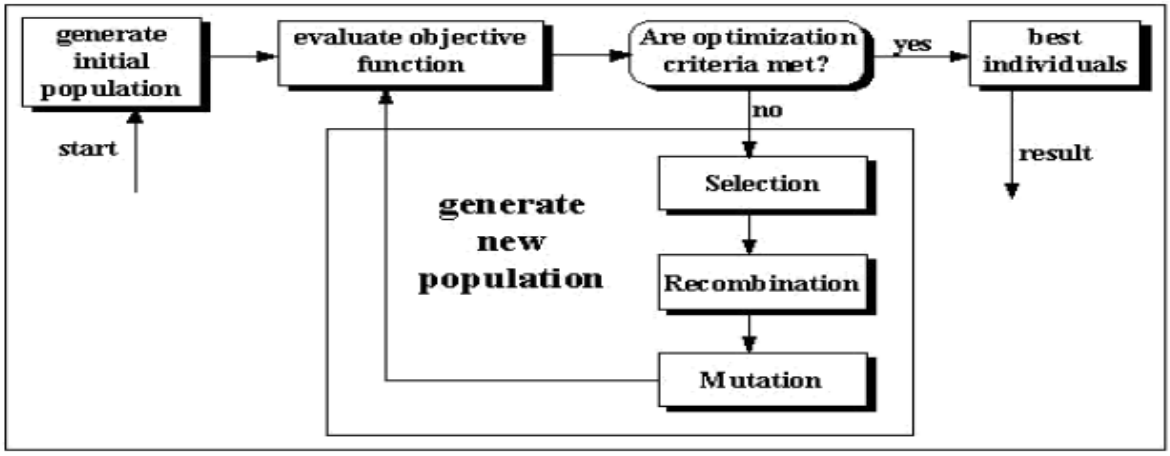


Figure 4: System Architecture of IDS using Genetic Algorithm.

Algorithm

Algorithm: Initialize chromosomes for comparison
Input: Network audit data (for training)
Output: A set of chromosomes
1. Range = 0.125
2. for each training data
3. If it has neighboring chromosome within Range
4. Merge it with the nearest chromosome
5. Else
6. Create new chromosome with it
7. End if
8. End for

Algorithm2: Predict data/intrusion type (using GA)
Input: Network audit data (for testing), Recalculated set of chromosomes
Output: Type of data.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

1. Initialize the population
2. Crossover Rate = 0.15, MutationRate = 0.35
3. While number of generation is not reached
4. For each chromosome in the population
5. For each recalculated chromosome
6. Find fitness
7. End for
8. Assign optimal fitness as the fitness of that chromosome
9. End for
10. Remove some chromosomes with worse fitness
11. Apply crossover to the selected pair of chromosomes of the population
12. Apply mutation to each chromosome of the population
13. End while

- P. Jongsuebsuk and N. attanapongsakorn. IEEE 2013[8] proposed a fuzzy genetic algorithm for real time intrusion detection system to classify behavior of intrusion and network attack data, while a genetic algorithm is an optimization algorithm that can help finding appropriate fuzzy rule and give the best/optimal solution. Given experimental results show that our fuzzy GA can efficiently detect online network dataset within 2-3 seconds. Where 2 seconds belong to the preprocessing time and less than a second for the detection time, while it takes only a fraction of a second to detect attacks in the KDD99 dataset.In given approach having two experimental results first fuzzy algorithm classify the attack on online dataset and KDD dataset with high accuracy and false alarm rate, while second experiments illustrated detection rate of each attack

System Architecture

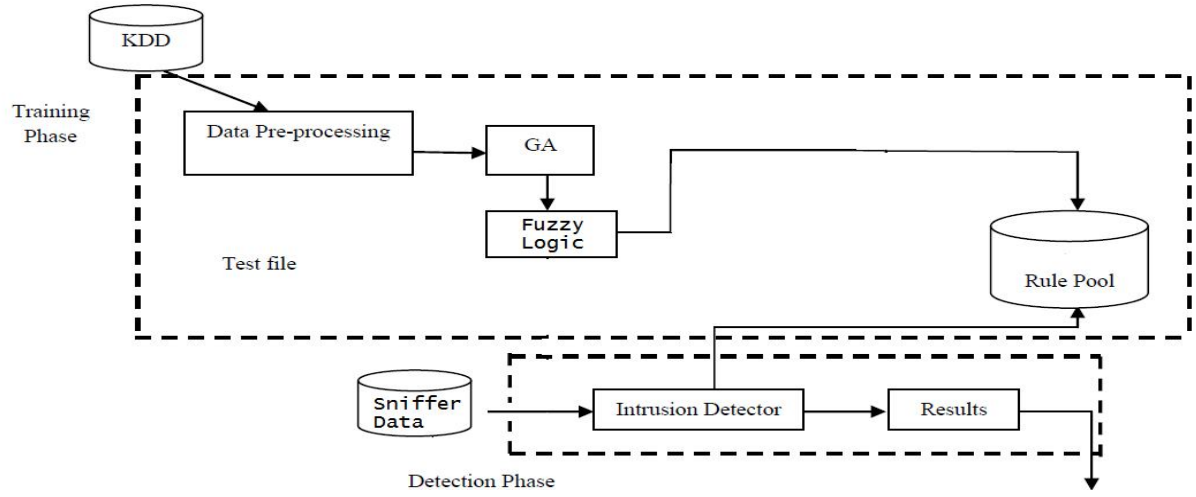


Figure 5: System architecture of Fuzzy Genetic Algorithm for Real Time IDS

Algorithm

Fuzzy Genetic

For each record {for each rule {for each attribute {prob = fuzzy ();totalprob = totalprob + prob;}
If (totalprob> threshold) {class is attack;true negative ++ ;}
Else{class is normal;true positive++ ;}

Fuzzy Algorithm

- *if (data value is between "b" to "c"))*
- *then prob =0.0*
- *else if (data value between "a" to "b")*
- *then prob =attribute_ value- a/b-c*

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

- *else if (data value between "c" to "d")*
- *then prob =d- attribute_value/d-c*
- *else then prob = 1.0*

Paper Title	Advantages	Disadvantages
Real Time Data Mining-based Intrusion Detection	With the help of CIDF will get drastic supervision for detection.They are working on sensor base network audit data so its very efficient to provide security to real time network systems.	It will be very lengthy process implementing for CIDF framework. They have use data mining approach and clustering approaches so it will generate maximum probable solution and hard to detect actual attacks.They have not focused on how to actually detect a sensor base attacks so, we they don't have any figures on final detection rates
Real Time Intrusion Detection System Using Genetic Algorithm	It eliminates the need for an attack to be previously known to be detected because malicious behavior is different from normal behavior by nature.Using a generalized behavioral model is theoretically more accurate, efficient and easier to maintain than a fingerprinting system.It uses a constant amount of computer resources per user, drastically reducing the possibility of depleting available resources.	They are rules dependent .If the behavior of the packets flowing in the network is new, then the system cannot take any decision. So they purely work in the basis of the initial rules provided.It cannot create its own rule depending on the current situation.It requires manual energy to monitor the Inflowing packets and analyze their behavior.Very poor detection rates for U2R and R2L.
Real-Time Intrusion Detection with Fuzzy Genetic Algorithm	Having a good detection rate rather than all existing systems.Minimum false alarm rate and false negative ratio.Working for both datasets KDDCUP 99 as well online dataset.	There is no optimal solution for threshold so sometime it will affect on actual detection rate.They have not classified overall detection rate for all attacks.

Table 2: Analysis for IDS

.

IV. CONCLUSION

We studiedvarious existing systems and examine the experimental results. All experimental results showsthat given approaches can efficiently detect online network attackrapidly. Finally we got detail ideas of IDS and IDS terminology as well as different attack types and DARPA dataset.

V. FUTURE WORK

After completion of whole review we conclude that we can develop this system on real time sniffer dataset as well as on KDD CUP 99 DARPA dataset. For further research we can also develop parallel Genetic approach for IDS system.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

REFERENCES

[1]BiswajitPanja, OlugbengaOgunyanwo, PriyankaMeharia "Training of Intelligent Intrusion Detection System using Neuro Fuzzy" 2014 IEEE SNPD 2014, June 30-July 2, 2014, Las Vegas, USA
[2] HachmiFatma, Limam Mohamed "A two-stage technique to improve intrusion detection systems based on data mining algorithms" 978-1-4673-5814-9/13/$31.00 ©2013 IEEE
[3] SaeedKhazaee, Maryam Sharifi Rad "Using fuzzy c-means algorithm for improving intrusion detection performance" 2013 13th Iranian Conference on Fuzzy Systems (IFSC) 978-1-4799-1228-5/13/$31.00 ©2013 IEEE.
[4] Manish Kumar, Dr. M. Hanumanthappa " Intrusion Detection System using Stream Data Mining and Drift Detection Method" IEEE - 31661 July 4 - 6, 2013, Tiruchengode, India
[5] Ling Zhang1 ,Zhongying Bai1, Shoushan Luo1, Guanning Cui1, Xing Li1 "A DYNAMIC ARTIFICIAL IMMUNE-BASED INTRUSION DETECTION METHOD USING ROUGH AND FUZZY SET"
[6] P. Jongsuebsuk, N. Wattanapongsakorn, C. Charnsripinyo "Real-Time Intrusion Detection with Fuzzy Genetic Algorithm" 978-1-4799-0545-4/13/$31.00 2013 IEEE
[7] Wei Li "Real Time Intrusion Detection System Using Genetic Algorithm" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 3, MARCH 2012
[8]Wenke Lee, Salvatore J. Stolfo_, Philip K. Chan_ "Real Time Data Mining-based Intrusion Detection" Computer Science Department,North Carolina State University,Raleigh,NC,27695
[9]RistoVaarandi "Real-time Classification of IDS Alerts with Data Mining Techniques" Reprinted from *Proceedings of the 2009 IEEE MILCOM Conference*.
[10] Tao Peng, WanliZuo "Data Mining for Network Intrusion Detection System in RealTime" IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.2B, February 2006