Intrusion Prevention Against Distributed Denial-of-Service(DDoS) on the cloud

Vanitha.R
M.tech Student(CSE),SRM University, Ramapuram,Chennai.

Abstract
Cloud computing means delivery of computing resources over the internet. Cloud users can install vulnerable software to virtual machine which leads to violate the security of cloud. Many possible attacks in cloud, the major one is Distributed Denial–of-service (DDoS).In general this attack happens at the earlier stage of actions and compromise the virtual machine. To prevent vulnerable virtual machine from being compromised in the cloud intrusion detection and prevention systems are used. They identifies possible attacks and stop their occurrence. Cloud provide the potential to diminish DDoS attack by counter the attack and employ the idle resources of the cloud. The Distributed intrusion detection system for virtual environment proposed and implemented by chung et al. work for small scale environment and leads to lack of scalability. In this paper a framework developed based on genetic algorithm and KDD dataset are proposed to perform better in terms of reducing false positive rate and cost compares to other approaches.

Keywords
Cloud computing, Compromised virtual machine, Distributed Denial of Service, Intrusion prevention, NSL-KDD dataset, genetic algorithm

1. Introduction

Cloud computing

Cloud computing provide as to access the application over the internet. The application may be e-mail, web conference etc., Cloud means internet or network or something present at remote location.It refers to manipulate, configure, and access the application through the online. The cloud model composed by three service model, four deployment model and five characteristics. The characteristics are broad network access, rapid elasticity, resource pooling, on-demand self service and measured service. The services to be offered on private network is called broad network access. Pooled resources means that customers can take up computing resources from pool. Services scaled smaller or larger called elasticity .On demand self-service means user can manage their computing resources.

Service models are classified as
1. Software as a service (SaaS)
2. Platform as a service (Past)
3. Infrastructure as a Service (IaaS)

In SaaS application provided with operating system, network, software and hardware. Padas provides only network and hardware, the user can install their own application and software. In IaaS network and hardware are provided. Deployment model includes four types of cloud services. They are private, public, community and hybrid. Public cloud offered over the internet, whereas private cloud is used and managed by specific organization. Community cloud shared by several organization. The combination of different methods are called hybrid cloud.

Cloud services are popular because of their low cost and complexity network. The security and privacy of personnel content is a major issue in cloud computing. It is always risk when handover the reliable information to cloud provides. Another issue is lock-in, that is switching from one cloud service provides to another is difficult. Virtualization is one of the technique that works behind the cloud to make it flexible, reliable and usable. It allows sharing of resource to multiple organization. The cloud users have a control over the software installed on their virtual machine.

DISTRIBUTED DENIAL-OF-SERVICE(DDOS)

Distributed Denial-of-Service is to make the computing resource try to stop responding legitimate user. There are different types of DDos attack that target the network components like router, firewall, ISP in different ways. A DoS attack commonly consists of efforts to indefinitely or temporarily suspend or interrupt services of a host connected on the Internet. Distributed denial-of-service attacks are send by multiple people or systems,whereas denial -of-service attacks are send by single system. In general DDoS attacks target sites or services hosted on webservers such as banks, root nameservers and credit card payment gateways.

The Distributed denial-of-service has the following symptoms;

- Slow down the network performance
- To make a website unavailable to intended user.
- The no of spam mails will be increased.
- Failure to access any web site

Manuscript received April 5, 2016
Manuscript revised April 20, 2016

- Disconnect a wireless or wired internet connection
- Long time denial of access to the internet or any web services

Basically DDoS attack occurs at three layers of OSI model. Layer 3 & 7 are common attack detected and blocked easily. But layer 4 is difficult to find and the experts should monitor and analyze the attack to prevent.

The attack at layer 3&7 is called infrastructure DDoS and attack at layer 4 is called Application DDoS attack. The infrastructure attack sends the no.of request to damage bandwidth capacity of system. Application attack reduce the performance of system by attacking specific application. Infrastructure attacks are TCP synchronization flooding attack, reflection attack, UDP flooding attack, ICMP flooding attack. Application layer attacks are classified as request flooding attack, asymmetric attack, repeated one-shot attack and application exploit attack.

A DDoS attack can be classified into five families:

- Utilization of computational resources, such as memory, bandwidth, disk space,processor time or disk space.
- Interruption of configuration information, like routing information.
- Interruption of state information, like unsolicited resetting of TCP sessions.
- Break of physical network components.
- Obstruct the communication media between the intended users and the victim so that they can no longer communicate adequately.

In many cases DDoS attack involves spoofing the sender IP addresses so that it’s difficult to identify the location of attacking machine and to prevent filtering of the packets

2. Related Work

2.1 Intrusion Prevention System

Intrusion detection is the process of monitoring the events occurring in a network or computer system and analyzing them for signs of all possible attacks, which are violations or imminent threats of violation of computer security policies, standard security practices or legitimate user policies. Events have many causes, such as malware (e.g., worms, spyware), attackers gain the unauthorized access from the internet, and certified users who misuse their privileges or try to gain additional rights for which they are unauthorized. Although many incidents are malicious in nature, some others are not; for example, a person may mistype the address of a computer and accidentally attempt to connect to a different syste m without authorization.

An intrusion detection system (IDS) is a software which automates the detection process. An intrusion prevention system (IPS) is software which has all the potential of an intrusion detection system and can also attempt to stop probable incidents.

2.2 Uses of IDPS Technologies

IPSs are primarily focused on identifying possible threats. For example, an IDPS can detect when an attacker has successfully compromised a system by exploit a susceptibility in the system. The IDPS could report the incident to security administrators, who would immediately initiate incident response actions to reduce the damage caused by the incident. Then the IDPS logs information that could be used by the incident handlers. Many IDPSs can also be configured to identify violations of security policies. Many IDPSs can also identify inspection activity, which may indicate an attack is imminent. Some attack tools and forms of malware, mostly worms, perform reconnaissance activities such as host and port scans to recognize targets for succeeding attacks. An IDPS should be able to block reconnaissance and inform security administrators, who can take actions if needed to modify other security controls to prevent associated incidents. Because reconnaissance activity is so repeated on the internet, reconnaissance finding is often performed primarily on protected internal networks.

Identifying security policy problems.

An IDPS can offer some degree of quality control for security policy implementation, such as duplicate firewall rulesets and alerting when it sees network traffic that should have been blocked by the firewall but was not because of a firewall configuration error.

Documenting the existing threat to an organization. IDPS logs information about the threats that they detect. Understanding the occurrence and characteristics of attacks, the computing resources is helpful to identify the appropriate security measures to protect the resources. The information can also be used to instruct management about the threats that the organization faces.

Deterring individuals from violating security policies. If individuals are conscious that their actions are being monitored by IDPS technologies for security policy violations, they may be less expected to commit such violations because of the risk of detection.

2.3 Key Functions of IDPS Technologies

There are many types of IDPS technologies, which are classified primarily by the types of events that they can identify and the methodologies that they use to identify incidents. The monitoring and analyzing events to identify unwanted activity, all types of IDPS technologies typically perform the following functions:

Record the information related to observed events. Information is recorded locally, and also sent to separate systems are centralized log servers, secured information. Notifying security administrators of important observed events is known as an alert, and takes place any of several methods, includes: e-mails, messages on the IDPS user interface, pages, Simple Network Management Protocol (SNMP) traps, user-defined programs and scripts and syslog messages. A notification message includes only basic information regarding an event; administrators need to access the IDPS for added information. Producing reports. Reports to be summarized for the monitored events.

IPS technologies are differentiated from IDS by one characteristic: IPS technologies are differentiated from IDS by one characteristic: IPS technologies can respond to a detected threat by attempting to prevent it for succeeding. They use many response techniques, which are divided into the following groups:

The IPS stops the attack itself.

The session of user or connection of network that is being used for the attack to be terminated.

Block access to the target from the offending IP address, user account, or any other attacker attribute

Block all access to the targeted service, host, application, or any other resource.

The IPS changes the security environment. The IPS would change the configuration of other security controls to interrupt an attack. Common examples to reconfigure a network device (e.g., switch, router, firewall) to block access from the attacker or to the target, and altering a host-based firewall on a target to block incoming attacked packets. IPSs may apply the patches to a host if the IPS detects that the host has susceptibility actions.

The IPS may change the content of attack. Other IPS technologies can eliminate/replace malicious portions of an attack to make it perfect. For example, an IPS removing an infected file attachment from mail and then allowing the cleaned email to reach corresponding recipient. An example is an IPS acts as a proxy and normalizes incoming requests, which means the proxy repackages the payloads of the requests, by discarding the header.Certain attacks can be discarded as part of normalization process.

3. Common Detection Methodologies

IDPS technologies use many methodologies to detect incidents they are,signature-based, anomaly-based, and stateful protocol analysis. Most IDPS technologies use multiple detection methodologies, either integrated or separated, to provide broad and accurate detection.

3.1 Signature-Based Detection

A signature is a pattern which corresponds to a known threat. Signature-based detection is the process of comparing signatures against experimental events to recognize possible incidents.

Signature-based detection is effective for detecting known threats but ineffective for detecting previously unknown threats, threats are differentiated by the use of evasion techniques, and many variants of known threats. Signature-based detection is the easiest detection method because it just compares the current activity, such as a packet or a log entry, to a list of signatures by using string comparison operations. Signature-based detection technologies have understanding of many application protocols or network and couldnot track and understand the state of complex communications.

3.2 Anomaly-Based Detection

Anomaly-based detection is the process of comparing definitions of which activity is considered normal against observed events to categorize important deviations. An IDPS using anomaly-based detection has profiles that represent the normal behavior of such things as users, hosts, applications or network connection. The profiles has been developed by monitoring the characteristics of typical activity over a period of time. Profiles can be developed by many behavioral attributes, such as the number of failed login attempts for a host, the level of processor usage for a host in a given period of time and the number of e-mails sent by a user.

The major benefit of anomaly-based detection methods is that they can be very effective at detecting previously unknown threats. Profiles for anomaly-based detection may be either be static or dynamic. A static profile is unchanged unless the IDPS is purposely directed to generate a new profile. A dynamic profile is adjusted continuously as additional incidents are observed. Because networks and systems change over time, the corresponding actions of normal behavior also change; a static profile will eventually becomes not correct, so it needs to be regenerated periodically. But dynamic profiles do not have this problem, but they are vulnerable to avoidance attempts from attackers.

3.3Types of IDPS Technologies

3.3.1 Network-based IDS (NIDS) is an intrusion detection system which monitors network traffic. It use the technique like packet sniffing, and analyze the collected network data, it tries to discover unauthorized access to a computer network. A typical NIDS facility includes a number of sensors to monitor packet traffic, no. of servers for NIDS management functions, and more management consoles for the human interface.

The traffic patterns analysis to detect intrusions may be done at the sensor or at the server, or combination of the two. Sensors are deployed in one of two modes: inline and passive. An inline sensor s are inserted into a network segment so that the traffic that is monitoring must pass through the sensor. The primary motivation for the use of inline sensors is to block an attack when intrusion is detected. The device which perform both intrusion detection and intrusion prevention function uses the passive sensors. A passive sensor monitors a copy of network traffic and does not allow the actual traffic to pass through the device. The passive sensor is more efficient than the inline sensor, because no need to add an extra handling step that contributes to packet delay. NIDS makes use of signature detection and anomaly detection.
3.3.2Host-Based IDS is an intrusion detection system that monitor and analysis the internals of a computing system as well as the network packets on its network interfaces.
3.3.3Stack-Based IDS is intrusion detection systems that inspect the packets as they go through the TCP/IP stack.

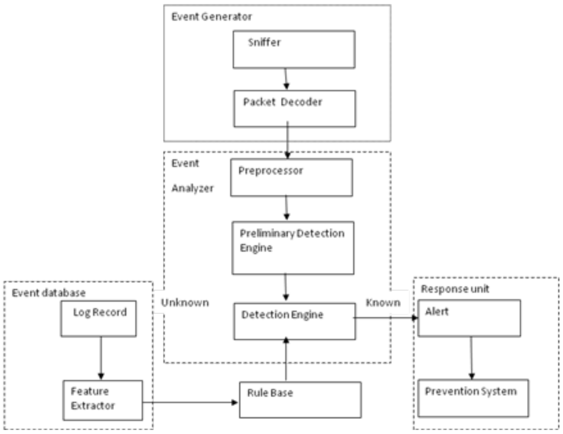
3.3.4 Protocol-Based IDS (PIDS) is an intrusion detection system which is installed on a web server, and is used for monitoring and analysis of the protocol in use by the computing system. A PIDS will monitor the dynamic activities and state of the protocol and will typically consist of a system or agent that may sit at the front end of a server, to monitor and analyze the communication between devices. Graph-Based IDS is an intrusion detection system which detects intrusions that involve connections between many hosts or nodes. A graph consists of nodes represent the domains and edges presents the network traffic between nodes.

4. Intusion Prevention In Cloud Computing

Intrusion Prevention System (IPS) is a new approach to defense networking systems, which may combine the techniques firewall with intrusion detection properly, which is a proactive technique, prevent from the attacks to enter the network by examining various data record and detection demeanor of pattern recognition sensor, an attack is identified, intrusion prevention block and log the offending data. IPS monitors network and take actions based on recommended rules when an event occurs. It sits inline on the network and passive in nature. IPSs take a further step from detection, some see them as next generation IDS systems. Intrusion prevention is an extension of intrusion detection. An organization can't protect its network with only firewall, an extra layer of protection must be provided. An intrusion prevention system provides an extra layer of protection by scanning all the network traffic and specific browser protection.

4.1 System design:

Major components of IDPS framework are Event generator, analyzer, and event database and response unit. Inside the major unit packet decoder, preprocessor, detection engine, log record and feature extractor, alert and prevention system are located.



4.1.1Event Generator:
Event generator components collect, filter and convert event data. An event generator collects the network packets, and generates suspicious intrusion events by filtering.
Packet Decoder:
Packet decoder usually known as sniffer takes packet from various types of network interfaces and prepares it to be sent to the detection engine. It is commonly known as sniffer. The interface may be Point to Point Protocol or Ethernet etc. **Sniffer** is a tool that can help you locate network problems by allowing you to capture and view the packet level data on your network. Network Sniffer can list all of the network packets in real-time from multi-network card and can also support capturing packets based on the applications (SOCKET, TDI etc.). You can capture and observe all traffic of the application which is a potential issue. Typical use of network sniffer is to analyze network traffic and bandwidth utilization, so that troubles in the network can be identified. The functions are Capturing packets, analyzing and recording traffic, Decrypt the packets and displaying in clear text, Converting data to readable format and Showing relevant information like protocol, IP, host or server name and so on.

4.1.2Event Analyzer
Analyzer components analyze any kind of event data transmitted to them .It plays a major role in IDPS. It consists of preprocessor, preliminary detection engine and detection engine.

Preprocessor: Preprocessors are components or plugins that can be used to change data packets before the detection engine does some operation to find out if the packet is being used by some intruder. Transform the packet to the format for data mining, re-structure and process code conversion before matching. For each network connection, the following three major groups of features for detecting intrusions are extracted. They are Basic features, Content features and Traffic features.

Preliminary detection engine: Mainly filter out normal network packets. classify the packets which has either normal behavior or abnormal behavior

Detection Engine: Detection Engine's responsibility is to detect if any kind of intrusion activity exists in a packet. The rules are read to internal data structure where they are matched against all packets. The detection engine takes the packet data from the packet decoder, preprocessor, and performing the detection process. The match of signature to packet is done on the transport and application layers. The matching on the transport layer is generally for checking the source and destination IP addresses and ports, or check the flags if it is TCP protocol. The application layer is for matching the payload in the packet to the attack signatures;

4.1.3Event Database

Database components are the repositories for any kind of data when the storage is necessary.

Logging And feature extractor System:

Log record Include packets information which produced by unknown network normal behavior and unknown intrusion behavior.

Feature extractor:

Make correlation analysis of the data in the log, take the new association rule, and add it to the rule base. It uses Apriority algorithm correlation analysis. Depends upon what the detection engine looks inside a packet, the packet used to log the activity or generate an alert. Logs are kept in tcpdump style files, text files or some other form.

4.1.4Response Unit

Response components issue commands in response to attacks and carry out actions such as resetting connections, killing processes, altering file permissions, etc

Alert and Prevention System:

Intrusion detection alerts are sent by detection engine when suspicious or anomaly traffic is detected. Based on the severity of alert based on alert correlation analysis, it decides what prevention strategies to take.

4.2 The Workflow:

The workflow of the intrusion detection and prevention system as follows. First, the packet decoder or sniffer grabs network packets which are analyzed. Then preprocessor will process the parsing packets by calling pretreatment function. Secondly, after through the preliminary detection engine, normal packets will be discarded of, and the abnormal packets will be processed by detection engine. Through matching rule, it shows that there are invaded behaviors when successful. At the same time, the system will transmit an alert and prevent intrusion behavior. If it is not successful, the new network normal behavior model will be recorded into log. It analyses the abnormal packets, which had been processed by the pretreatment; and then obtains potential or new intrusion behavior patterns through the association rules algorithm and produces the corresponding association rule set; Then it transforms the rule into the intrusion detection rule and adds it to the rule base. Finally, the system will make the correlation analysis for the log through the data mining algorithm. If there is a new rule generation, it will be added to the rule base. Then alert is transmitted to prevention system, corresponding countermeasures will be selected.

5. Methods and approaches

5.1 Genetic algorithm

Genetic algorithm is a search algorithm in which functions are based on the natural selection and genetics. It develops a population of high quality individual from a population of initial individuals. Each individual's represents the solution of the problem is called chromosomes and predetermined number of genes. The rule quality is determined by fitness function .It has two stages , first stage is training a set of rules to detect intruders are generated by using with network audit data .In second stage, the best rules with highest fitness are used to detect intrusion in real time environment. To verify the validity of this approach, KDD dataset is used. Every feature represents a one gene of chromosome and one byte is used to represent a feature. The rule is simple if then clause. The result of every rule is the confirmation of intrusion.

5.1.1 Approach

Genetic algorithms are a branch of evolutionary algorithms used in search and optimization techniques. The three dominant functions of a genetic algorithm i.e., selection, crossover and mutation correspond to the biological process. In a genetic algorithm, there is a population of strings (called chromosomes or the genotype of the genome), which encode and indent solutions (called individuals, creatures, or phenotypes). The solutions are represented in binary as strings of 0's and 1's, but other encodings are possible. The evolution starts from a population of randomly generated individuals and evolves over generations. In each generation, the fitness of each individual in the population is evaluated and multiple individuals are selected from the current population, and modified to form a new population. The new population is used for next iteration of the algorithm. Generally, the algorithm has been terminated when either a satisfactory level has been reached for the population or a maximum number of individuals are there in a generation. If the algorithm has terminated due to a maximum number of individuals, a satisfactory solution may or may not have been reached.

5.1.2 Process: It starts from initial population generation from p_firewall.log file generated by the firewall system. The packets are the filtered out on the basis of rules. Then the precised data packets go through several steps namely selection, crossover and mutation operation. These processes gets generate best individuals. The generated individuals are the verified by the fitness function to generate the population for next generation.

5.2 NSL-KDD dataset

To verify the effectiveness and the feasibility of the proposed IDPS system, we have used NSL-KDD dataset. It is a new version of KDDcup99 dataset. NSL-KDD dataset has some advantages over KDDcup99 dataset. It has solved some of the inherent problems of the KDDcup99, which is considered as standard benchmark for intrusion detection evaluation. The training dataset of NSL-KDD similar to KDDcup99 consist of 4,900,000 single connection vectors each contains 41 features and is labeled as either normal or attack type, with exactly one specific attack type. Due to following reasons, NSL-KDD has become more popular dataset than KDD cup 99 dataset for intrusion detection purpose.

- Redundant records of the training set are eliminated.
- Duplicate records of the test set are removed to improve the detection performance.
- Use of NSL-KDD dataset for classification gives an accurate evaluation of other different learning techniques.
- It is inexpensive to use NSL-KDD dataset for experiment purpose as it may consists of reasonable numbers of instances in the training set and testing set.

5.3 Experiments and Results and Analysis

For the implementation of our algorithm we used the NSL KDD intrusion detection datasets which are based on the DARPA initiative, which gives designers of intrusion detection systems (IDS) with a benchmark on which to evaluate different methodologies. Hence, a simulation is being made of a factitious military network with three ‘target’ machines running various operating systems and services. They used three additional machines to spoof different IP addresses for generate network traffic.

A connection is a sequence of TCP packets starting and ending at some well-defined times, between data flows from a source IP address to a target IP address under some well-defined protocol. It results in 41 features for each connection. Finally records all network traffic using the TCP dump format. The total simulated period is seven weeks. Normal connections are created on profile that expected in a network and attacks fall into one of four categories: User to Root; Remote to Local; Denial of Service; and Probe

5.4 Implementation Procedure

In the pre-calculation phase, we have made 23 groups of chromosomes according to training data. There are 23 (22+1) groups for each of attack and normal types presented in training data. No. of chromosomes in each group is variable and depends on the number of data and relationship among data in that group. Total no. of chromosomes in all groups were tried to keep in reasonable level to optimize time consumption in testing phase. In the testing or detection phase, in each test data, an initial population is made using the data and occurring mutation in different features. The population is compared with each chromosomes prepared in training phase. Portion of population, which are loosely related with all training data than others, are removed. Crossover and mutation occurred in the rest of the population which becomes the new generation. It runs until the generation size comes down to one. The group of the chromosome which is closest relative of only surviving chromosome of test data is returned as the predicted type. From the extracted features of the datasets, only the numerical features are taken for both continuous and discrete, under consideration for the simplification of the implementation. For most of the classes, our system performs well enough except normal data type which is because of ignoring non numerical features. Comparing with the entry of KDD, we can get better detection rate for denial of service & user-to-root and close detection rate for probe & remote-to-local. Following fundamental formulas are used to evaluate the performance of the system: The detection accuracy rate and the false alarm rate were calculated according to the following assumptions:

False Positive (FP): the total number of normal records that are classified as anomalous

False Negative (FN): the total number of anomalous records that are classified as normal

Total Normal (TN): the total number of normal records

Total Attack (TA): the total number of attack records

Detection Rate = [(TA-FN) / TA]*100

6.CONCLUSION AND FUTURE WORK

This research focuses on the building effective intrusion detection system with high detection accuracy and low false alarm rate. The proposed algorithm Genetic algorithm with NSL-KDD dataset is used for this purpose. Experimental results showed that the proposed algorithm gives better and robust representation of data as it was able to reduce the number of features resulting in 80.4% reduction in input data and it was able select significant attributes which leads to improve the detection accuracy to 96.7% with a false alarm rate of 3%.The results showed that the proposed algorithm is reliable and efficient in intrusion detection.

References

[1] Sebastian Roschke, Feng Cheng, Christoph Meinel,“ Intrusion Detection in the Cloud", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.

[2] Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, “A Cooperative Intrusion Detection System Framework for Cloud Computing Networks", 39th International Conference on Parallel Processing Workshops, 2010.

[3] Andreas Haeberlen,“ An Efficient Intrusion Detection Model Based on Fast Inductive Learning”, Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, 19-22 August 2007.

[4] Richard Chow, Philippe Golle, Markus Jakobsson, “Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control”, ACM Computer and Communications Security Workshop, CCSW 09, November 13, 2009.

[5] Kleber, schulter, “Intrusion Detection for Grid and Cloud Computing”, IEEE Journal: IT Professional, 19 July 2010.

[6] Irfan Gul, M. Hussain, “Distributed cloud intrusion detection model”, International Journal of Advanced Science and Technology Vol. 34, September, 2011.

[7] http://en.wikipedia.org/wiki/Cloud_computing.

[8] R. Graham, “FAQ: Network Intrusion Detection Systems”. March 21, 2000.

[9] D. Zamboni, “Using Internal Sensors For Computer Intrusion Detection”. Center for Education and Research in Information Assurance and Security, Purdue University. August 2001.

[10] K. Scarfone, P. Mell, “Guide to Intrusion Detection and Prevention Systems (IDPS)”. Computer Security Resource Center (National Institute of Standards and Technology). February 2007.

[11] A. Chittur, “Model Generation for an Intrusion Detection System Using Genetic Algorithms”.January 2005.

[12] W. Li, “Using Genetic Algorithm for Network Intrusion Detection”. “A Genetic Algorithm Approach to Network Intrusion Detection”. SANS Institute, USA, 2004.

[13] W. Lu, I. Traore, “Detecting New Forms of Network Intrusion Using Genetic Programming”.Computational Intelligence, vol. 20, pp. 3, Blackwell Publishing, Malden, pp. 475-494, 2004.

[14] M. M. Pillai, J. H. P. Eloff, H. S. Venter, “An Approach to Implement a Network Intrusion Detection System using Genetic Algorithms”, Proceedings of SAICSIT, pp:221-228, 2004.

[15] S. M. Bridges, R. B. Vaughn, “Fuzzy Data Mining And Genetic Algorithms Applied To Intrusion Detection”, Proceedings of 12th Annual Canadian Information Technology Security Symposium, pp. 109-122, 2000.

[16] J. Gomez, D. Dasgupta, “Evolving Fuzzy Classifiers for Intrusion Detection”, Proceedings of the IEEE, 2002.

[17] M. Middlemiss, G. Dick, “Feature selection of intrusion detection data using a hybrid genetic algorithm/KNN approach”, Design and application of hybrid intelligent systems, IOS Press Amsterdam, pp.519-527, 2003.

[18] Srinivas Mukkamala, Andrew H. Sung, Ajith Abraham, “Intrusion detection using an ensemble of intelligent paradigms”, Journal of Network and Computer Applications, Volume 28, Issue 2, April 2005, Pages 167-182

[19] S. Peddabachigari, Ajith Abraham, C. Grosan, J. Thomas, “Modeling intrusion detection system using hybrid intelligent systems”, Journal of Network and Computer Applications, Volume 30,Issue 1, January 2007

[20] M. Saniee Abadeh, J. Habibi, C. Lucas, “Intrusion detection using a fuzzy genetics-based learning algorithm”, Journal of Network and Computer Applications, Volume 30, Issue 1, January 2007

[21] Tao Peng, C. Leckie, Kotagiri Ramamohanarao, “Information sharing for distributed intrusion detection systems”, Journal of Network and Computer Applications, Volume 30, Issue 3, August 2007

[22] M. Crosbie, E. Spafford, “Applying Genetic Programming to Intrusion Detection”, Proceedings of the AAAI Fall Symposium, 1995.

[23] T. Xia, G. Qu, S. Hariri, M. Yousif, “An Efficient Network Intrusion Detection Method Based on Information Theory and Genetic Algorithm”, Proceedings of the 24th IEEE International Performance Computing and Communications Conference (IPCCC ‘05), Phoenix, AZ, USA.2005.