Improved Hybrid Intrusion Detection System (HIDS): Mitigating false alarm in Cloud Computing

Ajeet Kumar Gautam*, Dr. Vidushi Sharma**, Shiv Prakash*** and Maanak Gupta****
*M.Tech, Gautam Buddha University, Greater Noida
**Associate Professor, Gautam Buddha University, Greater Noida
*** Associate Professor, MMM Engineering College, Gorakhpur
****MS, Northeastern University, Boston, USA

Abstract- *Cloud computing is one of the fastest growing fields in Information Technology. It is an internet based computation model in which customers' login to the cloud to access data and applications stored on a remote server on pay-as-you-use basis. Gartner has estimated that the cloud market would be at $150 billion by 2013. The pace at which this area is booming has also led to some security issues as far as the security of customer information is concerned. Since login to the cloud is generally free, it is high likely that intruders could also get access to the servers and compromise the security. Organizations generally use an Intrusion Detection System (IDS) to mitigate such network attacks. Methodologies like Anomaly based, Signature based or honeypot are used in these IDS. Researchers have also hybridized methodologies like anomaly with signature, signature with honeypot etc. to reduce risks. But very few have tried to work on hybridization of anomaly and honeypot technology. In this paper, we have coupled the advantages of hybridization of Anomaly and Honeypot technology to develop hybridized IDS.*

Keywords - *Intrusion Detection and Prevention System (IDPS), Hybrid Intrusion Detection System (HIDS), KFSensor, FlowMatrix, Packet Tracer*

I. INTRODUCTION

Hybrid intrusion detection systems [1][2] are those detection systems where we deploy more than one detection methodology. If we use only signature based detection methodology [3] in Intrusion Detection and Prevention System then it will be capable enough to capture only those attacks whose definition is stored in its database otherwise it will leave all other attacks. Similarly if we use only the anomaly based detection methodology [4], it will give us more false alarms. Thus all the Intrusion Detection Systems have some limitation. But, if we employ more than one intrusion detection methodologies than we can get a more secure intrusion detection system (HIDS) [5]. Anomaly based IDS generates large number of false positive alarms and we can reduce these false alarms by associating this technology with honeypot based technology. Honeypot technology attracts the intruder by acting as a dummy server and the moment the attacker gets in trap, the honeypot creates its signature and stores it in the database of the firewall. The next time, whenever that intruder tries to attack again to the network, as the signatures are already present, the attacker would be prohibited to enter to the network. An important thing to be discussed here is that if a client is getting allude towards the dummy server of honeypot, it means, the client is an attacker. Hence, the demerit of anomaly based technology of creating false alarms is reduced to a great extent. We have used KFSensor for honeypot technology and FlowMatrix for anomaly based detection methodology. Following sections discuss and propose the research done in designing HIDS.

The paper is divided into four sections. Section II presents related work and in section III we have described the proposed approach and written an algorithm for the Hybridized IDS. Section IV describes architecture for proposed approach. Finally, conclusion has been provided in section V.

II. RELATED WORK

There are number of hybrid intrusion detection systems that employ different detection methodologies, which researchers have gone through. A Hybrid Real Time Agent Based Intrusion Detection and Response System [6] were proposed to increase the security in wireless networks. The researchers have merged signature and anomaly based IDS. CAIDS (Cooperative anomaly and intrusion detection system) [7] is one such Intrusion Detection System. It integrates two different detection engines NIDS (Network Intrusion Detection System) and ADS (Anomaly Detection System). Another hybrid IDS scheme based on biological immunology and mobile agent [8] was developed that could be a solution to the security threats and system flaws from the transfer of immune pathological mechanisms into IDS. But due to rapid development of intrusion and attack techniques the proposed IDS is vulnerable to new threats due to negligence to immune pathology. An intelligent intrusion detection and response system [9] is based on hybrid ward hierarchical clustering analysis. It distinguishes between real attack and normal traffic. The results of the hybrid statistical analysis are feedback to the IDS' alert monitor to identify real attacks and isolate benign traffic. This intelligent detection and response strategy enhances the ability of the IDS to accurately detect and respond to subsequent threats and benign traffic in critical segments of real network infrastructures. An adaptive network intrusion detection system [10] uses two stage architecture. In the first stage a probabilistic classifier is used to detect potential anomalies in the traffic. In the second stage a HMM based traffic model is used to narrow down the potential attack IP addresses. Many researchers integrate honeypot technology to intrusion detection system. Honeypots can attract an attacker towards it and work in cooperation with Fire Wall. The system will refuse the visit of the intruder whose IP address is set in the Fire Wall as blacklist by the honeypot. AAIDHP (An Architecture for Intrusion Detection using Honey Pot) was developed which is based on honey pot technology. The approach solves the problems information overload, unknown attacks, false positives and false negatives. Many researchers have studied the feasibility of honey pot technology and intrusion prevention system together and have proposed a new intrusion prevention system model which is based on immune principle of intrusion prevention system and honeypot technology.

From the above related work we can conclude that there are certain shortcomings to all the HIDS. We have gone through such as in a signature based IDS if an attacker attacks slowly and organized, the attack may go undetected through the IDS, as signatures include factors which are based on duration of the events and the actions of attacker do not match. For the unknown attacks there are no signatures updated or an attacker attack in the mean time when the database is updating. Thus, signature-based IDS fail's to detect unknown attacks. Anomaly based IDS suffer from false-positive readings. In a honeypot technology it will not detect those attacks where an attacker did not communicate with it. Hence, there is a need to develop an Intrusion Detection System which can overcome the given problem.

III. PROPOSED WORK – IMPROVED HIDS

We are proposing an improved HIDS that has coalesce the benefits of two individual Intrusion Detection Systems i.e. Honeypot and Anomaly based to derive a Hybridized IDS. We will try to present this scenario with the help of an example explained as below:

A. Scenario Example:

The chairperson of an organization (say- ABC) implements IDS (say- XYZ) to protect his organization's network and the intruder sitting in some other network is trying to get access to the organization's network.

A.1. If ABC implements XYZ which is based on Honeypot Technology:

Honeypots are used for luring and trapping attackers, capturing information and generating alerts when someone is interacting with them. The activities of attackers provide valuable information for analyzing their attacking techniques and methods.
However, the drawback with Honeypots is that they only track and capture activity that directly interacts with them. They cannot detect attacks against other systems in the network. Thus, we cannot implement honeypot alone in an organization.

A.2. If ABC implements XYZ is only Anomaly based IDS:

To overcome such a situation an anomaly based IDS is developed which is capable of detecting unknown attacks and all types of new attacks. It establishes patterns of data collected from normal network behavior. It takes periodical samples of the network activity and compares the samples with the pattern and if it finds any significant difference, it marks it as an anomaly. Thus we find that anomaly based IDSs are more capable of detecting abnormality but still not widely accepted by the people as it does not meet usability requirements and also buzz a lot of false alarms.

A.3. If ABC implements XYZ which is both honeypot based and Anomaly based IDS:

If we combine both honeypot based IDS and the anomaly based IDS then we can get better results as honey pot based IDS can bring more and more attackers toward itself. Later we can make signature for these attacks and update it to database. Anomaly based IDS can hinder any unknown attack or anomaly in the whole network. Thus combining both the system will harden the IDS.

B. Flow Chart for Improved Hybrid Intrusion Detection System:

Figure 1 shows a flowchart that describes the entire working of IDS at the server end. The process starts with network scanning for any type of attack either the known or unknown. We have designed architecture with different networking tools such as firewall, routers, switch and nodes. There are two nodes, one node installed with honeypot based IDS and at other installed with anomaly based IDS.

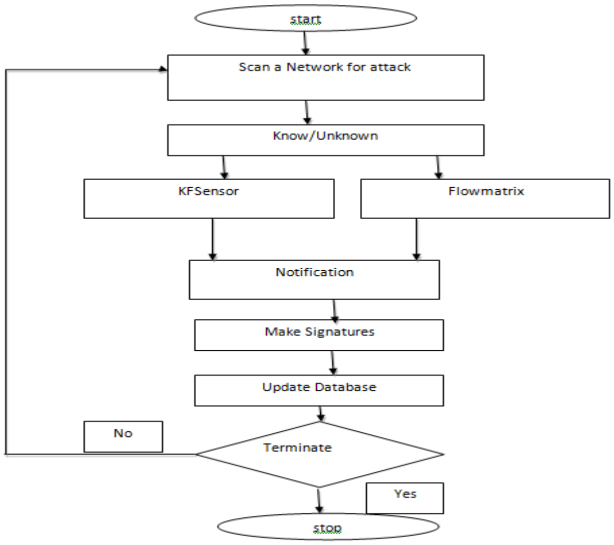


Figure 1: Flowchart

C. Algorithm for Improved Hybrid Intrusion Detection System:

To implement such a system we have designed architecture in the network lab as a real time implementation. An algorithm is presented in which explores the working of entire system within the organization. Through the algorithm we can clearly understand the types and time of the event that take place during the entire process of intrusion detection system.

IDS (Combination of Honeypot based and anomaly based IDS)

```
Scan a network for attacks
if(attack known or unknown){
run(KFSensor);
notify
run(FlowMatrix);
notify
make signatures
update database
}
if(terminate)
stop execution
else
goto 1
```

The above algorithm is defined as:
Step 1: Scan the network for any attack.
Step 2: For any type of attack, either known or unknown attack run KFSensor and FlowMatrix.
Step 3: Both the IDS will notify it to the administrator,
Step 4: If an attack goes undetected by KFSensor, FlowMatrix will detect the attack for sure and for the next time we can make signature for the new attacks and update to the database.

IV. ARCHITECTURE OF HYBRIDIZED IDS

A. Design of a network in packet tracer

Before implementing the network in real time to analyze it properly, we initially configured and simulated the architecture on packet tracer [11][12]. This made it easy to configure all the network devices. Following Figure 2 shows the architecture design which is developed in packet tracer.

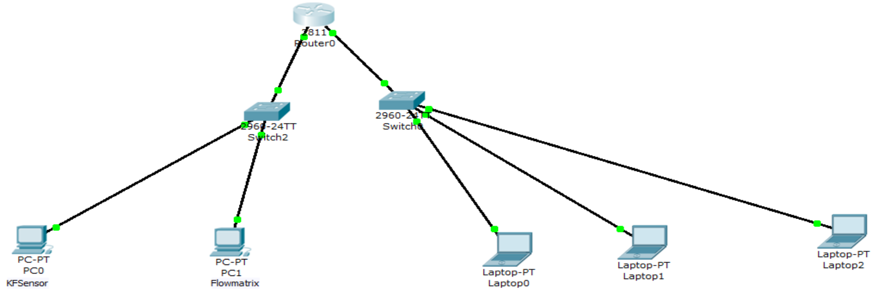


Figure 2: Network Design in Packet Tracer

After Verifying and validating the system in packet tracer we had built the above architecture in the network lab with similar configuration. The architecture is depicted in figure 3 below-

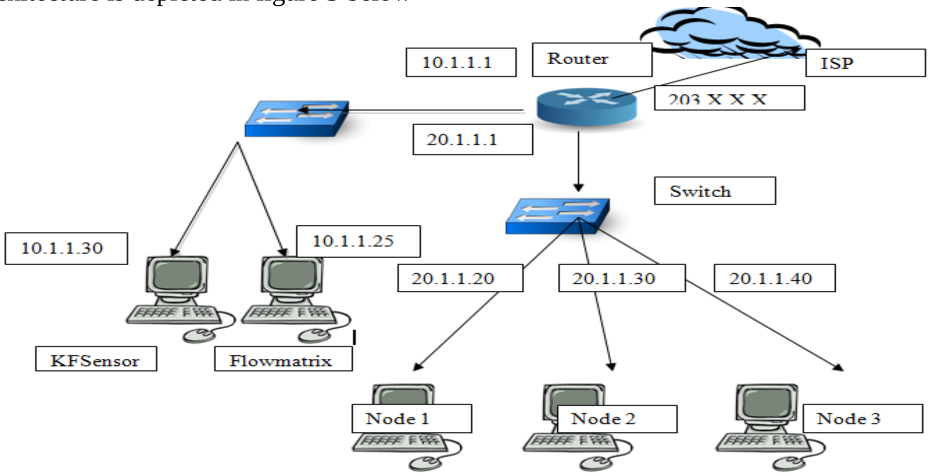


Figure 3: Architectural Design which is implemented as a real time in the Network Lab

We have made a network with nodes, routers and switches. Two nodes are servers and rest three is connected to the router through switch. Router helps to route packets to different networking devices and to connect LAN to WAN. The servers communicate with the nodes with the help of the router via switch. In both servers we have installed different Intrusion Detection Systems (IDSs). In one of the servers we have installed honeypot based IDS and in the other server anomaly based IDS. Honeypot attracts the attacker whenever he tries to perform a malicious activity across the network and later makes their signatures and updates it in the database. Anomaly based detection system analysis the network and records the normal network traffic and whenever it finds any anomalous behavior it buzzes an alert. Both these systems working together can strongly restrict an attacker coming to your private network. For a honeypot technology we have used KFSensor and for anomaly based IDS FlowMatrix.

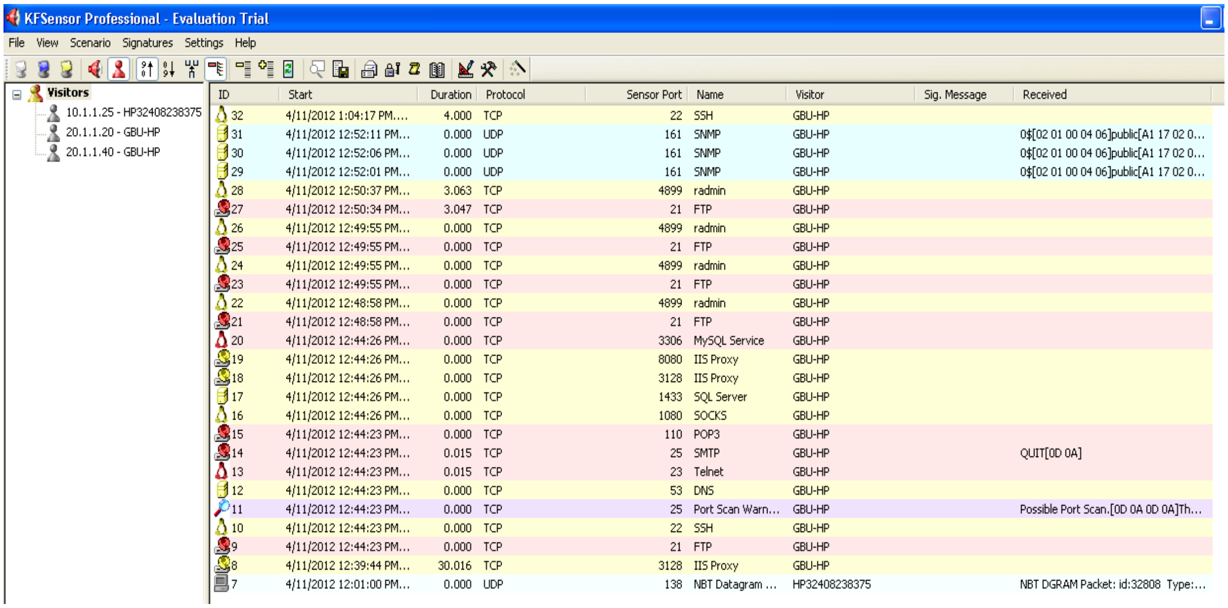
A. KFSensor

KFSensor [13][14] is a host based IDS which works on the honeypot based technology. It is open source software which can be downloaded from the internet. KFSensor is installed in one of the node from where it disguise the attacker and the moment it allures the attacker, it adds the definitions of that attacker to the database for the next time and restrict the entry of that attacker or intruder to the main network of the organization. In the architecture discussed above we have installed KFSensor in one of the server and we record data to analyze and validate the algorithm.

B. FlowMatrix

FlowMatrix [15] is application software which one can downloaded from the internet free of cost. FlowMatrix is based on Anomaly based detection methodology. It compares the samples from the normal traffic with the regular samples obtained from the network and the moment it finds the difference between the normal and the regular sample it gives an alert. Figure 5 shows the GUI of Honeypot based respectively.

Following figures 4 and figure 5 shows the GUI of Kfsensor and FlowMatrix respectively.



ID	Start	Duration	Protocol	Sensor Port	Name	Visitor	Sig. Message	Received
32	4/11/2012 1:04:17 PM....	4.000	TCP	22	SSH	GBU-HP		
31	4/11/2012 12:52:11 PM...	0.000	UDP	161	SNMP	GBU-HP		0$[02 01 00 04 06]public[A1 17 02 0...
30	4/11/2012 12:52:06 PM...	0.000	UDP	161	SNMP	GBU-HP		0$[02 01 00 04 06]public[A1 17 02 0...
29	4/11/2012 12:52:01 PM...	0.000	UDP	161	SNMP	GBU-HP		0$[02 01 00 04 06]public[A1 17 02 0...
28	4/11/2012 12:50:37 PM...	3.063	TCP	4899	radmin	GBU-HP		
27	4/11/2012 12:50:34 PM...	3.047	TCP	21	FTP	GBU-HP		
26	4/11/2012 12:49:55 PM...	0.000	TCP	4899	radmin	GBU-HP		
25	4/11/2012 12:49:55 PM...	0.000	TCP	21	FTP	GBU-HP		
24	4/11/2012 12:49:55 PM...	0.000	TCP	4899	radmin	GBU-HP		
23	4/11/2012 12:49:55 PM...	0.000	TCP	21	FTP	GBU-HP		
22	4/11/2012 12:48:58 PM...	0.000	TCP	4899	radmin	GBU-HP		
21	4/11/2012 12:48:58 PM...	0.000	TCP	21	FTP	GBU-HP		
20	4/11/2012 12:44:26 PM...	0.000	TCP	3306	MySQL Service	GBU-HP		
19	4/11/2012 12:44:26 PM...	0.000	TCP	8080	IIS Proxy	GBU-HP		
18	4/11/2012 12:44:26 PM...	0.000	TCP	3128	IIS Proxy	GBU-HP		
17	4/11/2012 12:44:26 PM...	0.000	TCP	1433	SQL Server	GBU-HP		
16	4/11/2012 12:44:26 PM...	0.000	TCP	1080	SOCKS	GBU-HP		
15	4/11/2012 12:44:23 PM...	0.000	TCP	110	POP3	GBU-HP		
14	4/11/2012 12:44:23 PM...	0.015	TCP	25	SMTP	GBU-HP		QUIT[0D 0A]
13	4/11/2012 12:44:23 PM...	0.015	TCP	23	Telnet	GBU-HP		
12	4/11/2012 12:44:23 PM...	0.000	TCP	53	DNS	GBU-HP		
11	4/11/2012 12:44:23 PM...	0.000	TCP	25	Port Scan Warn...	GBU-HP		Possible Port Scan.[0D 0A 0D 0A]Th...
10	4/11/2012 12:44:23 PM...	0.000	TCP	22	SSH	GBU-HP		
9	4/11/2012 12:44:23 PM...	0.000	TCP	21	FTP	GBU-HP		
8	4/11/2012 12:39:44 PM...	30.016	TCP	3128	IIS Proxy	GBU-HP		
7	4/11/2012 12:01:00 PM...	0.000	UDP	138	NBT Datagram ...	HP32408238375		NBT DGRAM Packet: id:32808 Type:...

Figure 4: GUI of KFSensor

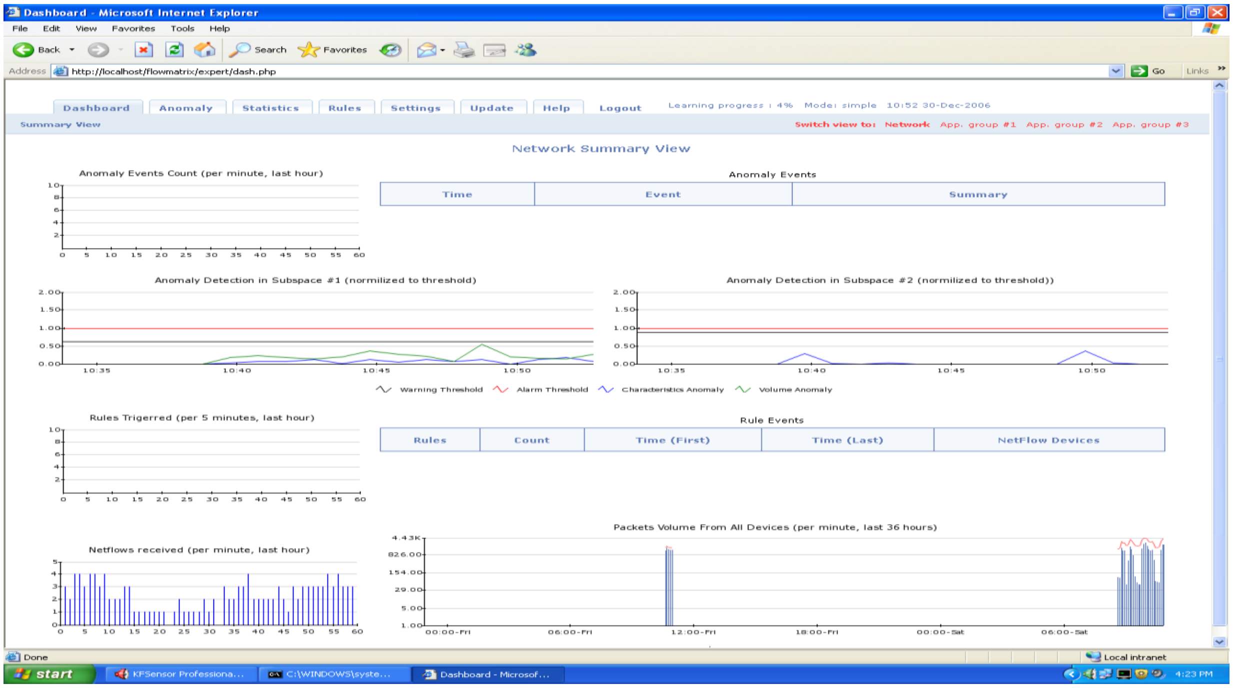


Figure 5: GUI of FlowMatrix

V. CONCLUSION AND FUTURE ENHANCEMENT

We’ve gone through numerous HIDS provided by different researchers and have found some shortcomings in them. Hence, in order to overcome their inadequacies, we have proposed a Hybrid Intrusion Detection System by fusing anomaly detection based methodology and honeypot based methodology. The methodologies used in this HIDS can overcome each other’s shortcomings. The discussed Improved Hybrid Intrusion Detection System can locate and identify the statistical data of any particular intruder. We have developed a framework and to implemented it in real time to record and analyze the data. We also developed the frame work in Packet Tracer before actually implementing it in real time. The fusion of the mentioned technological assets in designing the HIDS gives it a cutting edge in the field of cyber security in cloud computing, which puts it on the top spot.

We’ve validated the algorithm on Hybrid Intrusion Detection System after creating the architecture in the Network Lab. The coding will be initiated in the future.

VI. REFERENCES

[1].Jiqiang Zhai and Yining Xie, "Research On Network Intrusion Prevention System Based On Snort. International Conference on Strategic Technology, in *Proc*. in *IEEE*, (2), 2011, Pp. 1133-1136.

[2]. Moses Garuba, Chunmei Liu and Duane Fraites, "Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems" In International Conference on Information Technology: New Generations, in *Proc.* of *IEEE*, Pp. 592-598, 2008.

[3]. Farzaneh Izak Shiri, Bharanidharan Shanmugam and Norbik Bashah Idris, "a parallel technique for improving the performance of signature-based network intrusion detection system", Conference on Communication Software and Networks (ICCSN) in Proc. of IEEE, 2011, Pp. 692-696.

[4]. Mahbod Tavallaee, Natalia Stakhanova, and Ali Akbar Ghorbani, "Towards Credible Evaluation of Anomaly-Based Intrusion-Detection Methods", Journal of Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews" in *Proc*. in *IEEE*, 2010, Pp. 516-524.

[5].Dwen-Ren Tsai, Wen-Pin Tai and Chi-Fang Chang,"A Hybrid Intelligent Intrusion Detection System to Recognize Novel Attacks", in *Proc*. of *IEEE*, 2003, Pp. 428-434.

[6].Vaidehi Kasarekar and Byrav Ramamurthy, "Distributed Hybrid Agent Based Intrusion Detection and Real Time Response System", in Proc. in IEEE, 2004, Pp. 739-741.

[7].Marios D. Dikaiakos, Athena Vakali, Pankaj Mehra, Dimitrios Katsaros and George Pallis, "Cloud Computing: Distributed Internet Computing for it and Scientific Research," in Proc. in Internet Computing, IEEE Vol. 13, 2009 Pp. 10-13.

[8].Xuan Wu Zhou, Xiao Yuan Yang, Ping Wei and Yu Pu, "A hybrid immune intrusion detection system based on mobile agent", International Conference on Computer-Aided Industrial Design and Conceptual Design (CAIDCD), in Proc. in IEEE, 2006, Pp. 1-5.

[9].Emmanuel Hooper, "An Intelligent Intrusion Detection and Response System Using Hybrid Ward Hierarchical Clustering Analysis", International Conference on Multimedia and Ubiquitous Engineering, in IEEE, 2007, Pp. 1187-1192

[10].R Rangadurai Karthick, Vipul P. Hattiwale and Balaraman Ravindran, "Science Adaptive Network Intrusion Detection System using a Hybrid Approach", Fourth International Conference on Communication Systems and Networks (COMSNETS), in IEEE, 2012 , Pp. 1-7.

[11].CISCO (2008). "Packet Tracer 5.0 Brochure" Available:
http://www.cisco.com/web/learning/netacad/downloads/pdf/PacketTracer5_0_Brochure_0707.pdf

[12].CISCO (2010). ""Cisco Packet Tracer Data Sheet" Available :
http://www.cisco.com/web/learning/netacad/course_catalog/docs/Cisco_PacketTracer_DS.pdf

[13].Key Focus (2003) "KFSensor overview" Available: http://www.keyfocus.net/kfsensor/

[14]. Key Focus (2003) "KFSensor overview" Available: http://www.keyfocus.net/kfsensor/download/

[15]. AKMA Lab (2010). "FlowMatrix download" Available: http://www.akmalabs.com/downloads_flowmatrix.php