An Improved Hybrid Intrusion Detection System in Cloud Computing

Ajeet Kumar Gautam[†], Vidushi Sharma[†], Shiva Prakash^{††}

[†]School of Information and Communication Technology Gautam Budha University Greater Noida, UP, INDIA

^{††}Department of Computer Science and Engineering, Madan Mohan Malviya Engineering College, Gorakhpur Uttar Pradesh, INDIA

Abstract

Today, security is a major concern. Cloud computing and Intrusion Detection and Prevention Systems are one such measure to mitigate these attacks. Different researchers have proposed different IDSs time to time some of these IDS's combine features of two or more IDSs which are called as Hybrid Intrusion Detection Systems. Most of the researchers combine the features of Signature based detection methodology and Anomaly based detection methodology. For 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. Sometimes, for an unknown attack there is no signature updated or an attacker attack in the mean time when the database is updating. Thus, signature-based IDS fail to detect unknown attacks. Anomaly based IDS suffer from many false-positive readings. Thus there is a need to hybridize those IDS which can overcome the shortcomings of each other. In the journal we have proposed a new approach to IDS (Intrusion Detection System) which is more efficient than the traditional IDS (Intrusion Detection System). The IDS is based on Honeypot technology and Anomaly based Detection Methodology. We have designed Architecture for the IDS in a packet tracer and then implemented it in real time. We have discussed results on the basis of experiments performed in the network lab. Both the honeypot and anomaly based IDS have some shortcomings but if we hybridized these two technologies, the newly proposed HIDS is capable enough to overcome these shortcomings with much enhanced performance. In this journal, we present a new hybrid intrusion detection system (HIDS) that combines the positive features of two different detection methodologies - Honeypot methodology and anomaly based intrusion detection methodology. In the experiment we ran both the Intrusion Detection System individually first and then together and record the data from time to time. From the data we can conclude that the resulting IDS is much better in detecting intrusions from the existing IDSs.

Keywords

Intrusion Detection and Prevention System (IDPS), Hybrid Intrusion Detection System, KFSensor, FlowMatrix, Paket Tracer

1. Introduction

Cloud computing is a recent research topic in the area of computing environment[1][2][3]. Several researchers have made contribution. Almost all the organizations whether

small scale organizations or large scale organizations, they are making use of cloud technology but due to security factors[4][5] The technology is still not working. Many researchers have gone through the security issues in cloud computing. Wang Jun-Jie and Mu Sen [6] discussed various security issues in cloud computing and its countermeasures. However, the paper is very theoretical and there are no methods that can validate his work. Thereafter Meiko Jensen, J"org Schwenk, Nils Gruschka and Luigi Lo Iacono [7] discussed the technical security issues in cloud computing. To provide security in cloud computing there are different areas in it such as ensuring confidentiality of virtual machines, compromised hypervisor, malicious insider and other network attacks discussed in the next chapter. Different researchers propose different ideas to mitigate risks such as Jinzhu Kong [8] discussed how to protect the confidentiality of virtual machines against distrusted host. The researcher acquaints the concept of virtualization and deals with the security of the virtualized system. Many researchers propose models to mitigate network attacks in cloud computing like Lucian Popa, Minlan Yu, Y. Steven Ko, Sylvia Ratnasamy and Ion Stoica [9] design a hypervisor based CloudPolice and Saketh Bharadwaja, Weiqing Sun, Mohammed Niamat and Fangyang Shen [10] design Collabra, which is a Xen hypervisor based collaborative intrusion detection system. Later on Jakub Szefer and B. Ruby Lee [11] works in the area which is entirely different from all other researches they put forward the case of hardware protection of guest Virtual Machines from compromised hypervisors.

Other researchers' work in developing an Intrusion detection and prevention system to stop intruders from attacking the organization's network. They used a hybrid detection methodology in intrusion detection and prevention system. Dwen Ren Tsai, Wen Pin Tai, and Chi-Fang Chang [12] proposes a hybrid intelligent intrusion detection system to recognize novel attacks through data mining of the behaviors of attacks. However, this hybrid system has partly solved the problem to recognition novel attacks of intrusion later Vaidehi Kasarekar and Byrav Ramamurthy in [13] developed a Hybrid Real Time Agent

Manuscript received August 5, 2013 Manuscript revised August 20, 2013

Based Intrusion Detection and Response System to increase security in wireless networks.

Thereafter, a lot of research is being done to combine a signature based IDS and an anomaly based IDS like Kai Hwang, Ying Chen, Hua Liu [14] proposes CAIDS (Cooperative anomaly and intrusion detection system). CAIDS integrates two different detection engines NIDS (Network Intrusion Detection System) and ADS (Anomaly Detection System). Similarly Yu-Xin Ding, Min Xiao and AI-Wu Liu [15] have done research and implementation on snort-based hybrid intrusion detection system. The researchers combine misuse detection system and anomaly detection system. They make use of SNORT for misuse based detection system. Thus, we can see that different researchers incorporate different methodology in hybrid detection system. Working in same direction Xuanwu Zhou, Xiaoyuan Yang, Ping Wei and Yupuhu [16] developed a hybrid IDS scheme based on biological immunology and mobile agent that can 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. Later, Emmanuel Hooper [17] proposes an intelligent intrusion detection and response system using hybrid ward hierarchical clustering analysis and R Rangadurai Karthick, Vipul P. Hattiwale and Balaraman Ravindran[18] describe an adaptive network intrusion detection system, that uses a 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. They 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. In this direction Zhi-Hong Tian, Bin-Xing Fang and Xiao-Chun Yun [19] design AAIDHP (An Architecture for Intrusion Detection using Honey Pot). The approach solves the problems information overload, unknown attacks, false positives and false negatives later Guan Xin and Li Yun-Jie in 2010 [20] study the feasibility of honey pot technology and intrusion prevention system together and thus proposed a new intrusion prevention system model that is based on immune principle of intrusion prevention system and honeypot technology.

In the journal we have proposed a new architectural design to IDS (Intrusion Detection System) which is more efficient than the traditional IDS (Intrusion Detection System). The IDS is based on Honeypot technology [33][34] and Anomaly based Detection Methodology[35]. To implement such a system we have designed an architecture in the network lab and collect data to validate the proposed Hybrid intrusion Detection System.

2. ARCHITECTURAL DESIGN

We have considered a network, simulated and configured first on packet tracer[36][37] and then implemented it in real time to analyze the network properly, so that while developing it in real time it became easy to configure all the network devices. Figure 1 shows the network configured in packet tracer. The network consists of three nodes and a server. Server is connected to the router to route packets to different networking device and to connect LAN to WAN. Behind the routers we are using 4 nodes, one is made into a server and the other three are connected to a router through a switch. The server communicates with the nodes with the help of the router via switch. In a server we have installed two types of Intrusion Detection Systems (IDSs). One of the systems is based on honeypot technology and the other is anomaly based IDS. Honeypot can attract the attacker whenever it tries to perform a malicious activity across the network and later with this system we can make their signatures and update these signatures in the database whereas anomaly based detection system can analyse the network and record the normal network traffic and whenever it finds any anomalous behavior it throws an alert. Both these systems can strongly restrict an attacker while coming to your private network. For a honeypot technology we are using KFSensor and for anomaly based IDS we are using FlowMatrix.



Figure 1: Network configured in packet tracer

3. RESULT AND ANALYSIS

To validate our algorithm we have implemented the system into three phases:

Phase 1: In phase 1 we have studied KFSensor and analyzed a system for 10 days and record some results. Here we find that though KFSensor is capable to detect those attacks for which the different systems directly interact with it but, it cannot identify those attacks which are done by the systems that are not directly linked by it.

Phase 2: In phase 2 we have studied FlowMatrix and analyze a system again for 10 days and record some results. We found that FlowMatrix is capable of detecting various attacks either know attacks or unknown attacks in the network, however it does not attract a attacker like KFSensor do, more over it may give various false positives. Phase 3: In phase 3 we have installed both KFSensor and FlowMatrix and analyse a system again for 12 days. Here we find different results that attacks which go undetected by KFSensor are detected by FlowMatrix and with KFSensor we can get some new definitions of attack in database. A combined log is generated which captures the attacks and the administrator can take corrective actions.

All the three phases are described below in details and there results are displayed.

3.1 ANALYSIS OF PHASE 1

There are three nodes for attack or to create network traffic. Which have an IP address as 20.1.1.20, 20.1.1.30 and 20.1.1.40 and the node with IP address 10.1.1.25 is server with FlowMatrix and the node with IP address 10.1.1.30 is server with KFSensor. We have created network traffic through different tools such as Attack Ping, Free Port Scanner, Free SNMP etc. Here we have used many more attacking tools to attack at different networking devices such as router, switch, server and other nodes. While attacking from these tools some logs are generated. Through the log we found that KFSensor generate records of only those nodes which are directly communicating with the server and ignore the rest of the nodes. This is the major drawback in IDS which incorporate only honeypot technology. Since, we have also installed FlowMatrix which is anomaly based IDS we found some deviations in the anomaly graph in FlowMatrix if the attacks takes place at some other point in the network which are not recorded by KFSensor.

In the Figure 2 below shows the network activity of all the nodes and the attacks by the three nodes 20.1.1.20, 20.1.1.30 and 20.1.1.40.

Both the ids KFSensor and FlowMatrix has their own way of detecting attacks In KFSensor we can see that the honeypot can attract an attacker towards itself thus with KFSensor we not only detect an attack whose definitions are already exists in its database but also detect new attacks through honeypot technology and later make signatures of these attack and update to database. Drawback of honeypot is that they can only track and capture activity that directly interacts with them. They cannot detect attacks against other systems in the network. In Figure 3 below we can see the ids which is on anomaly based methodology "FlowMatrix" . FlowMatrix is capable of detecting all types of attack in the network.

Riteros Professional - Enduring Tal	De 1		a logal h	100	/	Shows the	ip address of
File View Scenario Signatures Settings Help				/		nodes with	KFSensor and
3 8 8 4 【 11 🗐 🖬 9 8 1 9 6	8400 ¥	11					
1916B · D	2	Duttion Ato.	Sers Name	Visitor	Sig. Message	Received	
101125-1493340829835-Adivity	5/1/2012 12:04:20 PM	0.072 TCP	80 IS	ue-K		A cat is fine too. Desudesudesu	
101130 - ue-K - Adivity	\$17/0012121420 PM	0.004 TCP	80 IS	ue K		A cat is fine too. Desudesudesu	
ALSO	5/7/0012123420 PM	0.219 TCP	80 IS	væ.K		A cat is fine too. Desudesudesu	
14.36.195135	\$/7/0012120420 PM	0.45 TCP	80 IS	ue K		A cat is fine too. Desudesudesu	
-A 14373624	5/7/00/2125/4/21 PM	0.42 TCP	80 IS	un-X		A cat is fire too. Decodecudecu	
A 10/19/10	\$/7/00121214/21 PM	ODEL TOP	80 B	ue K		A cat is fire too. Desudesudesu	
A 1140 21234	\$170012121421 PM	0.382 TCP	80 IS	un X		A cat is fire too. Decodecudero	
A DAMAGE AND CHASSING AND	\$77.00021214-22 PM	All TO	N N	un-K		A cat is fine too. Decodecodeco	
- 1 1456/360-3000-40/360/4000	\$700001010460700M	0.0% 1/2	N 15	un M		A satisfies the Decelectron.	
1100 771 120 . Culo 120 771 02 11 1	\$71,0110 1343-37 DM	0138 109	8 K	un N		A cat in fina ten Danulanularu.	
# 1243 307 X. Guin X. 31748 12 Ha	(7)000 10/00700	130 170	N N	un M		A de la frection de conservation - a L'artic fau tras Decoleculeus	
4 1240 716108 - Gale-108 7164012 +	CO00101048-200746-2004	0.042 1/0	8 K	un M		A valor in the second and and an a	
A MUNITUM Sec-DUTIONI. Orga	COMPLEXANT COM	A100 1/5	N N	1075 110.M		A tel o lite ini venetoretori - A tel o fisa tea Bandandano	
₩ 14.100.18.274 - 0.4200019224_rimets.	27/2012 122422 FML	A118 T/5	0 10	1070 		A cal o ine too o coo coo coo o	
A 1109 5722 - 04299057022 - dirett	21/06616862PM	448 IV	N D N N	WP95		A GE S THE ICO. VEWOEWOEW A set is first tax. Providencies	
4 14200-8312 - 14-201-83-102 date.	COMPLETENCE AND	0.00 TUP	N D	1009N		A CALISTING TOOL DESUDESUPER	
142071307 - mu-6/14207130-7 dy.	2//20212123R259M	UND TUP	A R	URPR,		A cet is the too. Ursudesudesu	
1124-1411	STORE LEAKED PM	0.00 107	N D	1969K		A cat is time too. Desudesudesu	
2103	\$11212123R259M	011/10/	8 D	uter,		A cat is the too. Desudesudesu	
201149-680-HP - Advidy	STORE LEARBORN.	0.96 102	N 15	V#9(A cat is fine too. Desudesudesu	
31000 -1 310000 -1 310000 -1 310000 -1 310000	\$77/2012 12:04:23 PM	0,508 109	80 15	19-90 19-90		A cat is fine too. Desudesudesu	
231631224 - 6346-131-24.bobs.	\$77/2012 12:14:23 PM	0.373 TCP	80 IS	un K		A cat is fine too. Desudesudesu	
2317A428+429-044-28-abbin.	5/1/2012 12:04:24 PM	0.485 TCP	80 IS	ue-K		A cat is fine too. Desudesudesu	
211750-62-0-75-6Labbiate.	\$77,0012120434 PM	0.714 TCP	80 IS	ueX		A cat is fine too. Desudesudesu	
- 1217 KN - 62-17-85-74 abbiate. \$1239	5/7/2021204/35PM	0.064 TCP	80 IS	væ-K		A cat is fine too. Desudesudesu	
- 323,258 eQ-2-2-2-56.comp. 41250	\$77/202121214/3 PM	OSU TOP	80 IS	ue K		A cat is fine too. Desudesudesu	
241922 · · 2414-252 http://www.acounter.org	57/002120435 PM	0.315 TCP	N K	WeX	<hr/>	A cat is fine too. Desudesudesu	
- 122 ALLELER (* 44) STERMALL (* 122	KON21248 RM.	0.565 TCP	8/1S	ueR		A cat is fine too. Desudesudesu	
2124520-024-46200.htt.a 🕌 1255	SUUGTSTATE ANT	0.000 TCP	0 DOS Attack	we-W		Connections 250(00 MARchive C.,	1
- 🖁 244.112.255 - 604.4-112-255 hodi 🔒 12594	5/1/2021212/4/8/PM	0.072 TCP	N IS	ue-K		A cat is fine too. Desudesudesu	
- 1538 - c-N 5-19-48 hell ca.co. 1258	\$77.0012,45911 PM/054	413 10	22 154	ueX			-
265173.8 · (-3) 962-38 hull.cs	STORE STORE	401 102	22 SSH	- Mill			
\$ 11277 . A.1. 27. X Row of A	STOCIC ZOBUS PAUSE	405 107	22 SSH	/weK			
				/		(mar Barriso	Voltore BIS Franke NJ/7907
		-	1			And Mariny	NIN NIN
🔮 🔒 🖉 🔮 🖉		-		-	-	-	• 18 1 sanzanz
			/				
		າດຕໍ່ກ		(
Shows the nodes		109(D	eniai oi	service)			
	2	ttack d	etected 1	w KESen	sor		
connected to a network	_ ª	math u	uuuu	yarou	301		

Figure 2: Network activity of all the nodes and the attacks by the three nodes 20.1.1.20, 20.1.1.30 and 20.1.1.40.



Figure 3: Anomaly based IDS- FlowMatrix

3.1.1. Analysis of KFSensor at GBU networks

We have not only analyzed KFSensor only to the network which we have created at the network lab but also to other different network such as to Gautam Buddha University main network. We have analyzed it on 4rth may in between 10-11 p.m. and get some valid results, some attacks were also noticed.

In the table 1 below we have analysed the following characteristics of KFSensor and conclude that KFSensor is a Host based Honeypot intrusion detection system which can attract the attacker towards itself to protect the organization from attack and block that user in future to enter the organization's premises by updating that user's signature into its database. It gives lesser false alarm but is highly vulnerable to be taken over by bad guys and also they are not capable to detect attack from those users who do not directly communicate with it.

lers a	10	Sat	Dustice	Pro	Sers.	Name	Vsitor	Sg. Message	Received	
195.134.52.224 - 19513452224.oz	0 360	5/4/202100329 PM.	8.000	LEP	1711	UDF Packet	HACKERZONE-PC		RL 13 Kilden: Webs/Webs/Unferen-	
124.114.67.46 - 46.67.114.124.br	1 359	5/4/2012 10/00 15 PM.	0.000	UDP	87	DHCP	shedrank-PC		DHCh Boot Result (12) Hardware	
6.14.201.27 · cpc17-grim16-2-0	1358	5/4/202100303 PM	0.000	100	57	DHCP	Asing HP		DK2 BootFequet 02 Hardware	
499.216.108 - Statk-108.210.99.	0 357	5/4/202100309 PM	6.000	UDP	181	UDF Packet	HACKERZONE PC		10.1310(dpg////wiid/7/5mg.	
Ph.104.231.13 - Kecent Activity	0 3955	5/4/2012 18/03/04 PM	1000	UDP	2947	UDF Packet	172133225		INTROCAASESLAUEWACTING.	
AUTORALIST - SALARANGAL	1355	5/9/2012 10:02 51 PM.	1000	LEP	5	DHCP	Arrab-17		DK2 Bot Femer B3 Hadsan	
28.09.137 · (pe-24-92-97-137a)	1354	5/4/202100252 PML	0.000	LEP	57	CHC2	mitor		DK2-BootFrauet/94Hodows	
18 100 201 /S - Recent Lethilly	1 353	5/4/202100239 PM	0.000	UDP	57	CHCP	AVET-PC		DIC? Boot Ferner 114 History	
10.8 201 245 - 348 261 8 109 re	0 352	5/8/2012 18-02-49 PML	0.000	LIDO	1211	UDF Packet	HACKERZONE-PC		KL48 Kildea Walic JAffman	
4 184 142 719 - ext-1868-eth.4	周期	\$14/2021210422678M	1000	LEP	138	NST Detectore	hatterd-PC		NET DEPLAY Packet intelling Ty.	
207.2017 - Recent Artikity	(8 1951	512/20210-002-02-004	1.000	UNP	1711	IDP Packet	HWORTERONE-AC		ELES Midea // Weikely/Midea	
M137.18.24 - 24-18-137-185.8L	330	5/8/2012 1842 14 PM	6.000	100	9	OHCE	Vien-PC		DHCR Boot Facular Bill Hardware	
M151.68.886 - cpe-164-153-68.	0 848	\$12/2022 10:02 16 PM	0.000	IDP	1947	UDF Packet	172183275		INTRO-ALBERT MERIANDERS.	
82.53.40.109 - Recent Activity	1 347	54/2121002712M	1000	IEP	10010	10P Public	172133157		178 FF 00 0017 10 10 10 10 10 10 00 0	
19.185.48.115 - Recent Activity	\$ 345	5/8/2012 18:02 75 PM	6.000	UDP	10019	005 Artack	177183161		Constient 2000 Blidder C.	
库148.248.33 - cable 178-148-2.	0 345	\$1/212104213 PM.	6.000	LEP	10032	UDF Packet	17213 \$ 168		100 FF 00 00 0C OF 00 00 00 00 00 0	
8.197.155.91 - : - 58-197-155-91	0 34	5/8/2012 18:02 22 PM	1.000	IEP	1005	UDP Padet	172183151		1F0 FF 00 0012 00 10 10 10 10 10 10 0	
19.235.68.70 Recent Activity	0 342	5/2/202210-02-22-20	0.000	UDP	10017	UDF Packet	172183353		IEO FF 00 00 80' 00 00 00 00 00 00 00 0	
73.202.384 - mell-223.202.78	0 342	\$1/2021000212 PM.	0.000	UDP	1005	UDP Packet	172133368		190 FF 00 00 12 00 10 10 10 10 10 00 0.	
12.164.114.11 - b-internet.212.1.	0 341	5/8/202100220 PML	1.000	UDP	10017	UDP Packet	172183367		100 FF 00 00 BC 00 00 00 00 00 00 00 0	
42311238-512311238-static.	0 340	5/4/2017 10:02 20 PM	1000	LEP	1009	UDP Packet	172183358		IFO FF 00 00 17 80 80 10 10 10 10 00 0.	
5.158.212.211 - Recent Activity	(\$ 2020	\$12/2112 10:03 21 DM	6.000	Ino	10017	UDD Darket	172133167		IND FF NO DO D." OF THIS OF AD AD AD A.	
18.172.198.145 - 138.172.108.14.	0 338	5 1/212180212 PM	6.000	LEPP	10017	UDP Packet	172123161		IN 0 57 00 00 00 00 00 00 00 00 00 00 00 0	
19.186.1.80.244 - 109-186-1.80-2.	@ ×17	512/212/16/03/12/204	0.000	UDP	10000	UDE Pariet	172133162		1F0 FF 00 0012 00 00 10 10 10 10 00 0.	
KISCICKIO - DILICKISS PAL.	10 10 15	12/21210-00-18 PM	1.00	Inp	10077	IDP Parket	17213-2162		TO FF OLDO ST OF COLOR OF ON O	
13.37.10.230 - Necest Activity	@ XIS	5/8/201218-0218-0M	8.000	LEP	1005	UDP Packet	17213.3162		170 F7 60 60 12 60 80 30 30 30 30 00 0.	
21.4.264.48 . mod. 171.4.264.4	@ 211	5/2/21210-0312 PM	1.000	tro	10017	UDF Packet	17213316		ICO FF DO DO DC OR OR OR OR OR OR O.	
52171/3179, 143,179 mm.ht	(TRE	512/21210-0212 00	1.000	UDP	10000	UDP Packet	172183157		170 FT 00 00 17 40 80 10 10 10 10 10 10	
12.244.156.138 - Brown Activity	0 322	518/2012 1842 15 PM	6.000	UDP	10017	UDP Packet	172183167		10 FT 60 00 BC OF 00 00 00 00 00 00 00 00 00 00 00 00 00	
74.118.58.46 - 0400463644160.	@ xn	5/2/202180216 201	6.000	upp	1905	UDP Packet	17213316		F0 FF 00 00 12 00 00 10 10 10 10 10	
19.100.155.60 - Recent Activity	10 100	512/2757184515 2M	1.00	100	10017	100 Darlet	17213 3162		TO FE MODOLE" OF CRIME OF MODIA	
2 110 151 IK - Insuffund. 27.11	(0 303)	\$12/21/2100152M	1.000	Inp	10010	100 Parket	172133167		IFO FE IND IN 12 IN IN IN IN IN IN AN	
terrel 1	2	President and an and here				Sec. of Sec. of Sec.	11000000000		Activity in the second of the local data	

Figure 4: Logs generated by KFSensor when connected to Gautam Buddha University, Greater Noida, INDIA network

172192250 - Katikay-PC	10	Stat	Duration	Pro.,	Sers	Name	Visitor	Sig. Message	Received	_
17219.2.251 - MBA	8475	54/2012 11-30-33 PM	0.000	109	67	DHOP	17219317		DHCP: Boot Request(0.4)Handwar.	
172192252 - deven-PC	8462	54/20211211-29-23 PM_	0.000	LOP	67	DHCP	17219317		DHCP. Boot Request(0A)Hardwar	
172192253 - Vodafone-PC	@ 4348	5/4/2012 11:27:44 PM	0.000	LOP	1211	UDP Packet	17219317		100 02 801dpps////6bv/eha5fm4kzs_	
1/219/200- Apporniayant-PC	0 4306	5/4/2012 11/27/24 PM_	0.000	LOP	1211	UDP Packet	17219317		(00.02.80)dpp:///iBbvieho5fm4kzs	
1/22533	@ 4262	5/4/2012 11-27-04 PM_	0.000	UDP	1211	UDP Packet	17219317		\$00.02.803dpp:///i8bivehq5fm4kzs	
17710223 MEVENN	@ 4221	5/4/2012 11-26-44 PM	0.000	LOP	1211	UDP Packet	172.19.3.17		(01.02.80)dop:///i8bvieha5fm4kzs	
# 17710350, GLIMENER	@ 4176	5/4/2012 10:17:14 PM_	0.000	UDP	1211	UDP Packet	17219317		(0) 02 803dpp.///dbv/ehg5/m4kzs	
172193300-1FN0N0-9C	@ 4174	54/202 10:16:54 PM	0.000	LEP	1211	UDP Packet	17219317		(0) 02 80)dpp:////8bviehg5fm4kzs	
172193110	@ 4171	5/4/2012 10:16:34 PM	0.000	LOP	1211	UDP Packet	172.193.17		(00.02.80)dpp:////dbv/ehq5fev4kzs	
172193138 - sami-PC	@ 4357	5/4/2012 10:16:14 PM	0.000	UCP	1211	UDP Packet	17219317		(01.02.80)dpp:///6bviehq5fm4kzs	
172193363 - abhishek-PC	@ 4363	5/4/202101554 PM	0.000	LOP	1211	UDP Packet	17219317		[00.02.80]dpp:///ifbviehq5fm4kzs	
17219336 - kame-PC	@ 4350	5/4/2012 10:15:34 PM_	0.000	LOP	1711	UDP Packet	17219317		(00.02.80)dpp:///dbviehq5fm4kzs	
172193176	@ 4156	5/4/2012 10:15:14 PM	0.000	109	1211	UDP Packet	17219317		(0) 02 80)dpp:///iBbviehq5fm4kzs	
172193180	@ 4153	5/4/2012 10:14:54 PM	0.000	UDP	1211	UDP Packet	17219317		(01.02.80)dpp:////8bs/ehq5fm4kzs	
172193182 - HP-HP	@ 4348	5/4/2012 10:14:34 PM	0.000	LOP	1211	UDP Packet	17219317		(01.02.80)dpp:////8bviehq5fm44zs	
\$ 172193.192 - RANSCIM-PC	@ 4144	5/4/2022101414 PM	0.000	UCP	1211	UDP Packet	17219317		(00.02.80)dpp:////dbviehq5fm4kzs	
172193196 - Lyna/Ultimate	@ 4137	5/4/2012 10:13:54 PM	0.000	UDP	1211	LIDP Packet	17219317		(0) 02 80]dpp:///ifbviehq5fm4kzs	
172193197 - jtendra-PC	\$ 4129	54/202 10:13:34 PM_	0.000	UDP	1211	UDP Packet	17219317		(01.02.80)dpp:///i6bviehq5fm4kzs	
172.19.3.299 - Gremio	@ 4125	5/4/202101314 PM_	0.000	LOP	1211	UDP Packet	17219317		(01.02.80)dpp:///i8bviehq5fm4kzs	
21/10/32/W	3 4122	54/202101306 PM_	0.000	UDP	67	DHCP	17219317		DHCP: Boot Request(04)Hardwar	
1/219/201 • Hpubligh Heu	@ 4120	5/4/2012 10:12:54 PM	0.000	UDP	1211	UDP Packet	17219317		(XI 02 80)dpp:///dbviehq5fm4kzs	
172103392, shan.90	0 1015	\$4/2012 10:12:33 PM_	0.000	LOP	1211	UDP Packet	17219317		[01 02 81]dpp:///f8bviehq5fm4kzs	
177193.74 - Jonie - FC	@ 1718	51478412 310.36 PM.364	0.000	UDP	1	UDP Packet	12219317		(0) 02 80)dpp:///i6bviehq5fm4kzs	
172193.375 - NAGAR-PC	\$1717	5/4/201 310.26 PM.838	0.000	101	1211	DOS Attack	17239217		Connections: 250(00 0A)Active C	
177193206-UI-PC	@ 1716	5/4/28/2310/06 PM.300	0.000	unk	1711	UDP Packet	172317		(0) 02 80)dppu///i8bviehq5fm4kzs	
172193.007 - GUPTA-ELECTRICAL	000	4/2012 34946 PM.372	0.000	UDP	184	UDP Parket	17219317		(01.02.80]dpp:///i8bviehq5fm4kzs	
172193209 - dhamendra-PC	@ 1714	5-05012 109-26 PM 372	0.000	UCP	1711	UDP Partet	17219317		(01.02.80)dpp:///i8buiehq5fm4kzz	
172193210 - Himare-HP	@ 1713	54/201 1906 PM.384	0.000	LOP	1211	UDP Parket	17219317		[00.02.80]dpp:///i8bviehq5fm4kzs	
172193211 - nic-PC	@ 1712	\$4/2023/08 PM/48	0.000	UDP	1711	UDP Parket	17219317		(0) 02 80)dpp:///6bviehq5fev4kzs	
172193212 - Eminem-PC	@ 1711	5/4/2012 308:26 PI 102	0.000	UDP	1211	UDP Parket	17219317		(00.02.80)dpp:///i8bviehq5fm4kzs	
172193215-AKA94-PC	@ 1710	54/202 30806 PM 413	000	LOP	1211	UDP Parket	17219317		(00.02.80)dpp:///idbviehq5fm4kzs	
# 177193716. turkhonis.Dr	@ 1709	5/4/2012 3:07:46 PM.427	100	LOP	1211	UCP Parket	17219317		(01.02.80)dpp:///ifbiviehq5fm4kzs	
	1.000			1						

Figure 5: Attack noticed when connected to GBU main network

5

Properties	KFSensor
Detect novel attacks	Yes
Sends Alert by Email	Yes
Easy Administration	Yes
User Friendly	Yes
System Requirements	Low
Detect attacks from other nodes which do not communicate to it	NO
Risk (Taken over by the bad guys)	Very High
False Alarm	Lesser
Host Based/Network Based	Host Based

Table 1: Characteristics observed through overall experiment of KFSensor

3.2 ANALYSIS OF PHASE 2

The detailed analysis of Phase 2 is given as-



Figure 6: FlowMatrix showing the alert which is not capture by KFSensor

In phase 2 we have studied FlowMatrix and we find that it not only detects an attack, where the systems are directly communicating with the server "where FlowMatrix is installed" but also, it can detect those attacks where the nodes are not directly communicating with server. This is the major advantage and main motive of hybridizing KFSensor with FlowMatrix. Figure 7 shows the ids KFSensor and the network activities on 11th April between 11 a.m. to 1:05 p.m.

listors	p	Sat	Duration	Patacal	Setson Port	Nare	Votor	Sc. Mettage	Riceved
111125-16924023075	12	4012021041781-	4.000	102	22	554	GUHP		
1 21.1.1.21-98/-19	321	401202125211PM	0.000	UDP	161	389	GL+P		0602010000405(public)4107020
1 211.0 - 20.47	30	401(20121252.06PM	0.000	UDP	161	989	(B)+F		0102 01 00 04 05 public 41 17 02 0
-	12	4)1(20121252.0. PM	0.000	UDP	161	989	COUHF.		06020100040506664117020
	138	4)1(20121250 3"PM	3.063	107	4599	sadnin	(CL)+P		
	10	MR HC 02512105(11)+	3,047	107	21	ED.	(QUHP		
	13	4)1(20121249.55 PM	0.000	107	409	sednin	GUHP		
	13	4/11/2012 12:49:55 PM	0.000	107	21	FTP	63.44		
	14	4)1120121249-55PM	0.000	107	499	sedim	8.44		
	23	4)1,201212-49-55 PM	0.000	107	21	FTP	8,44		
	122	4)1(2012124858PM	0.000	10	4299	selm	63.HP		
	121	4)11/2012124858 PM	0.000	107	21	E19	68,44		
	130	4)1(2021244-35PH	0.000	10	3306	MySQL Service	(B)+#		
	\$19	401(20121244:SIPM	0.000	107	8080	IS hury	63,+4		
	33	4)1(20121244-35PM	0.000	109	3138	Bhury	63.HP		
	11	4)11(20121244-25PM	0.000	107	1631	SQ Server	68,0+4		
	15	41120121244-SIPM	0.000	107	1080	5005	BHP.		
	15	401,20121244-21PM	0.000	107	110	ADPS .	8.4		
	AH.	41120121244-23PM	0.065	10	3	9/17	61.14		(unimer)
	1 th	4)1,00121244-03FM	0.05	107	23	feiet	63.1+F		
	1t	41120212442388	0.000	10	53	th5	63.1+4		
	PI	4)1(20121244-23PM	0.000	107	3	Pat Son Ner.	63,1+4		Rossble Port Scan (00 04 00 34) Th
	1 20	4)1(20121244-23PM	0.000	107	22	55H	8.44		
	1	4)11,12012 12:44 23 PM	0.000	10	21	FTP	8.4		
	1	4)11(20121239.44 PM	30.06	10	3128	IS have	BUHP		
	國;	4/11/2012 12-01 (0 PM	0.000	UDP	138	MST DeLegram	HP32408238375		NET DORAW Radiet: Id:12808 Type:

Figure 7: KFSensor detecting activities by only those node which directly communicate with it

We ran both FlowMatrix and KFSensor together but we can see that the results are entirely different in FlowMatrix and KFSensor. The alert in FlowMatrix is different from KFSensor. In figure 8 we can see both KFSensor and FlowMatrix together and find that it is FlowMatrix which is showing an alert however in the KFSensor there are no such warnings or alert.

	10	Ret	Duration	Protocol	Sensor Port	Nate	Vetor Sq	Hessage	Received
A 10.1.1.25 - HP32408238375	12	4/11/2012 1:04:17 PM	4.000	10P	22	594	(BUHP		
3 20.1.1.20 · GUHP	10 31	4/11/2012 12:52:11 PM	0.000	UDP	161	549	(BUHP		08(02 01 00 04 06) with (A1 17 02 0
20.1.1.40 - GUHP	30	4/11/2012 12:52:06 PM	0.000	UDP	161	5MP	(BUHP		0\$(02 01 00 04 06);x8h(A1 17 02 0
	129	4/11/2012 12:52:01 PM	0.000	UDP	161	5MP	(8UHP		0\$(02.01.00.04.06);w8k(A1.17.02.0.
	0.20	4/11/2012 12:50:37 PM	3.063	TOP	4099	radmin	(20HP		
	20	4/11/2012 12:50:34 PML	3.047	TOP	21	F19	(2UHP		
	28	4/11/2012 12:49:55 PM	0.000	10	4099	radmin	QUHP		
	100	4/11/2012 12:49/55 PPL	0.000	10	21	19	CEUHP		
	100	4/11/2012 12:49:35 975	0.000	10	4277	rages -	(8116		
	Xm	4/11/2012 12:40:50 PM	0.000	10	4700	rafeit.	GUR		
-	1.00	4/11/2012 12:49:58 (91	0.000	TOP	21	F19	GUHP		
0	A 20	4/11/2012 12:44:26 PM	0.000	TOP	2006	MdQ Service	GUHP		
1	\$19	4/11/2012 12:44:25 PM	0.000	109	8080	IIS Provy	(BUHP		
nomalous	A10	4/11/2012 12:44:26 /91	0.000	TCP	3128	115 Provy	(BUHP		
	17	4/11/2012 12:44:26 PM	0.000	TOP	1433	SQL Server	(BUHP		
lert m	Å 16	4/11/2012 12:44:25 PM	0.000	TOP	1000	500/5	GUHP		
-	\$ 15	4/11/2012 12:44:23 PM	0.000	TOP	110	POP3	(BUHP		
FSensor	8 14	4/11/2012 12:44:23 PM	0.015	109	25	SHIP	(2014P		QUET[00 0A]
	410	4/11/2012 12:44:23 PM	0.045	TOP	23	Telvet	CBU-HP		
	12	4/11/2012 12:44:23 PML	0.000	TOP	53	(N)	(BUHP		
	100	4/11/2012 12:44:23 PM	0.000	109	25	Port Scan Warn	QUHP		Possible Port Scan, (30 GA 60 GA(Th.
	210	4/11/2012 12:44:23 PML	0.000	10	22	104	CEUHP		
	8	4/11/2012 12:44/23 PPL.	20.014	109	112	THE BARRIER	(8)/#		
	11	4/11/2012 12:41:00 PM	0.000	IDP	130	MET Following	MERTADOTORIES		NET TOTAL Parties IN 17900 Taxet
	,	Anomaly Dete	tion	in Subspac	e #2 (no	rmilized	to threshold))		
								A	nomalous alert Flowmatrix

Figure 8: Comparison between KFSensor and FlowMatrix

Through the table 2 below we can go through the characteristics we had gone through the complete experiment. Thus, we come to know that though FlowMatrix is more prone to unknown attack, yet they can detect more attacks than KFSensor

Table 2: Characteristics observed while doing experiments with FlowMatrix

Properties	FlowMatrix
Detect novel attacks	Yes
	No(Some Anomaly Based
Sends Alert by Email	IDS do send Alerts by
	Email)
Easy Administration	Lesser than KFSensor
User Friendly	Yes
System Requirements	High
Detect attacks from other	
nodes which do not	Yes
communicate to it	
Risk (Taken over by the bad	VoruLow
guys)	very Low
False Alarm	Higher
Host Based/Network Based	Network Based

3.3 ANALYSIS OF PHASE 3

In phase 3 we have studied both KFSensor and FlowMatrix together and found that if we use both KFSensor and FlowMatrix together, it can become a much effective IDS. As through honeypot we can find out all those new attacks where an attacker directly communicates with KFSensor and through FlowMatrix we can detect attacks where nodes are directly or indirectly communicating with FlowMatrix. As in phase 1 we have shown that KFSensor only recognize those attacks where a node communicate with it thus all other attacks goes undetected which are detected by FlowMatrix. Figure 9 shows that as the node with ip address 20.1.1.20 do DoS attack to node with IP address 10.1.1.25 it gives an alert. However if the node try to do DoS attack to some other network devices other than server then KFSensor will not give an alert to an administrator.

File	View Scenario Signatures Setti	ngs Help						
3	🛢 🗟 🝕 🤱 計 👭 🕷	•	😫 🔍 🖬 🔒 🏭 🖉 🛽	11 🗹 🛠 🗄	2			
Ξ	Visitors	ID	Start	Duration	Protocol	Sensor Port	Name	Visitor
	10.1.1.1 - Recent Activ	0 5	3:19:55 PM.789	0.000	ICMP	0	ICMP Echo	GBU-HP
	10.1.1.25 - HP1918782	07	3:19:56 PM.803	0.000	ICMP	0	ICMP Echo	GBU-HP
	20.1.1.20 - GBU-HP - R	X 9	3:19:57 PM.817	0.000	ICMP	0	ICMP Echo	GBU-HP
	20.1.1.40 - BU-HP - R	O 11	3:19:58 PM.831	0.000	ICMP	0	ICMP Echo	GBU-HP
	-	O 13	3:19:59 PM.845	0.000	ICMP	0	ICMP Echo	GBU-HP
		OP 15	3:20:00 PM.859	0.000	ICMP	0	ICMP Echo	GBU-HP
		O 17	3:20:01 PM.873	0.000	ICMP	0	ICMP Echo	GBU-HP
		O 20	3:20:02 PM.886	0.000	ICMP	0	ICMP Echo	GBU-HP
		<u></u> 22	3:20:03 PM.900	0.000	ICMP	0	ICMP Echo	GBU-HP
		O 24	3:20:04 PM.914	0.000	ICMP	0	ICMP Echo	GBU-HP
		O 26	3:20:05 PM.928	0.000	ICMP	0	ICMP Echo	GBU-HP
		O 28	3:20:06 PM.942	0.000	ICMP	0	ICMP Echo	GBU-HP
		O 30	3:20:07 PM.956	0.000	ICMP	0	ICMP Echo	GBU-HP
		O 32	3:20:08 PM.970	0.000	ICMP	0	ICMP Echo	GBU-HP
		Q 34	3:20:09 PM.984	0.000	ICMP	0	ICMP Echo	GBU-HP
1		0 36	3:20:10 PM.998	0.000	ICMP	0	ICMP Echo	GBU-HP
	Network activity	O 38	3:20:12 PM.012	0.000	ICMP	0	ICMP Echo	GBU-HP
	by node 20.1.1.20	0 40	3:20:13 PM.026	0.000	ICMP	0	ICMP Echo	GBU-HP
		Q 42	3:20:14 PM.040	0.000	ICMP	0	ICMP Echo	GBU-HP
		Q 44	3:20:15 PM.054	0.000	ICMP	0	ICMP Echo	GBU-HP
		Q 46	3:20:16 PM.068	0.000	ICMP	0	ICMP Echo	GBU-HP
		9 48	3:20:17 PM.082	0.000	ICMP	0	ICMP Echo	GBU-HP
		9 50	3:20:18 PM.096	0.000	ICMP	0	ICMP Echo	GBU-HP
		0.52	3:20:19PM:110	0.000	ICMP	0	ICMP Echo	GBUTHP
	(X 54	3:20:20 PM.156	0.000	ICMP (0	DOS Attack	GBU-HP
		\$ 55	3:20:20 PM.129	0.000	ICMP -	0	ICMP Echo	GBU+HP
						1		
				~				1
			DOS(Denial of Serv	vice) attack	by 20.1.1.4	0 detected	lby	
			KFSensor					
1								

Figure 9: Node with IP address 20.1.1.20 does DoS attack to node with IP address 10.1.1.25

Thus we deploy yet another ids with KFSensor i.e. FlowMatrix which is capable of detecting those attacks in the network which goes undetected by KFSensor. Figure 10 will shows that an attack which goes undetected by KFSensor is detected by FlowMatrix.



Figure 10: Attack which goes undetected by KFSensor is detected by FlowMatrix.

In	Figure	11	we	can	find	the	com	bine	log	from	KFSen	sor
an	d Flowl	Mat	trix									



🕴 KFSensor Protessional - Evalu	ation Trial									
File View Scenario Signatures Sett	ings Help									
38843843	٩ C	I R L A A Z		* *						
🗄 🧏 Visitors	D	Ĵøi	Duration	Protocol	Sensur Port	Nane	Yelur	Sig. Nessage	Rocived	
-10 1.1.25 - IP12401230375	12	4/11/2012 1:04:17 PM	4.000	10P	22	59H	GUHP			
	31	4/11/2012 12:52:11 PM	0.000	LEP	161	SMP	GUHP		0\$(02 01 00 04 06)public(%), 17	020
🛔 2011.40+20HP	30	4/11/2012 12:52:06 PM	0.000	LEP	161	SMP	GUHP		0\$(02 01 00 04 06)public(%), 17	020
	32	4/11/2012 12:52:01 PM	0.000	LEP	161	SMP	GUHP		0\$(02 01 00 04 06)public(%; 17	020
	28	4/11/2012 12:50:37 PM	3.063	10P	\$829	radinin	GUHP			
	30	4(11)2012 12:50:31 PM	307	10P	21	FTP	GUHP			
	126	4(11)2012 12:49:55 PML	0.000	10P	\$829	radinin	GUHP			
	<u>3</u> 2	4)11)2012 12:49:55 PM	0.000	10P	21	FTP	GUHP			
	024	4)11)201212:49:55 PM	0.000	10P	4099	radnin	GUHP			1
	32	4)11)2012 12:49:55 PM	0.000	10P	21	FTP	GUHP	No		
	022	4/11/2012 12:48:58 PM	0.000	10P	6899	radnin	GUHP		,	
	321	4)11)2012 12:48:58 PM	0.000	10P	21	FTP	GUHP	Anom	alous	
	Å 20	4)11)2012 12:44:25 PML.	0.000	10P	3326	MySQL Service	GUHP	found	in	
	19	4)11)201212:44:25 PML	0.000	10P	8080	IIS Proxy	GUHP	Tound		
	3 18	4)11)2012 12:44:25 PML=	0.000	10P	3128	IS Prozy	GUHP	KFSe	nsor	
	10	4)11)2012 12:44:25 PML=	0.000	10P	1433	SQL Server	GUHP			
	16	4/11/2012 12:44:25 PM	0.000	10P	1080	500/5	GUHP			
	215	4/11/2012 12:44:23 PM	0.000	102	001	POF3	GUHP			
	314	4)11)201212:44:23 PM	005	102	25	SMIP	GUHP		ómímet]	
	Q 13	4)11)201212:44:23 PM	0.05	10P	23	Telnet	GUHP			
	12	4)11)201212:44:23 PM	0.000	1CP	8	ORS	GUHP			
	PII	4(11)2012 12:44:23 PM	0.000	10P	3	Port Scan Warn	GBUHP		Possible Part Scan, (00 0A 00 0	4 л
	10	4(11)2012 12:44:23 PM	0.000	10P	22	29H	COUHP			
	3	1/11/2012 12:11:23 PM	0.000	10P	21	FIP	COUHP			
	38	1(11)2012 12:39:11 PM	30.016	10P	3128	IS Holy	CaUHP			
	87	1/11/2002 12:00:00 PML.	0.000	LEP	138	NBT Detagram	HP32408238375		NET D'GRAM Packet: 18 32908 1	lype:

Figure 11: Combine log from KFSensor and FlowMatrix

Table 3: Characteristics observed while doing experiments with KFSensor and FlowMatrix

Properties	KFSensor	FlowMatrix		
Detect novel attacks	Yes	Yes		
Sends Alert by Email	Yes	No(Some Anomaly Based IDS do send Alerts by Email)		
Easy Administration	Yes	Lesser than KFSensor		
User Friendly	Yes	Yes		
System Requirements	Low	High		
Detect attacks from other nodes which do not communicate to it	NO	Yes		
Risk (Taken over by the bad guys)	Very High	Very Low		
False Alarm	Lesser	Higher		
Host Based/Network Based	Host Based	Network Based		

Through the table 3 above, we can determine the characteristics of both KFSensor and FlowMatrix which we have analyzed throughout the experiments. We can see that the characteristics which are not good for KFSensor are good for FlowMatrix and the characteristics which are not good for FlowMatrix are good for KFSensor. Thus, if we merge both the systems together we can get the better detection system also KFSensor is Host based detection system and FlowMatrix is Network based detection system thus if we deploy both these system together we can get fully secured intrusion detection system.

4. CONCLUSION

We have developed an improved framework for hybrid intrusion detection system in cloud computing to ensure the confidentiality in organization. We have used two technologies for this framework- honeypot technology and anomaly based IDS. For the honey pot technology we have used KFSensor and for anomaly based IDS we have used FlowMatrix. We have given an algorithm and on that basis we designed an architecture and implement it as real time. We have studied the behavior of the implemented system and introduced various attacks which were detected by the system and alert was generated against it. The combined log generated can help the network administrator to take the corrective actions. The work can be further extended by developing a framework to incorporate the anomaly based attacks.

REFERENCES

- [1] Cloud Security Alliance (2010). "Top Threats to Cloud Computing V1.0" Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pd f
- [2] Wang Jun-Jie and Mu Sen, "Security Issues and Countermeasures In Cloud Computing", International Conference On Grey Systems And Intelligent Services (Gsis), in Proc. in IEEE, 2011, Pp. 843-846.
- [3] Meiko Jensen, J"Org Schwenk, Nils Gruschka and Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing", International Conference On Cloud Computing, in Proc. in IEEE 2009, Pp. 109-116.
- [4] Jinzhu Kong, "Protecting the Confidentiality of Virtual Machines Against Untrusted Host", International Symposium on Intelligence Information Processing And Trusted Computing, in Proc. in IEEE, 2010, Pp. 364-368.
- [5] Lucian Popa, Minlan Yu, Steven Y. Ko, Sylvia Ratnasamy, and Ion Stoica, "Cloudpolice: Taking Access Control Out of The Network", Proceedings of The Ninth ACM Sigcomm Workshop On Hot Topics In Networks, ACM. 2010.
- [6] Saketh Bharadwaja, Weiqing Sun, Mohammed Niamat and Fangyang Shen, "Collabra: A Xen Hypervisor Based Collaborative Intrusion Detection System", in International Conference on Information Technology: New Generations in Proc. in IEEE, 2011, Pp. 695-700.
- [7] Jakub Szefer, Ruby B. And Lee, "a case for hardware protection of guest virtual machines from compromised hypervisors in cloud computing", International Conference On Distributed Computing Systems Workshops in Proc. in IEEE, 2011, Pp. 248-252
- [8] Kai Hwang, Ying Chen and Hua Liu, "Defending Distributed Systems Against Malicious Intrusions and Network Anomalies", International Workshop on Security in Systems and networks in Proc. in IEEE, 2005.
- [9] Yu-Xin Ding, Min Xiao and Ai-Wu Liu, "Research and Implementation On Snort-Based Hybrid Intrusion Detection System" in International Conference On Machine Learning And Cybernetics, in Proc. in IEEE, 2009, Pp. 1414-1418.

- [10] Zhi-Hong Tian, Bin-Xing Fang and Xiao-Chun Yun, "An architecture for intrusion detection using honey pot", International Conference on Machine Learning and Cybernetics, in IEEE, (4), Pp. 2096-2100.
- [11] Guan Xin and Li Yun-jie, "An new Intrusion Prevention Attack System Model based on Immune Principle", International Conference on e-Business and Information System Security (EBISS), in IEEE, 2010, Pp. 1-4.
- [12] Roderick Douglas, "Lecture Notes on Cloud Technologies, Sheffield Hallam University, Sheffield, U.K. 2011.
- [13] Andy Bechtolsheim (2008). "Cloud computing", Available: http://netseminar.stanford.edu/seminars/Cloud.pdf
- [14] F5 Networks (2009). "Cloud Computing Solutions" Available: http://www.f5.com/solutions/cloud-computing/
- [15] Cisco (2004) "Cloud", Available: Http://Www.Cisco.Com/Web/Solutions/Trends/Cloud /Index.Html
- [16] Craig Baldinng (2008). "Itg2008 World Cloud Computing Summit", Available: <u>Http://Cloudsecurity.Org/</u>
- [17] Roderick Douglas, "Lecture Notes on Cloud Technologies, Sheffield Hallam University, Sheffield, U.K. 2011.
- [18] Reese, George (2009) "Cloud Application Architectures", O'reilly Media Available: http://shop.oreilly.com/product/9780596156374.do
- [19] Rittinghouse, John (2009) "Cloud Computing: Implementation, Management, And Security" Available: http://lawlist.law.suffolk.edu/highlights/stuorgs/jhtl/book_re views/2009_2010/Josh%20Matloff%20Book%20Review.pdf
- [20] Andrew J. Younge, Robert Henschel, James T. Brown, Gregor Laszewski, Judy Qiu and Geoffrey C. Fox, "Analysis Of Virtualization Technologies For High Performance Computing Environments", Fourth International Conference On Cloud Computing, in Proc. in IEEE, 2011, Pp. 9-16.
- [21] Key Focus (2003) "KFSensor overview" Available: http://www.keyfocus.net/kfsensor/
- [22] Key Focus (2003) "KFSensor overview" Available: http://www.keyfocus.net/kfsensor/download/
- [23] AKMA Lab (2010). "FlowMatrix download" Available: http://www.akmalabs.com/downloads_flowmatrix.php
- [24] CISCO (2008). "Packet Tracer 5.0 Brochure" Available: http://www.cisco.com/web/learning/netacad/downloads/pdf/ PacketTracer5_0_Brochure_0707.pdf
- [25] CISCO (2010). ""Cisco Packet Tracer Data Sheet" Available : http://www.cisco.com/web/learning/netacad/course_catalog/

docs/Cisco_PacketTracer_DS.pdf



He has done his M.Tech in Software Engineering from Gautam Buddha University, Greater Noida, Uttar Pradesh, INDIA. He has got an scholarship from the Uttar Pradesh government to study one semester of his M.Tech from Sheffield Hallam University, United Kingdom. He has also got a life time Cambridge University for ESOL (English

certificate from Cambridge University for ESOL (English Speaking for the Foreign Languages).



Assistant Professor at School of Information & Communication Technology, Gautam Buddha University, Greater Noida, Uttar Pradesh, INDIA. Her teaching areas includes - Networks, Research Techniques in ICT, Sensor Networks, IT Applications and Management. Her research work includes: Performance evaluation of

Information Systems and Networks Consulting Interests : Performance evaluation of Information Systems and Networks MDPs/ FDPs :



Assistant Professor in Department of Computer Science and Engineering in Madan Mohan Malviya Engineering College, Gorakhpur. He is currently doing his Phd work. He has more than 10 years of experience in teaching in various government aided institutions. He has also contributed in several research publications.