



IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 Issue: VI Month of publication: June 2014 DOI:

www.ijraset.com

Call: 🛇 08813907089 🕴 E-mail ID: ijraset@gmail.com

### INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

# An Advanced Hybrid Intrusion Detection System in Cloud Computing Environment

Vikas Singh<sup>#1</sup>, Amit Kumar<sup>#2</sup>, Astt. Prof. Devender Kumar<sup>\*3</sup>

<sup>#\*</sup>Department of Computer Science & Engineering MERI – College Of Engineering & Technology Asanda (Near Sampla) Bahadurgarh, Haryana /

Abstract: Today, Cloud Computing Security (also known as Cloud Security) is the major concern. Cyber-attacks have not only grown to an unimaginable volume but also a sophistication and variety that would have been hard to believe a few years back. Cloud Computing holds the potential to eliminate the requirements for setting up high cost computing infrastructure for the I.T based solution and services that the industry uses. In computer networking, cloud computing is computing that involves a large number of computers connected through a communication network such as the Internet. Cloud computing and Intrusion detection and prevention system are one such measure to reduce these attacks. Different researches have proposed different IDS's time to time. Most of the researchers combine the features of Anomaly based detection methodologies and Signature based methodologies. Intrusion Detection System which is more efficient than the traditional Intrusion Detection System. In this paper, we present a modified Hybrid Intrusion Detection System that combines the advantages of two different detection methodologies. Anomaly based intrusion detection methodology and Honeypot methodology. We use both the IDS individually and then together and maintain the data record time to time. From the data record we find conclusion that the resulting Intrusion Detection System is much better in detection intrusions from the existing Intrusion Detection Systems.

Keywords: IDPS (Intrusion Detection and Prevention System), Hybrid IDS, Cisco Packet Tracer, Flow Matrix, KFSensor, SNORT.

#### 1. INTRODUCTION

Cloud computing represents one of the most significant shifts in information technology many of us are likely to see in our lifetimes. Reaching the point where computing functions as a utility has great potential, promising innovations we cannot yet imagine. Cloud computing is a recent computing model; provides consistent access to wide are distributed resources. It promises to provide a flexible IT architecture, accessible through Internet for light weight portable device.[1][2]. It revolutionized the IT word with its service availability assurance, rapid accessibility and scalability. Cloud computing denotes the infrastructure as a "Cloud" from which businesses and customers are competent and capable to access applications from anywhere in the world using on demand techniques. There are various issues that need to be dealt with respect to security and privacy in a cloud computing scenario.

#### 2. RELATED WORK

There are many researcher have gone through the various security issues related to cloud computing environment. Dimitrios Zissis and Dimitrios Lekkas[2] discussed security issues in cloud computing but they have no method to validate his work. After that Meiko Jensen, Nils Gruschka and Luigi Lo Lacon[3] gives various technical security issues in cloud computing environment. Milan Yo, Lucian Popa, Y.Steven Ko, Sylvia Ratnasmy and Ion Stoica design a hypervisor based cloud police[4] and Seongwook Jin[5] Architectural Support for Secure Virtualization under a Vulnerable Hypervisor.

# INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Other researcher works on developing on Intrusion Detection and Prevention system to stop intruders form attacking. They used hybrid intrusion detection and prevention. Zhi-Hong Tian gives An architecture for intrusion detection using honeypot[6]. After their Andy Bechtolsheim developed a hybrid real time agent based intrusion detection and prevention system for wireless network.

There after a lot of research is being done to combine an anomaly based IDS and Signature based IDS. Kai Hwang, Ying Chen, Hua Liu[7] propose Cooperative anomaly and intrusion detection system (CAIDS). Similarly J.Gomes[8] and his colleague have done research and implement on Snort based hybrid IDS. Emmanuel Hooper[9], An Intelligent Intrusion Detection and Response System Using Hybrid Ward Hierarchical Clustering Analysis.

Some researchers try to integrate honeypot technology to IDS. Honeypot attract an attacker towards it and works in cooperation with firewall. The firewall will stop the intruder visit whose IP address is set in the firewall as blacklist by honeypot technology. Prof. Smita Jawale[10] design architecture for Intrusion Detection System using Virtual Honeypots. This overcomes the problem information overload, false positive, false negative and unknown attacks.

Here we have to propose a new Intrusion detection and prevention system design which is more efficient than traditional IDS. The Intrusion Detection System (IDS) is based on Anomaly Detection Methodology and Honeypot Technology. To implement this system we have design architecture in the computer network lab and collect data to validate the proposed Hybrid Intrusion Detection System.

#### 3. ARCHITECTURE FOR HIDS

First of all we consider a network, simulated and configured on Cisco packet tracer and then implemented it in real time to analyze network properly. Figure 1 shows the network architecture



configured in Cisco<sup>r</sup> packet tracer[11][12]. The network architecture consists of three nodes and a server. Server is connected to router to route data packets to various networking device and to connect LAN to WAN. Behind the router we are using four nodes, one is server and other three are connected to router through a switch. The server communicated with the nodes using router via switch. We have installed two types of Intrusion Detection System. One is based on Honeypot technology and other is based on anomaly IDS. Honeypot can attract the attacker whenever it tries to perform malicious activities over the computer network and later with this system we can make and update their signature in database whereas anomaly based IDS can analyze the network and record the normal traffic and whenever it finds any anomalous activity is warns. Both these system strongly restrict an attacker to attack on computer network. We use KFSensor[13][14] that is Honeypot technology based and FlowMatrix[15] that is anomaly based IDS.

#### 4. RESULT AND STUDY:

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

Phase I. In this phase first of all we studied KFSensor and study the system with KFSensor for 10 days and record some results. In this phase we find that KFSensor is capable to detect those attacks for which different systems directly contact or interact with it but KFSensor cannot detect those attacks which are done by the systems that are not directly connected or interact by it.

Vol. 2 Issue VI, June 2014

ISSN: 2321-9653

# INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Phase II. In this phase we studied FlowMatrix and study the system again for 10 days and record some results. We find that the anomaly detection based FlowMatrix is capable of detecting various attacks either known or unknown attacks in the computer network but it may give various false positives.

2 0.0.0.0 - Activity 2 100.100.100.3 - Activity	and the second second second	2007.5	LOT BOOK)	PLun	DELOCK FOR	Teams.	ARKOL	Dig. 19855
2 100.100.100.3 - Activity	42222	5/7/2014 4:27:13 PM.281	40.031	TOP	21	FTP	5Y512	
	A42017-	5/7/2014 4:27:36 PM.734	0.000	TOP	4899	radmin	5Y512	
169.254.254.7 - Recent Act	42216	5/7/2814 4:27:36 PM.531	0.015	TCP	3128	IIS Proxy	SY512	
169.254.254.38 - Recent A	42215	5/7/201 4:27:36 PM.343	0.000	TCP	1433	SQL Server	SY512	
172.16.2.1 - ABHILEET-LAADPA	A 42214	5/7/2024 4:27:36 PM.343	0.000	TCP	1080	soors /	SY512	
172.16.2.3 - HEMANT-6F31188	A 42213	5/072014 4:27:36 PM.140	0.000	TCP	_113	ident	SY512	
172.16.2.5 - SANDEEP-F28801	42212	5/7/2014 4:27:36 PM.140	0.000	TOP	110	PORS	SY512	
172.16.2.6 - LIBRARY Activity	42211	5/7/2014 4:27:36 PM.140	0.000	TCP	53	DNE	SY512	
172.16.2.7 - Activity	342210	5/7/2014 4:27:36 PM.140	0.000	TCP	25	SMTP	SY512	
2 172.16.2.8 - PRAMOD - Activity	A 42209	5/7/2014 4:27:36 PM. 140	0.000	TOP	22	SSH	SY512	
2 172 16 2 10 - VINAV - Artubu	42200	5/7/2014 1:27:36 PM.140	0.000	TCP	23	Teinet	SY512	
3 173 16 3 11 - CAMPER ALLON	42207	5/7/2014 4127:36 PM.140	0.000	TCP	21	RTP	SY512	
17210211- SHOLEP-15100	42206	5/7/2014 4:27:36 PM.140	0.000	TCP	19	chargen	SY512	
1/2.16.2.200 · SANJAT · ACTIVEY	42205	5/7/2014 4:27 36 PM.140	0.000	TCP	17	Quote of the day	SY512	
Trans.2.212 - Direction - Ac.	42204	5/7/2014 4:27:36 PM.140	0.000	TCP	13	Daytime	SY512	
172.16.20.7 - SYS7 - Addwity	A 42203	5/7/2014 4:27:36 PH.140	0.000	TCP	9	Discard	SY512	
172.16.20.8 - SYS8 - Activity	42202	5/7/2014 4:27:36 104.140	0.000	TCP	7	Echo	SY512	
172.16.20.9 - SYS9 - Activity	\$42185	5/7/2014 4:22:03 PM.515	42.000	TCP	21	FTP	SY512	
172.16.20.10 - SYS10 - Activity	42172	5/7/2014 4:20:15 PM.234	0.219	TCP	21	Teinet	SYS12	
172.16.20.12 - SYS12 - Rec.	\$42069	5/7/2014 3:55:35 PM.091	0.000	TCP	8080	IIS Proxy	SY512	
172-16-20.13 - SY513 - Addvity	42068	5/7/2014 3:55:35 PM.031	0.000	TCP	4899	radmin	SY512	
172.16.20.14 - 5Y514 - Activity	42067	5/7/2014 3:55:35 PM.031	0.000	TCP	3188	IIS Proxy	SYS12	
172.16.20.42 - 5Y542 - Activity	42066	5/7/2014 3:55:34 PM.828	0.000	TCP	1133	SQL Server	SY512	
172.16.20.43 - 5YS44 - Activity	42065	5/7/2014 3:55:34 PM.828	0.000	TOP	1080	500/5	SY512	
172.16.20.249 SYS5 - Activity	A 42064	5/7/2014 3:55:34 PM.640	0.000	TCP	113	ident	5Y512	
172.16.22.242 SY56 - Activity	\$42063	5/7/2014 3:55:34 PM.640	10.000	TCP	110	POP3	SY512	
8	42062	5/7/2014 3:55:34 PM.640	0,000	TCP	53	DNS	SY512	
	342061	5/7/2014 3:55:34 PM.640	0.000	TCP	25	SMTP	SY512	
	42060	5/7/2014 3:55:34 PM.640	0.080	TCP	23	Teinet	SY512	
	42059	5/7/2014 3:55:34 PM.640	0.000	TOP	22	55H	SY512	
	\$42058	5/7/2014 3:55:34 PM.640	0.000	TOP	21	FTP	SY512	
	42057	5/7/2014 3:55:34 PM.625	0.000	P	17	Quote of the day	SY512	
	Q 42056	5/7/2014 3:55:34 PM.625	0.000	TAP	/ 19	chargen	SY512	
	42055	5/7/2014 3:55:34 PM.625	0.000	TOP	13	Daytime	SY512	
	42054	5/7/2014 3:55:34 PM.625	0.000	TOP/	2	Discard	SY512	
	(0, 42053	5/7/2014 3:55:34 PM.625	0.000	TOP	1 7	Echo	5Y512	6
2	D.			1	1			
	-			1		Server	Running Visitors: 25	Events: 70/13
tart 👘 / dvanced Port Sca	mii 🏘	#Sensor Professiona					19 😤	R ( ) 180
	1. 191				1		7 /	
Shows Nodes with	TP add	tress	-	COL	Courses att.	ale dataata.	1 1	

Figure 2: Network activities of all the nodes and attacks by the three nodes 172.16.20.10, 172.16.20.11, 172.16.20.12

Phase III: in this phase we installed both KFSensor and FlowMatrix and study a system again for 10 days. Here we find the different results that attacks which cannot be detected by KFsensor and detected by FlowMatrix. The combine logs is generated which capture the attacks and than administrator can take corrective actions over the attacks.

Description of all three phases and its result given as

#### 4.1 Analysis of Phase I

There are three nodes for attack with IP address as 172.16.20.10, 172.16.20.11 and 72.16.20.12 and the node with IP address 172.16.20.13 is server FlowMatrix and the node with IP address 172.16.20.14 is server as KFSensor. We create network traffic by the help of different tools like attack ping, port scanner, free SNMP etc. when we attack using these tools some logs are generated. Through log we found that KFSensor generate the

records of only those nodes that are directly connected or communicated with the server and ignore rest nodes. This is the main disadvantage of IDS which include only honeypot technology. Hense, we have also use flowmatrix which is anomaly based IDS. We found some differences in the anomaly graph of FlowMatrix if the attacks takes place at some other point in the network which are not captured by KFSensor. Figure 2 shows the network activity of all the nodes and the attacks made by three nodes.

Both Intrusion Detection System FlowMatrix and KFSensor has their own way of detecting attacks. KFSensor based on honeypot technology can attract the attacker towards itself. Figure 3 given below shows that the FlowMatrix is based on anomaly based methodology and it is capable of detecting all types of attacks in network.



Figure 3: FlowMatrx (Anomaly Based IDS)

#### 4.1.1 Analysis of KFSensor at Personal 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 Personal network. We have analyzed it on 3<sup>rd</sup> May in between 03-04 p.m. and get some valid results, some attacks were also noticed

# INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

KFSensor Professional - Evaluation	Trial	the later is a	-	-	-	-	the second s	a Brandit Law	- 0 <mark>- X</mark>
File View Scenario Signatures	Settings	Help	_	_	_	-			
0 0 0 4 9 PH 1 W	-		77 60	Val	N				
3 3 3 3 Yular	C =								
60 172 220 222 . Rece	D	Start	Duration	Protocol	Sensor Port	Name	Visitor	Sig. Message	Received
107.160.3.134 - Recen	221	3/6/2014 3:47:20 PM.286	21.208	TCP	1433	SQL Server	116.202.204		
116,202,91,100 - Rece-	220	3/6/2014 3:47:20 PM.979	13.193	TCP	1433	SQL Server	116.202.204	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Typ
116,202,91,254 - Rece-	219	3/6/2014 3:45:50 PM.052	60.004	TCP	1433	SQL Server	116.202.99.22		
116,202,99,22 - Recen_	218	3/6/2014 3:46:36 PM.929	0.184	TCP	1433	SQL Server	116.202.91.2	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 00 0A]TDS Packet: Num:2 Typ
116,202,204,15 - Rece.	217	3/6/2014 3:46:35 PM.926	0.274	TCP	1433	SQL Server	116.202.91.2	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Typ
199.83.94.77 - unassigne	3 216	3/6/2014 3:46:34 PM.662	0.243	TCP	1433	SQL Server	116.202.91.2	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Typ
222.186.10.53 - Recen_	215	3/6/2014 3:46:23 PM.521	5.701	TCP	1433	SQL Server	116.202.91.2		
	3 214	3/6/2014 3:46:33 PM.351	0.175	TCP	1433	SQL Server	116.202.91.2	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Typ
	213	3/6/2014 3:46:28 PM.003	0.613	TCP	1433	SQL Server	116.202.91.2	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Typ
	3 212	3/6/2014 3:46:31 PM.131	0.156	TCP	1433	SQL Server	116.202.91.2	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Typ
	3211	3/6/2014 3:46:25 PM.263	0.263	TCP	1433	SQL Server	116.202.91.2	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Typ
	210	3/6/2014 3:45:55 PM.560	0.366	TCP	1433	SQL Server	116.202.99.22	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Typ
	3 209	3/6/2014 3:45:53 PM.859	0.221	TCP	1433	SQL Server	116.202.99.22	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 00 0A]TDS Packet: Num:2 Typ
	208	3/6/2014 3:45:52 PM.339	0.321	TCP	1433	SQL Server	116.202.99.22	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Typ
	207	3/6/2014 3:45:51 PM.045	0.210	TCP	1433	SQL Server	116.202.99.22	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 00 0A]TDS Packet: Num:2 Typ
	3 206	3/6/2014 3:45:10 PM.477	2.960	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0(00 0A)Login Details:(00 0A) Host: 5
	205	3/6/2014 3:45:09 PM.682	0.007	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0(00 0A)Login Details(00 0A) Host: 5
	3 204	3/6/2014 3:45:08 PM.776	0.001	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.000 0A/Login Details(00 0A) Host: 5
	203	3/6/2014 3:45:07 PM.911	0.000	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0(00 0A)Login Details(00 0A) Host: 5
	3 202	3/6/2014 3:45:04 PM.200	0.001	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0(0D 0A)Login Details(0D 0A) Host: 5
	3 201	3/6/2014 3:45:03 PM.171	0.001	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0(0D 0A)Login Details(0D 0A) Host: 5
	3 200	3/6/2014 3:45:02 PM.371	0.009	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0(00 0A)Login Details(00 0A) Host: 5
	199	3/6/2014 3:45:01 PM.598	0.012	TCP	1433	SQL Server	222.186.10.53	9Qt Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0(0D 0A)Login Details(0D 0A) Host: 5
	199	3/6/2014 3:45:00 PM/877	0.010	TOR	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0(00 0A/Login Details(00 0A) Host: 5
	197	3/6/2014 3:45:00 PM.044	0.001	TCP	( 1433 :	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0(0D 0A)Login Details(0D 0A) Host: 5
	196	376-3014 3:44-58 PM.975	0.093	JCP	1453	SQL Server	222.186.10.53	SQL Server lagen ättempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0(00 0A)Login Details:(00 0A) Host: 5
	195	3/6/2014 3:44:58 PM.023	0.002	TCA	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0(00 0A(Login Details(00 0A) Host: 5
	194	3/6/2014 3:44:57 PM.238	0.002	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0(0D 0A)Login Details:(0D 0A) Host: 5
	193	3/6/2014 3:44:56 PM.423	0.006	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0(0D 0A)Login Details:(0D 0A) Host: 5
	192	3/6/2014 3:44:55 PM.216	0.138	TCP	163	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0(0D 0A)Login Details(0D 0A) Host: 5
	191	3/6/2014 3:44:51 PM.308	0.001	TCP	1433	SQL Server	222.186.10.53	QL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0(0D 0A]Login Details(0D 0A] Host: 5
	1 100	315 /301 # 3.44.50 Di # 540	0.007	TCB	1177	mir.	222 100 10 52	·····	TOCOL ALL MARKET THE 1440 THE ALL TOMODAY LA DAUGHO BHT HERE C
,	r			-	-		/		C
0.0	-			/	_	A	tacks by 199.8	3.94.77	Server: Visit Visitors: 8 Events: 221/221
		C 14 6	0 6						- Q. 13 347 PM
									3/6/2014

Figure 4: KFSensor at Personal networks

In the table 4 below we have analyze 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 taken over by bad guys and also they are not capable to detect attack from those user who do not directly communicate with it.

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	NO
Don't Communicate to it	
Risk (Taken over by the bad guys)	Very High
False Alarm	Lesser



Table 1: Characteristics observed through overall experiment of KFSensor

### 4.2 ANALYSIS OF PHASE 2

The detailed analysis of Phase 2 is given as-



Figure 5: FlowMatrix showing the alert which is not capture by KFSensor

In phase 2 we have studied Flowmatrix and we find that it not only detect 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 6 shows the IDS KFSensor and the network activities on 14<sup>th</sup> May between 09 a.m. to 11:00 a.m

# INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

🕻 KFSensor Professional - Evaluation Trial 🗧 🛛 🖉									
File View Scenario Signatures Setti	ngs Help								
😔 🛢 😫 🝕 🤱 計 뷰 뽂	-t - 0	🛯 🔍 🖬 📾 🔐 Z	i 🛍 🔟	*	N				
🖃 🧏 Visitors	ID	Start	Duration	Pr	Sens	Name	Visitor	Sig. Message	Received 🔥
172.16.2.5 - SANDEEP-F	O 49	5/14/2014 10:24:54 AM	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 0B 84 00 01 0
172.16.2.7 - Recent Ac	O 48	5/14/2014 10:24:42 AM	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]<[00 01 0
172.16.20.10 - SY510	O 47	5/14/2014 10:24:35 AM	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]D[00 01 0(
3 0.0.0.0 - Recent Activity	8 46	5/14/2014 10:24:14 AM	0.000	UDP	138	NBT Datagram	SANDEEP-F280016		NBT DGRAM Packet:
111.235.66.105 - Rece	45	5/14/2014 10:24:10 AM	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]q[00 01 00
169.254.254.31 - Rece	O 44	5/14/2014 10:23:54 AM	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 0B 83 00 01 0
169.254.254.38 - Rece		5/14/2014 10:23:42 AM	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05];[00 01 00
169.254.254.52 - Rece-	42	5/14/2014 10:23:35 AM	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]C[00 01 0(
172.16.2.1 - ABHITEET-LA	O 41	5/14/2014 10:23:10 AM	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]p[00 01 00
172 15 2 3 HEMANT-6	OP 40	5/14/2014 10:23:04 AM	0.000	UDP	17500	Dropbox LAN S	192.168.9.85		{"host_int": 5557303
172 16 20 11 - SVS11 - A	39	5/14/2014 10:22:58 AM	0.000	UDP	138	NBT Datagram	172.16.2.7		NBT DGRAM Packet:
172.16.20.12 SUS12 A	O 38	5/14/2014 10:22:54 AM	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 0B 82 00 01 0
172 16 20 107 SVS 27	137	5/14/2014 10:22:48 AM	0.000	UDP	67	DHCP	0.0.0.0		DHCP: Boot Request
102.160.001 Dasab	O 36	5/14/2014 10:22:42 AM	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]:[00 01 00
192.166.9.65 - Recent	O 35	5/14/2014 10:22:35 AM	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]8(00 01 00
	<b>(</b> ) 34	5/14/2014 10:22:34 AM	0.000	UDP	17500	Dropbox LAN S	192.168.9.85		("host_int": 5557303
	<u>@</u> 33	5/14/2014 10:22:34 AM	0.000	UDP	17500	Dropbox LAN S	192.168.9.85		{"host_int": 5557303
	8,32	5/14/2014 10:22:33 AM	0.000	UDP	138	NBT Datagram	SY510		NBT DGRAM Packet:
	昌 31	5/14/2014 10:22:29 AM	0.000	UDP	138	NBT Datagram	HEMANT-6F31188A		NBT DGRAM Packet:
	O 30	5/14/2014 9:21:13 AM	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]+[00 01 00
	O 29	5/14/2014 9:21:06 AM	0.000	UDP	17500	Dropbox LAN S	192.168.9.85		{"host_int": 5557303
	@ 28	5/14/2014 9:20:57 AM	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 0B 80 00 01 0
	27	5/14/2014 9:20:51 AM	0.000	UDP	138	NBT Datagram	5Y5-27		NBT DGRAM Packet:
	O 26	5/14/2014 9:20:44 AM	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]8[00 01 00
	O 25	5/14/2014 9:20:37 AM	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]@[00 01 0
	<b>10</b> 24	5/14/2014 9:20:36 AM	0.000	UDP	17500	Dropbox LAN S	192.168.9.85		{"host_int": 5557303
	<b>0</b> 23	5/14/2014 9:20:36 AM	0.000	UDP	17500	Dropbox LAN S	192.168.9.65		{"host_int": 5557303
	Q 22	5/14/2014 9:20:13 AM	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]m[00 01 0
	<sup>(9)</sup> 21	5/14/2014 9:19:57 AM	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 0B 7F 00 01 0
	Q <sup>2</sup> 20	5/14/2014 9:19:44 AM	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]7[00 01 00
	B 19	5/14/2014 9:19:43 AM	0.000	UDP	138	NBT Datagram	ABHIJEET-1AADFC		NBT DGRAM Packet:
	18	5/14/2014 9:19:37 AM	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]?[00 01 0C
	B <sup>17</sup>	5/14/2014 9:19:36 AM	0.000	UDP	138	NBT Datagram	SYS11		NBT DGRAM Packet:
	B 16	5/14/2014 9:19:35 AM	0.000	UDP	138	NBI Datagram	57512		NBT DGRAM Packet:
	9 15	5/14/2014 9:19:13 AM	0.000	UUP	5678	UDP Packet	169.254.254.38		
1	14	5/14/2014 9:18:57 AM	0.000	UDP	5678	UDP Packet	169.254.254.31		100 00 0B [~[00 01 0 💌

Figure 6: KFSensor detecting activities by only those node which directly communicate with it

We had run 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 33 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.

8 8 4 <u>7</u> 11 14 %		1 🛛 🔍 🔓 🗃 🖓 🖓 🖬 🗷		*	2				
Visitors	ID	Start	Duration	Pr	Sens	Name	Visitor	Sig. Message	Received
172.16.2.5 - SANDEEP-F_	Q 49	5/14/2014 10:24:54 AM	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 08 84 00 01
172.16.2.7 - Recent Ac	Q 48	5/14/2014 10:24:42 AM	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]<[00 01
172.16.20.10 - SYS10	@ 47	5/14/2014 10:24:35 AM	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]D[00 01
3 0.0.0.0 - Recent Activity	圆46	5/14/2014 10:24:14 AM	0.000	UDP	138	NBT Datagram	SANDEEP-F288016		NBT DGRAM Packet
111.235.66.105 - Rece	@ 45	5/14/2014 10:24:10 AM	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]q[00 01
169.254.254.31 - Rece	@ 44	5/14/2014 10:23:54 AM	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 08 83 00 01
169.254.254.38 - Rece	@ 43	5/14/2014 10:23:42 AM	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05];[00 01
169.254.254.52 - Rece	@ 42	5/14/2014 10:23:35 AM	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]0[00 01
2 172.16.2.1 - ARHONET-1A	@ 41	5/14/2014 10:23:10 AM	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01];(00 01
172.16.2.3 - HEMANT-6	Q 40	5/14/2014 10:23:04 AM	0.000	UDP	17500	Dropbox LAN S	192.168.9.85		("host_int": 55573
2 172 16 20 11 - 6 11 - 6	圆 39	5/14/2014 10:22:58 AM	0.000	UDP	138	NBT Datagram	172.16.2.7		NBT DGRAM Packet
172.16.20.11 - STS11 - A	O 38	5/14/2014 10:22:54 AM	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 08 82 00 03
A 172-16-20-12 - 31512 - A	1 37	5/14/2014 10:22:48 AM	0.000	UDP	67	DHCP	0.0.0.0		DHCP: Boot Reque
1/2.16.20.19/ - 515-2/	@ 36	5/14/2014 10:22:42 AM	0.000	UDP	5678	LIDP Packet	169.254.254.52		[00 00 05]:[00 01
192.168.9.85 - Recent	@ 35	5/14/2014 10:22:35 AM	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]B[00 01
	Q 34	5/14/2014 10:22:34 AM	0.000	UDP	17500	Dropbox LAN S	192.168.9.85		{"host_int": 55573
	0 32	5/14/2014 10:22:34 AM	0.000	UDP	17500	Dropbox LAN S	192.168.9.85		{"host_int": 55573
	32	5/14/2014 10:22:33 AM	0.000	UDP	138	NBT Datagram	SYS10		NBT DGRAM Packet
	圆 31	5/14/2014 10:22:29 AM	0.000	UDP	138	NBT Datagram	HEMANT-6F31188A		NBT DGRAM Packe
	0 30	5/14/2014 9:21:13 AM	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]n[00 01
	0 0	5/14/2014 9:21:06 AM	0.000	UDP	17500	Dropbox LAN S	192.168.9.85		("host_int": 55573
No anomalous	Q 28	5/14/2014 9:20:57 AM	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 08 80 00 01
	劃27	5/14/2014 9:20:51 AM	0.000	UDP	138	NBT Datagram	SYS-27		NBT DGRAM Packet
alert m	O 26	5/14/2014 9:20:44 AM	0.000	UDP	5678	UDP Packet	169.254.254.52		(00 00 05)8(00 01
FSansor	@ 25	5/14/2014 9:20:37 AM	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]\$[00 01
ST Sensor	@ 24	5/14/2014 9:20:36 AM	0.000	UDP	17500	Dropbox LAN S	192.168.9.85		{"host_int": 55573
	O 23	5/14/2014 9:20:36 AM	0.000	UDP	17500	Dropbox LAN S	192.168.9.85		{"host_int": 55573
	@ 22	5/14/2014 9:20:13 AM	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]m[00 01
	@ 21	5/14/2014 9:19:57 AM	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 08 7F 00 01
	@ 20	5/14/2014 9:19:44 AM	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]7[00 01
	昌19	5/14/2014 9:19:43 AM	0.000	UDP	138	NBT Datagram	ABHIDEET-1AADFC		NET DGRAM Packet
	@ 18	5/14/2014 9:19:37 AM	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]7[00 01
	周17	5/14/2014 9:19:36 AM	0.000	UDP	138	NBT Datagram	51511		NBT DGRAM Packet
	月16	5/14/2014 9:19:35 AM	0.000	UDP	138	NBT Datagram	51512		NBT DGRAM Packe
	@ 15	5/14/2014 9:19:13 AM	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01][00 01 0
	@ 14	5/14/2014 9:18:57 AM	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 08]-[00 01
>	<								



Figure 7: Comparison between KFSensor and Flowmatrix

Through the table 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, they can detect more attacks than KFSensor

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

Table 2: Characteristics observed while doing experiments with Flowmatrix

### 4.3 ANALYSIS OF PHASE 3

In phase 3 we have studied both KFSensor and Flowmatrix together and find that if we used both KFSensor and Flowmatrix together it can became 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 not directly communicate with flowmatrix. As in phase 1 we

# INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

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 32 shows that as the node with ip address 192.165.9.85 do attack to node with IP address 172.16.20.11 it gives an alert. However if the node try to do attack to some other network devices other than server then KFSensor will not give an alert to an administrator.

Visitors	ID	Start	Duration	Pr	Sens	Name	Visitor	Sig. Message	Received
& 0.0.0.0 - Recent Activity	0 68	5/14/2014 11:05:07 AM	0.000	UDP	17500	Dropbox LAN S	192.168.9.85		("host int": 5557;
111.235.66.105 - Rece	0 67	5/14/2014 11:05:07 AM	0.000	LIDP	17500	Dropbox LAN S	192,168,9.85		("host int": 5557.
169.254.254.31 - Rece	<b>B</b> 66	5/14/2014 11:05:04 AM	0.000	UDP	67	DHCP	0.0.0.0		DHCP: Boot Regu
169.254.254.38 - Rece	@ 65	5/14/2014 11:04:55 AM	0.000	UDP	5678	LIDP Packet	169.254.254.31		[00 00 08 AD 00 0
169.254.254.39 - Rece	@ 64	5/14/2014 11:04:43 AM	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]e[00 01
169.254.254.52 - Rece	0 63	S/14/2014 11:04:37 AM	0.000	UDP	17500	Dropbox LAN S	192.168.9.85		{"host_int": 5557
172.16.2.1 - ABHLIEFT	@ 62	5/14/2014 11:04:36 AM	0.000	UDP	5678	LIDP Packet	111.235.66.105		[00 00 10]m[00 0
172.16.2.3 - HEMANT-6-	@ 61	5/14/2014 11:04:30 AM	0.000	UDP	5678	UDP Packet	169.254.254.39		[00 00 00]![00 01
172.16.2.5 - SAMPEEP-E2	60	5/14/2014 11:04:17 AM	0.000	UDP	67	DHCP	0.0.0.0		DHCP: Boot Regu
172 16 2.7 - Decent Ac	@ 59	5/14/2014 11:04:12 AM	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01 9A 00 I
172 16 2 8 . DOAMOD . A	圆58	5/14/2014 11:04:13 AM	0.000	UDP	138	NBT Datagram	ABHIJEET-1AADFC		NET DGRAM Pack
17210.2.0 - FRANCO - H.I.	0 57	5/14/2014 11:04:07 AM	0.000	UDP	17500	Dropbox LAN S	192.168.9.85		{"host_int": 5557
	0 56	5/14/2014 11:04:07 AM	0.000	UDP	17500	Dropbox LAN S	192.168.9.85		("host_int": 5557
172.16.20.11 - 57511	<b>圆</b> 55	5/14/2014 11:04:07 AM	0.000	UDP	138	NBT Datagram	51511		NET DGRAM Pack
172.16.20.12 - SY512 - A	@ 54	5/14/2014 10:25:42 AM	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]-[00 0
172.16.20.13 - SY513 - A	@ 53	5/14/2014 10:25:35 AM	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]E[00 0
172.16.20197 - SYS-27	<b>副</b> 52	5/14/2014 10:25:26 AM	0.000	UDP	138	NBT Datagram	51513		NBT DGRAM Pack
192.168.985 - Recent	圆51	5/14/2014 10:25:24 AM	0.000	UDP	138	NBT Datagram	PRAMOD		NBT DGRAM Pad
	@ 50	5/14/2014 10:25:10 AM	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]/[00 0
	Q 49	5/14/2014 10:24:54 AM	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 08 84 00 1
	Q 48	5/14/2014 10:24:42 AM	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]<[00 0
	@ 47	5/14/2014 10:24:35 AM	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]0[00 0
	昌+6	5/14/2014 10:24:14 AM	0.000	UDP	138	NBT Datagram	SANDEEP-F288016		NBT DGRAM Pad
	@ 45	5/14/2014 10:24:10 AM	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]q[00 0
	@ 44	5/14/2014 10:23:54 AM	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 08 83 00
	@ 43	5/14/2014 10:23:42 AM	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05];[00 0
	@ 42	5/14/2014 10:23:35 AM	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]0[00 0
etwork activity	@ 41	5/14/2014 10:23:10 AM	0.000	UDP	5678	UDP Packet	169.254.254.30		[00 00 01]p[00 0
vnode	Q 40	5/14/2014 10:23:04 AM	0.000	UDP	17500	Dropbox LAN S	192.168.9.85		("host_int": 5557
	1月39	5/14/2014 10:22:58 AM	0.000	UDP	1,38	NBT Datagram	172.16.2.7		NBT DGRAM Pack
	O 38	5/14/2014 10:22:54 AM	0.000	UDP	5678	LEP Packet	169.254.254.31		[00 00 08 82 00 0
	37	5/14/2814 10:22:48 AM	0.000	UDP	67	DHCP	0.0.0.0		DHCP: Boot Reg.
	Q 36	5/14/2014 10:22:42 AM	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]:[00 01
	@ 35	5/14/2014 10:22:35 AM	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]E[00 0
	Q 34	5/14/2014 10:22:34 AM	0.000	UDP	17500	Dropbox LAN S	192.168.9.85		{"host_int": 5557
	O 33	5/14/2014 10:22:34 AM	0.000	DEP	17500	Dropbox LAN S	192.168.9.85		{"host int": 5557

Figure 8: Network activity by Nodes and attacks detected by KFsensor

Thus we have deployed yet another IDS with KFSensor i.e. Flowmatrix which is capable of detecting those attacks in the network which goes undetected by KFSensor. Figure 33 will shows that an attack which goes undetected by KFSensor is detected by Flowmatrix.



Figure 8: Attack which goes undetected by KFSensor is detected by Flowmatrix.

In Figure 9 we can find the combine log from KFSensor and Flowmatrix

# INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)





Properties	KFSensor	Flowmatrix
Detect novel attacks	Yes	Yes
		No(Some Anomaly
Sends Alert by Email	Yes	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	NO	Yes		
communicate to it		2		
Risk (Taken over by the	Very	Very Low		
bad guys)	High	Very Low		
False Alarm	Lesser	Higher		
Host Based/Network	Host	Network Based		
Based	Based	Network Dased		

 Table 3: Characteristics observed while doing experiments with

 KFSensor and FlowMatrix

Through the table 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.

#### 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.

# INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

### LIST OF REFERENCES:

- [1]. Cloud Security Alliance: Top Threats to Cloud Computing V1.0. Available: http://www.cloudsecurityalliance.org/topthreats, 2010.
- [2]. Dimitrios Zissis, Dimitrios Lekkas: Addressing Cloud Computing Security Issues, Future Generation Computer Systems Dec 2010, pp 583-592.
- [3]. Meiko Jensen et. al. : On Technical Security Issues in Cloud Computing, IEEE International conference on Cloud Computing, 2009.
- [4]. Lucian Popa, Minlan Yu et. al. : Cloud Police: Access Control out of the Network, Hotnets, Monterey, CA, USA, Oct 2010.
- [5]. Seongwook Jin et. at. : Architectural Support for Secure Virtualization under a Vulnerable Hypervisor, Appears in the 44<sup>th</sup> Annual IEEE/ACM International Symposium on Microarchitecture, Porto Alegre, Brazil, Dec 2011.
- [6]. Zhi-Hong Tian et. at. : An architecture for intrusion detection using honeypot, International Conference on Machine Learning and Cybernetics, IEEE, Nov 2003, pp. 2096-2100.
- [7]. Kai Hwang et. at. : Defending Distributed Systems Against Malicious Intrusions and Network Anomalies, Parallel and Distributed Processing Symposium, Proceedings. 19th IEEE International, 2005.
- [8]. J. Gomez et. at. : Design of a Snort based Hybrid Intrusion Detection System, International Work-Conference on Artificial Neural Networks, Part- II, 2009. pp 515-522.
- [9]. Emmanuel Hooper, An Intelligent Intrusion Detection and Response System Using Hybrid Ward Hierarchical Clustering Analysis, International Conference on Multimedia and Ubiquitous Engineering, IEEE, 2007, pp 1187-1192.
- [10]. Prof. Smita Jawale et. at. : Intrusion Detection System using Virtual Honeypots, International Journal of Engineering Research and Applications, Mar 2012, pp 275-279.
- [11]. CISCO: Packet Tracer 6.0 Brochure, Available:http://www.cisco.com/web/learning/netacad/do wnloads/pdf/PacketTracer6\_0\_Brochure\_0707.pdf, 2013.

- [12]. CISCO: Cisco Packet Tracer Data Sheet, Available:http://www.cisco.com/web/learning/netacad/cou rse\_catalog/docs/Cisco\_PacketTracer\_DS.pdf
- [13]. Introduction to KFSensor- A windows based honeypot IDS, Available: http://blogs.microsoft.co.il/, Oct 2012.
- [14]. KFSensor- A windows based honeypot IDS download, Available: http://www.keyfocus.net.
- [15]. AKMA Lab: FlowMatrix download, Available:http://www.akmalabs.com/downloads\_flowmatri x.php, 2010.











45.98



IMPACT FACTOR: 7.129







INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 🕓 (24\*7 Support on Whatsapp)