Cloud Computing Based-Collaborative Network Security Management System Using Botnet

Miss Namrata A. Sable
M.E.(Computer science & Engineering),
Department of Computer Science & Engineering,
G. H. Raisoni College of engineering & Management,
Amravati. Maharashtra, India.
e-mail: namratasable10@gmail.com

Prof. Mr. D. S. Datar
Assistant Professor,
Department of Computer Science & Engineering,
G. H. Raisoni College of engineering & Management,
Amravati. Maharashtra, India.
e-mail:dineshdatar@raisoni.net

Abstract**—**Now-a-days due to increase in the users of internet the balancing of traffic in the network becomes most serious issue. Also the internet security is also the important factor in terms of internet worms, spam, phishing attacks and botnet too. Botnet is an internet connected program communicates with other similar program to perform malicious activities and to spread a Distributed Denial of service on the victim computer and also in network. And make that machine or network resource unavailable to its users. The botmaster which hides itself behind a server called Command & control(C & C) Server, and give commands to C & C to attack on the victim hosts and spread bot in the network. In this paper, we design a cloud computing- Based Collaborative Network Security Management System Using Botnet which balances the load in the network and check for each and every file transferring in the cloud for the bot. If the file contains the bot then the folder in which that file is saved, will be deleted from that client. In this way, we design a system to protect the cloud from botnet and prevent the cloud from botnet attack.

Keywords- Cloud Computing, Bot, Botnet Detection, Bootmaster, Command & Control server, Network Load-Balancing.

*****

I. Introduction

Internet is a very important factor for information infrastructure. However, Internet security is big challenge because of many security threats. The main e-crime attacks are spam, phishing attacks, and Internet worms. Botnet[1,2] is a collection of internet-connected computers whose security defences have been breached. Also botnet are the group of compromised computers controlled by one or group of attacker known as "Botmaster"[3]. The most of botmasters usually don't use their PC to control botnet, instead they use public server to transfer command and control to every bot. This server is called command and control server (C&C)[4]. After the Bot code has been installed into the compromised computers, the computer becomes a Bot or Zombie. The major attacks under botnet are, DDos Scanning [5], Phishing, Click fraud, spamming. The main difference between Botnet and other kind of malwares is the existence of Command-and-Control (C&C) infrastructure.

The main aim of the C&C server is to find out the vulnerable computer or machine in the network and directly attack on those vulnerable computers to install bot on those vulnerable computers in the network. In this way the C&C server spread the bots in the network.

Cloud Computing based Collaborative Network Security Management system(CNSMSUB) [6] allows us to check each and every file in the cloud for the detection of bot[7,8] in cloud. If that file contains the bot program then the folder containing the bot file will restrict the other files from that folder to be transferred in the cloud and make that folder unavailable to the network users. Means the Distributed Denial of Service attack (DDoS)[5] will occur over there because of botnet.

After detection of bot in the cloud to suppress [9] that bot from the cloud the folder containing the bot will be deleted by this security system from that client machine. Also this system balances the load in the network so that only one client should not be loaded by the network traffic [10]. The concept of network load-balancing [11,12,13] is applied to balance the network traffic.

In this paper, section 1 gives introduction to botnet and the main aim of the C&C server and botmaster. Section 2 gives the various attacks cause by the botnet[14]. Section 3 introduces the Cloud Computing[15,16]-Based Collaborative Network Security Management system(CNSMSUB) Using Botnet. Section 4 introduces the cloud based analysis of the Network Security Management system. Section 5 gives the experimental results. In section 6 Conclusion is given.

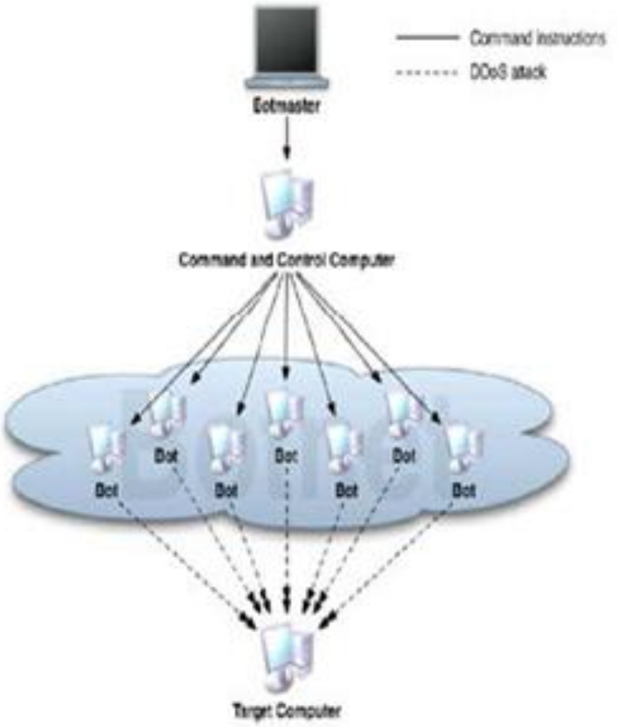


Figure 1.Connection of Botmaster, C&C Server and Botnet

II. Various Attacks by Botnet

There are various kinds of botnet attacks[14] such as:

1. Attack: Email social engineering attacks, promote user to open an attachment and follow an unsolicited link. When link or file exploits system becomes directly infected with malware. These attacks are commonly combined with phishing attacks that attempt to coerce the user into providing sensitive information.
2. Web Client Attack: This is the technique to spread malware through Web. The victim is lured to malicious web sites, often hosted on other systems under the attacker's control, where multiple exploits may be tried in an attempt to compromise vulnerabilities in the victim's browser or system. If successful, the malware is installed without the user's knowledge.
3. Instant messaging attacks: IM contacts are sent unsolicited instant messages from the compromised user's IM account. These messages look legitimate but in reality take the user to malicious web sites or begin the download and installation of malicious files.
4. Distributed denial of service attacks[5]: Current bot variants commonly include the ability to participate in distributed denial of service (DDoS) attacks against internet targets for revenge or profit. The basic idea behind a DDoS is to exhaust some resource required to provide a service, slowing or stopping the ability to process legitimate requests. Flooding attack is common approach to DDOS attack. ICMP and UDP flooding attacks target the bandwidth used to provide service. They spread this message by sending large volume of data that consume all bandwidth of connection. SYN flooding targets the TCP protocol stack. Because the client executing the DDoS attack never sends the final ACK packet required to complete the "TCP 3-way Handshake, the memory used to hold the connection half open is consumed until a timer expires and it is eventually freed.
5. Click Fraud: Click fraud happens when visits are made to an online advertisement or other resource charged to the sponsor on a per-click basis, by illegitimate means. Bots are commonly used to execute click fraud because they can easily be directed to send web requests that represent "clicks" on the internet ads of certain affiliates. These additional "clicks" boost their affiliate revenues paid by the advertisers.
6. Key-logging: Software key loggers capture keyboard events and record the keystroke data before it is sent to the intended application for processing. Data is capture by the spyware prior to encryption. Major targets like, credit card information, authentication credential, email info.

III. Cloud Computing Based Collaborative Network Security Management System

A. *System Design and Implementation*

CNSMSUB[6] means Collaborative Network Security Management System is developed for the prevention of network as well as cloud from botnet attack. The term collaborative refers to the system that is used to provide security to the data transferring from one network to another as well as from one cloud to another. During the systems operation, the collaborative mechanism runs as expected to balance the load in the network, and to check the file transferring in the network as instructed by the security center or the server machine. Figure 2 illustrates the whole procedure of network.

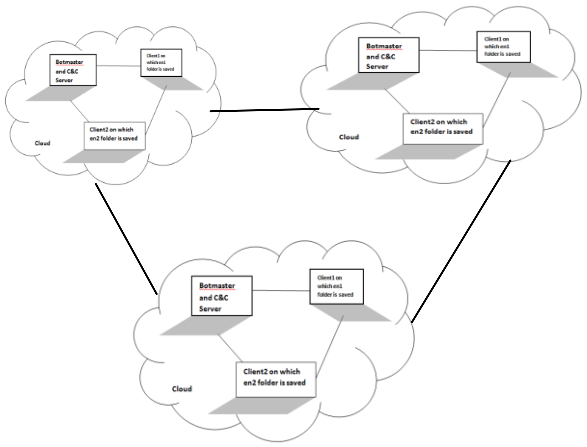
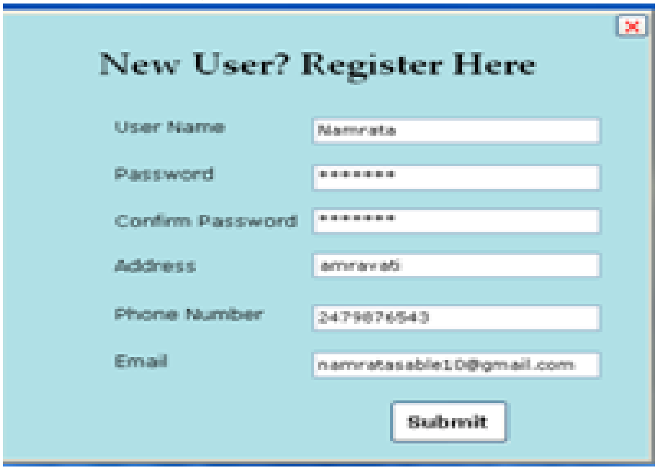

Botmaster and C&C Server
Client1 on which en1 folder is saved
Client2 on which en2 folder is saved
Cloud
Botmaster and C&C Server
Client1 on which en1 folder is saved
Client2 on which en2 folder is saved
Cloud
Botmaster and C&C Server
Client1 on which en1 folder is saved
Client2 on which en2 folder is saved
Cloud

Figure 2. CNSMSUB architecture

CNSMSUB is a cloud based system which balances the traffic in the network by Load-Balancing[11,12,13]. In this system there are one server which may be calles as a C&C[4] server which is used to transfer the data in the network and two client machines Client1 and Client2. This C&C server also act as a Botmaster[3] hides itself behind the server and sends commands to the server to find the vulnerable systems or computers in the network. And to attack on the vulnerable client in the cloud and spread the spread DDoS attack on the infected client. The infected client will not be able to send or receive the data through and from the network.

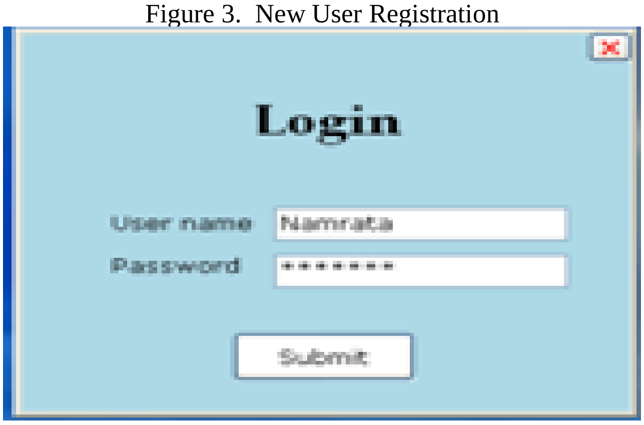
To access this server new user has to register on the server. And the registered user have to login on the server every time to access the server.



New User? Register Here

User Name Namrata
Password *******
Confirm Password *******
Address amravati
Phone Number 2479876543
Email namratasable10@gmail.com

Figure 3. New User Registration



Login

User name Namrata
Password *******

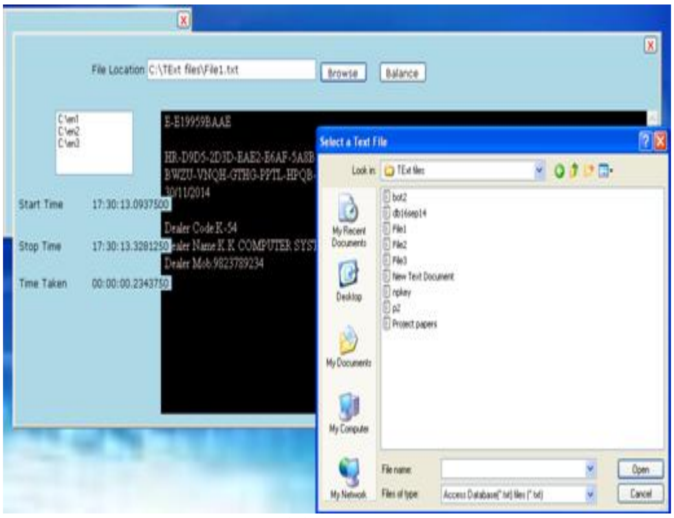
Figure 4. Registered User Login

1. Load Balancing in the Network

The concept of load-balancing is used in CNSMSUB to balances the traffic in the network so that only on client should not be flooded with the network traffic. In load balancing concept we have connected to client to the server machine and created two folders en1 and en2 on two clients respectively. The size of both folder is 1MB. When the file is transferred from the server machine

After login user can transfer file through network. If the user transfer the file less that 1MB the file will save on the en1 folder of client1. But if the file size is more than 1MB then upto 1MB size the file will save on the en1 folder if the client1 and remaining file will save on the en2 folder of the client2.

This is shown in figure below.


File Location C:\TExt files\File1.txt

C:\en1
C:\en2
C:\en3

Start Time 17:30:13.0937500

Stop Time 17:30:13.3281250

Time Taken 00:00:00.2343750

E-E19959BAAE

HR-D9D5-2D3D-EAE2-E6AF-5A8B
BWZU-VNQH-GTHG-PPTL-HPQB
30/11/2014

Dealer Code K-54
Dealer Name K K COMPUTER SYS
Dealer Mob 9823789234

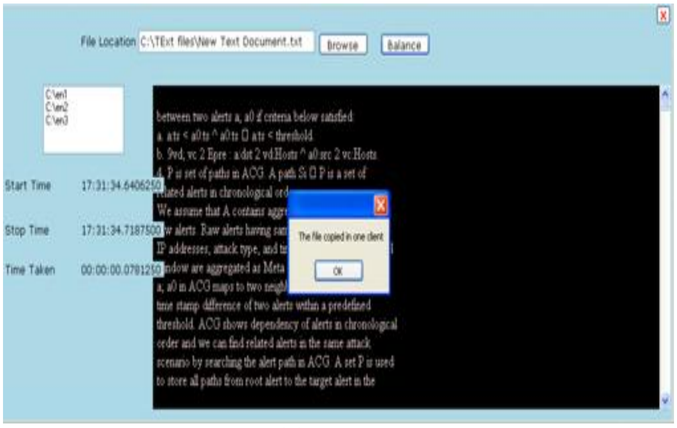
Select a Text File

Look in: TExt files

bot2
db16sep14
File1
File2
File3
New Text Document
npkey
p2
Project papers

File name:
Files of type: Access Database(*.txt) files (*.txt)

Figure 5. Balancing of file having size less than 1MB


File Location C:\TExt files\New Text Document.txt

C:\en1
C:\en2
C:\en3

Start Time 17:31:34.6406250

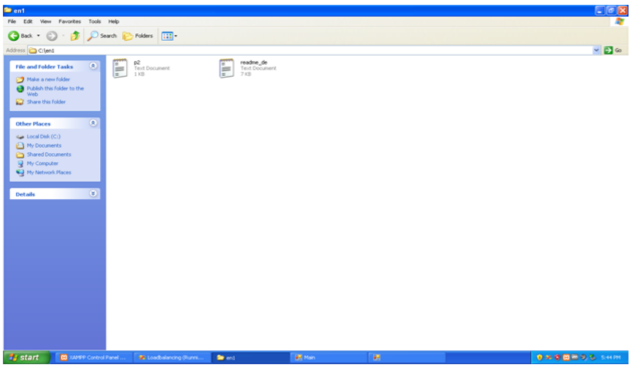
Stop Time 17:31:34.7187500

Time Taken 00:00:00.0781250

between two alerts a, a0 if criteria below satisfied
a. a.ts < a0.ts ^ a0.ts □ a.ts < threshold
b. 9vd, vc 2 Epre : a.dst 2 vd.Hosts ^ a0.src 2 vc.Hosts
4. P is set of paths in ACG. A path Si □ P is a set of
related alerts in chronological ord
We assume that A contains aggr
w alerts. Raw alerts having sam
IP addresses, attack type, and ti
ndow are aggregated as Meta
a, a0 in ACG maps to two neigh
time stamp difference of two alerts within a predefined
threshold. ACG shows dependency of alerts in chronological
order and we can find related alerts in the same attack
scenario by searching the alert path in ACG. A set P is used
to store all paths from root alert to the target alert in the

The file copied in one client

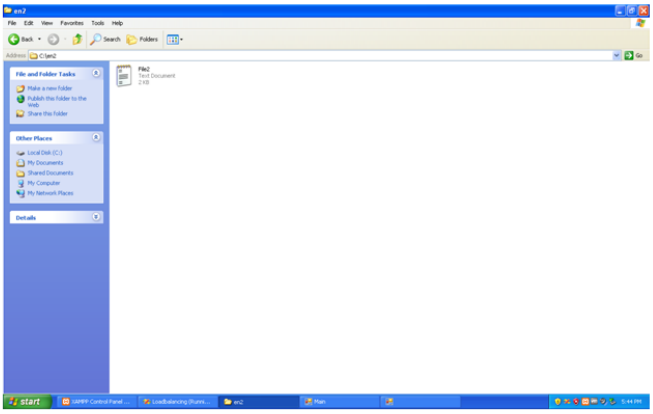
Figure 6. Balancing of file having size more than 1MB


Address C:\en1

p2
Text Document
1 KB

readme_de
Text Document
7 KB

Figure 7. Files in en1 folder of client1


Address C:\en2

File2
Text Document
2 KB

Figure 8. Files in en2 folder of client2

In this way we can balance the traffic in the network. When we transfer the file in the network or in the cloud via serve, the start time, stop time and the time taken by the file to transfer from the server is calculated by the CNSMSUB system. We have analyze the data of four files transferring from the server and the data of file size versus time taken is as follows:

TABLE I. ANALYSIS OF FILE TRANFER THROUGH SERVER

fsize(bits)	time taken(Sec)
3174	6.708
402	0.125
6287	11.718
172	0.125

The graph of the above table can be plotted as:

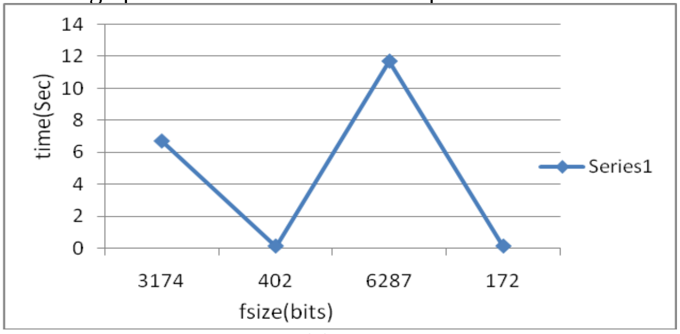


Figure 9. Graph of file size Vs Time taken

From the above graph it is clear that the the file having more size take more time to transfer in the network and vice-versa.

IV. EXPRIMENTAL RESULTS

A. Cheking of Files transferring in Network

The administrator of this CNSMSUB system keep the data of all the files transferred in the network through server in its database and that files can be check for bot. this is shown in figure below:

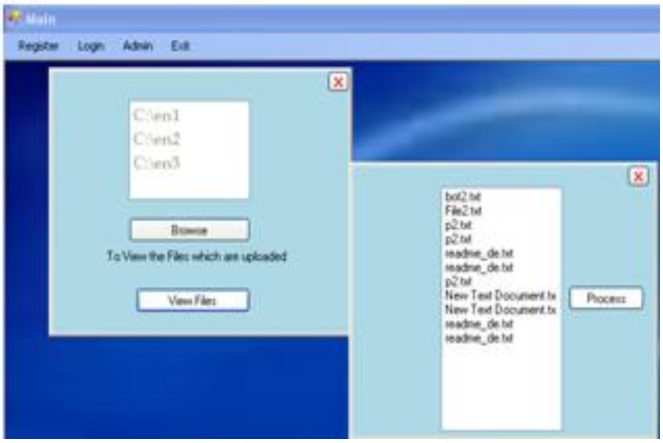
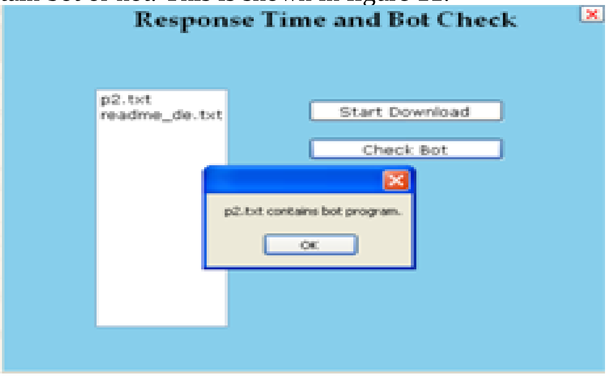


Figure 10. Database of All the files transferred in the network

B. *Detection of Bot in cloud*

After processing the file we can check whether that file contain bot or not. This is shown in figure 11.



p2.txt contains bot program.

Figure 11. Detection of Bot

If processed file contains bot then the folder either en1 from client1 or en2 from client2 will not be able to transfer or receive the data through and from the network. Because whenever a botnet attacks on the particular system it spreads a Distributed Denial of Service(DD0S)[5] attack on the victim machine or host. And that machine or host cannot send receive the data through and from the network. DDos attack makes all the resources from the victim machine unavailable for its intended users.

And the CNSMSUB system will delete the folder containing bot from its client.

V. CONCLUSION

A novel method for the detection of bot from the cloud using CNSMSUB has been presented. The CNSMS is very useful to countermeasure distributed network attacks.

In this paper, we proposed using cloud computing systems that detects the bot from the network or from the cloud and make the folder or client unavailable for its intended users means it spreads the DDoS attack on the victim host. And after the detection of b0t to suppress that bot from the cloud the system deletes the folder containing the bot from the client. In this way the system is used to protect the cloud from the botnet attack.

The results show that the proposed scheme is practical and can be generalized for the analysis of other network attacks in the future

VI. ACKNOWLEDGEMENT

The authors would like to thank all the beloved friends and colleagues for their support and guidance throughout the project.

REFERENCES

[1] Rupal B. Jaiswal and Shivraj Bajgude," Botnet Technology", 3rd International Conference on Emerging Trends in Computer and Image Processing (ICETCIP'2013) ,Kuala Lumpur (Malaysia), pp. 169-175, January 8-9, 2013.

[2] Banday, M.T., Qadri, J.A., Shah, N.A. (2009). "Study of Botnets and Their Threats to Internet Security ," . Sprouts: Working Papers on Information Systems, 9(24). http://sprouts.aisnet.org/9-24.

[3] Seiichiro Mizoguchi, Keisuke Takemori, Yutaka Miyake, Yoshiaki Hori, Kouichi Sakurai, "Traceback Framework against Botmaster by Sharing Network Communication Pattern Information" , 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2011, Seoul, Korea, June 30-July 02, 2011

[4] Ashutosh Singh, Annie H. Toderici, Kevin Ross, Mark Stamp, "Social Networking for Botnet Command and Control", I.J. Computer Network and Information Security ,2013,6, 11-17 .

[5] Vrizlynn L. L. Thing, Morris Sloman, and Naranker Dulay," A Survey of Bots Used for Distributed Denial of Service Attacks", 22nd IFIP International Information Security Conference (SEC), Sandton, Gauteng, South Africa, May 2007.

[6] Zhen Chen*, Fuye Han, Junwei Cao, Xin Jiang, and Shuo Chen," Cloud Computing-Based Forensic Analysis for Collaborative Network Security Management System ", TSINGHUA SCIENCE AND TECHNOLOGY,l05/12l lpp40-50 Volume 18, Number 1, February 2013.

[7] Meenakshi Thapliyal , Anchit Bijalwan, Neha Garg, Emmanuel Shubhakar Pilli," A Generic Process Model for Botnet Forensic Analysis",Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013) pp98-102.

[8] Jignesh Vania, Arvind Meniya, H. B. Jethva," "A Review on Botnet and Detection Technique", International Journal of Computer Trends and Technology, volume4Issue1-2013pp23-29.

[9] F. Han, Z. Chen, H. Xu, and Y. Liang, A collaborative botnets suppression system based on overlay network, International Journal of Security and Networks, vol. 7, no. 4, 2012.

[10] Paul Barford, Jeffery Kline, David Plonka and Amos Ron, "A Signal Analysis of Network Traffic Anomalies", IN PROCEEDINGS OF ACM SIGCOMM INTERNET MEASUREMENTWORKSHOP 2002 .

[11] Ankush P. Deshmukh , Prof. Kumarswamy Pamu," Research Paper Applying Load Balancing: A Dynamic Approach", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 6, June 2012 pp201-206.

[12] "Implementing Microsoft Network Load Balancing in a Virtualized Environment" http://go.microsoft.com/fwlink/?LinkId=18371

[13] Rajesh George Rajan, V.Jeyakrishnan, "A Survey on Load Balancing in Cloud Computing Environment", IJARCCE, Vol. 2, Issue 12, December 2013 pp4726-4728.

[14] Jing Liu, Yang Xiao, Kaveh Ghaboosi, Hongmei Deng, Jingyuan Zhang,"Review Article Botnet: Classification, Attacks, Detection, Tracing, and PreventiveMeasures",

EURASIP Journal onWireless Communications and Networking Volume 2009, Article ID 692654, 11 page

[15] Alexa Huth, James Cebula ,” The Basics of Cloud Computing “,United State- Computer Emergency Readiness Team,2011. http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf.

[16] Mladen A. Vouk, “Cloud Computing – Issues, Research and Implementations”, Journal of Computing and Information Technology - CIT 16, 2008, 4, pp235–246.

[17] Information Guide on “VMware Virtual Networking Concepts “.

Authors

Namrata A. Sable has received her B.E. in Information Technology from KDK college of Engineering, Nagpur, RTMNU, Nagpur. She is pursuing her Master of Engineering in Computer Science and Engineering from G. H. Raisoni College of Engineering & Management, SGBAU, Amravati. Her area of interest includes cloud Security and Network Security.

Prof. Dinesh S. Datar has received his B.E. in Information Technology from Government College of Engineering, SGBAU, Amravati. And received his M.Tech in CTA from PIT college, Bhopal, RGPD university, Bhopal. His area of interest includes cloud Security and Network Security.