

**Special Issue: 2nd International Conference on Advanced Developments in Engineering and Technology
Held at Lord Krishna College of Engineering Ghaziabad, India**

Secure Cloud Environment against Botnet Attack

Ram Kumar Sharma

M.Tech. Scholar

Department of CSE

Al-Falah School of Engg. & Tech.

Faridabad Haryana

Dr. Jitender Rai

Department of CSE

Tecnia Institute of Advanced Studies

Amit Kumar Tyagi

Department of CSE

Pondicherry Engg. College

Puducherry

ABSTRACT

Cloud computing is emerging as a legitimate alternative model for the sourcing and provision of digitized platforms for business organizations today. Cloud provides Platform as a Service (PaaS), Software as a Service (SaaS) an Infrastructure as a Service (IaaS) and promise reduced IT costs and complexity, combined with improved access and flexibility. Botnet is the collections of bots or collection of compromised computers that are remotely controlled by its BotHerder. The term 'Bot' is nothing but a derived term from "ro-Bot" which is a generic term used to describe a script or sets of scripts designed to perform predefined function in automated fashion.

Today's Malware and Botnets are recognized as a global problem and therefore reside in a complex system with many dependencies. Millions of computer systems are infected with often multiple types of malware. These computer systems are organized in several hundreds of different botnets.

Hence the objective of the paper is to implement or create a secure cloud computing environment against botnet attack.

1. INTRODUCTION

Cloud Computing: Cloud Computing is defined as a computing paradigm where services and data reside in shared resources in scalable data centres, and those services and data are accessible by any authenticated device over the Internet.

Some key attributes that distinguish cloud computing from conventional computing. Cloud computing offerings are:

- Abstracted and offered as a service.
- Built on a massively scalable infrastructure.
- Easily purchased and billed by consumption.
- Shared and multi-tenant.
- Based on dynamic, elastic, flexibly configurable resources.
- Accessible over the Internet by any device.

Today, we have identified three main categories of services that fall within our broad cloud computing definition.

Software as a service (SaaS): Software deployed as a hosted service and accessed over the Internet.

Platform as a service (PaaS): Platforms that can be used to deploy applications provided by customers or partners of the PaaS provider.

Infrastructure as a service (IaaS): Computing infrastructure, such as servers, storage, and network, delivered as a cloud service, typically through virtualization.

Botnet: Botnet is used to define networks of infected end-hosts, called bots that are under the control of a human operator commonly known as a Botmaster. Hence the following services are provided by bots to its Botmaster:

- Robust network connectivity
- Individual encryption and control traffic dispersion
- Limited Botnet exposure by each Bot
- Easy monitoring and recovery by its Botmaster

2. Expected Benefits and Risks:

My decisions about how and when to move services to clouds are based on the balance between risk and reward. As the technology evolves, I expect this balance to shift so that the benefits begin to outweigh the risks for a growing number of applications and services.

2.1 Benefits:

Potential benefits of cloud computing includes:

Agility, Adaptability, and Flexibility:

A business group that wants to deploy a new application can do so relatively quickly using cloud computing services, compared with weeks or months it can take with the traditional enterprise model of buying servers, installing them, and then deploying the application to the new servers. In many cases, users can purchase cloud services with a credit card and begin to use them almost immediately.

Because cloud computing is built on a massively scalable shared infrastructure, cloud suppliers can in theory quickly provide the capacity required for very large applications without long lead times. Purchasers of IaaS capacity can run applications on a variety of virtual machines (VMs), with flexibility in how the VMs are configured. Some cloud computing service providers have developed their own ecosystem of services and service providers that can make the development and deployment of services easier and faster. Adding SaaS capacity can be as easy as getting an account on a supplier's host.

Cloud computing is also appealing when we need to quickly add computing capacity to handle a temporary surge in requirements. Rather than building additional infrastructure, cloud computing could in principle be used to provide on-demand capacity when needed.

Cost Savings:

There is a perception that cloud computing can reduce cost. To date, savings have generally been more clearly shown for small to medium-size businesses (SMBs). Cost savings can be a factor in propelling enterprise cloud adoption. The relatively low upfront cost of IaaS and PaaS services, including VMs, storage, and data transmission, can be attractive—especially for addressing tactical, transient requirements such as unanticipated workload spikes. An additional advantage is that businesses pay only for the resources reserved; there is no need for capital expenditure on servers or other hardware.

2.2 Risks:

A "Risk" is the likelihood of a threat agent taking advantage of vulnerability and the corresponding business impact.

The features that make cloud computing so appealing, combined with the fact that services are publicly accessible, can also lead to many potential risks. ENISA classifies Cloud Computing (CC) risks into three categories:

Organizational Risks

Technical Risks

Legal Risks

Generally Cloud Computing is based on a new utilization of technology and many risks that used to be present in other technological implementations do still exist, and are realized as not cloud specific. Risks like social engineering, physical security, lost or stolen backups, and loss or compromise of security logs are just a few examples of such general security risks.

Hence a list of some tasks needed to secure a cloud system against Malware/ Botnet attack which are:

1. Build a list of all known Botnets and a data repository for associated traffic data samples that could be used to develop and test detection and mitigation algorithms in future to detect Botnet attack.
2. Develop an algorithm using the characteristics which can be identified as common among all Botnets as a first order detector.
3. Determine if it is practical for network providers to use network flow data to detect and mitigate Botnets
4. Investigate various ideas developed and its possible extension be extension to build anti-bot applications that could be applied the way anti-virus or anti-spyware are used today.
5. Generation of a robust Botnet capable of maintaining control of its remaining bots even after a substantial portion of the Botnet population has been removed by defenders.
6. How to prevent significant exposure of the network topology when some bots are captured by defenders.
7. Monitoring and obtaining the complete information of Botnet by its Botmaster.
8. Create a program that either prevents or warns you about navigating to a known spyware site.

The relevance of ongoing work in certain fields of detection and analysis of security incidents is increased by the advent of cloud computing:

1. Virtual-machine introspection is uniquely suitable for incident analysis in a cloud context; further research about virtual-machine introspection in general and its use for incident and risks handling in the cloud should be conducted.
2. To make the most of virtual-machine introspection and the snapshot feature of virtualization, research in memory forensics must be intensified.
3. The collection of information via live forensics on running systems must be subjected to a systematic approach.
4. Methods for incident detection and analysis based on event information such as log file correlation and visualization must be improved and adapted to the specific requirements on incident handling in the cloud. This is of special importance for incident handling in PaaS and SaaS contexts, where most relevant information will be available as event logs.
5. Detection methods that allow for detection with little or no information about the infrastructure that is monitored (e.g., virtual machines under customer control as treated by Christodorescu et al. [6] or web applications under customer control as treated by machine learning / anomaly-detection approaches to web-application firewalling) must be improved.

3. Botnet Attack

A Botnet is a tool for malicious users (attackers). Botnet used for financial gain or for destructive purposes and to misuse or steals the valuable data of users. Hence here some of Botnets attacks are:

- a. DDoS (Distributed denial of service) attacks
- b. Spamming
- c. Click fraud/Harvesting of information
- d. Spreading new malware
- e. Manipulating online polls
- f. Google Ad Sense abuse

How a Botmaster can attack in a cloud environment:

Hence among the various type of Botnet attack, attack can be performed by Botmaster inside a cloud environment as:

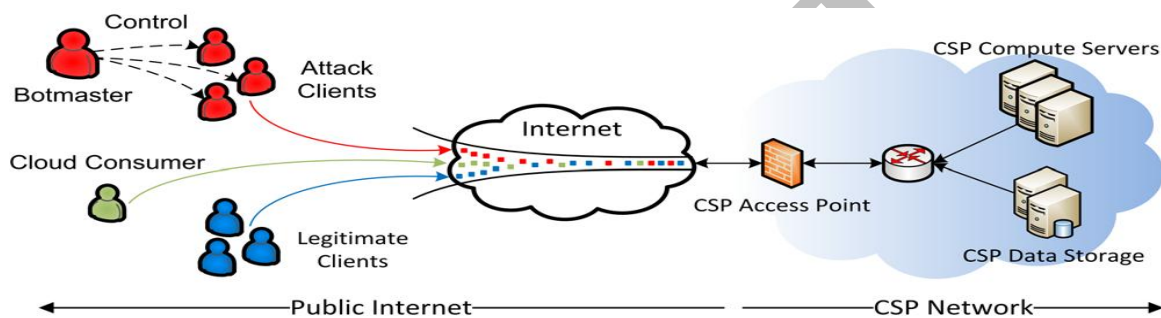


Figure 1: Cloud Network Attack Diagram

Emerging Botnet Use in future:

1. Malware and Botnets on Mobile Phones
2. Appearance Of White Worms
3. More Complex And Potentially Dangerous Malware
4. Advances of Botnet Infrastructure And Distribution
5. Fast Flux Service Network Based Bot

4. Botnet Detection

Generally Botnet detection and tracking has been a major research topic in recent years due to increase in the malicious activity. Due to the presence of malicious activity (Botnet) from a long time, till now only few formal studies have examined the Botnet problem. So different techniques have been proposed to detect Bot which are described as follows:

4.1. Honey net-based methods

Generally Honey net based method consists of Honey pot and Honey wall [10]. Honey pot denotes an end host which is very vulnerable to malicious attacks and is often successfully compromised in a very short time span. And Honey wall denotes software which is used to monitor, collect, control, and modify the traffic through the Honey pot, e.g. Snort [1, 4]. Honey net work used only un patched versions of all versions of Windows as Honey pot, and Snort inline used as Honeywall device to track Botnets on a daily basis report (i.e., the Honeynet would have been rebuilt in every 24 hours). So based on using both results we detect the location and behavior of bots in a network.

Now beside of this functionality, this paper has also listed a set of suggestions from which we can elaborate “how to write a useful Botnet tracking IRC clients” [10]. First, this client shall have SOCKSv4 and multi-server support to tracking bots. Second, some useful packages, such as libadns, libcurl, and Perl Compatible Regular Expression (PCRE) shall be included in this client. And at last, the modularity and certain functionalities, such as no threading, shall be inconsideration throughout the design of this client.

A similar Honey net has been constructed [1, 10], in which Honey wall element shall be able to capture and inspect all the traffic payloads to retrieve Botnet information such as the DNS/IP address of the C&C server with the corresponding port number and the authentically data to join the C&C channel and capable of isolating the Honey pots from other machines in the local network by blocking outgoing connections containing suspicious keywords linked to possible malicious activities. These papers only offer a single vantage point of view on Botnet activities, thus missing a substantial portion of Botnet spreading behaviors.

So in order to capture the comprehensive actions of the Botnets, Rajab et al. [2] have constructed a multifaceted and distributed measurement infrastructure by combining a modified version of the nepenthes platform with the Honey nets i.e. we can say confidentially here, Honey net is a powerful tool for understanding Botnet technology and characteristics, and tracking Botnet behaviors.

4.2. Passive traffic monitoring

Beside of a successfully paper Honey net, to collect Botnet data or attacker location is a difficult task much more today. So another approach is setting up here “passively monitor the real Internet traffic” which is used to detect or extract the Botnet related packets [10]. Till now, presence of various types of different data such as Internet traffic data, DNS data, BGP route views, Net flow data, and proprietary enterprise data, and on the complexity and response time requirements, many Intrusion Detection System (IDS) designs have been already proposed to detect the Botnets and their location but no solution is perfect to give a better result in compare to this technique. This technique classified as behaviour-based, DNS-based, and data-mining based respectively as described and summarized in the following sections:

This technique classified as:

1. Behaviour based technique: Based on the presence information and data, this method can be further categorized into two ways
 - 1.1 Signature-based detection
 - 1.2 Anomaly-based detection
2. DNS-based detection: This technique is a hybrid of behavior based and data-mining based techniques which is performed on DNS traffic.
3. Data-mining based detection: This technique is mostly used to detect the Bot in an abnormal traffic and in a high volume of traffic data.

5. Proposed Integrated Model

Hence in future my research work will on cloud integrity and blinding issues in service provider layers.

Proposed Integrated model should include:

- Nebulas
- Cloud Views
- Trusted Cloud Computing Platform
- Private Virtual Infrastructure (PVI) and Locator Bot
- Trading storage for computation

CONCLUSION

Results (Expected): Integrated Proposed Model with reasonable security parameters provide a higher level security for above issues. And as discussed cloud computing is an emerging area in internet history. So in our proposed method we want to develop a secure system against malware or botnet attack with easy accessible, good reliable and flexible results for its users.

REFERENCES:

1. M. West Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle, and M. Zajicek. Handbook for Computer Security Incident Response Teams (CSIRTs). Technical Report CMU/SEI-2003-HB-002, Carnegie Mellon SEI, 2003.
2. RajkumarBuyya, Rajiv Ranjan, and Rodrigo N. Calheiros "Inter Cloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services." Springer LNCS, 2010
3. Liang-Jie Zhang and Qun Zhou. "CCOA: Cloud Computing Open Architecture", IEEE International Conference on Web Services, 2009.
4. Balachandra Reddy Kandukuri, Ramakrishna Paturi V, AtanuRakshit"Cloud Security Issues", IEEE International Conference on Services Computing,2009.
5. George Resse, "Cloud Application Architecture", OReilly, 2009
6. RajkumarBuyya, Chee Shin Yeo, and SrikumarVenugopal. "Market-Oriented Cloud Computing:Vision, Hype, and Reality for Delivering IT Services as Computing Utilities", HPCC, 2008
7. V.Krishna Reddy, Dr L.S.S.Reddy , "Security Architecture of Cloud Computing", International Journal of Engineering Science and Technology (IJEST), September 2011
8. Kamal Dahbur et al. "A Survey of Risks, Threats and Vulnerabilitiesin Cloud Computing", ACM , 2011
9. Bernd Grobauer et al. "Towards Incident Handling in the Cloud: Challenges and Approaches" ACM, 2010.
10. Amit Kumar Tyagi, G.Aghila, "a wide survey on botnet", IJCA,November 2011,