Chapter 13
A Proactive Approach to Intrusion Detection in Cloud Software as a Service

Baldev Singh
Lyallpur Khalsa College, India

Surya Narayan Panda
Chitkara University Rajpura, India

ABSTRACT

Cloud computing environment is very much malicious intrusion prone hence cloud security is very vital. Existing network security mechanisms face new challenges in the cloud such as DDOS attacks, virtual machine intrusion attacks and malicious user activities. This chapter includes brief introduction about cloud computing, concept of virtualization, cloud security, various DDOS attacks, tools to run these attacks & various techniques to detect these attacks, review of threshold methods used for detection of DDOS attacks & abnormal network behavior and proposed dynamic threshold based algorithmic approach. Although various cloud security measures are prevailing to avoid virtual machine attacks and malicious user activities but these are not foolproof. Hence, new security methods are required to increase users' level of trust in clouds. By scrubbing traffic at major Internet points and backbone connection, a defense line is created for mitigation of DDOS attacks. Dynamic threshold algorithm based approach is proposed as a proactive approach to detect DDOS attacks for achieving secure cloud environment.

INTRODUCTION TO CLOUD COMPUTING

Technology of cloud computing provides a way of using computing and storage resources by using Internet and remote servers. It presents a new way of using remote resources. The usage of computing resources is charged on usage basis where a user contracts services from a service provider by paying according to what it uses. Cloud computing makes it happen to use the applications without particular installation on personal computers, it is only by accessing and using the services by way of Internet. Cloud computing is an enabled service that may be used for various benefits to its like ease of deploying computer and information technology resources for fresh business, a lesser amount of system operating and maintenance costs and lessening of deployment time in any setup.

DOI: 10.4018/978-1-4666-8510-9.ch013

The National Institute of Standard and Technology (NIST) defines Cloud Computing as the model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., Networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell & Grance, 2009). Cloud Computing is one of the fastest growing service models on the Internet. Various large scale IT service providers, like Amazon and IBM, share their data centers, by using virtualization concepts, for the public usage of their computational resources. By using cloud computing, the users of cloud can minimize many startup financial overheads as well as obtain an increase in the availability and scalability for their cloud-hosted applications. In addition, cloud users can avail on-demand service with the ease of Pay-As-You-Go subscription.

VIRTUALIZATION

Virtualization is one of the crucial component being used in cloud computing. It becomes a key element to provide a set of dynamically scalable resources such as storage, software, processing power and other computing resources as services to users which could be accessed over the Internet on demand. A user needs only a browser and an Internet connection to use these resources. Virtual machines (VMs) are created within a virtualization layer (Jin et al, 2011). A cloud is built up of numerous host machines these physical machines then run multiple virtual machines, which is what are presented to the end-users.

Virtual machines are only limited in the way that their specifications cannot exceed that of their host machine. A virtual machine is a software implementation of a computing environment in which an operating system (OS) or program can be installed and run. The virtual machine typically emulates a physical computing environment, but requests for CPU, memory, hard disk, network and other hardware resources from the host machine that are managed by a virtualization layer which translates these requests to the underlying physical hardware. Researchers get the ability to test applications, their deployments and upgrades more efficiently by using VMs. They don't need to have multiple OS and installation configurations.

CLOUD SECURITY

Security is one of important issues prevailing in the cloud environment. Cyber attacks against large internet ventures keep on rising and they directly affect the cloud users. Cloud customers (organizations) are questioning the security of moving their computational assets toward the cloud. These improper operations are generally conducted for a number of reasons. Financial gain can also be a motivation to steal valuable information from sensitive organizations such as those in the banking sector. Cyber surveillance operations typically conducted to gather information about financial or industrial adversaries are some of the new trends over the internet. Existing network security mechanisms face new challenges in the cloud such as DDOS attacks (Bhuyan, Kashyap, Bhattacharyya & Kalita, 2013), virtual machine intrusion attacks and malicious user activities. Hence, new security methods (Tao, Hui, Feng & Cheng, 2012), (Subashini & Kavitha,2011) are required to increase users' level of trust in clouds. Presently, cloud service providers implement data encryption for the data centers, virtual firewalls and access control lists.