Cloud Security Challenges and Intrusion and Detection System in Cloud Computing

Kavya1, Vinay Kumar2

1Department of Data Engineering and Cloud Computing, REVA University Bengaluru, INDIA
2Assistant Professor, Department of Information Science, REVA University Bengaluru, INDIA

ABSTRACT
Cloud computing is an upcoming technology that affects IT infrastructure, network services, and applications. Cloud security plays an important role which has attracted a lot of research and development effort in past few years. It is essentially one of the most important and on demand services technologies that IT offers today. It attempts to provide services to users on pay as use basis of the services provided in the cloud. With its various service models, It promises to reduce the operational and costs for the service providers on one hand, and for the users by providing the opportunity to access services according as per the end user needs. It is a new computing model that makes the IT world to use services that help in outsourcing data, computing and so on. However, security is an important concern. Adversaries are able to launch DDoS (Distributed Denial of Service) attacks. These attacks compromise some of the Virtual Machines and then perform DDoS activities. The compromised Virtual Machines are known as zombies. With respect to cloud computing networks detecting and countermeasure of zombies exploration attacks is difficult.

Keywords---- DDoS, Cloud Computing, IT

I. INTRODUCTION

From past few years, most of the people are concerned to have computers in their offices, schools and homes. The main reason behind that was to aware of the world and communicate and exchange data by these devices. Today people are interested about the Internet and its high speed for cost effective and efficient communication. In addition, often they need many more services to the existing service provided by the Internet. These services are known as cloud computing tasks that are delivered by the Internet Service Providers (ISP), Cloud computing represents a different way to architect and remotely access computing resources. One has to create an account with any cloud service provider, such as Microsoft or Amazon or Google, to begin building and deploying applications systems into a cloud. While there are important security, privacy and regulatory issues that system activity need to sort through before full migration to the cloud, and cloud owners need to strengthen cloud services in these areas before enterprise applications can be effectively hosted in the cloud, there are benefits that cloud computing offers today that can be leveraged in the deployment of many enterprise applications.
as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) models. PaaS model facilitates users by providing platform on which applications can be developed and run. IaaS deliver services to users by maintaining large infrastructures like hosting servers, managing networks and other resources for clients. SaaS model makes user worry free of installing and running software services on its own machines. Presently, Salesforce.com, Google and Amazon are the leading cloud service providers who extend their services for storage, application and computation on pay as per use basis. Data, application and services non-availability can be imposed through Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks and both cloud service provider and users become handicap to provide or receive cloud services. For such type of attacks Intrusion Detection System (IDS) can be emplaced as a strong defensive mechanism. Intrusion Detection Systems are host bases and network based and distributed IDSs. Host based IDS (HIDS) monitors on specific host machines, network-based IDS (NIDS) identifies intrusions on key points of network and distributed IDS (DIDS) executes both on host as well as network. IDSs gives an alerts for the network analyzer which are based on true positives alarms when actually intrusion takes place and false positive alarms in case of a wrong detection by the system.

![Cloud Service models](image)

**Fig 2. Cloud Service models**

### II. TYPES OF CLOUDS

For most businesses, organizations, or governmental agencies IT environment, there are three relevant types of clouds: Private (internal), Public (external), and Hybrid (mixed). Each cloud infrastructure has unique characteristics and applications offers different advantages and disadvantages.

A. **Private Cloud**

A private cloud is a cloud computing platform permits enterprises to implement cloud technologies at their onsite hardware and software. Enterprises are implementing a private cloud within areas of their infrastructure in which a cloud model makes the most importance. A private cloud provides benefits of cloud computing without the loss of control and security risks associated with other cloud infrastructure models. A private cloud provides virtualization technology to enhance scalability, resource management, and hardware utilization. In addition, it incorporates data center automation of management and chargeback metering for consumption and services-based billing capabilities. Identity-based security protocols ensure that only authorized users have access to appropriate applications, resources and infrastructure. Private cloud refers to cloud infrastructure developed internally by organizations need to combine the agility of the cloud with the security and control of in-house systems. Infrastructures of private cloud are completely managed and corporate data are fully maintained and secured by the organization itself. Private clouds provide the following advantages—

* Ability to rapidly bring new services online without caused by commissioning or provisioning server infrastructure.
* Increased utilization of hardware and software infrastructure flexible greater ROI for capital expenditure.
* Greater data security, control and conforming with industry-specific regulations.
* Centralized control usage, compliance and security policies via use of multiple shared resources.
* Frictionless development as developers can get results and repeatedly develop cycles rapidly.

B. **Public Cloud**

Public cloud infrastructure is provisioned for open use by the public. It is owned, leased, managed, and operated by a business, academic, or government organization, or some combination of all. Public cloud
applications, architecture, storage and resources are made available to the all public by service providers. End users without actually possessing these resources can access to them easily on demand via a Web browser from a simple laptop or personal computer, wherever they are needed and with minimal management or service provider effort. Some characteristics of Public Cloud are—

- Increased agility by resulting to changes in the business environment.
- Reduced expenditure in IT hardware and software, in favor of operational expenditure.
- IT outsourced to specialists, providing access to more expertise at lower cost.

C. Hybrid Cloud

The Hybrid cloud infrastructure providing is a combination of the Public and Private Cloud, frequently choose by organizations that require greater control over data they hold, but still to run certain workloads on public cloud infrastructure as required. For example, a company may employ an inside cloud to share physical, virtual resources and applications over a network through hybrid cloud, but extend these capabilities and requirements when needed such as at peak processing times. Implementing a composed cloud infrastructure provides enterprises to select and choose applications within the private investors inside on a public versus private cloud. For example, this model permits financial applications with all information to remain behind a firewall and software such as collaboration, management, customer service, or supply chain can exist on a public cloud.

The various types of cloud infrastructure have been describe in the following figure.

Figure 3. Types of Cloud Computing

III. CLOUD SECURITY CHALLENGE

Cloud data confidentiality issue

Confidentiality is the major issue data over cloud is one of the a fiercely security concerns. Encryption of data can be found by traditional techniques. However, encrypted data can be secured and controlled from a malicious user but the privacy of data from the administrator of data at service providers end could not be hidden. Searching and indexing on encrypted data remains a role of concern in that case. Above mentioned cloud security issues are consider as dynamicity of cloud architecture are facing new challenges with rapid implementation of different service paradigm.

Network and host based attacks on remote Server

Host and network intrusion attacks on remote hypervisors are a major security issues, as cloud vendors use virtual machine technology in cloud. DOS and DDOS attacks are launched to accede to service availability to end users.

Cloud security auditing

Cloud auditing is a difficult task to check compliance of all the security policies through cloud vendor. Cloud service provider has the control of sensitive user data and processes, so an automated or third party auditing mechanism for data integrity check and forensic analysis with control is needed. Privacy of data from third party auditor is major issue of cloud security.

Lack of data interoperability standards

Interoperability results into cloud user data lock-in state. If a cloud user wants to shift to other service provider due to certain reasons it would not be done, as cloud users data and application may not be compatible with other vendors data storage platform. Security and confidentiality of data would be in the hands of cloud service provider and cloud user will be made as dependent on a single service provider.

Proper security controls should be implemented according to accounting, threat, and vulnerability risk assessment matrices in the cloud. While cloud security concerns can be merged into multiple dimensions will be in extension of time have been aggregated into three general areas: Security and Privacy, Conformity, and Legal or Contractual Issues. Advocates of cloud computing promise applications, and many believe that the claims are not merely hype—that cloud services will be a defining characteristic of the next events security of computing. Security could be the cloud’s Achilles’heel, however, and must be variety for cloud computing to reach its potential. Information systems cover a spectrum of requirements—from total protection to complete intervals—and internal risk evaluation are the means by which an organization evaluates the trade-offs and decides level of security is acceptable and appropriate by cloud. Cloud computing not only adds new layers to the question of computer security; it often also adds complexity in understanding the parameters that feed into a risk assessment. Because the systems and staff of a cloud provider are not under the
control of a customer, institutions that use cloud services rely on contracts—and, to be sure, a certain amount of trust—for security information. Vendors offer different levels of transparency, and this becomes an important component of institutional efforts to evaluate cloud services.

IV. INTRUSION DETECTION SYSTEM

Intrusion detection systems (IDS) are an absolutely necessary component of defensive measures protecting computer systems and network over the cause to system. It becomes crucial part in the Cloud computing environment. The main aim of IDS is to detect different attacks in environment and provide the proper response. An IDS is defined as the technique that is used to detect and respond to intrusion activities of system from internal effect host or network. There are mainly two categories of IDSs, which are listed in Table 1.

<table>
<thead>
<tr>
<th>Types of IDS</th>
<th>Host level (HIDS)</th>
<th>Network level (NIDS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Based</td>
<td>Host Based</td>
<td>Networked and Networked</td>
</tr>
<tr>
<td>Hybrid</td>
<td>Hybrid</td>
<td>Hybrid</td>
</tr>
<tr>
<td>File Integrity</td>
<td>File Integrity</td>
<td>Honeypots</td>
</tr>
</tbody>
</table>

In addition, the IDS can be defined as a defense system in each problem, which detects fault and unauthorized activities in a network. The key is to detect and possibly prevent activities that may reduce system security, or some hacking attempt in progress including reconnaissance/data collection phases that involve for example, port scans. One key feature of intrusion detection systems is their ability to provide a view of unusual activity and to issue alerts notifying administrators and/or blocking a suspected connection. Intrusion detection is defined as the process of identifying and responding to malicious activity reached at computing and networking resources. In addition, IDS tools are capable of distinguishing between insider attacks originating from inside the organization (coming from own employees or customers) and external ones (attacks and the threat posed by hackers).

In addition, the IDS can be defined as a defense system in each problem, which detects fault and unauthorized activities in a network. The key is to detect and possibly prevent activities that may reduce system security, or some hacking attempt in progress including reconnaissance/data collection phases that involve for example, port scans. One key feature of intrusion detection systems is their ability to provide a view of unusual activity and to issue alerts notifying administrators and/or blocking a suspected connection. Intrusion detection is defined as the process of identifying and responding to malicious activity reached at computing and networking resources. In addition, IDS tools are capable of distinguishing between insider attacks originating from inside the organization (coming from own employees or customers) and external ones (attacks and the threat posed by hackers).

Once an intrusion has been detected, IDS issues alerts notifying administrators. The next step is undertaken either by the administrators or the IDS itself, by taking advantage of additional functions of countermeasures (specific block functions to terminate sessions, backup systems, routing connections to a system trap, legal infrastructure etc.) – following the organization’s security policy (Figure 4). An IDS is an element of the security policy. Among various IDS tasks, intruder identification is one of the fundamental ones. It can be useful in the forensic research of incidents and installing appropriate patches to enable the detection of future attack attempts targeted on specific persons or resources.

4.1 Host Based Intrusion Detection System (HIDS)

Host based of IDS involves software or agent components, which is run on the server, router, switch or network appliance. However, the agent versions must report to a console or can be run together on the same host as addressed in Figure 5. Basically, HIDS provides poor real-time response and cannot effectively defend against one-time catastrophic events. In fact, HIDSs are much better in detecting and responding to long term attacks and multiple check such as data thieving.
4.2 Network Based Intrusion Detection System (NIDS)

Network based of IDS captures network traffic packets such as TCP, UDP and IPX/SPX) and analyzes the content against a set of RULES or SIGNATURES to determine if a POSSIBLE activities addressed. False positives are common when an IDS system is not configured or “tuned” to the environment traffic it is trying to analyze and detected. Figure 6 shows the network based Intrusion Detection System architecture.

Table 2 summarizes the differences between the Host based Intrusion Detection system (HIDS) and Network Based Intrusion Detection System. However, the host-based and network-based systems are both required in the Cloud computing environment because they offer significantly different benefits with multiple usage. For IDS, we need to use detection, deterrence, response, damage assessment, attack anticipation, and prosecution.

V. INTRUSION DETECTION SYSTEM IN CLOUD COMPUTING

As mentioned before, Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for faults over the system, defined as attempts to compromise the confidentiality, integrity, availability, reliability, or through the security mechanisms of a computer or network. Intrusions are caused by attackers accessing the systems from the Internet or by authorized users of the systems who attempt to gain additional benefits for which they are not authorized or by authorized users who misuse the sources given to them. Intrusion Detection Systems (IDSs) are software or hardware products that automate this monitoring and analysis process by detection.

The Intrusion Detection Service (IDS) service increases a Cloud’s security level by providing two methods of intrusion detection for identification. First method is behavior-based method which dictates how to compare recent user actions to performed their behavior. The second approach is knowledge-based method that detects known trails left by attacks or certain sequences of actions from a user of action represent an attack. The audited data is sent to the IDS service core, which analyzes...
the behavior using artificial intelligence to detect alterations. It has two subsystems namely analyzer system and alert system. In order to detect the intruders the following techniques should be verified in either HIDS or NIDS.

5.1 Anomaly Detection (AD).

Basically, Anomaly Detection was introduced in the late of 1980’s with identifying Intrusion detection expert system (IDES). Anomaly detectors identify abnormal behavior (anomalies) on a host or network environment. They function on the assumption that attacks are different from “normal” (legitimate) activity and can therefore be detected by systems by their differences. Anomaly detectors construct profiles information representing normal behavior of users, hosts, or network connections. These profiles are constructed from historical data collected over a period of operations. Then collect event data and use a variety of measures to determine when monitored activity deviates from the norm. There are many measures and techniques that are used in anomaly detection including: Threshold detection, Statistical measures, Rule-based measures, other measures, including neural networks, genetic algorithms, and immune system models.

5.2 Signature Detection (SD).

Misuse detectors analyze system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack. As the patterns corresponding to known attacks are called signatures, misuse detection is sometimes called “signature-based detection”. The most common form of misuse detection used in commercial products specifies each pattern of events corresponding to an attack as a separate signature. In this work, we will focus on applying IDS on IaaS which is the most flexible model for ID deployment. So, we need to identify the locations that should be considered when thinking about ID in the IaaS Cloud. There are four primary "spots":

• In the virtual machine (VM) itself: Deploying ID in the VM allows monitoring the activity of the system, and detecting and alerting on issues that may arise.
• In the hypervisor or host system: Deploying ID in the hypervisor allows to not only monitor the hypervisor but anything traveling between the VMs on that hypervisor. It is a more centralized location for ID, but there may be issues in keeping up with performance or dropping some information if the amount of data is too large.
• In the virtual network: Deploying ID to monitor the virtual network (i.e., the network established within the host itself) allows monitoring the network traffic between the VMs on the host, as well as the traffic between the VMs and the host. This "network" traffic never hits the traditional network.
• In the traditional network: Deploying ID here allows to monitor, detect, and alert on traffic that passes over the traditional network infrastructure.

VI. CONCLUSION

Cloud computing is a paradigm shift in which computing is moved away from personal computers and even the individual enterprise application server to a _cloud_ of computers. A cloud is a virtualized server pool which can provide the different computing resources of their clients. Users of this system need only be concerned with the computing service being asked for. The underlying details of how it is achieved are hidden from the user. However, as with any other technological shift or change, security benefits and risks need to be addressed before the full benefits of cloud computing can be realized. Because of their distributed nature, cloud Computing environments are easy targets for intruders looking for possible vulnerabilities to exploit. Different IDS techniques are used to counter malicious attacks in traditional networks. For Cloud computing, enormous network access rate, relinquishing the control of data & applications to service provider and distributed attacks vulnerability, an efficient, reliable and information transparent IDS is required.

REFERENCE


[18] Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth, SANS Institute, 2004


[31] Google Cloud. Available at:www.googlecloud.com


[34] https://cloudsecurityalliance.org/


[37] https://blog.cloudsecurityalliance.org/

[38] IDPS: An Integrated Intrusion Handling Model for Cloud Computing Environment Hassen Mohammed Alsafi, Wafaa Mustafa Abduallah and Al-Sakib Khan Pathan.