ISSN No. 0976-5697

Volume 2, No. 6, Nov-Dec 2011

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Study on Various Security Methods in Cloud Computing

V. Sandhya
Department of Information & Technology,
GITAM University, Hyderabad Campus,
Hyderabad PIN: 502329, Andhra Pradesh, India.
vsandhyaou@gmail.com

Abstract – Cloud Computing can be considered as a new technology in offering services to its end users on demand. Many organizations are trying to move to cloud environment to increase return on investments . As such the quality of services provided to its users plays a vital role, many organizations are focusing towards a trusted and secured services to its customers. In order to provide a secure service different approaches are followed either it may be a detective or a preventive approach. The main goal of the service provider is to ensure its end users that the data and information stored in the cloud is protected. This article presents a overall study of different security mechanisms that are implemented by the service providers.

Keywords –Security, cloud computing, customer, on-demand.

I. INTRODUCTION

Cloud computing is a form of parallel and distributed system where the resources are shared dynamically and services are provided to customers on demand. In this computing environment the users has to pay only for the duration they utilize the resources as it is called 'pay –per-usage'. It can be compared to that of utility computing such as electricity. A Resource may be processor, network bandwidth, storage etc., the services offered by a cloud provider is classified as Infrastructure as a service (IAAS) where computing resources, storage space are provided to the customers on demand (Amazon s3). Platform As A Service (PAAS) provides development environment as a service to the end users (Google App Engine), Software As A Service (SAAS) a single copy of software made available to customers on demand(Google Docs). Clouds can be categorized in to three deployment models.

- ***a. Public clouds*:** Resources and services are available to any organizations or person. They can subscribe and utilize the resources in the cloud computing environment.
- ***b. Private Clouds***: Resources are allowed to be accessed only within the organization.
- ***c. Hybrid Clouds***: Combination of public and private clouds where resources are available globally or within the organization.

In this article section 1 presents a brief introduction to cloud computing, Section 2 covers security issues that a cloud provider intended to satisfy the customers, Section 3 we discuss in detail about different security methods that are followed in cloud computing environment based on different attack such as DOS,DDOS and finally about trustworthiness in cloud. In Section 4 we conclude on the various security methods.

II. SECURITY ISSUES

The basic security issues that arises in a virtualized environment such as cloud is confidentiality, Integrity and availability (CIA) [1].According to Gartner list the security issues that are highlighted are[2]

- ***a. Privileged Access*:** Is there any privileged or specialized access to data? If so who administrates the access rights of these privileges?
- ***b. Regulatory Compliance***: Is there any security certifications? Does the cloud provider agree for external audits?
- ***c. Data Location:*** *Is* there any control over location of data given by the cloud service provider?
- ***d. Data Segregation***: Is data encrypted at all stages? These encryption methods are properly tested?
- ***e. Recovery:*** If data is lost, to what extent the cloud provider can restore? What is the time taken for restoration?
- ***f. Investigative Support:*** Can Cloud provider allow for investigation in case of inappropriate or illegal activity?
- ***g. Long Term Viability:*** If the cloud provider moves out of business will the data be returned to customer? If so what is the format?

III. CLOUD SECURITY

In a cloud computing environment data is moved to centralized cloud rather than storing at user's local computer. This makes users worried about their privacy .Cloud environment should ensure customers data integrity and privacy along with interoperability of data along multiple cloud service providers. Cloud is a distributed system, there is a risk of many security attacks such Denial of service attack (DOS),Distributed Denial of service attack(DDOS).A DOS attack takes place by preventing an authorized users from accessing resources. This attacks is caused by flooding packets such as SYN flooding, UDP flooding there by denying the access to the target node. A DDOS attack is a coordinated attack done indirectly through many compromised computing system[3].To overcome this type of attacks Intrusion Detection Systems(IDS) are used.

A. Intrusion Detection System:

An IDS collects information related to network traffic, analyzes the traffic and sends the report to the system administrator to take necessary action against any malicious

attack [4].IDS are of two types, they are Host Based IDS (HIDS) and Network based IDS(NIDS).A HIDS analyzes data based on the data collected by operating system, where as a NIDS analyzes the data collected from network. Normal IDS can detect and send response in three ways. The IDS may notify or send manual response or a an automatic response.

The third kind of IDS is a Distributed Intrusion Detection System (DIDS).DIDS can detect attacks on a single host as well as in a network [3]. The main aim is to aggregate data generated by individual IDS. A kind of DIDS known as Cooperative DIDS is a slight modification to DIDS used in a cloud computing environment. In this system IDS is deployed in each Cloud Computing region. When an attack occurs any IDS can exchange alerts with other IDS's depending on the ***severity*** of the attack as defined in the block table. Finally based on the evaluation of the trustworthiness of the alerts a new blocking rule is added in to the block table. In this way any attack can be detected in the early stage and prevent from a victim IDS. The remaining IDS in the cloud computing region can resist from same attack.

B. *Identity and Access Management (IAM)*:

In this method organizations resources and data are protected by enforcing rules and policies such as authentication, authorization and auditing methods. Many challenges exist in this system such as avoiding duplication of identities, attributes and credentials [4].The core responsibility is to manage the access control for services beyond the organizations internal network. Digital Identity Management involves provisioning and de provisioning, authentication and authorization, self service, password management, compliance and Auditing. The two protocols used for IAM are SAML and OAuth [4].

C. Sec-SLA:

Service Level Agreement (SLA) is a formal written agreement between a service provider and the customer stating the services and penalties when failed to provide the agreed services.SLA indicates the quality of service the service provider ensures to his customer. This is a conventional way of ensuring quality of service and performance to the customer. SLA is a way of ensuring transparent security in clouds such as public clouds when compared to hybrid or private clouds. Variation to SLA known as Sec-SLA [5] is a specific security SLA that extends to the traditional SLA by ensuring security related services such as backup policy, protection against malicious attack. Different levels of security can be provided by using security metrics. For a backup policy the metrics can be backup frequency, backup location, back up format. Each of these metrics has security levels. For example backup frequency minimum service level is one day and maximum service level as 1 hour. Sec-SLA is described using three steps.[5]

a. Policy analysis:

Data related to guidance's and policies to create Sec-SLA.

b. Architectural Analysis:

Identify customers requirements based on infrastructure.

c. Interviews:

Data related to security aspects are collected from the customer.

D. Sec-Mon (Monitoring Sec-SLA):

Sec-Mon is next step after ensuring sec-SLA. Architecture is proposed [6] for ensuring sec-SLA. The architecture consists of software, hardware, people and process and it has to satisfy the security principles such as integrity, privacy, availability, authenticity and non-repudiation.

E. Trusted Security:

In a cloud computing environment most of the computation are completed on server side where servers are managed within the data centers and is optimized for performance and efficiency parameters. In this type of computation the user has no control over the Hardware as most of the computation is handled outside the vicinity of the user [6]. This is achieved using a technology called ***"virtualization"*** where users can execute applications designed for different operating systems on a single machine instead of multiple pieces of hardware for each required operating system. Virtual Machines are also known as ***"Hypervisors***" that emulates a Hardware device. To protect the customers data in cloud a new method based on hardware attestation is used. In this method a centralized verification service called "cloud verifier" identifies customer's integrity and the system that hosts it [6].

A centralized management of cloud data is needed. Cloud Verifier is a service present in the cloud that monitors the state of the cloud platform [6] and user's virtual machines. In this method host is tested indirectly by vouching the enforcement of properties. One of the approaches followed is Integrity measurement using Trusted Platform Module (TPM) .The TPM generates the Integrity measurement sensitive code and data signed by a key tied to the physical Hardware.TPM is a special coprocessor that can generates various cryptographic keys. A special key called Endorsement Key [EK] is used to uniquely identify TPM and the associated client.

IV. CONCLUSION

Cloud computing has become the new platform where computing is regarded as on-demand service. Many organizations are planning to move to cloud to enhance their return on investments and reduce infrastructural setup and resources. The decision on migrating to cloud has to be taken by considering many parameters and issues. One important parameter is security which plays a vital role in this environment. Once the organization takes decision to move to cloud it loses control over its data as the cloud providers have several servers distributed around the world. Protecting customers data and integrity raised many challenges and at the same time gave rise to many types of attacks such as DOS, DDOS etc., In this article we highlighted the different types of attack and the possible existing security methods to overcome these attacks. We also presented the security issues arising when moving to a cloud environment.

V. REFERNCES

[1]. Farad Sabah," Cloud Computing Security Threats and Responses" Faculty of Computer Engineering Azad University,Iran .ICCN,2011 IEEE Proceedings. Page No 245-249

[2]. Ramgovind S, Eloff MM, Smith E," The Management of Security in Cloud Computing" ,2010 IEEE proceedings.

[3]. Chi-Chun Lo, Chun-Chieh Huang, Joy Ku "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks", 2010 39th International Conference on Parallel Processing Workshops

[4]. Sameera Abdulrahman Almulla, Chan Yeob Yeun " Cloud Computing Security Management". July 2011 IEEE 4th International conference on cloud computing, CLOUD 2011.

[5]. Shirlei Aparecida de Chaves, Carlos Becker Westphall and Flavio Rodrigo Lamin,"SLA Perspective in Security Management for Cloud Computing", 2010 Sixth International Conference on Networking and Services.

[6]. Joshua Schiffman,Thomas Mayer,Hayawardh Vijaya Kumar,Trest Jaeger and Patrick McDaniel " Seeding clouds with trust Anchors",CCSW 10,October 2010