ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

Security Threats in Cloud Computing

Rashmi Konnur[1], Keerti Dullolli [2], Sudeepkumar Kundgol [3]

U.G. Student, Department of Computer Application, KLE's BCA College, Hubballi, Karnataka, India[1]

U.G. Student, Department of Computer Application, KLE's BCA College, Hubballi, Karnataka, India[2]

Assistant Professor, Department of Computer Application, KLE's BCA College, Hubballi, Karnataka, India[3]

ABSTRACT: Cloud computing is a technology that uses the internet and central remote servers to maintain the data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. The simple example of cloud computing is Yahoo email, g mail, or Hotmail etc. All we need is just an internet connection and we can start sending emails.

KEYWORDS: Cloud computing; Data security; Network security; Cloud service provider security.

I. INTRODUCTION

Cloud computing is a technology that uses the internet and central remote servers to maintain the data and applications. Cloud computing is broken down into three segments: "application" "storage" and "connectivity." Each segment serves a different purpose and offers different products for businesses and individuals around the world.
A simple example of cloud computing is Yahoo email, Gmail, or Hotmail etc. All you need is just an internet connection and you can start sending emails. The server and email management software is all on the cloud (internet) and is totally managed by the cloud service provider Yahoo, Google etc. The Cloud Security Alliance has put together a list of the nine most prevalent and serious security threats in cloud computing. The security threats are as follows:

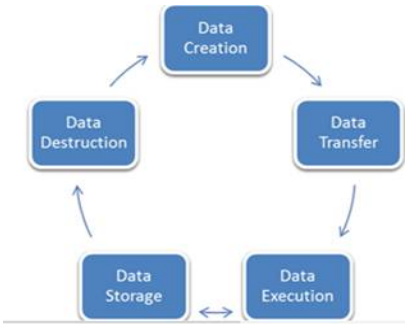

Fig 1: Data life cycle in cloud computing.

A.Data Threats

1) Data Breaches:

Data breach is defined as the leakage of sensitive customer or organization data to unauthorized user. Data breach from organization can have a huge impact on its business regarding finance, trust and loss of customers. This may happen accidently due to flaws in infrastructure, application designing, operational issues, insufficiency of authentication, authorization, and audit controls [2].
An example of data breach is cross VM side channel attack introduced by Y. Zhang et al. that extracts cryptographic keys of other VMs on the same system and can access their data [3].

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

2) Data Loss:
Data loss is the second most important issue related to cloud security. Like data breach, data loss is a sensitive matter for any organization and can have a devastating effect on its business. Data loss mostly occurs due to malicious attackers, data deletion, data corruption, loss of data encryption key, faults in storage system, or natural disasters. 44percent of cloud service providers have faced brute force attacks in 2013 that resulted in data loss and data leakage [4].

B. Network Threats
1) Account or Service Hijacking:
Account hijacking involves the stealing of user credentials to get an access to his account, data or other computing services. These stolen credentials can be used to access and compromise cloud services. The network attacks including phishing, fraud, Cross Site Scripting (XSS), botnets, and software vulnerabilities such as buffer overflow result in account or service hijacking. This can lead to the compromise of user privacy as the attacker can eavesdrop on all his operations, modify data, and redirect his network traffic. 1n 2009 a legitimate service was purchased from Amazon's EC2, and compromised to act as Zeus botnet [5].

2) Denial of Service:
Denial of Service (DOS) attacks are done to prevent the legitimate users from accessing cloud network, storage, data, and other services. DOS attacks have been on rise in cloud computing in past 5 years and 81percent customers consider it as a significant threat in cloud [1]. They are usually done by compromising a service that can be used to consume most cloud resources such as computation power, memory, and network bandwidth. This causes a delay in cloud operations, and sometimes cloud is unable to respond to other users and services.

C. Cloud Environment Specific Threats
1) Insecure Interfaces and APIs:
Application Programming Interface (API) is a set of protocols and standards that define the communication between software applications through internet. Cloud APIs are used at all the infrastructure, platform and software service levels to communicate with other services. Infrastructure as a Service (IaaS) APIs are used to access and manage infrastructure resources including network and VMs, Platform as a Service (PaaS) APIs provide access to the cloud services such as storage and Software as a Service (SaaS) APIs connect software applications with the cloud infrastructure.

2) Malicious Insiders:
A malicious insider is someone who is an employee in the cloud organization, or a business partner with an access to cloud network, applications, services, or data, and misuses his access to do unprivileged activities. Cloud administrators are responsible for managing, governing, and maintaining the complete environment. They have access to most data and resources, and might end up using their access to leak that data. Other categories of malicious insiders involve hobbyist hackers who are administrators that want to get unauthorized sensitive information just for fun, and corporate espionage that involves stealing secret information of business for corporate purposes that might be sponsored by national governments.

3) Abuse of Cloud Services:
The term abuse of cloud services refers to the misuse of cloud services by the consumers. It is mostly used to describe the actions of cloud users that are illegal, unethical, or violate their contract with the service provider. Abusing of cloud services was considered to be the most critical cloud threat in 2010 [2], and different measures were taken to prevent it. However, 84percent of cloud users still consider it as a relevant threat [1]. Over the years, different attacks have been launched through cloud by the malicious users. For example, Amazon's EC2 services were used as a command and control servers to launch Zeus botnet in 2009 [6]. Famous cloud services such as Twitter, Google and Facebook as a command and control servers for launching Trojans and botnets.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

4) Insufficient Due Diligence:
The term due diligence refers to individuals or customers having the complete information for assessments of risks associate with a business prior to using its services. Cloud computing offers exciting opportunities of unlimited computing resources, and fast access due which number of businesses shift to cloud without assessing the risks associated with it.

5) Shared Technology Vulnerabilities:
Cloud computing offers the provisioning of services by sharing of infrastructure, platform and software. However, different components such as CPUs, and GPUs may not offer cloud security requirements such as perfect isolation. Moreover, some applications may be designed without using trusted computing practices due to which threats of shared technology arise that can be exploited in multiple ways. In recent years, shared technology vulnerabilities have been used by attackers to launch attacks on cloud. One such attack is gaining access to the hypervisor to run malicious code, get unauthorized access to the cloud resources, VMs, and customer's data.

II. SOLUTION

A. Data Security

1) Protection from Data Breaches:
Some measures that must be taken to avoid data breaches in cloud are to implement proper isolation among VMs to prevent information leakage, implement proper access controls to prevent unauthorized access, and to make a risk assessment of the cloud environment to know the storage of sensitive data and its transmission between various services and networks.
Considerable amount of research has been carried out for the protection of data in cloud storage. Cloud Proof [8] is system that can be built on top of existing cloud storages like Amazon S3 and Azure blob to ensure data integrity and confidentiality using encryption. To secure data in cloud storage attributed based encryption can be used to encrypt data with a specific access control policy before storage. Therefore, only the users with access attributes and keys can access the data [9]. Another technique to protect data in cloud involves issuing scalable and fine grained data access control [10]. In this scheme, access policies are defined based on the data attributes.
This is achieved by combining techniques of attribute based encryption, proxy re-encryption, and lazy re-encryption

2) Protection from Data Loss:
To prevent data loss in cloud different security measures can be adopted. One of the most important measures is maintaining backup of all data in cloud which can be accessed in case of data loss. Different data loss prevention (DLP) mechanisms have been proposed in research and academics for the prevention of data loss in network, processing, and storage.
R Chow et al. proposed the usage of Trusted Computing to provide data security. A trusted server can monitor the functions performed on data by cloud server and provide the complete audit report to data owner. In this way, the data owner can be sure that the data access policies have not been violated [11]. Tomoyoshi T. et al. proposed a system to protect moving data of a company inside a USB even if it is lost.

B. Network Security

1) Protection from Account or Service Hijacking:
Account or service hijacking can be avoided by adopting different security features on cloud network. These include employing intrusion detection systems (IDS) in cloud to monitor network traffic and nodes for detecting malicious activities. An IDS system for cloud was designed by combining system level virtualization and virtualmachine monitor (responsible for managing VMs) techniques

2) Protection from Denial of Service:
To avoid DOS attacks it is important to identify and implement all the basic security requirements of cloud network, applications, databases, and other services. Applications should be tested after designing to verify that they have no loop holes that can be exploited by the attackers. The DDOS attacks can be prevented by having extra network bandwidth, using IDS that verify network requests before reaching cloud server, and maintaining a backup of IP pools for urgent cases.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

C. Cloud Environment Security

1) Protection from Insecure Interfaces and APIs:

To protect the cloud from insecure API threats it is important for the developers to design these APIs by following the principles of trusted computing. Cloud providers must also ensure that all the APIs implemented in cloud are designed securely, and check them before deployment for possible flaws. Strong authentication mechanisms and access controls must also be implemented to secure data and services from insecure interfaces and APIs.

2) Protection from Malicious Insiders:

The protection from these threats can be achieved by limiting the hardware and infrastructure access only to the authorized personnel. The service provider must implement strong access control, and segregation of duties in the management layer to restrict administrator access to only his authorized data and software.

3) Protection from Abuse of Cloud Services:

The implementation of strict initial registration and validation processes can help in identifying malicious consumers. The policies for the protection of important assets of organization must also be made part of the service level agreement (SLA) between user and service provider. Packets and all the updated security devices in network should be installed.

4) Protection from Insufficient Due Diligence:

It is important for organizations to fully understand the scope of risks associated with cloud before shifting their business and critical assets such as data to it. The service providers must disclose the applicable logs, infrastructure such as firewall to consumers to take measures for securing their applications and data [11]. Moreover, the provider must setup requirements for implementing cloud applications, and services using industry standards. Cloud provider should also perform risk assessment using qualitative and quantitative methods after certain intervals to check the storage, flow, and processing of data.

5) Protection from Shared Technology Vulnerabilities:

In cloud architecture, hypervisor is responsible for mediating interactions of virtual machines and the physical hardware. Therefore, hypervisor must be secured to ensure proper functioning of other virtualization components, and implementing isolation between VMs. Moreover, to avoid shared technology threats in cloud a strategy must be developed and implemented for all the service models that include infrastructure, platform, software, and user security. The baseline requirements for all cloud components must be created, and employed in design of cloud architecture

III. CONCLUSION

Cloud computing is getting widely adopted in businesses around the world. In this paper we have focused on most severe threats on cloud computing that are considered relevant by most users and businesses. We have divided these threats into categories of data threats, networks threats, and cloud environment specific threats. The impact of these threats on cloud users and providers has been illustrated in the paper. Moreover, we also discuss the security techniques that can be adopted to avoid these threats.

REFERENCES

[1] T. T. W. Group et al., "The notorious nine: cloud computing top threats in 2013," Cloud Security Alliance, 2013.
[2] C. S. Alliance, "Top threats to cloud computing v1. 0, Cloud Security Alliance, USA, 2010.
[3] Y. Zhang, A. Jules, M. K. Reiter, and T. Ristenpart, "Cross-vm side channels and their use to extract private keys," in Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012, pp. 305–316.
[4] "Cloud security report spring 2014," https://www.alertlogic.com/ resources/cloud-security-report//, last Accessed: 2014-11-08.
[5] "Zeus bot found using amazon's ec2 as c and c server," http://www. theregister.co.uk/2009/12/09/amazon ec2 bot control channel//, last Accessed: 2014-11-15.
[6] "Amazon ec2 cloud service hit by botnet, outage," http://www.cnet.com/uk/news/amazon-ec2-cloud-service-hit-by-botnet-outage/, last Accessed: 2014-11-15.
[7] K. Kortchinsky, "Cloudburst: A vm-ware guest to host escape story," Black Hat USA, 2009.
[8] R. A. Popa, J. R. Lorch, D. Molnar, H. J. Wang, and L. Zhuang, "Enabling security in cloud storage slas with cloudproof." in USENIX Annual Technical Conference, vol. 242, 2011.
[9] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384–394, 2014.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in INFOCOM, 2010 Proceedings IEEE.Ieee, 2010, pp. 1–9.
[11] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation withoutoutsourcing control," in Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, 2009, pp. 85–90.

BIOGRAPHY

Rashmi Konnur studying in KLES's BCA P C Jabin Science College Hubballi. Under Karnataka University dharwad . her research interest includes the security threats in cloud computing

Keerti Dullolli studying in KLES's BCA P C Jabin Science College Hubballi. Under Karnataka University dharwad . her research interest includes the security threats in cloud computing

Sudeepkumar kundgol received his BE and Mtech in Computer Science Engineering from Visvesvaraya Technological University Karnataka in 2008 and 2015 respectively. He is currently with department of Computer application KLE's P.C Jabin Science College Hubblli, Karnataka. His research interest includes the privacy preserving in smart grid, cloud computing, etc..