National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

A Survey - Security and Privacy Issues In Cloud Computing

Sheela D V
Soundarya Institute of Management and Science, Bangalore University, Karnataka, India

ABSTRACT

Cloud Computing is inevitability as the number of connected devices are growing and also the computing and storage needs. Cloud computing converts the way Information Technology is encouraged and succeeded, cost worth, faster invention, faster time-to-market, and the capable to measure applications on demand. Security of the cloud is a major challenge today which has to be addressed. Several new technologies are emerging to keep the cloud services secure and efficient at the same time. This paper discusses the cloud services, risk associated with it and security measures in cloud computing.

Keywords : Public cloud, Private cloud, Hybrid cloud, Infrastructure as a service (Iaas), Software as a service (Saas), Platform as a service (Paas)

I. INTRODUCTION

Cloud Computing [1] is gaining importance in leaps and bounds and is expected to increase its usage in years to come. Cloud computing enables resources to be shared in a pool that can be rapidly provisioned and can be offered to the user with minimal interaction of the service provider. The main aim of the cloud computing is to provide secure, [2] quick and convenient data storage and computing service to the users. This paper discusses available types of cloud and various types of services offered to the end users in succeeding sections. The clouds which are accessible to the masses by internet wherein the user uses the service like application and storage are called public clouds.[10] The Clouds which are owned by a single company and are restricted to be used by its own set of people are called private cloud.[9] The Hybrid approach,[11] combines the above two types and is discussed in detail further in this paper. The highlight of the security issue on cloud computing is focused in the SPI model i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Internet as a service (IaaS) and id discussed in detail in this paper.

The Saas is the service provided to the user for using application running on the cloud. The PaaS[5] is the service offered by the service provider to install customer's own application on the service provider's cloud infrastructure without installing any additional tools and software on their local machines. The Iaas is the service provided to the user to utilize the facility of storage, processing and networking so that customer can run and deploy any software or tool on this platform. The paper then discusses and identifies the main vulnerabilities in these kinds of systems and also the threats related to these systems.

II. METHODS AND MATERIAL

2.1 TYPES OF CLOUDS

Cloud computing comes in basic three forms: public clouds, private clouds, and hybrids clouds. Virtual private clouds and Community clouds are few

modifications of the basic clouds. Depending on the type of data public, [10] private, and hybrid clouds, can be analyzed in terms of security and management requirement.

Fig.1 Types of cloud

2.2 PUBLIC CLOUDS

A public cloud [10] is basically the internet and is implemented using a shared data center infrastructure of hardware and software that is shared by multiple users. The data center is off-premises. Public Cloud service providers use the internet to provide resources, such as applications and storage to the general public, or on a 'public cloud. Examples of public clouds include Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google App Engine and Windows Azure Services Platform. The disadvantages of the public cloud is limited configuration, security, and specifications of SLA, making it unideal for services using delicate data that is subject to compliancy principles.

2.3 PRIVATE CLOUDS

Private clouds are data centers which are owned by a single company that provides flexibility, scalability, provisioning, automation and monitoring. A Private Cloud[9] is implemented using a dedicated infrastructure of hardware and software that is used privately by an organization. The data center can be on-premises or off-premises. It is not shared with another organization. The goal of a private cloud is to use the cloud "as- a-service" for its employees to gain the benefits of cloud architecture rather than offerings to external customers. Private clouds are quite expensive with typically uncertain economies of scale. This type of cloud can be an option for Small-to-Medium sized enterprises and is mostly used by large scale enterprises. Private clouds are focused on security and compliance, and keeping resources within the firewall.

2.4 HYBRID CLOUDS

A Hybrid Cloud [11] is any combination of Private cloud and public cloud. Similarly it is also a combination of Virtual Private Cloud and one or more Public Clouds. The resources are shared among the Clouds in Hybrid approach. By using a Hybrid approach, companies can maintain control of an internally managed private cloud while relying on the public cloud as and when needed. For example during peak times a single application, or portions of applications can be transferred to the Public Cloud. This will also be useful during expected disruption: floods, scheduled maintenance windows, power failure. Due to the cost, it is hard to maintain an off-premise disaster recovery site for most organizations. Though there are some lower cost solutions and alternatives that slow down the band an organization gets, at this times the recovery of the data quickly reduces. Cloud based

Disaster Recovery (DR)/Business Continuity (BC) services allow organizations to contract failover out to a Managed Services Provider that maintains multi-tenant infrastructure for DR/BC, and specializes in getting business back online quickly.

2.5 VIRTUAL PRIVATE CLOUDS

A Virtual Private Cloud is created using a shared data center infrastructure of hardware and software. The data center is most likely off-premises. It is shared with multiple organizations. If the data center is not shared then that is a Private Cloud. The topmost layers of the Cloud Computing Stack (PaaS and SaaS) in a Virtual Private Cloud is dedicated to the

organization. The lower layer of IaaS is shared among various users in a Virtual Private Cloud. A Virtual Private Cloud can join in a Hybrid Cloud also.

2.6 COMMUNITY CLOUDS

A Community Cloud acts as a Private Cloud, Virtual Private Cloud, Public Cloud, or Hybrid Cloud. The design of a Community Cloud meets the need of a community. Such communities involve people or organizations that have shared interests. The communities such as industrial community, research community, standards community, and so on. So, a Community Cloud is not considered to be a cloud since it looks like it. Only few member organization data center support the Community Cloud.

2.7 TYPES OF CLOUD SERVICES

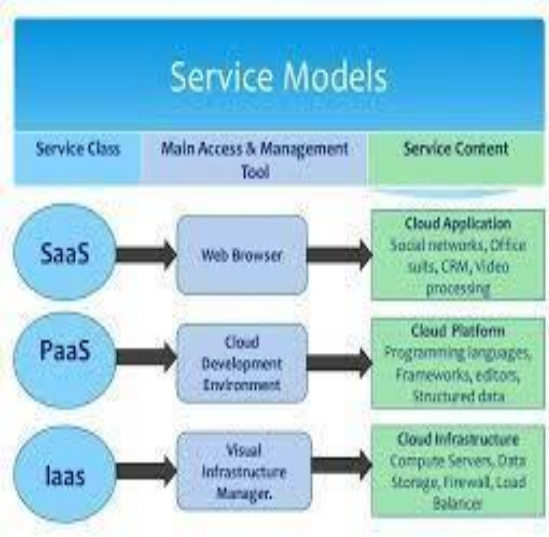

Fig.2 Types of Cloud Services

2.8 INFRASTRUCTURE AS A SERVICE (IaaS)

This service provides the customers with a collection of bare metal devices and software which are required to fulfill the computational and storage needs of the users. IaaS gives business access to web architecture, like storage space, servers, and connections, without purchasing and managing this infrastructure. It is economical to both service provider and user, in particular IaaS allows an internet business a way, to develop and grow on demand. Both PaaS [5] and SaaS clouds are a layer overlaid on IaaS clouds. The examples of IaaS are Amazon EC2 and Rack space Cloud.

2.9 PLATFORM AS A SERVICE (PaaS)

It is a layer over Iaas. PaaS has all flavors of operating environment to meet the various computational needs of the customer. The customer has the freedom to run any application without any additional expenditure of the operating environment and hardware requirements. Some examples of a PaaS [5] system include Mosso, Google App Engine, and Force.com. Main benefit of a PaaS is that it is an economical option for the user where the user can initiate application with no stress of the platform required for that application. A little porting may be required if you are dealing with an existing app. PaaS offers a lot of scalability by design because it is based on cloud computing. If you want a lean operations staff, PaaS is an option which will provide maximum output with limited staff.

2.10 SOFTWARE AS A SERVICE (SaaS)

SaaS is the topmost layer in the cloud stack which encompasses the software/applications [18] for the users. SaaS delivers the software services to the user over web. SaaS offers the users the advantage of not installing any software on their personal computers and neither the burden of maintenance of software which they use as per their computational needs. Examples of SaaS running on cloud are Gmail and Sales force, but it is not necessary that all SaaS has to be based on cloud computing.

III. THREATS RISKS OF CLOUD COMPUTING

There are a number of security risks [14] associated with cloud computing that must be adequately addressed:

1. LOSS OF GOVERNANCE.

While using public cloud, user have to surrender control to the cloud provider over a number of issues that may affect security. The service agreements provided by the service provider may not offer an assurance to solve such issues on the part of the cloud provider. This leaves a gap in security defense.

2. RESPONSIBILITY AMBIGUITY.

Responsibility of security issues may be split between the provider and the customer. This division of responsibility creates a critical vulnerability of unallocated responsibilities of critical security issues. This split is likely to vary depending on the cloud computing model used (e.g., IaaS vs. SaaS).

3. AUTHENTICATION AND AUTHORIZATION.

Cloud resources can be accessed from anywhere in the world on the Internet. This brings out a very important requirement of establishing with certainty the identity of a user especially if users now include employees, contractors, partners and customers. Authentication and authorization thus becomes a critical requirement to ensure security.

4. ISOLATION FAILURE.

Multi-tenancy and shared resources are main characteristics of public cloud computing. The isolation of storage, memory, routing and even reputation between tenants becomes a challenge which has to be dealt with for secure cloud operations (e.g. so-called guest- hopping attacks).

5. COMPLIANCE AND LEGAL RISKS.

It is very necessary for the service provider to prove that the services provided by the cloud comply with the industry standards for the customer to be completely satisfied before hiring the cloud service. The service provider must permit audits by the cloud customer. The customer must themselves verify that the cloud provider has appropriate certifications in place.

6. HANDLING OF SECURITY INCIDENTS.

he customer may hand over detection; reporting and successive management of security incidents to the cloud service provider, but these incidents affect the customer. Notification rules need to be discussed in the cloud service agreement so that customers are not caught unaware or informed with an unacceptable delay.

7. MANAGEMENT INTERFACE VULNERABILITY.

Interfaces to manage public cloud resources are usually accessible through the Internet. Since they allow access to larger number of resources than traditional hosting providers, they pose an increased risk, especially when combined with remote access and web browser vulnerabilities.

8. APPLICATION PROTECTION.

The defense-in-depth security approach is based on a clear demarcation of physical and virtual resources, and on trusted zones. In cloud computing the responsibility of infrastructure security is delegated to the cloud provider. The organizations now need to re plan perimeter security at the network level by incorporating more controls at the user, application and data level.

9. DATA PROTECTION.

Data Protection covers unauthorized exposure or leakage of sensitive data as well as the loss or unavailability of data. It is impossible for a customer (in the role of data controller) to keep a check on the data handling practices of the cloud provider. This problem increases greatly for cases of multiple transfers of data.

10. MALICIOUS BEHAVIOR OF INSIDERS.

Malicious actions of insiders within an organization can cause substantial damage, given the access and authorizations they enjoy. In the cloud computing environment this risk increases since such activity

might may occur within the customer organization or the provider organization.

11. BUSINESS FAILURE OF THE PROVIDER.
Such failures could render data and applications essential to the customer's business unavailable over an extended period.

12. SERVICE UNAVAILABILITY.
This could be caused by hardware, software or communication network failures.

13. VENDOR LOCK-IN.
Proprietary services of a specific cloud service provider could make the customer depend on that provider only. Absence of portability of applications and data among cloud service providers creates a chance of data and service unavailability in case of a change in providers; therefore it is an aspect of security issue. The absence of interoperability of interfaces associated with cloud services ties the customer to a particular provider and switching of provider becomes a difficult task.

14. INSECURE OR INCOMPLETE DATA DELETION.

After termination of a contract with a provider the data of the user may not be completely deleted. Backup copies of data usually exist, and there is a chance that this data may be mixed with other customers' data. The benefit of multi-tenancy thus posses a considerable risk to the customer than dedicated hardware.

IV. CLOUD SECURITY GUIDANCE

The applications and data which are critical for the customers to maintain are forwarded to the cloud to avail the cloud services. This section provides a recommended series of steps for cloud customers to estimate and manage the security of their use of cloud services, with the goal of mitigating risk and delivering an appropriate level of support.

1. Ensure effective governance, risk and compliance processes exist
2. Audit operational and business processes
3. Manage people, roles and identities
4. Ensure proper protection of data and information
5. Enforce privacy policies
6. Assess the security provisions for cloud applications
7. Ensure cloud networks and connections are secure
8. Evaluate security controls on physical infrastructure and facilities

PRESENT SECURITY SYSTEM IN CLOUD

There are mainly seven categories of the cloud security. The three major problems identified after referring to the various references are legal issues, compliance and loss of control over data.
Network Security Interfaces Data Security Virtualization Governance Legal Issues E- Discovery
Various sub security issues under these main categories which ensure a secure cloud system are:-

1. Network Security:-
The issue related to the communication of the networks and their configuration with respect to cloud computing setup.

Firewall: - One of the most efficient and successful protection can be achieved by installing firewall which will analyze and control communication of data and applications. It prevents the DoS attacks and any other abnormal instance on the cloud. Main advantages of a firewall are Secure Data Centre, Secure Remote Access, Identity and Management

Transit security: - Existing infrastructure of VPN (Virtual Private Network) model should be exercised

to protect the cloud from side channel attack spoofing, man in middle and sniffing.

2. Interfaces

All issues related to human and electronic interfaces like user interface, programming interface, administrative interface etc for accessing and controlling the cloud network are critical in securing the user's interest. Main interfaces which provide secure system are:

a. Application programming Interfaces (API)

b. Administrative Interface c. User Interface

c. Access authentication

3. Data Security:-

a. Confidentiality Integrity and Availability (CIA) protection must be ensured by all available means.

b. Redundancy: Mission critical data integrity and availability must be ensured while catering for redundant storage of data.

c. Data disposal: Deletion is the common technique used for the data disposal but in the parlance of cloud all the log reference, hidden backup, registers and complete destruction of data should be ensured.

4. Virtualization: - VMs (Virtual Machine) isolation and vulnerabilities of the third party virtual platform like hypervisor must be addressed to ensure the security of the user's data and application. a. Cross- VM attacks:- It calculates the providers traffic ingress and egress rate in order to steel cryptographies key and increase changes of VM placement attacks.

b. VM identification: - Lack of controls for identifying virtual machines that are being used for executing a specific process or for storing files.

c. Data leakage: - Exploitation of the hypervisor vulnerabilities in order to leak data from virtualized infrastructure.

5. Governance:-

Problems related to administrative and technical controls in cloud computing solutions are:-

a. Data control: - Moving data to the cloud means losing control over redundancy, location, file systems and other relevant configurations

b. Compliance: - Includes requirements related to service availability and audit capabilities. c. SLA: Mechanisms: - to ensure the required service availability and the basic security procedures to be adopted. Service Level Agreement between the Provider and the company should be ensured for frequent Audits and resolution of the critical issues.

d. Loss of service: - Very strong and robust disaster recovery policies and also customer side redundancy should be implemented to avoid service outages in the cloud environments.

e. Audit: - Helps security and availability assessments to be done by customers and third party participants. Fair methodology should be adopted for continuous analyzing service conditions.

6. Legal issues:- Issues related to judicial requirements and laws, like different data storage location and privilege escalation management.

a. Data storage location: - For the achievement of redundancy the data is stored in various multiple geographic locations. No common cyber laws across the globe directly or indirectly affect the law enforcement measures.

b. E-Discovery: - Confiscated hardware for investigation may also affect the stored data of other customers also. Data disclosure is critical in this case.

V. CONCLUSION

Cloud computing is the future of computing and storage technology. The exponential increase of connected devices and the need of small and portable devices for complex computation warrant

the growth of cloud computing technology. This paper has discussed the cloud technology, various security threats and prevention measures for ensuring a secure cloud system. The need for security is increasing along with the increasing demand of cloud computing services and the balance has to be maintained hand-in-hand.

VI. REFERENCES

[1]. Brian F. Cooper , Adam Silberstein , Erwin Tam , Raghu Ramakrishnan , Russell Sears, Benchmarking cloud serving systems with YCSB, Proceedings of the 1st ACM symposium on Cloud computing, June 10-11, 2010, Indianapolis, Indiana, USA [doi>10.1145/1807128.1807152]

[2]. "Security Guidance for Critical Areas of Focus in Cloud Computing", Cloud Security Alliance, Dec. 2009, [online] Available:

[3]. T. Ristenpart, "Hey You Get Off of My Cloud! Exploring Information Leakage in Third-Party Compute Clouds", Proc. 16th ACM Conf. Computer and Communications Security (CCS 09)

[4]. "Security of virtualization, cloud computing divides IT and security pros". Network World. 2010-02-22. Retrieved 2010-08-22.

[5]. Boniface, M.; et al. (2010), Platform-as- a-Service Architecture for Real-Time Quality of Service Management in Clouds, 5th International Conference on Internet and Web Applications and Services (ICIW), Barcelona, Spain: IEEE, pp. 155– 160, doi:10.1109/ICIW.2010.91

[6]. Amies, Alex; Sluiman, Harm; Tong, Qiang Guo; Liu, Guo Ning (July 2012). "Infrastructure as a Service Cloud Concepts". Developing and Hosting Applications on the Cloud. IBM Press. ISBN 978-0-13-306684- 5.

[7]. Foley, John. "Private Clouds Take Shape". InformationWeek. Retrieved 2010- 08-22.

[8]. Jump up^ Haff, Gordon (2009-01-27). "Just don't call them private clouds". CNET News. Retrieved 2010-08-22.

[9]. "There's No Such Thing As A Private Cloud". InformationWeek. 2010-06-30. Retrieved 2010-08-22.

[10]. Jump up^ Rouse, Margaret. "What is public cloud?". Definition from Whatis.com. Retrieved 12 October 2014.

[11]. Jump up^ "Mind the Gap: Here Comes Hybrid Cloud – Thomas Bittman". Thomas Bittman. Retrieved 22 April 2015.

[12]. "Business Intelligence Takes to Cloud for Small Businesses". CIO.com. 2014-06- 04. Retrieved 2014-06-04.

[13]. Désiré Athow. "Hybrid cloud: is it right for your business?". TechRadar. Retrieved 22 April 2015.

[14]. Srinavasin, Madhan (2012). "'State-of- the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment". ACM ICACCI'.

[15]. "Swamp Computing a.k.a. Cloud Computing". Web Security Journal. 2009-12-28. Retrieved 2010-01-25

[16]. "Top Threats to Cloud Computing v1.0" (PDF). Cloud Security Alliance. Retrieved 2014-10-20.

[17]. Winkler, Vic. "Cloud Computing: Virtual Cloud Security Concerns". Technet Magazine, Microsoft. Retrieved 12 February 2012.

[18]. "Software as a Service (SaaS)". Cloud Taxonomy. Open crowd. Retrieved 24 April 2011.

Cite this article as :

Sheela D V, "A Survey - Security and Privacy Issues In Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 13-19, September-October 2019.

Journal URL : http://ijsrcseit.com/CSEIT19473