ISSN 2348 - 2249
Volume-2, Issue-2, June-2014
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

# Survey Paper On Various Security Concerns In Cloud Computing And Approach To Enhance Security

**Gurjot Singh Sodhi**
Department of Computer Engineering
SUSGOI, Tangori
India
er.gurjotsinghsodhi@gmail.com

**Gurjit Singh Bhathal**
Department of Computer Engineering
Punjabi University, Patiala
India
gurjit.bhathal@gmail.com

***Abstract*** **-** Cloud computing emerges as a new computing paradigm which aims to provide reliable, customized and Quality of Service guaranteed dynamic computing environments for end-users. However, adopting a cloud computing paradigm may have positive as well as negative effects on the data security of service consumers. In a cloud computing environment, data and the application is controlled by the service provider. This leads to a natural concern about data safety and also its protection from internal as well as external threats. The major issues in cloud computing is the security of data being stored on the provider's cloud and privacy while the data is being transmitted. This paper deals with the major security concerns that needs to be taken into consideration to ensure that unauthorized intruder can't access your file or data in cloud.

***Keywords –*** SLAs-Service Level Agreements, CSP – Cloud, Service Provider, Cloud Customer or Client, VM – Virtual Machine, SaaS , PaaS , IaaS, Virtualization

## I. INTRODUCTION

Today in the ever expanding IT environment, the IT budget is becoming tighter and smarter but the user requirements are still escalating. So to meet Business and User requirements, focus needs to be shifted on something that generates results in most efficient and cost effective manner.

Cloud computing technology enables the IT industry to utilizes their existing infrastructure and also adding some new dimensions to their businesses. However this new technology does raise some concerns, but chief among them is the Security of user content in Cloud.

Cloud Computing is a form of distributed computing that is yet to be standardized [1]. Its important to note that all Cloud Services are not equal. Clear Terms and conditions should be agreed among the Client and the Provider for all the security requirements, and roles must be defined for operations, management and reporting.

### A. What is Cloud Computing ?

Cloud computing provides a model for enabling on-demand network access to a shared pool of computing resources (for example: networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction.[2]

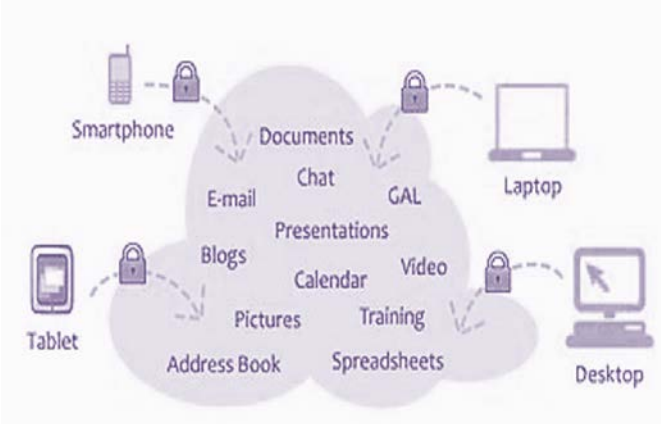


Fig. 1 Cloud Computing [3]

### B. Cloud Deployment Models

Deployment models are defined to distinguish between different models of ownership and distribution of the resources used to deliver cloud services to different customers. The most common deployment models, as defined by NIST, include:

**Private cloud** – The cloud infrastructure is operated solely for a single organization (client). It may be managed by the organization itself or a third-party provider, and may be on-premise or off-premise. However, it must be solely dedicated for the use of one entity.

**Community cloud** – The cloud infrastructure is shared by several organizations and supports a specific community with shared requirements or concerns (for example, business model, security requirements, policy, or compliance considerations). It may be managed by the organizations or a third party, and may be on-premise or off-premise.

**Public cloud** – The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. Public cloud infrastructure exists on the premises of the cloud provider.

**Hybrid cloud** – The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by technology to enable portability. Hybrid clouds are often used for

 

ISSN 2348 - 2249
Volume-2, Issue-2, June-2014
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

redundancy or load-balancing purposes—for example, applications within a private cloud could be configured to utilize computing resources from a public cloud as needed during peak capacity times (sometimes called "cloud-bursting").

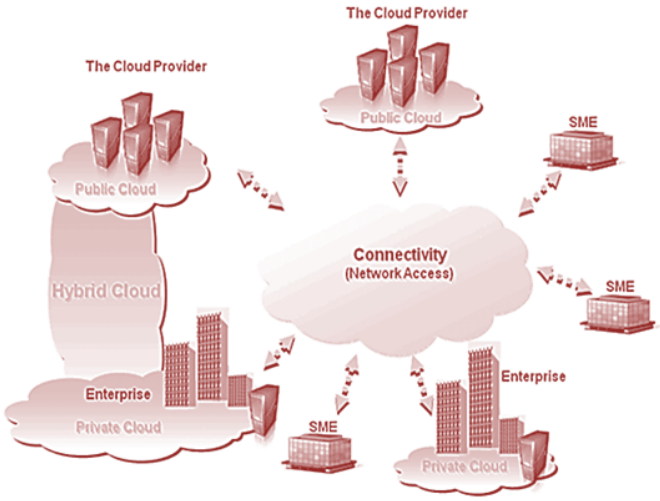


Fig. 2 Cloud Deployment Models

### C. Cloud Service Models

Service models identify different control options for the cloud customer and cloud provider. The three most commonly used Service Models are :

**Software as a Service (SaaS)** – Capability for clients to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser, or a program interface.

**Platform as a Service (PaaS)** – Capability for clients to deploy their applications (created or acquired) onto the cloud infrastructure, using programming languages, libraries, services, and tools supported by the provider.

**Infrastructure as a Service (IaaS)** – Capability for clients to utilize the provider's processing, storage, networks, and other fundamental computing resources to deploy and run operating systems, applications and other software on a cloud infrastructure.

## II. SECURITY CONSIDERATIONS

Security is a principal concern when entrusting an organization's critical information to geographically dispersed cloud platforms not under the direct control of that organization. In addition to the conventional IT information system security procedures, designing security into cloud software during the software development life cycle can greatly reduce the cloud attack surface.

The security posture of a cloud system is based on its security architecture. While there is no standard definition for security architecture, the Open Security Alliance (OSA) defines security architecture as "the design artifacts that describe how the security controls (= security counter measures) are positioned, and how they relate to the overall IT Architecture.

Secure cloud communications involves the structures, transmission methods, transport formats, and security measures that provide confidentiality, integrity, availability, and authentication for transmissions over private and public communications networks.

### A. Service Level Agreements (SLAs)

Typically, cloud-hosting agreements are concerned with "up-time" and high availability, with little or no mention or assurance of security. However, the client is ultimately responsible for ensuring the service they're using meets their security requirements and compliance obligations. Thus, SLAs and other written agreements between CSP and the Client should clearly identify their responsibilities.

Failure to develop and agree upon appropriate SLAs may result in issues for the client if the cloud service does not meet the needs and demands of their business.

### B. Data Acquisition

The client will ultimately determine how and when the cardholder data is acquired in the cloud environment. End-to-end processes and data flows must be documented across both client and cloud provider networks, so that it is clearly understood where cardholder data is located and how it is traversing the infrastructure.

### C. Data Life-Cycle

For all Cloud models, it must be made a compulsion for CSP to provide clear requirements for Data retention, storage and disposal, in order, to ensure that sensitive data is-

Retained for as per SLAs.

Stored in Secured location.

Accessible only to Authorized user.

### D. Data Integrity

When a data is on a cloud anyone from any location can access those data's from the cloud. Cloud does not differentiate between a sensitive data from a common data thus enabling anyone to access those sensitive data's. Thus there is a lack of data integrity in cloud computing.

### E. Data Encryption and Key Management[4]

In a public-cloud environment, one client's data is typically stored with data belonging to multiple other clients. This makes a public cloud an attractive target for attackers. Strong data-level encryption should be enforced on all sensitive or potentially sensitive data stored in a public cloud.

At a minimum, key-management servers should be located in a separate network segment and protected with separate access credentials from the VMs that are using the keys and the data encrypted with them.

### F. Identity and Access Management

Individual user identification and authentication for both CSP and client personnel is essential for access control and accountability.

 

ISSN 2348 - 2249
Volume-2, Issue-2, June-2014
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

- Shared credentials (such as user accounts and passwords) should not be used in the CSP environment.
- Client accounts and passwords should be unique for each service

## III. HOW TO ENSURE SECURED CLOUD ENVIRONMENT

The implementation of Security in a Cloud Environment requires specialized technical knowledge and skills. So, Secure cloud computing communications should ensure the following :

### A. Confidentiality

Ensures that only those who are supposed to access data can retrieve it. Loss of confidentiality can occur through the intentional release of private company information or through a misapplication of network rights. Some of the elements of telecommunications used to ensure confidentiality are as follows:

- Network security protocols
- Network authentication services
- Data encryption services

### B. Integrity

Ensures that data has not been changed due to an accident or malice. Integrity is the guarantee that the message sent is the message received and that the message is not intentionally or unintentionally altered. Integrity also contains the concept of non-repudiation of a message source. Some of the constituents of integrity are as follows:

- Firewall services
- Communications Security Management
- Intrusion detection services

### C. Availability

Ensures that data is accessible when and where it is needed, and that connectivity is accessible when needed, allowing authorized users to access the network or systems. Also included in that assurance is the guarantee that security services for the security practitioner are usable when they are needed. Some of the elements that are used to ensure availability are as follows:

- Fault tolerance for data availability, such as backups and redundant disk systems
- Acceptable logins and operating process performance
- Reliable and interoperable security processes and network security mechanisms

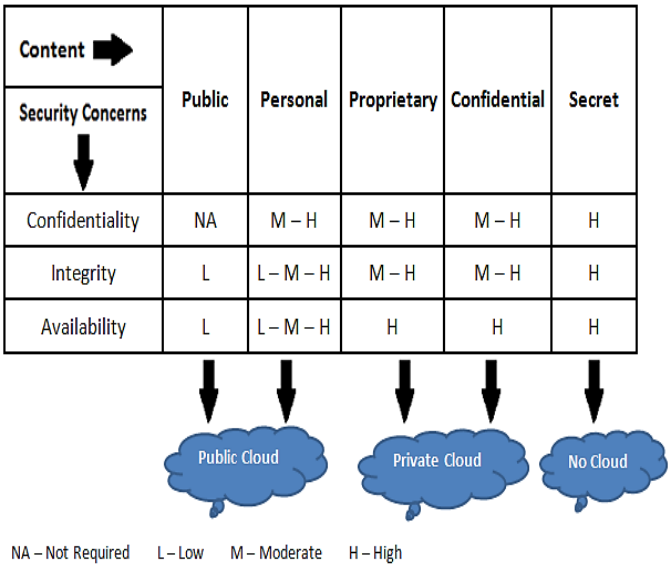


Fig. 3 Classifying User Content on Cloud

### D. Node Hardening

The default nodes issued by the Cloud Provider should not be considered secured as the provider may have used the default System Account, configured with a password and login rights.

This could possibly be used as a Backdoor to other nodes. Also few providers provide the Encrypted Disk operations.

- So before getting the Cloud Service, client must check –
- Unnecessary packages
- Boot/Startup Configurations
- Password Policies
- User Privileges
- Encryption Mechanisms

### E. Virtualization

The hypervisor is the software that provides the virtualization of the nodes and is responsible for ensuring that the nodes are securely segregated while in operation. A security flaw within this software would undermine the whole environment.

Due to the nature of virtualization, shared resources of the physical device will be used. An attacker may be able to leverage this relationship and gain access to resources allocated to other victim nodes. So, management of nodes should be done via a secure mechanism. The majority of providers use a web-based application or an API to manage nodes.

- Following Considerations should be taken into account -
- Secure channel Encryption
- Access Controls
- Up to Date Virtualized Environments
- Memory Separation Technique used
- Resource Exhaustion Prevention Policies
- Availability of Remote Booting for Recovery
- Routing Protocols used
- TCP/ICMP Filtering

 

ISSN 2348 - 2249
Volume-2, Issue-2, June-2014
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

## IV. CONCLUSIONS

The implementation of security controls in a cloud environment may require specialized technical knowledge and skills. It is therefore crucial that prior to migrating payment card operations into a cloud environment, an organization engages their technical, legal, information security, and compliance teams to work together to define the client's needs and evaluate potential cloud service offerings against those needs.

## REFERENCE

[1] *NIST Guidelines on Security and Privacy in Public Cloud Computing (SP SP800-144).*

[2] *The NIST Definition of Cloud Computing* (SP 800-145).

[3] *Tejas P. Bhatt, Ashish Maheta, "Security in Cloud Computing using File Encryption", International Journal of Engineering Research and Technology (IJERT), Vol. 1 Issue 9, November 2012.*

[4] *PCI Data Security Standard v2.0 Guidelines, February 2013.*

[5] *Assessing Cloud Node Security Whitepaper, March 2011*

 