

# Security in Cloud Computing

Shweta Singh  
DIT University ,Dehradun

**Abstract:** Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider. Cloud computing is an architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Thesecurity for Cloud Computing is emerging area for study and this paper providesecurity topic in terms of cloud computing based on analysis of Cloud Security treatsand Technical Components of Cloud Computing.

**Keywords:** Cloud, Services, Cloud service user, Cloud service provider, Security Issues , License Risk, DataAvailability

## 1. INTRODUCTION

The cloud computing is a new computing model which comes from grid computing, distributed computing, parallel computing, virtualization technology, utility computing and other computer technologies and it has more advantage characters such as large scale computation and data storage, virtualization, high expansibility, high reliability and low price service. The security problem of cloud computing is very important and it can prevent the rapid development of cloud computing. This paper introduces some cloud computing systems and analyzes cloud computing security problem and its strategy according to the cloud computing concepts and characters. The data privacy and service availability in cloud computing are the key security problem. Single security method cannot solve the cloud computing security problem and many traditional and new technologies and strategies must be used together for protecting the total cloud computing system.

We are conducting research on secure cloud computing .Due to the extensive complexity of the cloud , we contend that it will be difficult to provide a holistic solution to secure the cloud at present . Therefore our goal is to make increment enhancements to securing the cloud that will ultimately result in a secure cloud . In particular , we are developing a secure cloud consisting of hardware ,software and data . Our cloud system will

- (a) support efficient storage of encrypted sensitive data
- (b) store, manage and query massive amounts of data
- (c) support fine grained access control and
- (d) support strong authentication.

## 2. ARCHITECTURE OF CLOUD COMPUTING

Cloud management system is divided into four layers, respectively the Resources & Network Layer, Services Layer, Access Layer, and User Layer. Each layer includes a set of functions[1]:

The Resources & Network Layer manages the physical and virtual resources.

- The Services Layer includes the main categories of cloud services, namely, NaaS, IaaS, PaaS, SaaS/CaaS, the service orchestration function and the cloud operational function.

- The Access Layer includes API termination function, and Inter-Cloud peering and federation function.
- The User Layer includes End-user function, Partner function and Administration function.
- The Cross layer includes Management, Security & Privacy, etc. are considered as that covers all the layers.

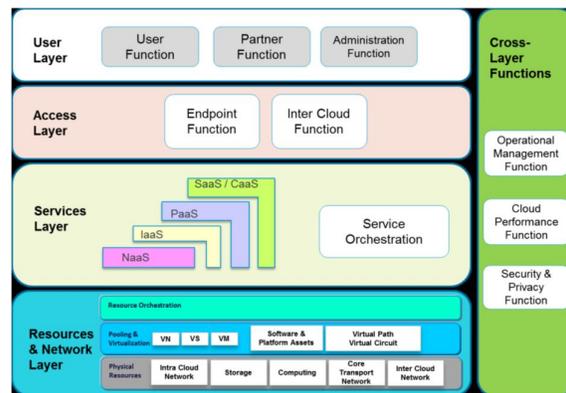


Figure. 1 The Cloud Computing Components

## 3. SECURITY SUBSYSTEM

The five functional security subsystems defined by IBM are as follows:

### 3.1 Audit and Compliance:

This subsystem addresses the data collection, analysis, and archival requirements in meeting standards of proof for an IT environment. It captures, analyzes, reports, archives, and retrieves records of events and conditions during the operation of the system .

### 3.2 Access Control:

This subsystem enforces security policies by gating access to processes and services within a computing solution via identification, authentication, and authorization[5]. In the context of cloud computing, all of these mechanisms must also be considered from the view of a federated access control system.

### **3.3 Flow Control:**

This subsystem enforces security policies by gating information flow and visibility and ensuring information integrity within a computing solution .

### **3.4 Identity and Credential Management:**

This subsystem creates and manages identity and permission objects that describe access rights information across networks and among the subsystems, platforms, and processes, in a computing solution [4]. It may be required to adhere to legal criteria for creation and maintenance of credential objects.

### **3.5 Solution Integrity:**

This subsystem addresses the requirement for reliable and proper operation of a computing solution

## **4. SERVICES PROVIDED**

Generally cloud services can be divided into three categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

### **4.1 Software-as-a-Service (SaaS):**

SaaS can be described as a process by which Application Service Provider (ASP) provides different software applications over the Internet. This makes the customer to get rid of installing and operating the application on own computer and also eliminates the tremendous load of software maintenance; continuing operation, safeguarding and support .SaaS vendor advertently takes responsibility for deploying and managing the IT infrastructure (servers, operating system software, databases, data center space, network access, power and cooling, etc) and processes (infrastructure patches/upgrades, application patches/upgrades, backups, etc.) required to run and manage the full solution. SaaS features a complete application offered as a service on demand. Examples of SaaS includes: Salesforce.com, Google Apps.

### **4.2 Platform as a Service (PaaS):**

PaaS is the delivery of a computing platform and solution stack as a service without software downloads or installation for developers, IT managers or end-users. It provides an infrastructure with a high level of integration in order to implement and test cloud applications.

The user does not manage the infrastructure (including network, servers, operating systems and storage), but he controls deployed applications and, possibly, their configurations. Examples of PaaS includes: Force.com, Google App Engine and Microsoft Azure.

### **4.3 Infrastructure as a Service (IaaS):**

Infrastructure as a service (IaaS) refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. Thus, it offers basic infrastructure on-demand services and using Application Programming Interface (API) for interactions with hosts,

switches, and routers, and the capability of adding new equipment in a simple and transparent manner. In general, the user does not manage the underlying hardware in the cloud infrastructure, but he controls the operating systems, storage and deployed applications. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. Examples of IaaS includes Amazon Elastic Cloud Computing (EC2), Amazon S3, GoGrid

## **5. CLOUD MODELS**

Four different cloud deployment models namely Private cloud, Public cloud, Hybrid cloud and Community cloud.

### **5.1 Private cloud:**

Private cloud can be owned or leased and managed by the organization or a third party and exist at on-premises or off-premises. It is more expensive and secure when compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user's access and the networks used are restricted. One of the best examples of a private cloud is Eucalyptus Systems .

### **5.2 Public Cloud:**

A cloud infrastructure is provided to many customers and is managed by a third party and exist beyond the company firewall. Multiple enterprises can work on the infrastructure provided, at the same time and users can dynamically provision resources. These clouds are fully hosted and managed by the cloud provider and fully responsibilities of installation, management, provisioning, and maintenance. Customers are only charged for the resources they use, so under-utilization is eliminated. Since consumers have little control over the infrastructure, processes requiring powerful security and regulatory compliance are not always a good fit for public clouds. In this model, no access restrictions can be applied and no authorization and authentication techniques can be used. Public cloud providers such as Google or Amazon offer an access control to their clients. Examples of a public cloud includes Microsoft Azure, Google App Engine.

### **5.3 Hybrid Cloud:**

A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other. These clouds would typically be created by the enterprise and management responsibilities would be split between the enterprise and the cloud provider.

In this model, a company can outline the goals and needs of services . A well-constructed hybrid cloud can be useful for providing secure services such as receiving customer payments, as well as those that are secondary to the business, such as employee payroll processing. The major drawback to the hybrid cloud is the difficulty in effectively creating and governing such a solution. Services from different sources must be obtained and provisioned as if they originated from a single location, and interactions between private and public components can make the implementation even more complicated. These can be private, community or public clouds which are linked by a proprietary or standard technology that provides portability of data and applications among the composing clouds. An example of a Hybrid Cloud includes Amazon Web Services (AWS)[4].

#### **5.4 Community Cloud:**

Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider and rarely offered cloud model.

These clouds are normally based on an agreement between related business organizations such as banking or educational organizations. A cloud environment operating according to this model may exist locally or remotely

### **6. SECURITY GUIDANCE**

General security guidance to deal with the above threats can be found in :

- **Encryption and Key Management:** Encryption provides data protection while key management enables access to protected data. It is strongly recommended to encrypt data in transit over networks, at rest, and on backup media. In particular, data encryption at rest (e.g., for long-term archival storage) can avoid the risk of malicious cloud service providers or malicious multi-tenants abuse. At the same time, secure key stores (including key backup and recoverability) and access to key stores must be securely implemented since improper (or access to) key storage could lead to the compromise of all encrypted data.
- **Identity and Access Management:** Secure management of identity and access control is a critical factor to prevent account and service hijacking. It is strongly recommended to prohibit sharing of account credentials, to leverage strong (multi-factor) authentication if possible, and to consider delegated authentication and managing trust across all types of cloud services.

### **7. THREATS FOR CLOUD SERVICE USER**

#### **7.1 Responsibility Ambiguity**

Cloud service users consume delivered resources through service models. The customer-built IT system thus relies on the services. The lack of a clear definition of responsibility among cloud service users and Providers may evoke conceptual conflicts. Moreover, any contractual inconsistency of provided services could induce anomaly, or incidents. However the problem of which entity is the data controller which on is the data processor stays open at an international scale (even if the international aspect is reduced to a minimal third party outside of the specific region like EU).

#### **7.2 Loss of Governance**

For an enterprise, migrating a part of its own IT system to a cloud infrastructure implies to partially give control to the cloud service providers. This loss of governance depends on the cloud service models. For instance, IaaS only delegates hardware and network management to the provider, while SaaS also delegates OS, application, and service integration in order to provide a turnkey service to the cloud service user.

#### **7.3 Loss of Trust**

It is sometime difficult for a cloud service user to recognize his provider's trust level due to the black-box feature of the cloud service. There is no measure how to get and share the provider's security level in formalized manner. Furthermore, the cloud service users have no abilities to evaluate security implementation level achieved by the provider. Such a lack of sharing security level in view of cloud service provider will become a serious security threat in use of cloud services for cloud service users.

#### **7.4 Service Provider Lock-in**

A consequence of the loss of governance could be a lack of freedom regarding how to replace a cloud provider by another. This could be the case if a cloud provider relies on non-standard hypervisors or virtual machine image format and does not provide tools to convert virtual machines to a standardized format.

#### **7.5 Unsecure Cloud Service User Access**

As most of the resource deliveries are through remote connection, non-protected APIs, (mostly management APIs and PaaS services is one of the easiest attack vector). Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

#### **7.6 Lack of Information/Asset Management**

When applying to use Cloud Computing Services, the cloud service user will have serious concerns on lack of information/asset management by cloud service providers such as location of sensitive asset/information, lack of physical control for data storage, reliability of data backup (data retention issues), countermeasures for BCP and Disaster Recovery and so on. Furthermore, the cloud service users also have important concern on exposure of data to foreign government and on compliance with privacy law such as EU data protection directive.

#### **7.7 Data loss and leakage**

The loss of encryption key or privileged access code will bring serious problems to the cloud service users. Accordingly, lack of cryptographic management information such as encryption keys, authentication codes and access privilege will heavily lead to sensitive damages on data loss and unexpected leakage to outside. For example, insufficient authentication, authorization, and audit (AAA) controls; inconsistent use of encryption and/or authentication keys; operational failures; disposal problems; jurisdiction and political issues; data center reliability; and disaster recovery can be recognized as major behaviors in this threat category.

### **8. THREATS FOR CLOUD SERVICE PROVIDER**

#### **8.1 Responsibility Ambiguity**

Different user roles, such as cloud service provider, cloud service user, client ITadmin, data owner, may be defined and used in a cloud system. Ambiguity of such user roles and responsibilities definition related to data ownership, access control, infrastructure maintenance, etc, may induce business or legal dissention (Especially when dealing with third parties. The cloud service provider is somehow a cloud service user)[6].

### 8.2 Protection Inconsistency

Due to the decentralized architecture of a cloud infrastructure, its protection mechanisms are likely to be inconsistency among distributed security modules. For example, an access denied by one IAM module may be granted by another. This threat may be profited by a potential attacker which compromises both the confidentiality and integrity.

### 8.3 Evolutional Risks

One conceptual improvement of cloud computing is to postpone some choices from the design phase to the execution phase. This means, some dependent software components of a system may be selected and implemented when the system executes. However, conventional risk assessment methodology can no longer match such an evolution. A system which is assessed as secure during the design phase may exploit vulnerabilities during its execution due to the newly implemented software components.

### 8.4 Business Discontinuity

The “as a service” feature of cloud computing allocates resources and delivers them as a service. The whole cloud infrastructure together with its business workflows thus relies on a large set of services, ranging from hardware to application. However, the discontinuity of service delivery, such as black out or delay, may bring out a severe impact related to the availability.

### 8.5 Supplier Lock-in

The platform of a service provider is built by some software and hardware components by suppliers. Some supplier-dependent modules or workflows are implemented for integration or functionality extension. However, due to the lack of standard APIs, the portability to migrate to another supplier is not obvious. The consequence of provider locked-in could be a lack of freedom regarding how to replace a supplier.

### 8.6 License Risks

Software licenses are usually based on the number of installations, or the numbers of users. Since created virtual machines will be used only a few times, the provider may have to acquire from more licenses than really needed at given time. The lack of a “clouded” license management scheme which allows to pay only for used licenses may cause software use conflicts.

## 9. SECURITY ISSUES...

- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability

### 9.1 Virtual Machine Security:

Virtualization is one of the main components of a cloud. Virtual machines are dynamic i.e. it can quickly be reverted to previous instances, paused and restarted, relatively easily. Ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization. They can also be readily cloned and seamlessly moved between physical servers. This dynamic nature and potential for VM sprawl makes it difficult to achieve and maintain consistent security. Vulnerabilities or configuration errors may be unknowingly propagated. Also, it is difficult to maintain an auditable record of the security state of a virtual machine at any given point in time. Full Virtualization and Para Virtualization are two kinds of virtualization in a cloud computing paradigm. In full virtualization, entire hardware architecture is replicated virtually. However, in para-virtualization, an operating system is modified so that it can be run concurrently with other operating systems. VMM (Virtual Machine Monitor), is a software layer that abstracts the physical resources used by the multiple virtual machines. The VMM provides a virtual processor and other virtualized versions of system devices such as I/O devices, storage, memory, etc. Many bugs have been found in all popular VMMs that allow escaping from Virtual machine. Vulnerability in Microsoft Virtual PC and Microsoft Virtual Server could allow a guest operating system user to run code on the host or another guest operating system. Vulnerability was found in VMware’s shared folders mechanism that grants users of a guest system read and write access to any portion of the host’s file system including the system folder and other security-sensitive files. Vulnerability in Xen can be exploited by “root” users of a guest domain to execute arbitrary commands. The other issue is the control of administrator on host and guest operating systems. Current VMMs (Virtual Machine Monitor) do not offer perfect isolation. Virtual machine monitor should be ‘root secure’, meaning that no privilege within the virtualized guest environment permits interference with the host system.

### 9.2 Network Security:

Networks are classified into many types like shared and non-shared, public or private, small area or large area networks and each of them have a number of security threats to deal with. Problems associated with the network level security comprise of DNS attacks, Sniffer attacks, issue of reused IP address, etc which are explained in details as follows.

A Domain Name Server (DNS) server performs the translation of a domain name to an IP address. Since the domain names are much easier to remember. Hence, the DNS servers are needed. But there are cases when having called the server by name, the user has been routed to some other evil cloud instead of the one he asked for and hence using IP address is not always feasible. Although using DNS security measures like: Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats but still there are cases when these security measures prove to be inadequate when the path between a sender and a receiver gets rerouted through some evil connection. It may happen that even after all the DNS security measures are taken, still the route selected between the sender and receiver cause security problems[7].

Sniffer attacks are launched by applications that can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted, it can be read and there are chances that vital information flowing across the network can be traced or captured. A sniffer program, through the NIC (Network Interface Card) ensures that the data/traffic linked to other systems on the network also gets recorded. It can

be achieved by placing the NIC in promiscuous mode and in promiscuous mode it can track all data, flowing on the same network. A malicious sniffing detection platform based on ARP (address resolution protocol) and RTT (round trip time) can be used to detect a sniffing system running on a network .

Reused IP address issue have been a big network security concern. When a particular user moves out of a network then the IP-address associated with him (earlier) is assigned to a new user. This sometimes risks the security of the new user as there is a certain time lag between the change of an IP address in DNS and the clearing of that address in DNS caches. And hence, we can say that sometimes though the old IP address is being assigned to a new user still the chances of accessing the data by some other user is not negligible as the address still exists in the DNS cache and the data belonging to a particular user may become accessible to some other user violating the privacy of the original user .

### 9.3 Data security:

For general user, it is quite easy to find the possible storage on the side that offers the service of cloud computing. To achieve the service of cloud computing, the most common utilized communication protocol is Hypertext Transfer Protocol (HTTP). In order to assure the information security and data integrity, Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) are the most common adoption. In a traditional on-premise application deployment model, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. However, in cloud computing, the enterprise data is stored outside the enterprise boundary, at the Service provider end. Consequently, the service provider must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data. Cloud service providers such as Amazon, the Elastic Compute Cloud (EC2) administrators do not have access to customer instances and cannot log into the Guest OS. EC2 Administrators with a business need are required to use their individual cryptographically strong Secure Shell (SSH) keys to gain access to a host. All such accesses are logged and routinely audited. While the data at rest in Simple Storage Service (S3) is not encrypted by default, users can encrypt their data before it is uploaded to Amazon S3, so that it is not accessed or tampered with by any unauthorized party[3].

### 9.4 Data Privacy:

The data privacy is also one of the key concerns for Cloud computing. A privacy steering committee should also be created to help make decisions related to data privacy. Requirement: This will ensure that your organization is prepared to meet the data privacy demands of its customers and regulators. Data in the cloud is usually globally distributed which raises concerns about jurisdiction, data exposure and privacy. Organizations stand a risk of not complying with government policies as would be explained further while the cloud vendors who expose sensitive information risk legal liability. Virtual co-tenancy of sensitive and non-sensitive data on the same host also carries its own potential risks[2].

### 9.5 Data Integrity:

Data corruption can happen at any level of storage and with any type of media, So Integrity monitoring is essential in cloud storage which is critical for any data center. Data integrity is

easily achieved in a standalone system with a single database. Data integrity in such a system is maintained via database constraints and transactions. Transactions should follow ACID (atomicity, consistency, isolation and durability) properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity. Data generated by cloud computing services are kept in the clouds. Keeping data in the clouds means users may lose control of their data and rely on cloud operators to enforce access control.

### 9.6 Data Location:

In general, cloud users are not aware of the exact location of the datacenter and also they do not have any control over the physical access mechanisms to that data. Most well-known cloud service providers have datacenters around the globe. In many a cases, this can be an issue. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in many enterprise architecture. For example, in many EU and South America countries, certain types of data cannot leave the country because of potentially sensitive information. In addition to the issue of local laws, there's also the question of whose jurisdiction the data falls under, when an investigation occurs. Next in the complexity chain are distributed systems. In a distributed system, there are multiple databases and multiple applications .

In order to maintain data integrity in a distributed system, transactions across multiple data sources need to be handled correctly in a fail safe manner. This can be done using a central global transaction manger. Each application in the distributed system should be able to participate in the global transaction via a resource manager.

### 9.7 Data Availability:

Data Availability is one of the prime concerns of mission and safety critical organizations. When keeping data at remote systems owned by others, data owners may suffer from system failures of the service provider. If the Cloud goes out of operation, data will become unavailable as the data depends on a single service provider. The Cloud application needs to ensure that enterprises are provided with service around the clock. This involves making architectural changes at the application and infrastructural levels to add scalability and high availability. A multi-tier architecture needs to be adopted, supported by a load-balanced farm of application instances, running on a variable number of servers. Resiliency to hardware/software failures, as well as to denial of service attacks, needs to be built from the ground up within the application. At the same time, an appropriate action plan for business continuity (BC) and disaster recovery (DR) needs to be considered for any unplanned emergencies.

## 10.CONCLUSION

Cloud service providers need to inform their customers on the level of security that they provide on their cloud. In this paper, we first discussed various models of cloud computing, security issues Data security is major issue for Cloud Computing. There are several other security challenges including security aspects of network and virtualization. New security techniques need to be developed and older security techniques needed to be radically tweaked to be able to work with the clouds architecture.

## 11.REFERNCES

- [1] A. Kundu, C. D. Banerjee, P. Saha, “Introducing New Services in Cloud Computing Environment”, International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.
- [2] Tim Mather, SubraKumaraswamy, ShahedLatif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O’ Reilly Media, USA, 2009.
- [3] Ronald L. Krutz, Russell Dean Vines “Cloud SecurityA Comprehensive Guide to Secure Cloud Computing”, Wiley Publishing, Inc.,2010
- [4] K. Vieira, A. Schuler, C. B. Westphall, and C. M. Westphall, “Intrusion detection techniques for Grid and Cloud Computing Environment,” IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010.
- [5] Marios D. Dikaiakos, DimitriosKatsaros, PankajMehra, George Pallis, Athena Vakali, “Cloud Computing: Distributed Internet Computing for IT and Scientific Research,” IEEE Internet Computing Journal, vol. 13, issue. 5, pp. 10-13, September 2009. DOI: 10.1109/MIC.2009.103
- [6] A. Williamson, “Comparing cloud computing providers,” Cloud Comp. J., vol. 2, no. 3, pp. 3–5, 2009.
- [7] AmanBakshi, Yogesh B. Dujodwala, “Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine,” ICCSN ’10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.