CLOUD COMPUTING-ATTRIBUTE AND RELIABILITY CONCERN

Dr.Rakesh Kumar Giri,

Assistant Professor,
Saisha Institutions, Chennai, India

Abstract: Cloud Storage, as the module that provides data storage service in the Cloud Computing architecture, has evolved into the core component of Cloud Computing in recent years. This is one of the benefits of cloud computing: it allows you to produce and save data on remote computers. However, this gain has the implied disadvantage of data security and privacy concerns. There are numerous techniques and methodologies for achieving data security in cloud computing, but it also comes with a number of concerns. In this paper, we discuss many aspects of data security.

***Index Terms* -** Cloud Security, Security Challenges, Cloud computing.

I. INTRODUCTION

The last decades have reinforced the idea that information processing can be done more efficiently centrally, on large farms of computing and storage systems accessible via the Internet. When computing resources in distant datacenters, are used rather than local Computing systems we talk about network-centric computing and network-centric content. Advancements in networking and other areas are responsible for the acceptance of the two new computing models: utility computing and computer clouds. In utility computing, they concentrate on software and hardware resources and pay per use phenomena can be applied. users can pay as they consume storage, computing and communication resources. While in utility computing cloud-like infrastructure is often required, for providing the computing services, its primary focus is on the business model. Cloud computing is a path to utility computing hold by major IT companies such as Amazon, Apple, Google, HP, IBM, Microsoft, Oracle, and others. The most widely used definition of the cloud computing model is introduced by NIST [1] as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”. The term “computer cloud” is overloaded as it covers infrastructures of different sizes, with different management, and a different user population.

II Cloud Deployment models

Several types of cloud deployment models are:

•**Private Cloud** - the infrastructure is operated solely for an organization, it can be managed by the organization or a third party and can exist on or off the quadrangle of the organization.

•**Community Cloud** - the infrastructure is shared by several organizations and a specific community is there in community cloud that has shared concerns (e.g., security requirements, mission, policy, and compliance considerations). It can be managed by the organizations or a third party and can exist on or off the quadrangle of the organization.

•**Public Cloud** – In publuc cloud the infrastructure is made approachable to the general public or a large industry group and the organization’s selling cloud services owned it.

•**Hybrid Cloud** - The hybrid cloud is composed of two or more clouds (private, community, or public) that are bound togehther by a standardized technology by which data and application portability is enabled but they remain unique entities . Appplication and data portability like cloud bursting for load-balancing between clouds.

III Cloud Service delivery models

There are three cloud delivery models, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) deployed as public, private, community, and hybrid clouds. The following figure 1 describe the cloud computing service stack[2].

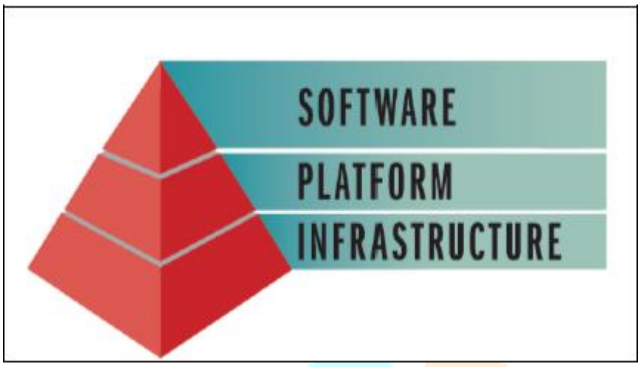

Figure1 Cloud computing service stack

SaaS applications are designed for end-users, delivered over the web.

PaaS is the set of tools and services which are designed to make coding and deploying those applications quick and efficient.

IaaS is the hardware and software that powers it all – servers, storage, networks, operating systems

Cloud computing delivery models, deployment models, defining attributes, resources, and organization of the infrastructure are summarized in figure 2.

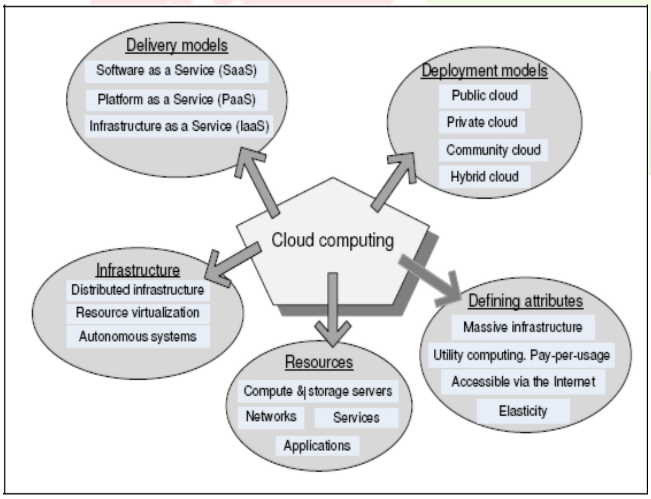

Figure 2 Cloud computing summary

IV Customer Data and its Security

In today's world of (network-, host-, and application-level) infrastructure, when we consider cloud computing at all levels security or data security becomes more important. Level of cloud computing are: infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). In this paper we describe several aspects of data security, including:

Data-in-transit Data-at-rest

Processing of data, including multitenancy Data lineage

Data provenance Data remanence

Data-in-transit: When we consider data-in-transit,then not using a vetted encryption algorithm is the primary risk. Although it is not easy for others to understand this requirement this is obvious to information security professionals, when using a public cloud, no matter whether it is IaaS, PaaS, or SaaS. It is also important to ensure that a protocol provides confidentiality as well as integrity , particularly if the protocol is used for transferring data across the Internet. Only encrypting data and using a non-secured protocol can provide confidentiality, but does not ensure the integrity of the data. **Data-at-rest**: When we consider data-at-rest then using

encryption to protect data-at-rest might seem obvious,but the reality is not that simple. If you are using an IaaS cloud service (public or private) for simple storage (e.g. Amazon's Simple Storage Service or S3), encrypting data-at-rest is possible—and is

strongly adviced. However,if you are using Paas or Saas cloud based application(Google Apps) then encrypting data-at-rest as a compensating control is not always feasible. Data-at-rest used by a cloud-based application is generally not encrypted, because encryption prevents indexing or searching of that data.

Multitenancy: Multitenancy implies sharing of computational resources [3],

Storage, services, and applications with other tenants. Multi- tenancy has different realization approaches as shown in figure 3. In approach 1, there is an own dedicated instance for each tenant with their own customizations (customization may include special development to meet customer needs). In approach 2, each tenant uses a dedicated instance, like approach 1, while all instances are same but having different configurations .

In approach 3, same instance is shared by all tenants with runtime configuration (the application is divided into core application component and according to the current tenant request extra components that are loaded – like SalesForce.com). In approach 4 a load balancer is there and tenants are directed to that load balancer which redirects tenants requests to a suitable instance according to current instances load. Approaches 3 and 4 are the most risky because of same processs in memory and hardware tenants are coexisting. And because of the resource sharing the confidentiality of tenants' IT assets voilated ,which leads to the need for secure multi -tenancy. For secure multi-tenancy Isolation among tenants' data (at rest transition) and location transparency where tenants have no control or knowledge over the specific resources , to avoid planned attacks that attempt to co-locate with the victim assets [4],In Iaas the isolation should consider VMs' storage, processing, memory, cache memories, and networks[3]. In PaaS, isolation should cover siltation among running services and APIs' calls[3]. In Saas isolation should isolate among transactions carried out on the same instance by different tenants and tenants' data[3].

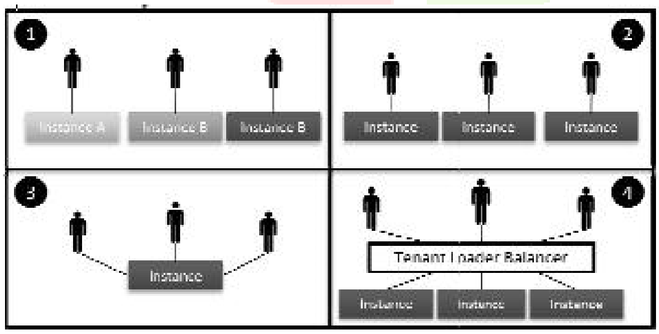

Figure 3 Multi-tenancy approaches[3]

Data Lineage: It is very useful to know within an organization which has put their data on the cloud that where and when the data was specifically located within the cloud whether the data in the cloud is encrypted or not. Data lineage is all about some questions like where data comes from , where it flows to and it is transformed while it travels through the enterprise. Because obviously , we can't manage that which we can't find. If we are aware of where data is and how it flows then only we can manage and secure the data appropriately while it moves across the computer network.. For example [3], the data might have been transferred to a cloud provider, such as Amazon Web Services (AWS), on date a1 at time b1 and stored in a bucket on Amazon's S3 in example1.s3.amazonaws.com, then processed on date a2 at time b2 on an instance being used by an organization on Amazon's Elastic Compute Cloud (EC2) inec2-67-202-51-

223.compute-1.amazonaws.com, then restored in another bucket, example2. s3.amazonaws.com, before being brought back into the organization for storage in an internal data warehouse belonging to the marketing operations group on date a3 at time b3 [3]. Following the path of data (mapping application data flows or data path visualization) is known as data lineage, and it is important for an auditor's internal ,external and regulatroy assurance. However, providing data lineage is very difficult and time-consuming, even when the environment is completely under an organization's control. And it is not possible to provide accurate data lineage for a public cloud.

Data Provenance: Data provenance is more chalenging and difficult than data lineage . Even data lineage can be established in a public cloud for some customers but proving data provenance is more challenging problem. Here not only integrity of the data is proved, but the more specific provenance of the data. The two terms little bit differ to each other but the important difference is there between the two terms. Integrity of data refers to data that has not been changed in an unauthorized manner or by an unauthorized person. Provenance means not only that the data has integrity, but also that it is computationally accurate; that is, the data was accurately calculated. There are many real-life examples in which data integrity is not sufficient and data provenance is also needed. Financial and scientific calculations are two obvious examples. How do can prove data provenance in the cloud computing environment where shared resources are used? Those resources are not under our physical or even logical control, even if we have some information about the systems then also we have no ability to track the systems used or their state at the times when we used them. So we can say data provenanace is much more difficult to achieve in cloud computing environment

Data Remanence: The final aspect of data security is data remanence. Data remanence is the residual representation of data that has been in some way nominally erased or removed. This residue may be due to data being left intact by a nominal delete operation, or through physical properties of the storage medium. Data remanence may make inadvertent disclosure of sensitive information possible, should the storage media be released into an uncontrolled environment (e.g., thrown in the trash, or given to a third party). The risk posed by data remanence in cloud services is that an organization's data can be inadvertently exposed to an unauthorized party—regardless of which cloud service we are using (SaaS, PaaS, or IaaS). When using SaaS or PaaS, the risk is almost certainly unintentional or inadvertent exposure. However, that is not reassuring after an unauthorized disclosure, and potential customers should question what third-party tools or reviews are used to help validate the security of the provider's applications or platform.

V Provider Data and Its Security

In addition to the security of our own customer data, customers should also be concerned about what data the provider collects and how the CSP protects that data. Specifically with regard to the customer data, what metadata does the provider have about our data, how is it secured, and what access do we, the customer, have to that metadata? As the volume of data with a particular provider increases, so does the value of that metadata. Storage For data stored in the cloud (i.e., storage-as-a-service), we are referring to IaaS and not data associated with an application running in the cloud on PaaS or SaaS. The same three information security concerns are associated with this data stored in the cloud (e.g., Amazon's S3) as with data stored elsewhere:

Confidentiality Integrity Availability.

Confidentiality: When it comes to the confidentiality of data stored in a public cloud, we have two potential concerns. First, what access control exists to protect the data? Access control consists of both authentication and authorization. the second potential concern: how is the data that is stored in the cloud actually protected? For all practical purposes, protection of data stored in the cloud involves the use of encryption.

Integrity: Integrity of data refers to data that has not been changed in an unauthorized manner or by an unauthorized person. Confidentiality does not imply integrity; we can encrypt our data for confidentiality purposes, and then also we can not verify the integrity of the data. Encryption alone is sufficient only for confidentiality, but integrity also requires the use of message authentication codes (MACs). For using MACs on encrypted data we can use block symmetric algorithm in cipher block chaining (CBC) mode, and then a one-way hash function can be included.. Data integrity is also important when we use bulk of data especially with Iaas. If the customer has many gigabytes (or more) of its data in the cloud for storage, how does the customer check on the integrity of the data stored there? There are IaaS transfer costs associated with moving data into and back down from the cloud, as well as network utilization (bandwidth) considerations for the customer's own network. What a customer really wants to do is to validate the integrity of its data while that data remains in the cloud without having to download and replied that data. This task is even more difficult because it must be done in the cloud without explicit knowledge of the whole data set. Customers generally do not know on which physical machines their data is stored, or where those systems are located. Additionally, that data set is probably dynamic and changing frequently. Those frequent changes obviate the effectiveness of traditional integrity insurance techniques.

Availability: Assuming that a customer's data has maintained its confidentiality and integrity, we must also be concerned about the availability of our data. There are currently three major threats in this regard

The first threat to availability is network-based attacks **The second** threat to availability is the CSP's own availability. No CSPs offer the sought-after "five 9s" (i.e., 99.999%) of uptime. A customer would be lucky to get "three 9s" of uptime.

Finally, prospective cloud storage customers must be certain to ascertain just what services their provider is actually offering.

VI Conclusion

In this paper we first discussed the cloud computing and its characteristics and then the security issues for cloud. These issues include the Customer data & its security and Provider data & its security .In Customer data security we considered data-in-transit, data-at-rest, multitenancy data lineage, data provenance and data remanence .Every aspect which we have discussed about customer data is an important one at all levels as Iaas, Paas and Saas whether these are deployed at any cloud .Likewise Provider data also needs security and the security concerns for provider data are the same as with the data stored elsewhere other than cloud like Data confidentiality, Data integrity and Data availability. This paper shows that there are several types of security challenges at each level of cloud computing.

REFERENCES

[1] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing, "2009, v15.pdf, Accessed Apri2010.

[2] Maneesha Sharma, Himani Bansal, Amit KumarSharma ,"CloudComputing: Different Approach & Security Challenge " International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012, 421.

[3]Mohamed Al Morsy, John Grundy and Ingo Müller. Computer Science & Software Engineering, Faculty of Information & Communication Technologies Swinburne University of Technology, Hawthorn, Victoria, Australia {malmorsy, jgrundy, imueller}@ swin.edu.au " An Analysis of The Cloud Computing Security Problem" .