IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Data Security in Cloud Computing

Nyasa Singh
dept.ofComputerScience
kalinga University
Raipur C.G. India

Neha Sonkar
dept.ofComputerScience
kalingaUniversity
Raipur C.G. India

Madhu Sen
dept.ofComputerScience
kalinga University
Raipur C.G.India

Pooja P Raj
Assistant Professor
dept.ofComputerScience
Raipur C.G.India

Abstract— Cloud computing is web ("cloud") based mostly development and use of technology ("computing"). it's a method of computing within which dynamically scalable and infrequently virtualized resources ar provided as a service over the web. Cloud computing uses the web and also the central remote servers to support totally different knowledge and applications. it's associate internet-based technology. It permits the users to approach their personal files at any laptop with web access. The cloud computing flexibility could be a operate of the allocation of resources on authority's request. Cloud computing provides the act of uniting. Scientific computing within the twenty first century has evolved from mounted to distributed work atmosphere. the present trend of Cloud Computing (CC) permits accessing business applications from anyplace simply by connecting to the web. proof shows that, shift to CC organizations' annual expenditure and maintenance are being reduced to a larger extent. However, there are many challenges that return in conjunction with numerous advantages of cloud computing. Among these embrace security aspects. Our aim is to spot security challenges for adapting cloud computing and their solutions from globe for the challenge that don't have any correct mitigation ways known. This non-existence of world standards and pointers can be facilitate teachers to grasp the state of apply and formulate higher methods/standards to supply secure ability. The known cloud computing security challenges and solutions may be referred by practitioners to grasp that areas of security got to be targeted whereas adapting/migrating to a cloud computing atmosphere.

Keywords—Data Security, Cloud Computing, Data Protection, Privacy, Risks and threats

Introduction — The term word Cloud Computing has emerged recently and is not is widespread use. Of the several definitions which are available, one of the simplest is, "a network solution for providing inexpensive, reliable, easy and simple access to IT resources ". Cloud Computing is not considered as application oriented but service oriented. This service-oriented nature of Cloud Computing not only reduces the overhead of infrastructure and cost of ownership but also provides flexibility and improved performance to the end user. A major concern in adaptation of cloud for data is security and privacy. It is very important for the cloud service to ensure the data integrity, privacy and protection. For this purpose, several service providers are using different policies and mechanism that depend upon the nature, type and size of data. One of the advantages of Cloud Computing is that data can be shared among various organizations. However, this advantage itself poses a risk to data. In order to avoid potential risk to the data, it is necessary to protect data repositories. One of the key questions while using cloud for storing data is whether to use a third-party cloud service or create an internal organizational cloud. Sometimes, the data is too sensitive to be stored on a public cloud, for example, national security data or highly confidential future product details etc.

A.Cloud computing: service models:

Cloud computing can be accessed through a set of services models. These services are designed to exhibit certain characteristics and to satisfy the organizational requirements. From this, a best suited service can be selected and customized for an organization's use. Some of the common distinctions in cloud computing services are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure as a Service (IaaS), Hardware-as-a- Service (Haas) and Data storage-as-a-Service (DaaS). Service model details are as follows:

• **Software as a Service (SaaS):** The service provider in this context provides capability to use one or more applications running on a cloud infrastructure. These applications can be accessed from various thin client interfaces such as web browsers. A user for this service need not maintain, manage or control the underlying cloud infrastructure (i.e. network, operating systems, storage etc.). Examples for SaaS clouds are Salesforce, NetSuite.

• **Platform as a Service (PaaS):** The service provider in this context provides user resources to deploy onto cloud infrastructure, supported applications that are designed or acquired by user. A user using this service has control over deployed applications and application hosting environment, but has no control over infrastructure such as network, storage, servers, operating systems etc. Examples for PaaS clouds are Google App Engine, Microsoft Azure, Heroku.

• **Infrastructure as a Service (IaaS):** The consumer is provided with power to control process, manage storage, network and other fundamental computing resources which are helpful to manage arbitrary software and this can include operating system and applications. By using this kind of service, user has control over operating system, storage, deployed applications and possible limited control over selected networking components. Examples for IaaS clouds are Eucalyptus (The Eucalyptus Open source Cloud-computing System), Amazon EC2, Rackspace, Nimbus.

.

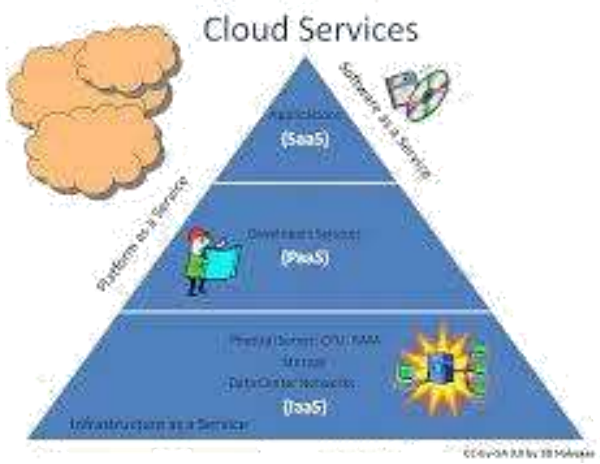

Fig 1 : Cloud Services

B. Risks and security concerns in cloud computing :

Several risks and security concerns are associated with cloud computing and its data. However, this study will discuss about the virtualization, storage in public cloud and multitenancy which are related to the data security in cloud computing

1.Virtualization- Virtualization is a technique in which a fully functional operating system image is captured in another operating system to utilize the resources of the real operating system fully.A special function called hypervisor is required to run a guest operating system as a virtual machine in a host operating system.Virtualization is a foundational element of cloud computing which helps in delivering the core values of cloud computing. However, virtualization poses some risks to data in cloud computing. One possible risk is compromising a hypervisor itself. A hypervisor can become a primary target if it is vulnerable. If a hypervisor is compromised, the whole system can be compromised and hence the data.

2. Storage in Public Cloud - Storing data in a public cloud is another security concern in cloud computing. Normally clouds implement centralized storage facilities, which can be an appealing target for hackers. Storage resources are complicated systems that are combination of hardware and software implementations and can cause exposure of data if a slight breach occurs in the public cloud. In order to avoid such risks, it is always recommended to have a private cloud, if possible, for extremely sensitive data.

3.Multitenancy- Shared access or multitenancy is also considered as one of the major risks to data in cloud computing. Since multiple users are using the same shared computing resources like CPU, Storage and memory etc. It is threat to not only a single user but multiple users.

C.Data security in cloud computing:

Data security in cloud computing involves more than data encryption. Requirements for data security depends upon on the three service models SaaS, PaaS, and IaaS. Two states of data normally have threat to its security in clouds; Data at Rest which means the data stored in the cloud and Data in Transit which means data that is moving in and out of the cloud. Confidentiality, and Integrity of data is based upon the nature of data protection mechanisms, procedures, and processes. The most significant matter is the exposure of data in above mentioned two states.

1. Data at Rest Data at rest refers to data in cloud, or any data that can be accessed using Internet. This includes backup data as well as live data. As mentioned earlier, sometimes it is very difficult for organizations to protect data at rest if they are not maintaining a private cloud since they do not have physical control over the data. However, this issue can be resolved by maintaining a private cloud with carefully controlled access.

2. Data in Transit Data in transit normally refers to data which is moving in and out of the cloud. This data can be in the form of a file or database stored on the cloud and can be requested for use at some other location. Whenever, data is uploaded to the cloud, the data at time of being uploaded is called data in transit. Data in transit can be very sensitive data like user names and passwords and can be encrypted at times. However, data in unencrypted form is also data in transit. Data in transit is sometimes more exposed to risks than the data at rest because it has to travel from one location to another. There are several ways in which intermediary software can eavesdrop the data and sometimes have the ability to change the data on its way to the destination. In order to protect data in transit, one of the best strategies is encryption.

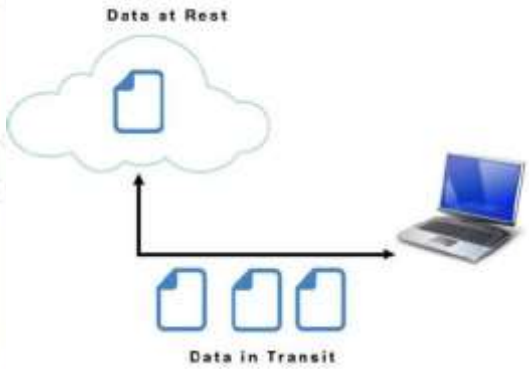

Fig 2 : Data at Rest and Transit

D.Majaor Security Challenges:

Undoubtedly it is not easy to secure and ensure the safety of linked computers because a series of computers and clients are involved; this is known as multi-tenancy. The cloud service providers and cloud computing have to face many challenges, particularly in the area of security issues. Thus, it is very important to consider how these challenges are mimicked and how security models are implemented in order to ensure the security of clients and establish a safe cloud computing environment. The major challenges involved are:

1. **Malicious attacks from management internally:**

Sometimes the architecture of cloud computing environments poses risks to the privacy and security of the customers.

Although it happens rarely, this risk is very difficult to deal with. Examples include the administrators and managers of cloud service providers who can sometimes act as malicious agents and threaten the security of the client using cloud computing application.

2. Insecure or incomplete data deletion In instances where clients request data to be deleted either partially or completely, this raises the question of whether it will be possible to delete the desired part of their data segment with accuracy. This makes it harder for the clients to subscribe to
the services of the cloud- computing.

3.Data interception Unlike with tradition computing, the data in cloud computing is segmented and distributed in transit. This poses more threats due to the vulnerability and fragility of the computing technology and, in particular, sniffing and spoofing, third party attacks and reply attacks.

4.Client's trust There must be strong authentication practices implemented to ensure that the client's data is being protected from unauthorized access.

5. Malicious users handling Malicious users can be attackers using cloud services with a malicious intent or an insiderwho has gained the trust of company but works to gain access to sensitive information stored in cloud.

6.Hijecking of sessions These kinds of attacks happen when a legitimate user is prone to phishing or insecure application interfaces that can be exploited by attackers. Through this kind of attacks, attackers gain user credentials and hijack legitimate user's sessions.

7.Wrong usage of CC and its services Cloud computing service providers give access to try their cloud services for a limited period of time for free. Some users utilize this trial period to misuse the resources obtained through CC service provider

E.Reasearch article:

• Reasearch paper

Hey, you, Get Off of My Cloud! Exploring Information Leakage in Third-Party Compute Clouds. by Thomas Risten part, Eran Trommer, Hovan Shaham, and Stefan Savage. In Proceedings of CCS 2009, pages 199–212. ACM Press, Nov. 2009.

First work on cloud cartography

• Attack launched against commercially available "real" cloud (AmazonEC2).

• Claims up to 40% success in co-residence with target VM

F.New risks in cloud:

• Trust and dependence

– Establishing new trust relationship between customer and cloud provider

– Customers must trust their cloud providers to respect
the privacy of their data and integrity of their computation

• Security (multi-tenancy)

– Threats from other customers due to the subtleties of how physical resources can be transparently shared between virtual machines (VMs)

G.Multi-tenancy:

• Multiplexing VMs of disjoint customers upon the same physical hardware

– Your machine is placed on the same server with other customers

– Problem: you don't have the control to prevent your instance from being co-resident with an adversary

• New risks

– Side-channels exploitation

• Cross-VM information leakage due to sharing of physical resource (e.g., CPU's data caches)

• Has the potential to extract RSA & AES secret keys

– Vulnerable VM isolation mechanisms

• Via a vulnerability that allows an "escape" to the hypervisor

H.Threat Model:

• Assumptions of the threat model:

– Provider and infrastructure to be trusted
– Do not consider attacks that rely on subverting administrator functions
– Do not exploit vulnerabilities of the virtual machine monitor and/or other software
– Adversaries: non-providers-affiliated malicious parties
– Victims: users running confidentiality-requiring services in the cloud

• Focus on new cloud-related capabilities of the attacker and implicitly expanding the attack surface

• Like any customer, the malicious party can run and control instances in the cloud

– Maximum of 20 instances can be run parallel using an Amazon EC2 account

• Attacker's instance might be placed on the same physical hardware as potential victims parties

• Attack might manipulate shared physical resources to learn otherwise confidential information

• Two kinds of attack may take place:

– Attack on some known hosted service

– Attacking a particular victim's service

I.Conclusion:

With the continuous growth and expansion of cloud computing, security has become one of the serious issues. Cloud computing platform need to provide some reliable security technology to prevent security attacks, as well as the destruction of infrastructure and services. There is no doubt that the cloud computing is the development trend in the future. Cloud computing brings us the approximately infinite computing capability, good scalability, service on-demand and so on, also challenges at security, privacy, legal issues and so on. But to solving the existing issues becomes utmost urgency. To protect against the compromise of the compliance integrity and security of their applications and data, firewall, Intrusion detection and prevention, integrity monitoring, log inspection, and malware protection. Proactive enterprises and service providers should apply this protection on their cloud infrastructure, to achieve security so that they could take advantage of cloud computing ahead of their competitors. These security solutions should have the intelligence to be self-defending and have the ability to provide real-time detection and prevention of known and unknown threats. To advance cloud computing, the community must take proactive measures to ensure security.

J.References:

[1] J. Srinivas, K. Reddy, and A. Qyser, "Cloud Computing Basics," Build. Infrastruct. Cloud Secur., vol. 1, no. September 2011.

[2] P. S. Wooley, "Identifying Cloud Computing Security Risks," Contin. Educ., vol. 1277, no. February, 2011

[3] F. Yahya, V. Chang, J. Walters, and B. Wills, "Security Challenges in Cloud Storage," .

[4] A. Alharthi, F. Yahya, R. J. Walters, and G. B. Wills, "An Overview of Cloud Services Adoption Challenges in Higher Education Institutions," 2015.

[5] V. J. Winkler, "Securing the Cloud," Cloud Comput. Secur. Tech. tactics. Elsevier., 2011

[6] T. Mather, S. Kumaraswamy, and S. Latif, "Cloud Security and Privacy,".