Cloud Computing : Analysis of Data security in Cloud Environment

Ms. Darshana B. Pedge[1],
Sinhgad Institute Of Computer Sciences (MCA)
Pandharpur,(MS), India
[1]darshana.pedge59@gmail.com

Mr. Vinayak V.Patil[2]
Sinhgad Institute Of Computer Sciences (MCA)
Pandharpur,(MS), India
[2]vinayakpatil4@gmail.com

***Abstract* -Cloud computing is a new emerging technology, providing dramatically scalable and virtualized resources, software and hardware on demand to consumers. Consumers can typically requests cloud services via a web browser or web service. By using cloud computing, consumers have benefits in the cost of hardware deployment, software licenses and system maintenance. On the other hand, it also has a security issues. In a cloud computing system, the computations are done in the cloud server where , the client side just send a request and wait for the result. Due to which several security issuesare arises such as data security, network security, multi-tenancy security, flooding attack, malware injection attack, virtualization, elasticity, Cloud Access Methods Security Issues etc.**

This paper introduces a detailed studyof the overview of cloud computing technology & data security in cloud. This paper at the last concludes with the essential measures to ensure data security in cloud.

***Keywords*- Cloud computing,Benefits, Data Security.**

I. INTRODUCTION

As this is an era of new technological trend such as, the rapid development in storage and processing technologies, the success of the internet & the computing resources have become cheaper, more powerful and more commonly available than ever before.[2] This has enabled the realization of a new computing model called cloud computing, in which resources (e.g., CPU and storage) are provided as general utilities that can be leased and released by users through the Internet in an on-demand fashion.

It helps consumers to reduce the usage of hardware, software license and system maintenance.

Moreover by using cloud computing consumers can get benefit in the form of cost, on-demand self services that reply rapidly, and can access broad network. By using internet consumers are able to use service application on clouds.

With Cloud Computing rapidly gaining popularity, it is important to highlight the resulting risks. As security and privacy issues are most important, they should be addressed before Cloud Computing establishes an important market share.

II. OVERVIEW OF CLOUD COMPUTING

This section presents a general overview of cloud computing, including its definition and a comparison with related concepts, characteristics and related technologies.

Definitions:

In this paper, we adopt the definition of cloud computing provided by The National Institute of Standards and Technology (NIST),[7] as it covers, in our opinion, all the essential aspects of cloud computing:

NIST definition of cloudcomputing:

"Cloud computing is 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.".

Cloud computing is a new operations model that brings together a set of existing technologies to run business in a different way most of the technologies used by cloud computing, such as

1. **Grid Computing:**

Grid computing is a distributed computing paradigm that coordinates networked resources to achieve a common computational objective.

2. **Utility Computing:**

Utility computing represents the model of providing resources on-demand and charging customers based on usage rather than a flat rate.

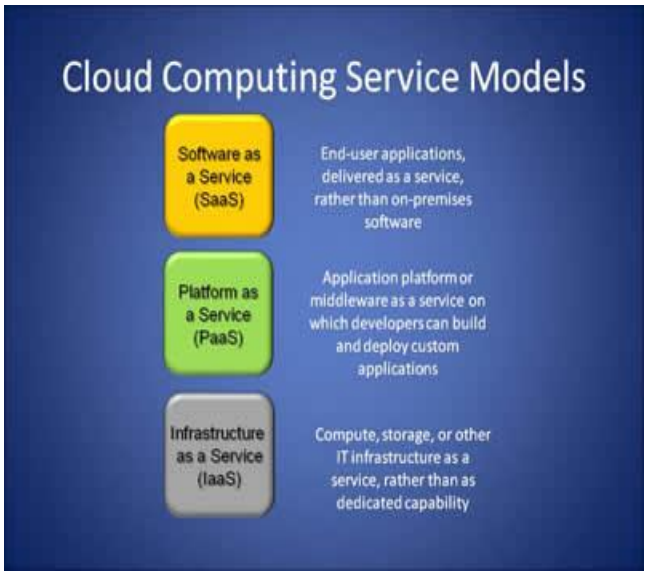
3. Virtualization:

Virtualization is a technology that abstracts away the details of physical hardware and provides virtualized resources for high-level applications. A virtualized server is commonly called a virtual machine (VM). Virtualization forms the foundation of cloud computing, as it provides the capability of pooling computing resources from clusters of servers and dynamically assigning or reassigning virtual resources to applications on-demand.

In summary, cloud computing leverages (power to accomplish) **virtualization** technology to achieve the goal of providing computing resources as a **utility.** It shares certain aspects with **grid computing and autonomic computing** but differs from them inother aspects. Therefore, it offers unique benefits and imposes Distinctive challenges to meet its requirements.

III.Cloud Computing Architecture:

The three types of service models areavailable within the cloud computing environment.[2]



SaaS (Software As a Service):

This model is designed to provide the application on rent to the user. The service is usually provided through some type of front end or web portal. While the end user can use this service from anywhere & pay monthly as per usage.
Eg: Salesforce.com

PaaS (Platform As a Service):

In this model of cloud computing, the provider provides a platform for youruse. Services provided by this model include all phases of the system development life cycle (SDLC) **.**It is a tool (Windows, LINUX) used by developers for developing application without installing any Software on the system.
Eg: GoogleApps

Iaas (Infrastructure As a Service):

As name suggest it is a buying of infrastructure facility. This model maintained and control by cloud service providers that support various operations like storage, hardware, servers and networking.
Eg: Amazon Web Services.

Cloud services can be deployed in four ways depending uponthe customers' requirements:

1. Public Cloud:A cloud infrastructure is provided to many customers and is managed by a third party. Wastage of resources is checked as the user pays forwhatever they use.

2. Private Cloud:Cloud infrastructure, made available only to a specific customer and managed either by the organization itself or third party service provider.
This uses the concept of virtualization of machines, and is aproprietary network.

4. Community cloud:Infrastructure shared by several organizations for a shared cause and may be managed by themor a third party service provider.

5. Hybrid Cloud:A composition of two or more cloud deployment models, linked in a way that data transfer takesplace between them without affecting each other.

Key Characteristics: of Cloud Computing:

• On-demand self-service
• Ubiquitous network access

• Location independent resource pooling
• Rapid elasticity
• Pay per use

With these beneficial characteristics, even though the cloud continues to grow in popularity , complications with data privacy and data protection still threaten the market.

IV. Data security in Cloud Computing

Cloud-based services use via the internet & storing data in the cloud, it can be risky and we have less control over data.

Data confidentiality and auditability topped the list of primary obstacles for the use of cloud computing technologies in their organizations, according to a recent survey of over 1100 Indian Business Technology professionals cloud adopters would have security concerns around storing and processing sensitive data in a public or hybrid or even in a community cloud.[8]

Frank Jennings, Head of Commercial, DMH Stallard LLP and author of the Report, stated: "Industry surveys consistently show that data security is the number one concern when it comes to cloud adoption. [8]

Many cloud service providers provide storage as a form of service.[5] They take the data from the users and store them on large data centre. Although these cloud service providers say that the datastored in the cloud is utmost safe but there have been cases when the data stored in these clouds have been modified orlost may be due tosome security violation or some human error.

Various cloud service providers adopt different technologies to safeguard the data stored in their cloud.[5]

There are two primary issues that we have to deal with when talking about data security in cloud:

- **Protection of the data:**Dealing with the confidentiality, integrity, and availability (CIA) criteria.
  Answering the important questions, such as, "What is the risk to the data? Are the controls in place adequate to mitigate the risk?"

- **Location of the data:** Dealing with the physical location of the "bits" answering questions like, "Do I know where the data resides? Does this violate any of my compliance requirements?"

Securing data must begin with data classification.

Here are some steps to follow:

1. Identify the data that will be processed or stored in the cloud.
2. Classify the information in regards to sensitivity towards loss of the CIA criteria. This would include identifying regulatory requirements for the data.
3. Define the rules by which particular information classes of instances must be stored, transmitted, archived, transported and destroyed. Many handling requirements result from contractual or regulatory requirements.

These service providers refer different encryption techniques like public key encryption and private key encryption to secure the data resting in the cloud.

Concern about security and privacy in the cloud will drive adoption of cloud encryption systems, but Gartner warns there are six security issues that businesses should tackle.

It is recommended that enterprises should first develop a data security plan that addresses security issues.[7]

Following are some of the security issues that must be addressed in security plan are as follows:

1.Violation notification and data location:

Not all data requires equal protection, so businesses should categories data intended for cloud storage and identify any compliance requirements in relation to data violation notification.

2.Rest - data management:

Businesses should ask specific questions to determine the cloud service provider's (CSP's) data storage life cycle and security policy.

Businesses should find out if:

- Multitenant storage is being used, and if it is, find out what separation mechanism is being used between tenants.
- Mechanisms such as tagging are used to prevent data being replicated to specific countries or regions.
- Storage used for archive and backup is encrypted and if the key management strategy include a strong identity and access management policy to restrict access within certain authorization.

3.Data protection in motion

As a minimum requirement, Gartner recommends that [7] businesses ensure that the CSP will support secure communication protocols such as SSL/TLS for browser access or VPN-based connections for system access for protected access to their services.

The research note says that businesses always encrypt sensitive data in motion to the cloud, but if data is unencrypted while in use or storage, it will lessen data violation.

In IaaS, it is recommended that businesses favor CSPs that provide network separation among tenants, so that one tenant cannot see another's network traffic.

4.Encryption key management:

Enterprises should always aim to manage the encryption keys, but if they are managed by a cloud encryption provider, Gartner says they must ensure access management controls are in place that will satisfy violation notification requirements and data location.

5. Access controls:

It is recommended that businesses require the CSP to support IP subnet access restriction policies so that enterprises can restrict end-user access from known ranges of IP addresses and devices.

The enterprise should demand that the encryption provider offer adequate user access and administrative controls, stronger authentication alternatives such as two-factor authentication, management of access permissions, and separation of administrative duties such as security, network and maintenance.

By addressing these data related security issues we will increases the confidence of protection of data in cloud.

V. CONCLUSION

Cloud computing offers real benefits to companies seeking a competitive edge in today's economylike the ability to free up staff for other duties, and the ability to pay for "as needed" services.

As there are advantages to cloud computing, there are also several key security issues that need to keep in mind.

The cloud security issues are attracting great attention as active research areas like information security, data protection, virtualization for academician.

Data confidentiality and auditability topped the list of primary obstacles for the use of cloud computing technologies in organizations. cloud adopters would have security concerns around storing and processing sensitive data in a public or hybrid or even in a community cloud. Data security & protection is very essential in cloud environment so from our study we have given some general solution specially regarding encryption technique used for security& protection of data in cloud but not directly addressing all data security issues . In future we are trying to look in to the more trust based solution for data in cloud computing environment.

VI. REFERENCES

1. Cloud Computing And Emerging It Platforms *Rajkumar Buyya1,2, Chee Shin Yeo1, Srikumar Venugopal1, James Broberg1, and Ivona Brandic3*
2. A Short Introduction To Cloud Platforms *David Chappell*
3. Cloud Computing *Dr. Wendy A. Warr, Wendy Warr & Associates*
4. Cloud Computing Making Virtual Machines Cloud-Ready
5. Cloud computing security, http://en.wikipedia.org/wiki/Cloud_ computing_security.
6. Gartner: Seven cloud-computing security risks. InfoWorld. 2008-07- http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing security-risks-853.
7. Peter Mell, and Tim Grance, "The NIST Definition of CloudComputing," Version 1510-7-09, http://www.wheresmyserver.co.nz/storage/media/faq-files/cloud-def-v15.pdf.
8. http://www.saltmarch.com/pressRelease24.html