Security and Issues of Cloud Computing in Mining Algorithms

Apeksha Jain
College Of Computer Science & Information Technology (CCSIT)
Teerthanker Mahaveer University, Moradabad (U.P.)
apekshajain7217@gmail.com
Dr. Rajeev Kumar
Associative professor
(CCSIT)
Teerthanker Mahaveer University, Moradabad (U.P.)

Abstract— **This document is used to define scope of requirements and of recruitment of youth. It can have solved the problem that is related to data like of accessing the applications, apps, and company data record etc. So it can be accessed everywhere when its needs because of this technology. It provides a platform to store data into a server .This paper is provide some useful information of cloud safety and security and also discuss these advantages or disadvantages of security in cloud computing. The aim is to provide a solution for the drawback occur in data and security problem.**

Keywords— Cloud, cloud Data and services, cloud Issue and Security**.**

I. INTRODUCTION

The platform of cloud computing provides the users for which they can access the applications, data as utilities over the internet. It allows user to create, configure and customize the business applications online.

Cloud computing is a technology which enables the user to access resources using front end mechanism. there is no need to install any software. The main scope of cloud computing is that information can access at any location via internet. The platform of cloud provides a service to restore, backed-up, update, managed, and remotely maintained the data.

.

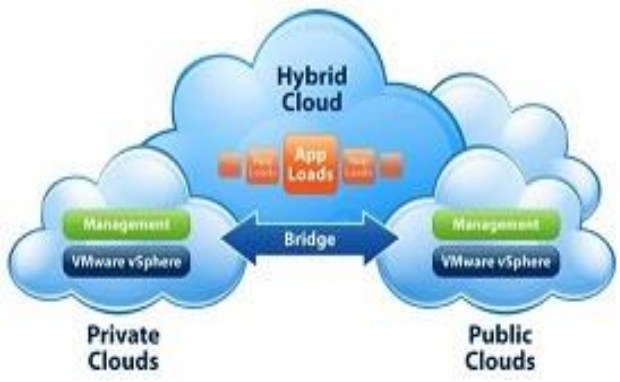
1) Type of cloud location

i) Public cloud
ii) Private cloud
iii) Hybrid cloud
iv) Community cloud

Public cloud is clearly define that cloud infrastructure (network) is same shared with others. It is not only a single user or organization. In a public cloud Resources are same used by the organizations.

Private cloud is clearly defined the cloud infrastructure (network) is not shared with others. It is only a single customer or organization. In other word Resources are not same that mean Private cloud not use shared resources.

In a private cloud security and control level is higher and cost reduction is minimal.

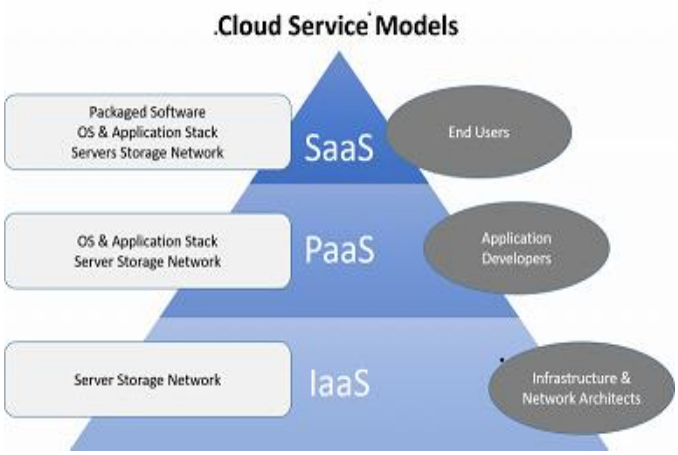


Hybrid cloud is combination of public cloud and private cloud. It is used on depending on their purpose. In a hybrid cloud most of the company are store their important or risky data into a form of private cloud and less risky data are store in the form of public cloud.

Community cloud is similar to public cloud. It is used to share data and data management, services and resource between the organizations in single country. E.g. mission, security requirement policy also shared an infrastructure by a several organization.
Example of community cloud is At bank, GOVT. Of country

2) cloud services

a) Saas (Software as a service)
b) Paas (Platform as a service)
c) Iaas (Infrastructure as a service)



Software-as–a service (Saas), mean that many various applications can have accessed by a user on a pay per basis. Cloud provide a infrastructure or a platform from running application without buying it
For example Laptop, Tabulate, PC's, etc are such devices that can be access the application from uses

Platform-as-a-service (Paas), Cloud is a Development Platform mean that user can create their application, and deploy with the help of Library Tool's, programming Languages**.**
For example "Salesforce","Google App Engine", etc. In this type of engine user can create or develop and deploy their application and own operating system can also be upgraded with help of Paas.

Infrastructure-as-a-service (Iaas), this type of layer is also known as base layer in cloud stack. Iaas provider many different type of cloud infrastructure like-Hard-ware based Load-Balancing, Services, Routers, Firewalls. This type of Application will be executed in an Instance Computer.
Some example of Iaas is Amazon, GoGrid etc.

II. Cloud security issue

There are many different issue and solution are define in this topic of cloud computing issue like security issue ,privacy issue , energy issue and data related issue etc. We are using many different type of services one of them like Google Gmail but we don't find issue because it is a big level company, they are not going to affect as a single user.

A. Security measurement for cloud computing

Round-the-clock physical security monitoring of our data centre facilities

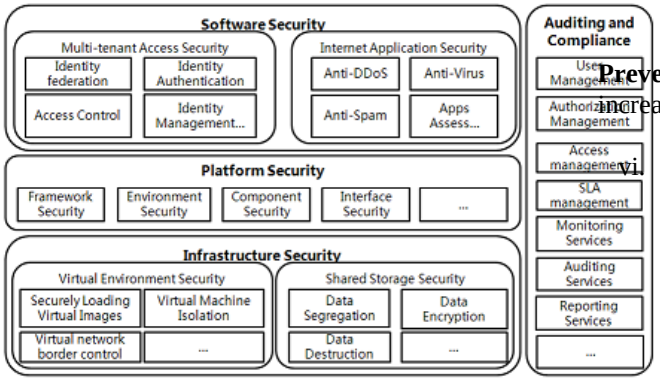
- Standardized and continuously monitored information security policy management
- Skilled, certified personnel to monitor, manage and maintain network infrastructure
- Use of various firewalls, intrusion detection and prevention systems
- Background checks, security training and non-disclosure agreements for employees
- Specialized threat identification and management team to counter threats of any type
- Policies, dedicated account manager and 24/7/365 monitoring to ensure security

B. Security Issue and Challenges in Cloud Computing

Cloud computing security issue is face by both Cloud providers and Cloud Customers.

a) The provider must ensure that
- Their Infrastructure Is Secure.
- Their Data and Application are protected.
- They provide a strong password and Authentication services to the customers.

b) The customer must ensure that
- To Protect Their Application
- To used strong password and Authentication.



Cloud Security Architecture

i. **Software Security** is a general phase that describes software. Software security includes antivirus software, Encryption software, firewall software and Spyware software .Antivirus software (virus protected software) and AntiSpyware (spyware removal software) are two most common type of security software Used for personal computer data security.

ii. **Platform Security** includes Architecture, Tools and Processes. Platform security used centralized security architecture. The main advantage of security architecture is cost effective due to the re-use of controls

iii. **Infrastructure security** Iaas security provide virtualization software security, customer guest OS or virtual server security. The issues of infrastructure security and cloud computing lie in the area of definition and provision of security specified aspects each party delivers. In case of public cloud there is multiple security issue in comparison of private cloud

iv. **Data Security** in a cloud computing data are store into a server there is a big issue to safely and secure to store data into a server because cloud provides a platform to store data and share distributed resources via open environment.

Remove problem that are related to data security problem we can use Authentication Password , Encryption and Decryption and many different type of compression services are provide in cloud computing .

v. **Data loss** in cloud server there is lot of data that should be stored by companies and consumers. In any process the data being corrupted. It is also known as data leakage Cloud data is store in a server so that is easy to Virus Infection that are delete one or more files ,in other form data are hacked or stolen by Network Intervention Attacked .

Prevention of data loss by implemented Data-Back-up, to increase our data Security Services.

vi. **Data Location** in cloud the issue is creating on the basis of Location, Availability, and Relocation security. Cloud also provides a data security and encryption of data to improve the security and services of cloud. The other service of cloud is to provide a suitable environment for deployment of data control over security and privacy.

vii. **Deletion of data** mean completely removing data from the storage media. Randering data completely irrecoverable. In other word making data inaccessible to anyone after it has been deem deleted. The data can't be completely removed is called incomplete data deletion. Cloud store data in a form of multiple copies the data deletion is majorly impossible because copies of data are saved in replica.

C. Security Services Advantages

1) **Data breaches prevention:** Strong data encryption can effectively prevent data breach cloud service database is properly designed and configured to keep hackers away from the system.

2) **Data loss prevention:** Data encryption may ward off hackers, the regularly updated offline data backups also reduce risks of data loss.

3) **More secure APIs:** APIs are important to maintain the cloud security service. Your service should help users to identify and improve weak APIs that can expose the organization.

4) **DoS prevention:** Cloud computing service will detect DoS attacks and provide effective responses to ensure 24/7 availability.

5) **Easy access information:** You can access the information anywhere and anytime.

D. Disadvantages of Security Services

1) **Downtime:** Cloud service is not working at a given time. Downtime is also called as idle time.

2) **Security:** It is a major issue in cloud, weak APIs that can expose the organization.

3) **Vendor lock:** The situation where customers are dependent cloud infrastructure and platform.

4) **Limited Control:** Cloud service provider the organization could have limited access and control the data apps

III. Future Work

There is a wide scope of cloud computing in future environment. Cloud should reduce the time and efforts wasted in submitting paper work and can be applied on large scale so that the purpose of the cloud data safety and security could be done efficiently. Cloud Security also helps in tracking and scheduling the task. The information can have accessed at any time with maintaining the security of it.

IV. Acknowledgement

The compilation of this research paper a lot of hard work and effort. I would like to express my sincere gratitude to my principal Dr. R. K. Dwivedi for giving me this wonderful opportunity to work on this research paper. I would also like to thanks my guide Dr. Rajeev Kumar, without his help the compilation of this research still would not be possible.

V. References

[1] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing," Version 15, 10-7-09, http://www.wheresmyserver.co.nz/ storage/media/faq-files/cloud-def-v15.pdf.
[2] Sun Cloud Architecture Introduction White Paper (in Chinese). http://developers.sun.com.cn/blog/functionalca/resource/ sun_353cloudc omputing_chinese.pdf.
[3] Cloud computing security, http://en.wikipedia.org/wiki/Cloud_ computing_security.
[4] Gartner: Seven cloud-computing security risks. InfoWorld. 2008-07-02. http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-853.
[5] Cloud Security Front and Center. Forrester Research. 2009-11-18. http://blogs.forrester.com/srm/2009/11/cloud-security-front-andcenter.html
[6] Cloud Security Alliance. http://www.cloudsecurityalliance.org.
[7] "IBM Discovers Encryption Scheme That Could Improve Cloud Security, Spam Filtering," at http://www.eweek.com/c/a/Security/IBMUncovers-Encryption-Scheme-That-Could-Improve-Cloud-SecuritySpam-Filtering-135413
[8] Lori M. Kaufman, "Data security in the world of cloud computing," IEEE Security and Privacy Journal, vol. 7, issue. 4, pp. 61-64, July- Aug 2009, ISSN: 1540-7993.
[9] Cloud Security Alliance (CSA). (2010). Available: http://www.cloudsecurityalliance.org/.
[10] Tackle your client's security issues with cloud computing in 10 steps, http://searchsecuritychannel.techtarget.com/tip/Tackle-your-clients-se curity-issues-withcloud- computing-in-10-steps.
[11] "Cloud Computing: Clash of the clouds". The Economist. 200910-15. Retrieved 2009-11-03.
[12]http://www.ibm.com/developerworks/0926 /diu/index.html
[13] www.google.com
[14]http://public.boulder.ibm.com/infocenter/com.ibm.rad /v7 /rad.75.html
[15] http://www.ibm.com/developerworks/