International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 3, ISSN No. 2455-2143, Pages 16-18
Published Online December – January. 2016 in IJEAST (http://www.ijeast.com)

VARIOUS SECURITY ISSUES AND THEIR REMEDIES IN CLOUD COMPUTING

Mridula Batra
Research Scholar,
Manav Rachna International University
Faridabad, India

Dr. Neha Gupta
Assistant Professor,
Manav Rachna International University
Faridabad, India

***Abstract* - The services of cloud computing is expending day by day. It has given shape to the theoretical infrastructure for future computations. The computational framework is running very fast worldwide towards cloud based architecture, though cloud computing is becoming very popular now a days but there are some other issues which should be considered-one of the major issue is security. In this paper, some major security issues has been analyzed and main emphasis is to rectify those issues.**

KEYWORDS - Cloud Computing, Cloud services, Infrastructure, Security.

I. INTRODUCTION TO CLOUD COMPUTING

Cloud computing is based on internet which compute shared resources which are provided to computer and other devices. Cloud computing emphasizes the utilization of shared resources at its maximum and along with it performs computational tasks for private or public networks. It is a realistic method to practice reduction in cost benefits and the future prospect of cloud computing is to establish data centre that can invest variable cost instead of heavy capital investment set up.

A. Categories of Cloud Computing

Private Cloud: - It is used to deliver services to individual or personal users from databases designed for business data. Such type of services is flexible as well as convenient while maintaining its original control security and managerial aspects.

Public Cloud: - In such type of clouds, services are delivered by third-party who all are involved in delivering cloud services with the help of internet.

Hybrid Cloud: - It is the mixture of private as well as public cloud. Generally, organizations run all the applications have the requirements of both public and private clouds. On private clouds important and secure applications are executed while public clouds are used for lengthy tasks and they run as and when required.

B. Advantages of Cloud computing

Self-service provisioning:- Any type of data can be retrieved as and when required for every type of applications by just molding the assets available on cloud.

Scalability: - Organizations dealing with cloud data can scale up and scale down with increase or decrease in demand respectively.

Variable Priced environment:- Values for resources on cloud are measured at a minute level, which help the users to price for the resources they have utilized.

II. SERVICES OF CLOUD

Infrastructure as a Service (Iaas):- It gives large storage and computational aspects of data over the Internet. It also provides capabilities of services over every kind of network (intranet or extranet). The exchange of service includes server space, storage system and sharing of network resources.

Platform as a Service (Paas):-- Platform is an environment that provides services on which other higher user- oriented applications can be created and executed, for example, a web site developer develop its own application and share space on internet to deploy its website by paying certain amount.

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 3, ISSN No. 2455-2143, Pages 16-18
Published Online December – January. 2016 in IJEAST (http://www.ijeast.com)

Software as a Service (SaaS): It means sharing the applications of the users of that cloud along with data as and when demand is generated. Single instance of a service can run on shared cloud and multiple instances run at end users platform.

TABLE I. COMPARISON BETWEEN THE THREE SERVICES

Iaas	Paas	Saas
In this services storage, database management and compute capabilities area offered.	This service provides design, development , build and test applications.	This is internet based application and offers the services to end-user.
Examples are:- Amazon, GoGrid, 3 Tera.	Google's App Engine, Force.com use such types of services.	Example of SaaS are:- Google, Salesforce, Microsoft

III. SECURITY AND PRIVACY

The major aspect to be considered while working on cloud is data security. As cloud is a collection of user's data stored at cloud's servers as well as on end user's computers. Authentication is the critical aspect in cloud computing. Along with the security, privacy of the individual users connected to the cloud servers should also be maintained. Modification in data over the cloud should be done with the permission of authenticated user. In a cloud provider platform different users share the data which is reside in the same data server, so the information can be leaked and hackers can alter the data through a single attack.

Maintenance of cloud security and privacy is a two-fold issue. Users and cloud service providers both should aware of terms and conditions for cloud data sharing and taking its services. Generally, for protection, private clods are more appropriate than public clouds.

A. Security issues in Cloud

The security prospects for cloud computing techniques are very active and cosmic. The main security issues are:

Network Security: - In cloud computing problems occur with network communications and configurations. The solution of network is that we can use services on cloud as an addition of customer's own networks (intranet), where security and privacy are locally applied.

Loss of Governance:- In case of public cloud, client leaves the control to the cloud provider for certain issues and at the same time cloud service level agreements (SLA) may not recommend an assurance to provide competence on the part of the cloud provider , so this gap affects the security.

Responsibility Ambiguity: - If the responsibilities of the consumer and the provider's organizations are not clear to each other, then important part of security protection are left imprudent.

Isolation Failure: - This type of threat includes the malfunctioning of storage space, system memory and routing algorithms.

Compliance and Legal Risks: - If the cloud provider does not provide the proof of their own compliance with the significant necessities or it does not allow the cloud consumer to do the audit then it may be put at risk.

Malicious Behavior of Insiders: - Damage can be occurred because of the nasty actions of persons working inside the company can cause huge damages to the data.

Business Failure of the Provider: - Sometimes the business of the cloud provider may lead to failure because of such failure such failures data may be unavailable to the consumer.

B. Cloud Security Directions

Implement Effective Monitoring risk management and dealing with complex processes existence: - Most of the cloud service providers (both public and private clouds) have their own policies and rules to ensure overall security of all the users and their applications exist on that cloud. Along with security management, they also focus on risk management for different types of risks present on clouds.

Effective Audit Implementation Policy Management: - Periodic report of all the transactions and utilization of services over the clouds are maintained by cloud service organization. There is a relevance and importance of these reports to see the effectiveness and efficiency of services provided.
There are certain important parts where certain types of audits are conducted:

1. It understands the inside aspects of cloud service provider which includes risks and checks on various governmental policies.

2. Access to the corporate audit trail.

Management of users, roles and their applications:- Users must be aware of cloud service provider's proper functionality of accessing user's data and handling their applications. Service providers have to build a faith in the users for proper implementation of all the policies and security issues. Cloud service providers allocate proper authentication and responsibilities to the various users for accessing cloud data.

Implantation of protection Policies for data and information:- Clod is a collection of data from various organizations distributed among multiple users over the network, so proper protection of all the data and information is required. Cloud service providers construct cloud architectures in a way that both data and information will be secured and protective from unauthorized users.

Enforce privacy policies: - Privacy is very important all around the world which includes rules and regulations related to personal identification and acquiring storage space and handling personal data and information. Privacy means limiting the access of data to the authorized users. Cloud service provider's architecture should have mechanism to implement the privacy of individual user and proper authentication before accessing the data on clouds.

Manage security terms in the cloud SLA: - While designing security terms and conditions, there should be a clear demarcation between customer's security responsibilities and cloud service providers responsibilities. An agreement should be clearly defined for all terms and conditions.

IV. CONCLUSION

There are massive projections for cloud computing but cloud computing is always surrounded by security threats which are directly linked to its advantages. It is beneficial to both the parties be it a business or the invader but security is always a concern. So, we have discussed various security threats and their probable solutions.

V. REFERENCES

[1] A. Agarwal, and A. Agarwal (2011), "The Security Risks Associated with Cloud Computing.International Journal of Computer Applications in Engineering Sciences", 1 (Special Issue on CNS),257-259.

[2] K. Hamlen, M. Kantarcioglu, L. Khan, and V. Thuraisingham(2010),"Security Issues for CloudComputing. International Journal of Information Security and Privacy", 4(2), 39-51. doi:10.4018/jisp.2010040103.

[3] P. Ryan, and S. Falvey (2012), " Trust in the clouds. Computer Law and Security Reviews", 28, 513-21.http://dx.doi.org/10.1016/j.clsr.2012.07.002

[4] M. Okuhara, "Shiozaki, T. and Suzuki, T. (2010). Security Architectures for Cloud Computing", FUJITSU Science Technology Journal, 46(4), 397–402.

[5] Ahmed Monjur, Hossain Mohammad Ashraf, "Cloud Computing And Security Issues In The Cloud", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[6] Red´ıgolo Fernando, Simpl´ıcio, "A quantitative analysis of current securityconcerns and solutions for cloud computing",Journal of cloud computing: Advances, Systems and Applications 2012, 1:11.

[7] N. Anand (2010), "The legal issues around cloud computing", http://www.labnol.org/internet/cloud-computing-legal-issues/14120.

[8] I Brandic, S Dustdar , T Anstett , D Schumm , F Leymann (2010), "Compliant Cloud Computing (C3): Architecture and Language Support for User-driven Compliance management in Clouds" , In: 2010 IEEE 3rd International Conference on Cloud Computing. pp 244–251, http://dx. doi.org/10.1109/CLOUD.2010.42