

## A Review of Multiple Layer Security of Cloud Server

Dr. Sandeep Dalal

Asst. Professor, DCSA  
Maharshi Dayanand University

Miss. Neetu Rani

Mtech Student, Reg. No: 1518090112  
Maharshi Dayanand University

### Abstract:

Cloud services are offering the flexible and scalable services. But there is always issue of security. When data is transferred from centrally located server storage to different cloud the compromise of person and private data would increase. There is always risk to the confidentiality and availability of data prior to selecting a cloud vender or choosing own cloud and cloud service migration. Cloud services usually have their security concerns that must be addressed. In this paper we have discussed the threats to cloud service and data in case of conventional security system and modern security system and proposed an idea to secure data on cloud using multiple layers of security

### [1] Cloud Computing

Cloud may be network or internet and it is something that is available at remote place. It provides services over network that are public and private. They are used in wide area network, local area network or virtual private network. Several application like email and web based conferencing executes on cloud.

Platform independency is offered by cloud computing because there is no need to install software on personal computer. So we can say that our business applications are mobile and collaborative due to cloud computing.

There are several services that are making cloud computing more feasible and easily accessible to the users.

Cloud computing is providing number of advantages but there are several risks associated with this technology.

### Advantages

Cloud computing provides several benefits and they are listed below

1. User on internet could access remote applications in form of utilities.

2. User at any time can change and configure the application online
3. Online development tools are offered by cloud computing.
4. Online deployment tools are provided by cloud computing.
5. Clients are provided platform independent access of cloud resources that are available on internet.
6. On-demand self services are offered by cloud computing and there is no need of interaction with cloud service provider.
7. Cloud computing operates at high efficiency and it does optimum utilization so it is highly cost effective.
8. Load Balancing feature of cloud computing represent that it is more reliable.

### [3] Need of Cloud Computing

1. Its provides 24x7 Support
2. Cloud computing pay as we use
3. It has lower Total Cost of ownership
4. Cloud computing provides Reliability, scalability, sustainability.

5. It provides Secure Storage Management Expenditure.
6. It is capable to Free up Internal Resources.
7. Such systems are Highly Automated.
8. These Systems are Utility Based.
9. It allows Easy & Agile Deployments.
10. Such systems are Device & Location Independent.

### Cloud Based Delivery

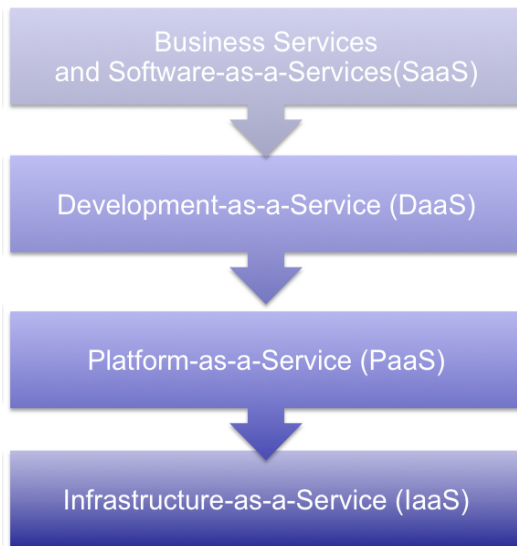


Fig 1 Cloud Based Delivery

### [2] Cloud Server model

Type of access to cloud has been defined by Deployment model. There are four types of accessibility in cloud that are public access, private access, Hybrid access and Community access.

#### Public Cloud

Access to general public is allowed by public cloud. Due to openness public cloud is less secure

#### Private Cloud

Due to its private nature private cloud is considered more safe and secure.

#### Community Cloud

Accessibility to a particular group is allowed by community cloud.

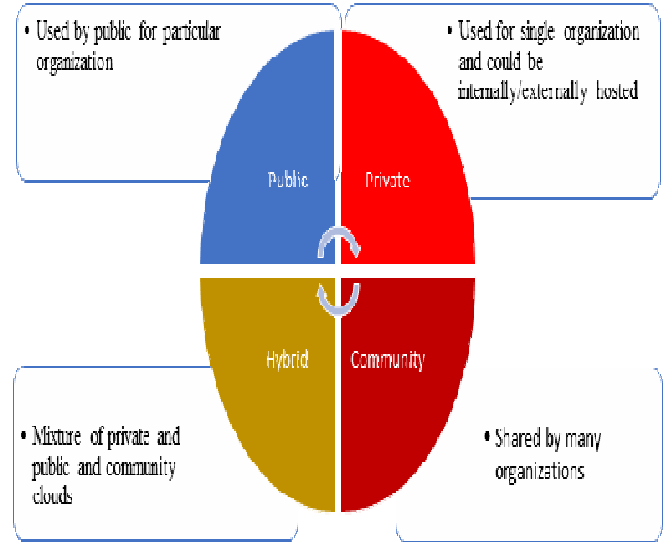


Fig 2 Cloud Server Model

### Hybrid Cloud

A Hybrid Cloud could be considered as combination of public cloud and private cloud where private cloud does critical tasks and public cloud does non-critical tasks.

### Service Models

There are three service models in cloud computing. First is Infrastructure as a Service, Second one is Platform as a Service and last one is Software as a Service.

### [4] Security issues in Cloud computing

Third party provides data and infrastructure management in cloud computing so the security of cloud is biggest concern. There is a risk in providing the sensitive data to cloud service provider. Any security breach could result in customer or business loss so vendors provide protection to the accounts.

Customer cannot switch from one cloud service provider to another quickly so he is dependent on cloud service provider for service. Customer management interface is usually accessible on network in case of various public cloud service providers.

Data security must be considered in cloud because data is frequently transferred over Internet. The basic mechanisms to protect data over cloud are data auditing, data access control, data authentication and data authorization.

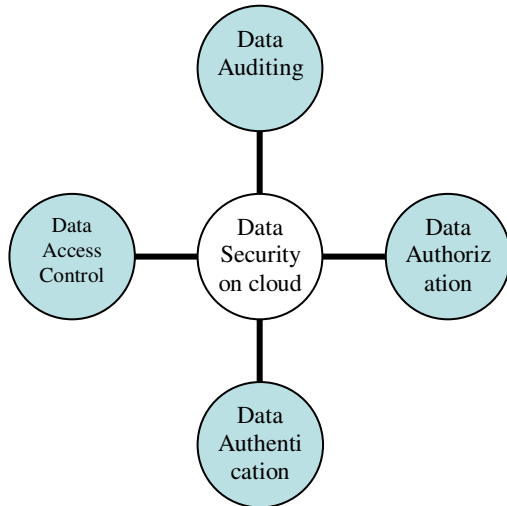


Fig 3 Data Security on cloud

### [5] Cryptography

Cryptography is the process of hiding plan data or information in form of cipher text. It is the process used to keep information safe and hidden. Modern Cryptography is the combination of computer science, mathematics and electrical engineering.

It is used in computer passwords and ATM Cards and e-commerce sites.

During data transmission data is encrypted before data is transferred.

The encrypted data is known as cipher text. This modification makes the data non readable. To understand this data user have to decrypt the data. Cryptanalysis is process of studying cipher text in order to find hidden data.

### Encryption    Decryption

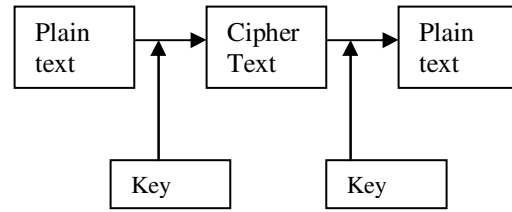


Fig 4 Encryption and Decryption process

### [6] OBJECTIVE OF RESEARCH

The objective of research is to provide security to cloud environment by providing additional security layer. In this research we would

1. Establish cloud based data transmission environment.
2. Perform the data transmission in cloud server and clients.
3. Investigate the security loop holes to existing security mechanisms.
4. Providing better security to cloud environment using cryptography to secure data from cryptanalyst.
5. Provide data transmission security using socket and port based programming.

### [7] FUTURE SCOPE AND CONCLUSION

Cloud has provided flexible and scalable services. But there would issue of security due to data transfer from one cloud server storage to another cloud. This research would reduce the risk to the confidentiality and availability of data prior to selecting a cloud vender or choosing own cloud. The security concerns of cloud services have been addressed in our research. In this research we would provide modern security system and proposed an idea to

secure data on cloud using multiple layers of security.

## Reference

1. Peter mill & Tim grance, “The NIST Definition of Cloud Computing”, 2011, National Institute of Standards & Technology ,Gaithersburg,MD 20899-8930, NIST Special Publication 800-145.
2. Ellen Messmer, “New security demands arising for virtualization, cloud computing”, 2011, security-demands-arising-for-virtualization—cloud computing.html
3. .Sumedha Kaushik & Ankur Singhal, “Network Security Using Cryptographic Techniques” 2012, volume 2, Issue 12.
4. Charles Miers, Fernando Redigolo & Marcos Simplicio, “A quantitative analysis of current security concerns & solutions for cloud computing ”, 2012, Journal of Cloud Computing: Advances, Systems & Applications electronic version of this article is
5. Rabi Prasad Padhay, “An Enterprise CSSloud Model for Optimizing IT Infrastructure”, 2012, International Journal of Cloud Computing & Services Science (IJ-CLOSER) Vol.1,
6. Nelson Gonzalez, et. al. , “A quantitative analysis of current security concerns & solutions for cloud computing ”, 2012, Journal of Cloud Computing: Advances, Systems & Applications doi:10.1186/2192-113X-1-11The electronic version of this article is complete one & could be found online
7. .CSA “Security Guidance for Critical Areas of Focus in Cloud Computing”, (2009), Tech. rep., Cloud Security Alliance.
8. Rowstron & P. Druschel. Pastry: Scalable, distributed object location & routing for large-scale peer-to-peer systems. *Accepted for Middleware, 2001*, 2001.
9. Ben Y. Zhao, John Kubiawicz, & Anthony Joseph. Tapestry: an infrastructure for fault tolerant wide-area location & routing. April 2001.
10. Andr´ea W. Richa C. Greg Plaxton, Rajmohan Rajaraman. Accessing nearby copies of replicated objects in a distributed environment. In *Proceedings of ACM SPAA*, pages 311– 320, June 1997.
11. Stefan Saroiu, P. Krishna Gummadi & Steven D. Gribble. A Measurement Study of Peer-to- Peer File Sharing Systems. July 2001.
12. Ion Stoica, Robert Morris, David Karger, M. Frans Kaashoek, & Hari Balakrishnan. Chord: A peer-to-peer lookup service for internet applications. August 2001.