International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)

International Conference on Information Systems and Computing (ICISC-2013), INDIA.

DATA SECURITY AND STORAGE IN CLOUD COMPUTING

J.Bhuvaneswari[1], R.Vaishnavi[2]

[1,2]*School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, India;*

Email: bhuvijana@gmail.com;rvaishnavi26@gmail.com

Abstract

As in modern internet era,Cloud Computing has been gaining more importance day by day.Various methodologies are implemented to provide security for the data being processed.In this paper, a review of data security and storage in cloud computing has been discussed.

***Keywords*-- Cloud computing ,Data storage , Data security**

I. INTRODUCTION

Cloud computing is the service delivered through the network or internet by using a computer resources.Telecommunication companies initially started offering point to point data circuits but later in 1990 , it started providing virtual private networks[1].The VPN is the technology for connecting computers to the remote isolated unaccesable computer network using internet or any other network. The advantages of VPN are comparable QOS and low cost.It also provides security and their connections are isolated in the network [2].The types of cloud computing are: public,private and hybrid clouds. Public cloud services provides services to the public using application and storage. Private cloud service is the service that are not feasible for ordinary people.Hybrid cloud computing is the services which offers both public and private cloud services. SaaS,IaaS and PaaS afe the major services in the cloud[3].

II. VARIOUS POLICY ISSUES

There are various policy issues involved in cloud such as Privacy, Reliability, Availability Anonymity ,Liability and Security.The cloud clients will have several motivation which varies from ordinary use to secure uses. For companies and other banking enterprises they needs very high security, for them,they must ensure that the cloud service providers must provide them.

Garter's Seven security issues such as .

- Privileged user access
- Regulatory compliance
- Data location
- Data segregation
- Recovery
- Investigative support

III. DATA SECURITY AND STORAGE

When using a public cloud, it is important that it must be capable of providing both confidentiality as well as integrity. Obviously when using protocols such as FTPS, HTTPS, SCP for data transfer through the internet, simply encrypting the data along with a non-secure protocols such as FTP, HTTP results in confidentiality but the intergrity of the data is not ensured. In IaaS services, it is strongly recommended for small storage and the encryption is possible.But in PaaS and SaaS cloud based application,compensating control is not possible because it may prevent it from searching or indexing.Applications provided with cloud computing are desisned with data tagging to prevent unauthorized access to user data.All the data must be encrypted to transfer or receive from cloud but there is no proper method to process encrypted data till 2009.In 2009, IBM developed a fully Homomorphic Encryption Scheme. .

Using the scheme , we can process the data without decryption.The limitation of this scheme is that it requires immense computational effort.It is always necessary for the cloud clients to know about exactly where the data has been stored and when the data has been updated.*Data lineage* is the process of data path visualization from the time when the data has been transferred to the cloud. Data lineage is time-consuming and in the case of public cloud service it is not possible.Even if Data lineage is established among public cloud service, the most challenging task is to provide *Integrity* as well as *Provenance*.Integrity of data is the process in which the data was not accessed by unauthorized person.Provenance refers to the computational accuracy along with the integrity.

The final aspect in cloud computing is the *Data Remanence*.The Data Remanence is the residual data representation present even after being deleted or erased.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

This may leads to a risk that any Organisation data can be easily affected by unauthorized access regardless of SaaS, IaaS and PaaS cloud services.Many cloud services providers referring the U.S. Department of Defense (DoD) 5220.22-M[5].

IV. Handling Cloud Computing Data Security

Multi-tenancy is when the requirement of high-risk client is met, then it automatically provides better security for all low-risk clients.Security asssessment in an organisation must be carried out periodically by person who are able to identify and fix the problems efficiently.Shared risk will appear in multi-tier service arrangement provider where the service provider acquire an infrastructure needed for it from another service provider,thereby,it potentially affects all parties.Staff Security Screening is important because usually cloud provider employs contractors to undergo an investigation of your employees under policy.

Distributed Data Center is needed to make the cloud servive provider less prone to geographical disasters ,in such a way eliminating the use of periodically tested disaster rcovery plan.Physical Security is nothing but the clients must have a good knowledge about the security levels of all the cloud service providers.Coding of the cloud service provider must be based on the standard methods that can be further documented and demonstrated to the client in future in oreder to make them sure about the secure coding process.Data Leakage is one drawbacks of every cloud provider , so it is always recommended to have a encrypted format of data is transmitted and received.[6]

V. Security Quality Requirement Engineering (Square)

The SQUARE methodology is more accurate and effective containing nine discrete steps.

- Agree on Definitions
- Identify Security Goals
- Develop Artifacts to support Security Requirements Definition
- Perform Risk Assessment
- Select Elicitation Techniques
- Elicit Security Requirements
- Categorize Requirements as to level (system software,etc.) and whether they are requirements or other kinds of constraints
- Prioritize Reuirements
- Requirements Inspection

REFERENCES

[1] Cloud Computing Wiki
[2] VPN
[3] Cloud Computing Security Threats and Responses Farzad Sabahi
[4] Gartner: Seven cloud-computing security risks
[5] S. K. Tim Mather, and Shahed Latif, Cloud Security and Privacy: O'Reilly Media, Inc , 2009
[6] C. Almond, "A Practical Guide to Cloud Computing Security
[7] Security Quality Requirements Engineering (SQUARE) Methodology Nancy R. Mead Eric D. Hough Theodore R. Stehney II