A Study of Data Storage Security Issues in Cloud Computing

Mini Singh [1] Alok Tripathi[2], Dr. Devesh Katiyar[3]
[1] Student of MCA,[2] Student of MCA, [3]Asst. Professor
Department of Computer Science
Dr. Shakuntala Misra National Rehabilitation University, Mohaan Road, Lucknow

***ABSTRACT*-Cloud computing provides facilities to its clients. Storing the data is primary service provided by cloud computing. Cloud service supplier hosts the data source and user can access the data from these servers. The features of data storage bring up various security challenges. An independent procedure is required to authorize that data is correctly hosted in to the cloud storage server. In this paper, the different methods that are used for sheltered data storage on cloud.**

INTRODUCTION

In this era a lot of customers or users need to compute a large data over it but sometime due to lack of memory management Client cannot perform some operations. So, here we introduce a storage system such as "Cloud Computing". The goal is to permits users to take profit from these technologies. Many enterprises are moving into cloud because it permits the users to save their data on clouds and can access at anytime from anywhere. In cloud environment Data break through is possible, while data from several Consumer and business corporations stay together in cloud. By sending the statistics to the cloud, the data owners transfer the control of their data to a third person that may raise security exertions. Sometimes the Cloud Service Supplier itself corrupts the data. Security is a key difficulty on cloud computing i.e. conserving confidentiality, reliability and accessibility of data. A clarification is to translate the data previously uploading it. This approach shows that the data is invisible to external users and cloud administrators but has the problem of plain text based searching procedure are not applicable. In this thesis, we check the security flaws in data storage and the mechanisms to overcome it.

CLOUD MODEL

Two types of models are used in cloud computing-
i) Deployment Model
ii)Service Model
In this model it tells about how the cloud is actually locating at remote location. In four ways we can access the cloud they are as follows-

i) Deployment Model

a) Public Cloud

In this it is easily accessible by all the users such public. But it is not much secure due to of its openness.

b) Private Cloud

In this it is only accessible within or under a business enterprise. It is more secure then the Public by a reason its private nature.

b) Hybrid Cloud

It is combination of both public as well as private. In this some activities performed by public cloud and some performed by private cloud.

2) Service Model

It means different types of application provide different servers all across the cloud-

a) Software as a Service-

It allows user to use different type of software to different application. It allows to client for paying according to uses and there is no need of maintenance and updating from user side. Server needs to do all it's updating according to need of customers. It provides cheap cost and only a single application needed instead of buying whole software. Example- Sales force, Zoho.

b) Platform as a Service-

It allows user to built its own application by providing different resources that required to build a software and which run on the provider's infrastructure. It means it provide a platform including all system requirements. Example- Microsoft, Azure, etc.

c)Infrastructure as a Service

It provides users storage and infrastructure network to keep customers make its own platform to deploy software. The top companies that use this service are Amazon (EC2), Teremark.

IV CHARACTERISTIC OF CLOUD COMPUTING

There are five attributes of cloud computing. The first one is on-demand self-service, where a user of services is provided the needed resources deprived of human intervention and consultation with cloud supplier. The second characteristic is wide network access, which means resources can be accessed from anywhere through a standard procedure by thin or thick user stages such mobile phone, laptop, and desktop computer. Resource pooling is another feature, which means the resources are combined in order for multi-tenants to distribute the resources In the multi-tenant model, resources are appointed dynamically to a client and after the client finishes it, it can be appointed to another one to reply to high resource request. Even if there sources are consigned to customers on request, they do not know the location of these assigned resources. Cloud environment architecture. Sometimes they know the location at a high-level notion, such as nation, state, and data centre. Storage, processing, memory, and network are the variety of resources that are allocated. Rapid elasticity is another feature, which means that resources are vigorously increased when needed and decreased when there is no need. Also, one of characteristics that a consumer needs is measured service in order to know how much is consumed.

V. ENCRYPTED DATA STORAGE FOR CLOUD

Since data in the cloud is located anywhere, it is significant that the data be encoded. We are using protected co-processor as element of the cloud structure to facilitate efficient encoded storage of confidential data. When appointed on the server, it is able to performing local computations that are completely hidden from the server. If tampering is sensed, then the protected co-processor dissipates the internal memory. Since the protected coprocessor is anti tamper, one could be tempted to run the entire confidential data storage server on the protected coprocessor. Pushing the whole data storage functionality into a protected co-processor is not viable because of many reasons. Performance will improve over time, but problems such as heat dissipation/power use (which must be controlled to avoid disclosing processing) will force a space between general purposes and protected computing. Another concern is that the software running on the SCP must be totally reliable and proved. This security obligation indicates that the software running on the SCP must be set aside as simple as probable. We can encode the sensitive data collections using random private keys and to ease the threat of key revelation, we can use tamper-resistant hardware to save some of the encryption/decryption keys (i.e., a master key that encodes all other keys). Elements of the recommended instruments.

VI. SECURITY AND PRIVACY PROBLEMS IN DATA STORAGE

Cloud Computing permit the users to save their data on the storage location corroborated by another person. Once the data is uploaded into the cloud the user throw away its control over the data and data can be damaged by the attackers. The attacker may be an internal(CSP) or external. Unofficial access is also a frequent practice due to feeble access control. The security information is arising the subsequent challenges: The security and privacy problems connected to data storage are confidentiality, integrity and availability.

VII. CONCLUSION

Due to these various organizations are not eager to run into cloud environment. Otherwise make sure that any sensitive data is not place into a public cloud and if any it is to be stored in encoded form. Efficient auditing methods also can be used for supplying data integrity.

VIII. REFERENCES

[1] V. Nirmala, R. K. Sivanandhan, Dr. R. Shanmuga Lakshmi, “Data Confidentiality and Integrity Verification using User Authenticator scheme in cloud”, Proceedings of 2013 International Conference on Green High Performance Computing (ICGHPC 2013). March 14-15, 2013, India.

[2] Arjun Kumar, Byung Gook Lee, Hoon Jae Lee, Anu Kumari, “Secure Storage and Access of Data in Cloud Computing”, 2012 International Conference on ICT Convergence (ICTC), 15-17 Oct. 2012.

[3] M. R. Tribhuwan, V. A. Bhuyar, Shabana Pirzade, “Ensuring Data Storage Security in Cloud Computing through Two-way Handshake based on Token Management”, 2010 International Conference on Advances in Recent Technologies in Communication and Computing.

[4] Mr. Prashant Rewagad, Ms. Yogita Pawar, “Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing”, 2013International Conference on Communication Systems and Network Technologies.

[5] Uma Somani, Kanika Lakhani, Manish Mundra, “Implementing Digital Signature with RSA Encryption Algorithm to enhance the data security of cloud in cloud computing “,1st international conference parallel,distributed and grid computing (PDGC-2010)

[6] M.Alzain ,E.Parded ,B.Soh,and Z.Thom ,”Cloud computing Security:from single to multi cloud ,”in system science (HICSS),2012 45th Hawaii International Conference on, Jan-2012,PP.5490-5499.