SECURED DATA ON MULTI CLOUD STORAGE SYSTEM

Prof. Dhanashri S. Patil

Lecturer in Computer Dept.,KJ College Of Engineering & Management Research, Pune, Maharashtra, India.

---***---

Abstract:-*Cloud storage is an important service of cloud computing, which presents service for data legatee to present their data in the cloud. This new prototype of data moderation and data access services recommends two major security establishments. The first is the protection of data virtue. Data legatee may not fully reliance the cloud server and apprehension that data stored in the cloud could be depraved or even extracted. The second is data ingress control. Data legatee may worry that some corrupt servers provide data approach to users that are restricted for benefit achievement and thus they can no longer await on the servers for access control.*

Key Words::Cloud computing, single cloud, multi-clouds, data integrity, data intrusion, service availability, cost-reduction.

1. INTRODUCTION

The storage services for cloud data storage among two entities are cloud user and cloud service providers. The cloud storage service is widely priced on two factors. How much data is to be stored on cloud servers and for how long the data is to be stored. In our system, we hypothesis that all the data is to be stored for same period of time. Each obtainable cloud service provider is associated with a factor, along with its price of supplying storage service per unit of stored data. Every Cloud Service Provider has a dissimilar level of quality of service offered as well as a different cost analogous with it. Therefore cloud user can withhold his data on more than one cloud, according to the required level of security, and their sustainable budgets. To access this cloud services security and reliability we are using different modules like:

1) Use of single cloud service provider.

2) Accepting multiple cloud serviceproviders.

The obstacle of single cloud service provider is that it can be easily hacked by any attacker. Multiple cloud service provider model provide better security and availability of user private data.

2. OBJECTIVES OF MULTI-COULD ARCHITECTURE

2.1 Security

Data and Information will be shared with external users In multi-cloud data Storage, therefore cloud computing users want to avoid important information from attackers or malicious insider is of critical importance. In Iaas, users are responsible for protecting operating system and cloud providers must provide protection for users data. Resources in the cloud are accessed through the Internet, frequently even if the cloud provider concentrates on security in the cloud infrastructure; the data is still transmitted to the users through networks which may be insecure.

1.Data integrity
2. Data intrusion
3. Service availability

these are the three Security factors.

2.2 Data Integrity

The data stored in the cloud may lost from damage while transferring from one place to another. Examples: Of the threats of attacks from both inside and outside the cloud provider.

2.3 Data Intrusion

Another security risk that may occur with cloud provider, such as the any particular cloud service will hack password. If someone obtains access to that cloud service password, they will be able to access all of the accounts instance and resources. Thus the abducted password allows the hacker to erase and to modify all the data inside any virtual machine instance for the stolen user account or even prevent its services. There is a possibility for the users email (Amazon user name) to be hacked for a discussion of the potential risks of email.

2.4 Service Availability

There is possibility that the service may be unavailable from time to time. If any user files unravel the cloud storage policy, the users web service may terminate for any reason at any time. Therefore Cloud provider maintain the backup and data authentication which assures that returned data is same as stored data is extremely important.

2.5Performance

In single architecture, there is one main cloud server which will process and response the requirement from the users. If more than expected no of clients will requested for data/service to the single server then the performance will slow down Each user will have to wait more for accessing his/her data. In case of overload, the server may hang sometime. In multi cloud we have more than one cloud server to process the users request So this divides the responsibility of handling requests among several servers. So ultimately we can provide better solution to our providers.

2.6 Cost-Reduction

Secured storage and data scope can be provided to the customers in the market of economical distribution of information in all the available service providers.In model customer decide his data among their several SPs available in the market. Also we provide decision for the customer, to which SPs he must choose to access data and quality of Service offered by service provider.

3.USE OF DATA ENCRYPTION TECHNIQUES

For ensuring more security in cloud environment, we can use data encryption. If the data is distributed in multi cloud environment as well as it is encrypted, we can protect our data in even better way. The data which is transmitted by the user, can be encrypted first and then we can store it on the cloud server. This will be helpful in producing two-way security to the customer's data. To store the data in multi-cloud environment The symmetric key or secret key algorithms are the best choice for such applications. Secure the key from access by illegal agents, because anyone that has the key can use it to decrypt your data or encrypt their own data, challenging it commenced from you. Secret-key encryption is also referred to as symmetric encryption because the same key is used for encryption and decryption. Secret-key encryption algorithms are very brisk (compared with public key algorithms) and are well suited for performing cryptographic transformations on large streams of data.

4. PROBLEM STATEMENT

In today's world users are cladding threats and frauds, deal with the cloud data storage. In our system, to diminish the threats facing cloud storage, we widen the cloud data storage to include multiple service providers, where each cloud storage correspond to a different service provider. Our stimulation behind such an extension is that, the opponent, similar to any other cloud user, is conceptual from the actual clouds of servers executed by different cloud service providers. So as a outcome we get guarded data storage in clouds.

4.1 Proposed System:

In this system, we prefer an inexpensive distribution of data among the available service providers in the market, to provide customers with data accessibility as well as secure data storage. In our model, the customer split his data between Several Cloud Service Provider's available in the market, based on users available budget. Also we supply a decision for the customer, to choose different Cloud Server Provider. User may determine Cloud Server Provider to store or to approach the data, regarding data access quality of service offered by Cloud Service Provider at the location of data retrieval.

This not only rules out the probability of a Cloud Service Provider, mishandling the customers data or breaking the privacy of data, but can easily make sure the data accessibility with a better quality of service. Our preferred approach will provide the cloud computing users a decision model, that provides a better security by give out the data over multiple cloud service providers in such a way that, none of the service provider can successfully get back meaningful information from the data pieces assigned at their servers.

Also, in extension, we issue the user with better certainty of accessibility of data, by maintaining expandability in data distribution. In this case, if a service provider undergo service disapproval or goes bankrupt, the user still can use of his data by regaining it from other service providers. So at the end we provide full security to the user regarding unpublished, Integrity and the attainability of data.

Above diagram is for Multi Cloud Storage System.The systemcontain four clouds and each cloud uses its own specific interface. These four clouds are storage clouds, so there are no codes to be carried out. System allows reading and writing operations with the storage clouds.These Clouds cope with altered cloud service providers.

4.2 Advantages:

1. The system supplies data unification,
Availability, Confidentiality in short Security.
2. By using cryptography data is secured.
3. Inexpensive and cost based on client
requirements.
4. Cloud data storage also redefines security
matters targeted on customers outsourced data.
5. Easy to keep large databases with security.
6. Keep away from database losses.

5. PROJECT SCOPE

Any other cloud user, is conceptual from the actual clouds of servers executed by different Cloud Service Providers, so by using this system we gets a security concerning, Confidentiality, Integrity obtainable matters.

System Architecture:

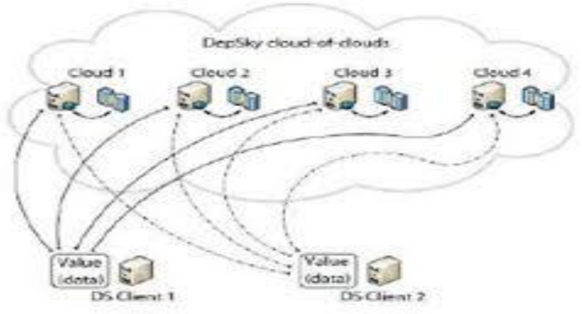

Figure:-Multi Cloud Storage System

Above diagram has following elements, these are
• Cloud Controller: The shift of industrial information technology towards pay-per-use servicebusinessmodel is known as Cloud Computing.
•Cloud Service ProviderCloud computing environment is provided by cloud service providers.
Thesecloud service providers are separate administrative entities. CSP has significant re- sources and expertise in building and managing distributed cloud storage servers.

6. CONCLUSION

It is clear that despite the fact that the use of cloud computing has quickly increased, cloud computing security is still regard as the major issue in the cloud computing environment. Customers don't want to misplace their private information as a result of spiteful insiders in the cloud. In addition, the loss of service accessibility has source of many problems for a large number of customers recently. Furthermore, data interruption leads to many problems for the users of cloud computing.The motive of this work is to study the recent research on single clouds and multi-clouds to marks the security risks and solutions. We have found that much studies has been done to ensure the security of the single cloud and cloud storage whereas multi-clouds have received less observation in the area of security. We support the relocation to multi-clouds due to its capability to minimize security risks that affect the cloud computing user.

REFERENCES

[1] P. S. Browne, Data privacy and integrity: an overview, In Proceeding of SIGFIDET 71 Proceedings of the ACM SIGFIDET (now SIGMOD), 1971.
[2] The Official Google Blog, A new approach to China: an update, online at http://googleblog.blogspot.com/2010/03/ new-approach-to-chinaupdate. html, March 2010.
[3] A. Shamir, How to share a secret, Commun. ACM 22, 11(November 1979).
[4] W. Itani, A. Kayssi, A. Chehab, Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures, Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, Dec 2009.
[5] N. Gruschka, M. Jensen, Attack surfaces: A taxonomy for attacks on cloud services, Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, 5-10 July 2010.
[6] B. Krebs, Payment Processor Breach May Be Largest Ever, Online at http://voices.washingtonpost.com/securityfix/ 2009/01Jan, 2009.
[7] P. F. Oliveira, L. Lima, T. T. V. Vinhoza, J.Barros, M. Medard, Trusted storage over untrusted networks, IEEE GLOBECOM 2010, Miami, FL.

USA.
[8] AModernLanguageforMathematical Programming,Onlineat http://www.ampl.com.

Books:
1. George Reese: Cloud Application Architectures

2. Garret, Paul. Making, Breaking Codes: An Introduction to Cryptology 3. Andy Mulholland: Enterprise Cloud Computing 4. Tim Mather: Cloud Security and Privacy

Websites:
www.slideshare.net/cloud-computing
www.researchgate.net/cloud-computing
www.rightscale.com/products/multicloud-platform

BIOGRAPHIES

Lecturer in Computer Dept.,
KJ College Of Engineering &
Management Research, Pune.
Maharashtra, India.
E-Mail :dhanashri8286@gmail.com