Enabling Data Security on Multi-cloud

Revanth K¹, Yashaswini² & Rajesh N³
¹² B.E, Dept of ISE, NIE, Mysuru, Karnataka, India
³ Assistant Professor, Dept of ISE, NIE, Mysuru, Karnataka, India

Abstract: Cloud over the network. Data integrity should be taken into account so that the data is correct, consistent and accessible. For ensuring the integrity in cloud computing environment, cloud storage providers should be trusted. Dealing with single cloud providers is predicted to become less secure with customers due to risks of service availability, failure and the possibility of malicious insiders in the single cloud. This paper deals with multi cloud environments to resolve these issues. The integrity of the data in multi cloud storage has been provided with the help of trusted third party computing is basically cost effective and on demand service offered to the clients. It is a model to access shared pool of configurable computing resources which include servers, storage, applications and also services to interaction provider. Cloud computing is computing on various resources.

1. Introduction

Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort, many organizations are relied on sharing of information. This information contains user private data as well as high secure data. Therefore need for secure and robust data resources are increased rapidly. Cloud data storage is a major solution to overcome this problem, but dealing with single cloud providers is becoming less satisfactory with customers due to major problems such as service availability failure for some time and malicious insider’s attacks in the single cloud. Hence, to provide a secure way to access a data need move towards ‘Multiple clouds’ or ‘Cloud of Clouds’. The multi-cloud works on the encrypted inputs to compute the encrypted output. The intermediate or final results have to decrypt, In proposed system, cluster of cloud storage is created and maintained accordingly to satisfy the user specific data access requirements. Here the replication of the user data to multiple clouds is done and update that information timely.

2. LITERATURE SURVEY

2.1 HAIL Model

Mohammed A. Alzain, Ben Soh and Eric Pardete describes, it is a distributed cryptographic system (High Availability and Integrity Layer) that allows a set of servers to prove to a client that a stored file is intact and retrievable. HAIL relies on a single trusted verifier. It aggregates cryptographic protocols for proof of recoveries with erasure codes to provide a software layer to protect the integrity and availability of the stored data, even if the individual clouds are compromised by a malicious and mobile adversary. HAIL has at least three limitations: it only deals with static data, it requires that the servers run some code and does not provide guarantee of confidentiality of the stored data.

2.2 DepSky Model

Alysson Bessani, Miguel Correia, Bruno Quaresma, Fernando Andre, Paulo Sousa [5] describes, the increasing popularity of cloud storage services has lead companies that handle critical data to think about using these services for their storage needs. However, the reliability and security of data stored in the cloud still remain major concerns. In this work, DepSky model is studied, a system that improves the availability, integrity, and confidentiality of information stored in the cloud through the encryption, encoding, and replication of the data on diverse clouds that form a cloud-of-clouds. Moreover, the monetary costs of using DepSky in this scenario is at most twice the cost of using a single cloud, which is optimal and seems to be a reasonable cost, given the benefits.

2.3 Survey on need for multi-cloud

S.Subashini, V.Kavitha [6] says, Cloud computing usage has increased rapidly in many companies. Cloud computing offers many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing plays a major role in the cloud computing, as customers often store important information with cloud storage providers but these providers may be unsafe. Dealing with single cloud providers is predicted to become less popular with customers due to risks of service availability.
failure and the possibility of malicious insiders in the single cloud. A movement towards “multiclouds”, or in other words, “inter-clouds” or “cloud-of-clouds” has increased recently. The purpose of authors is to survey recent research related to single and multi-clouds security and to address possible solutions. It is found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. Their work aspires to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing consumer.

3. System Design

This paper deals with the storage of data in more than one cloud hence multi-clouds are used. Cluster of cloud storage is created and maintained accordingly to satisfy the user specific data access requirements. Here the replication of the user data to multiple clouds is done and update that information timely. Therefore loss of data from single cloud does not create a permanent loss of information. The data access mechanism is implemented using Shamir’s Secret Sharing algorithm which generates the secret keys to authenticate the user. As the priority is given to the user data, it is also important to make available this data to a right person. Therefore, the secret keys are shared to the user via his or her mail id which is taken while registering a new user. It plays a role of double authentication to identify the unique person. Here, to access a file from cloud storage, user must provide the same set of secret keys with any threshold value. Also to provide more security to user data, Advanced Encryption Standard (AES) algorithm is used to encrypt the user data.

3.1.1 Interaction using trusted third party

The subsequent step is related with the interaction between two parties of multiple clouds using trusted third party (TTP). The main concern is to maintain data integrity while data is accessed from multiple clouds. TTP is formed so that the data exchanged from one cloud to the other must be secure and should not leak the information while moving the data.

3.1.2 Implementing cryptographic algorithm

The third party module has been linked up with the other clouds that have been created and thus perform the activity of maintaining security with the help of ECC cryptography algorithm. This prevents unauthorized user access. Encryption Let ‘m’ be message to be sent. Consider ‘m’ has point M on the curve. P is a point on curve. Randomly select a value k from [1 - (n-1)]. Two cipher texts are generated let it be B1 and B2. B1 = k * P  
B2 = M + (k * P)  
Decryption Use the following equation to obtain original message that was sent i.e m. 
M = B2 – d * B 
M is original data that was sent and d is random number in the range of (1 to n-1).

4. Conclusion

There are some combined benefits of multi-clouds and secret sharing scheme, such as, infrastructure deployment, data accessibility, user authentication etc. Multi-cloud is looking to be more secure, harder to compromise over single cloud data storage. Cloud computing is currently the latest trend when it comes to online computing, it may help the enterprise and the end user by providing their needs, but the provider has to make sure that they are valuable and customer data is safe.

5. References

Scientific and Research Publications, Volume 3, Issue 4, April 2013
