International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 03 | Mar-2016 www.irjet.net p-ISSN: 2395-0072

MULTICLOUD DATA SECURITY

Arun Singh[1], Darshan Jain[2], Paresh Chavan[3], Sweta Jain[4]

[1]*Student, IT, Rajiv Gandhi institute Of Technology, Maharashtra, India*
[2]*Student, IT, Rajiv Gandhi institute Of Technology, Maharashtra, India*
[3]*Student, IT, Rajiv Gandhi institute Of Technology, Maharashtra, India*
[4]*Professor, IT, Rajiv Gandhi institute Of Technology, Maharashtra, India*

Abstract - *Cloud Computing (CC) is a concept that has increased rapidly in many organizations and IT industry. It is a model for allowing ubiquitous, on demand access to a shared pool of configurable computing resources. Cloud computing and its solutions provide users and initiatives with various capabilities to store and process their data in third-party centers. This paper proposes a prototypical to securely store information or data into the cloud, by replicating and storing the data on multiple clouds providers in a fashion that preserves data confidentiality, integrity and ensures availability. Our approach preserves safety and privacy of user's sensitive information by replicating data across multiple clouds, by using a secret sharing approach that uses Shamir's secret sharing algorithm. This model avoids the negative properties of a single cloud and decreases the concerns of encryption techniques. For example sensitive material with cloud storage providers may be trusted. But, single cloud providers is a less popular with customers due to intimidation service availability failure and possibly of malicious contents in the 'single cloud'. A movement towards 'multi-clouds' has emerged formerly using Shamir's Secret Sharing Algorithm.*

Key Words: Multicloud, Secret Sharing, Security, Computing, Data Integrity.

1. INTRODUCTION

Adopting cloud computing can benefit organizations and industries to conduct their core business activities more effectively since the management and monitoring task for data cores is reduced. Businesses can too save on power costs as the resources needed are minimized. One may consider if cloud computing is such a great thing then why most of the businesses are not going for it and as per the research the reason is deprived security. The third party is tangled called CSP (Cloud Service Provider) to whom businesses have to provide their files with delicate data. This paper survey's recent research associated to security of single and multi-cloud comes up with possible solutions for conservation of security. However, multi-cloud computing is relatively new concept, biggest security aspects in cloud computing basically are data intrusion, data integrity and service availability are handled in much better way in multi-cloud than single cloud computing .This project work encourages the use of multi-cloud architecture. By organizing IT infrastructure and services over the network, an organization can acquire these resources on as-needed base and avoid the capital costs of software and hardware.

Fundamental Characteristics of Cloud Computing

1. Broad Network Access: cloud amenities can possibly gain access to over the network through the usage of standardized mechanism that hold up different users, like mobile phones, tablets, mainframes and work stations.

2. Self-service on Necessity: The user probably will make a judgment on the use of computing amenities such as server time and network storage, based on of their current needs, with no more communication with dissimilar service providers in cloud.

3. Combining of Computing Resources: In addition to classical virtualization, cloud computing uses in adding the capabilities of mechanization of services and multi-tenancy of users at shared information resources. Common use of the same technical resources is the vital feature of cloud computing.

4. High Elasticity: The client may simply rise or fall the capacities afforded using the current requirements. The capacities are limitless for the user.

2. LITERATURE SURVEY

Rahul Bhatnagar et al. (2013) in Security in Cloud Computing [5] have proposed an analysis of technical component and certain research in intimidations for cloud computing Users and threats for cloud service provider then to provide several security topics associated in cloud security and standardization (i.e. Storage Security, Data, information and Privacy Protection, Virtualization Security, Security Model and Framework, Security Management and Audit Technology).

Odunayo O. Owopetu (2013) in a research thesis Private Cloud Implementation and Security [4] have provided the easiest way to developed a private cloud for an enterprise using eucalyptus and possible ways of Effectively securing it. Thesis report is divided two part: In rest part basic

Information about cloud, cloud deployment model and cloud architecture. In second part describe the implementing private cloud using the Eucalyptus.

Santana sharia et al. (2012) in Security in Cloud Computing [7] have described the brainy details of cloud computing and type of services and security matters and certain challenges for data security in cloud environment and inspect several approaches for security in cloud computing and anally provide a dependable security in cloud computing for future work.

Jen-Shang Wang et al. (2011) in How to Manage Information Security in Cloud Computing [2] have described the key success factor whose determine the management information security and evaluating the hierarchical structure for key success factor. Based on these (external dimension, internal dimension, technology dimension and execution dimension) have analysis and categorization using fuzzy analytic hierarchy process.

Mohammed A. Alzain et al. (2011) in MCDB: using Multi-Clouds to ensure security in Cloud Computing [6] have proposed a mufti clouds database model and present the architecture of mufti cloud database model and describe the layers and components.

Shivashankar Ravi (2011) in a research thesis Security Approaches for Protecting Facts in Cloud Computing [8] have described the security threats and identify the safety methods for security in cloud computing and measured the protection challenge and security approaches of cloud computing and lastly identified from research methods quite a rare challenges and procedures used now study in future research work in Cloud Computing.

Uma Somani et al. (2010) in implementing the Digital Signature with RSA Encryption Algorithm to Boost the Data Security of Cloud in Cloud Computing [10] have described the cloud storage methodology and proposed algorithm and Implementing the RSA algorithm through Digital Signature and proposed the gradually process consumed in Digital Signature with RSA algorithm. If these implementing algorithms are combined in other encryption techniques (i.e. DES, AES etc.) then it's became robust and secure in cloud computing.

3. MOVING FROM SINGLE TO MULTI-CLOUDS

In this section we are going to inspect the relocation of cloud computing from the single to multi-cloud perspective. After all, we need to know what Multicloud is. Clearly, it is a more complex system than a hybrid cloud, which is usually a combination private and public cloud. The term "multi-clouds" was first time mentioned by Vukolic et al. in [1] and assume that the main purpose of shifting towards inter-clouds is to improve whatever was offered in single cloud by distributing the reliability, trust and the security among multiple cloud providers. Multi-cloud add more clouds to the mix (i.e. possibly two or more public IaaS providers, a private PaaS, private use-based accounting, etc.) which aims at reducing the risk of service availability failure, exploitation of data, loss of privacy, and the possibility of malicious insiders in the single cloud.

Shifting from single clouds to multi-clouds is to ensure the privacy and security of users' sensitive information is extremely important. Cachin et al. [3] claim that services of single clouds are still focus to outage. Moreover, K. Bowers et al. [9] showed that above 80% of enterprise management fear security threats and loss of control of data and schemes. To this end, they advise that cloud computing must not end with a single cloud provider, but rather users should focus on developing applications using the power of multi-clouds.

4. SECURITY USING SHAMIR SECRET SHARING

In cryptography, a secret sharing scheme is a method for distributing a secret amongst a set of participants, each of which is allocated a share of the secret. The secret can be recreated when the shares are united together, individual shares are of no use on their own. More formally, in secret sharing scheme there is only one dealer and n player. The dealer a secret to the players, but only when specific condition are fulfilled. The dealer achieves this by providing each player a share in such a way that any group of t(for threshold) or other troupes can together reconstruct the secret but no group of less than t players can. Such a system is called (t, n)-threshold scheme. This secret sharing algorithm was published by Adi Shamir in 1979 in [1]. It is a (k, n) threshold sharing scheme and is based on the Lagrange polynomial interpolation. Shamir's secret sharing consists of two part which are described in the following Dealing Algorithm in the beginning, the parameters k and n for the (k, n)-threshold and the global secret s ∈ Z q have to be defined. The value q has to be a prime, because only in prime residue class rings it is ensured, that every element has a defined multiplicative inverse element which is necessary for computation.

The first step is to choose k − 1 coefficients a1... ak−1 and set a0:= s. Then, a polynomial f(x) is built with f(x) = a0 + a1x + a2x + ak−1xk−1.
To create the shares, a variable i is set to i = 1,...,n and points with si = (if(i)) mod q of the polynomial f(x) are computed. In the end, every party gets at least one point si as a secret share, whereas the first part i of the share can be public and the next part f (i) has to be kept in private. The following shows an example of creating shared secrets.

(3, 5)-threshold, q = 11, s = a0 = 6

Choose random k − 1 coefficients and build polynomial
f(x) = a2x2 + a1x + a0:
a1 = 1, a2 = 3
f(x) = 3x2 + x + 6

Calculating shared secrets si = (if (i)) mod q with i ∈ {1,...,n}:

s1 = (1, 10), s2 = (2, 9), s3 = (3, 3), s4 = (4, 3), s5 = (5, 9)

This dealing phase is usually performed by a trusted dealer who has to forget all information about the creation especially the global secret s and the shares si to guarantee a real shared secret without a single point of attack.
Recomputation
To obtain the global secret s from the shared ones, k points si = (xi,yi) are needed. The aim in the phase is to identify the polynomial f(x) = a0+a1x+a2x+ak−1xk−1 with f(0) = a0 = s which was created during the dealing phase. This can be done by using the Lagrange interpolation with f(x) = L(x) for the k points. Due to the fact that only the value f(0) has to be computed the Lagrange basis polynomials (3) can be simplified by setting x = 0 and S ⊆ {1,...,n}kSk = k with S as the subset of parties which participate in the recomputation.

$$\ell_{j,0,S} := \prod_{\substack{m \in S \\ m \neq j}} \frac{-x_m}{x_j - x_m} \mod q \quad (4)$$

In the end, the global secret can be computed with the Lagrange formula (2) using the basis polynomials from (4)

$$s = L(0) = {}^{x}y_j `_{j,0,S} \mod q \quad (5)$$
$$j \in S$$

Due to the uniqueness of the Lagrange interpolation to obtain a polynomial with degree k−1 from k points it does not matter which parties are involved in the recomputation step, as long as there are exactly k shares.

The following listing shows an example how the global secret can be recomputed using the Lagrange interpolation.

$$\ell_{1,0,\{1,2,3\}} = \frac{-x_2}{x_1 - x_2} \cdot \frac{-x_3}{x_1 - x_3} = \frac{-2}{1-2} \cdot \frac{-3}{1-3} = 6 \cdot 2^{-1} = 6 \cdot 6 = 3 \mod 11$$
$$\ell_{2,0,\{1,2,3\}} = \frac{-x_1}{x_2 - x_1} \cdot \frac{-x_3}{x_2 - x_3} = \frac{-1}{2-1} \cdot \frac{-3}{2-3} = 3 \cdot (-1)^{-1} = 3 \cdot 10 = 8 \mod 11$$
$$\ell_{3,0,\{1,2,3\}} = \frac{-x_1}{x_3 - x_1} \cdot \frac{-x_2}{x_3 - x_2} = \frac{-1}{3-1} \cdot \frac{-2}{3-2} = 2 \cdot 2^{-1} = 2 \cdot 6 = 1 \mod 11$$

s	=	L(0) = y1 · `1,0,{1,2,3} + y2 · `2,0,{1,2,3} + y3 · `3,0,{1,2,3} mod q		
s	=	10 · 3 + 9 · 8 + 3 · 1 mod 11		
s	=	6		

Again, after the recomputation which should be performed by the trusted dealer, he has to forget everything to maintain the security of this mechanism.

5. CONCLUSION AND FUTURE SCOPE

It is clear that although the use of cloud computing has swiftly increased, cloud computing security is still considered the main concern in the cloud computing atmosphere. Customers do not want to lose their secretive information as an outcome of malicious present in the cloud. In addition, the loss of service accessibility has caused many problems for a huge number of customers recently. Furthermore, data intrusion leads too many problems for the users of cloud. The purpose of this effort is to survey the recent research on single clouds and multiple clouds to address the safety risks and solutions.
We have found that much research has been done ensure the security of the single cloud and cloud storage whereas Multicloud have received less attention in the zone of security. We support the moving to multi- clouds due to its ability to reduce security risks that affect the cloud computing user.

REFERENCES

[1] M. Vukolic, The Byzantine empire in the intercloud, ACM SIGACT News, pp. 105–111, New York, September 2010.

[2] Jen-Sheng Wang, Che-Hung Liu, Grace TR Lin, How to Manage Information Security in Cloud Computing, 978-1-4577-0653-0/11, IEEE, 2011.C. Cachin, I. Keidar and A. Shraer, Trusting the cloud, ACM SIGACT News, pp. 81–86, 2009.

[3] Sanjana Sharma, Sonika Sonit, Swati Senger, Security in Cloud Computing, National Conference on Security Concerns in Network Technologies, 2011.

[4] Odunayo O. Owopetu, Private Cloud Implementation and Security, Bachelor Thesis (UAS) , School of Computing Blekinge Institute of Technology SE - 371 79 Degree Program in Information Technology, Internet Technology, 2013.

[5] Ramgovind S, Eloff MM, Smith E, The Managing of Security in Cloud Computing, 978-1-4244-5495-2/10, IEEE, 2010.

[6] Mohammed A. AlZian, Eric Pardede and Ben Soh, MCDB: Using Multi-Clouds to Warrant Security in Cloud Computing, 976-0-7695-4612-4/11, IEEE, 2011.

[7] Sanjana Sharma, Swati Sengar, Sonika Soni, , Security in Cloud Computing, National Conference on Security Issues in Network Technologies, 2012.

[8] Venkata Sravan Kumar, Maddineni Shivashanker Ragi, Security Techniques for Guarding Data in Cloud Computing, Master Thesis Electrical Engineering, School of Computing Blekinge Institute of Technology SE - 371 79 Karlskroa Sweden, November 2011.

[9] K. D. Bowers, A. Juels and A. Opera, HAIL: A high-availability integrity layer for cloud storage, ACM, pp. 187–198, 2009.

[10] http://point-at-infinity.org/ssss/ Shamir's secret sharing scheme.