iJRASET
International Journal For Research in
Applied Science and Engineering Technology

Volume: 3 Issue: III Month of publication: March 2015

DOI:

Volume 3 Issue III, March 2015
ISSN: 2321-9653

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Survey of Cloud Security Techniques

Chirag Padsala[1], Rohit Palav[2], Paras Shah[3], Sachin Sonawane[4]
[1,2,3,4] *Computer Engineering, Atharva College of Engineering, University of Mumbai, India*

Abstract— Cloud storage is use to reduce the cost of storage in I.T fields and other benefits such as data accessibility through internet. Ensuring the security of cloud server is important so store sensitive data for example confidential data. In single cloud there is risk of data availability and security. If cloud server is attack but malicious content then there might be loss of data and its availability. So multiple cloud or cloud-of-clouds emerged to secure the data and increase its availability using Shamir's secret sharing algorithm. We reviewed many paper and research related on single and multi clouds security using Shamir's secret sharing key algorithm. The main motto of our project and paper is multi clouds, data security and reduce attackers and successful implementation of Shamir's secret sharing algorithm. It is a form of secret sharing, where a secret is divided into parts, which is giving each participant its own unique part, where some of the parts or all of them are required in order to reconstruct the secret key *[1]-[3].*

Keywords— Data accessibility, Data availability, Data security, Multi cloud, Secret sharing algorithm.

I. INTRODUCTION

Cloud computing allows us to store data remotely on a storage system known as cloud server. We can access the data on any device any time i.e. data is available 24x7. The cloud computing is an economical, service availability, adaptable and on demand service delivery platform for providing business through the internet. Cloud computing resources are be effectively utilizes and can be scaled irrespective to their physical boundaries and user's location. Hence, the opportunity for an organization to enhance their service deliverance efficiencies is achieved through cloud computing [6]-[7]. Cloud computing security is tedious issue in cloud system. Cloud server needs to get protected from malicious content and unauthorized user. For that cloud provider should address privacy and security on top priority. In single cloud system there is one cloud to storage our data. Disadvantage of single cloud is service availability failure for some time and malicious insider's attacks in the single cloud. Therefore single cloud is less popular. Due to which single cloud is moved towards "multi cloud", "cloud of clouds" and "inter-clouds". So our aim is to share data securely to the third party without any hacks. Every cloud users want to avoid un-trusted cloud provider for personal and important documents such as debit/credit cards details or medical report from hackers or malicious insiders is the importance. For security risk we are using Shamir's secret sharing algorithm to reduce the risk of data intrusion and loss of availability of data [1]-[5].

II. OBJECTIVE

The main objective of this paper is to secure cloud system. Other objective are as follows:

A. Data integrity.

B. Service availability.

C. Ensuring security.

D. Understanding the user requirement.

E. The user runs customer applications using the service provider's resources [1]-[2].

III. RELATED WORK

A. CipherText

Cipher-text is encryption of plaintext. Cloud computing is not trusted so it is necessary to maintain the confidentiality of data. In cipher-text policy the data is change in cipher form and been decrypted by the receiver to gain its originality. Here the user of the cloud encrypt the data before storing it in the cloud but its traditional version to secure the data in cloud and can be crack down or been steal. So we need more secure policy to maintain data on cloud [8].

B. Ciphertext Policy-Attribute Based Encryption

To overcome disadvantage of cipher policy, CipherText Policy-Attribute-based Encryption (CP-ABE) is a promising technique for access control of encrypted data, it requires trusted authority to manage attributes and distributed keys in the system. In this multi cloud system, users come from various domain with is manage by different authority. But existing CP-ABE cannot be used directly for data access control of multi authority cloud system, due to inefficiency of decryption and revocation [9].

C. Data Access Control for Multi-Authority Cloud Storage

This technique is use to overcome disadvantage of CP-ABE. Here data access is controlled by multiple authorities

DAC-MACS (Data Access Control for Multi-Authority Cloud Storage) is an effective and secure data access control scheme with efficient decryption and revocation. Data access control is a legitimate way of ensuring the security of data.

However, due to data exploitation and mistrustful cloud servers, the data access control becomes a taxing issue in cloud storage systems. Existing data access control schemes are no longer appropriate to cloud storage systems, because either they induce multiple encrypted copies of authentic data or fully trusted cloud server is necessary [7].

D. Shamir's approach

Data store in cloud are compressed or some time lost. To secure them before losing its originality, data needs to be encrypted before storing them into the cloud. Some time data are lost by cloud provider itself to avoid this we need more than one cloud to store same data. The same data needs to be encrypted before sending it off the cloud and needs to provide the proper authentication. Shamir's secret sharing is an algorithm in cryptography. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret [4].

1) Mathematical equation: Our goal is to divide some data D (e.g., the safe combination) into pieces D1, D2…,Dn in such a way that:

The Knowledge of any k or more Di pieces makes D easily computable.

The Knowledge of any k-1 or fewer Di pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).

This scheme is called (k,n) threshold scheme. If k=n then all participants are required to reconstruct the secret original data.

The essential idea of Adi Shamir's threshold scheme is that 2 points are sufficient to define a line, 3 points are sufficient to define a parabola, 4 points to define a cubic curve and so forth. That is, it takes points to define a polynomial of degree.

Suppose we want to use a threshold scheme to share our secret, without loss of generality assumed to be an element in a finite field.

Choose at random coefficients in , and let . Build the polynomial . Let us construct any points out of it, for instance set to retrieve . Every participant is given a point (a pair of input to the polynomial and output). Given any subset of these pairs, we can find the coefficients of the polynomial using interpolation and the secret is the constant term [4].

Shamir's secret sharing is an algorithm in cryptography. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.

2) Example: The following example illustrates the basic idea. Note, however, that calculations in the example are done using integer arithmetic rather than using finite field arithmetic. Therefore the example below does not provide perfect secrecy and is not a true example of Shamir's scheme.

Suppose that our secret is 1234$(S = 1234)$.

We wish to divide the secret into 6 parts$(n = 6)$, where any subset of 3 parts $(k = 3)$is sufficient to reconstruct the secret. At random we obtain two ($k - 1$) numbers: 166 and 94.

$$(a_1 = 166; a_2 = 94)$$

Our polynomial to produce secret shares (points) is therefore:

$$f(x) = 1234 + 166x + 94x^2$$

We construct 6 points $D_{x-1} = (x, f(x))$ from the polynomial:

$$D_0 = (1,1494); D_1 = (2,1942); D_2 = (3,2578); D_3 = (4,3402); D_4 = (5,4414); D_5 = (6,5614)$$

We give each participant a different single point (both x and $f(x)$). Because we use D_{x-1} instead of D_x the points start from $(1, f(1))$ and not $(0, f(0))$. This is necessary because if one would have $(0, f(0))$ he would also know the secret ($S = f(0)$)

3) Reconstruction: In order to reconstruct the secret any 3 points will be enough.

Let us consider,

$$(x_0, y_0) - (2,1942); (x_1, y_1) - (4,3402); (x_2, y_2) - (5,4414)$$.

We will compute Lagrange basis polynomials:

$$\ell_0 = \frac{x-x_1}{x_0-x_1} \cdot \frac{x-x_2}{x_0-x_2} = \frac{x-4}{2-4} \cdot \frac{x-5}{2-5} = \frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}$$

$$\ell_1 = \frac{x-x_0}{x_1-x_0} \cdot \frac{x-x_2}{x_1-x_2} = \frac{x-2}{4-2} \cdot \frac{x-5}{4-5} = -\frac{1}{2}x^2 + \frac{7}{2}x - 5$$

$$\ell_2 = \frac{x-x_0}{x_2-x_0} \cdot \frac{x-x_1}{x_2-x_1} = \frac{x-2}{5-2} \cdot \frac{x-4}{5-4} = \frac{1}{3}x^2 - 2x + \frac{8}{3}$$

Therefore,

$$f(x) = \sum_{j=0}^{2} y_j \cdot \ell_j(x)$$

$$= 1234 + 166x + 94x^2$$[1]

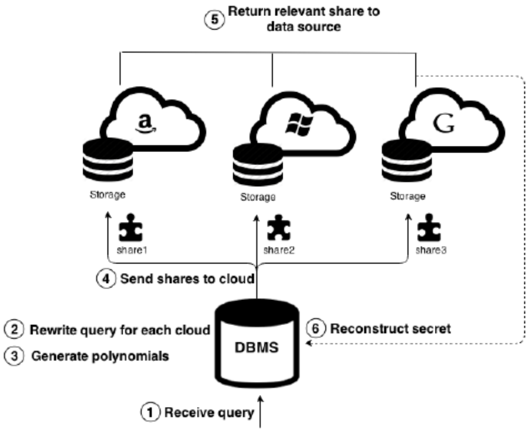

Fig. 1. System architecture of multi cloud system

IV. CONCLUSION

In this paper a brief introduction to cloud computing with enhancement of multiple authorities and multiple clouds (mirrored storage) is given. This allows us to store the data securely and access it whenever needed. Replicated storage allows to access data even when one server fails. Shamir’s secret sharing algorithm is used; this enhances the security by using key mechanism.

V. ACKNOWLEDGMENT

I would like to thank Prof. Sachin Sonawane for helping me in this work and also all the other people who have encouraged me for this research.

REFERENCES

[1] Md Kausar Alam, Sharmila Banu K “An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds”

[2] Monali Shrawankar, Ashish Kr. Shrivastava “Cloud Computing Security: From Single to Multi-Clouds,2012 ,45th Hawaii International Conference on System Sciences.”

[3] Review of methods for secret sharing in cloud Computing- “International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)”, Volume 2, Issue 1, January 2013

[4] Shamir, Adi (1979), "How to share a secret",Communications of the ACM 22 (11): 612–613

[5] Dawson, E.; Donovan, D. (1994), "The breadth of Shamir's secret-sharing scheme", Computers & Security 13: 69–78

[6] Hassan Takabi, James B.D., Joshi, Gail-Joon, Ahn,“Security and Privacy Challenges in Cloud Computing Environments”, University of Pittsberg, October 2010

[7] Kan Yang, Associate Member, IEEE, Xiaohua Jia, Fellow, IEEE, Kui Ren, Senior Member, IEEE, Bo Zhang, Member, IEEE, and Ruitao Xie, Student Member, IEEE. “DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems.”

[8] D.boneh, R.canetti, S.halevi, J. Katz “Ciphertext security from identity-based encryption”

[9] Bethencourt, J., Sahai A. and Waters, B. 2007. “Cipher-text Policy Attribute-Based Encryption”