IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 6, Ver. III (Nov. - Dec. 2016), PP 34-37
www.iosrjournals.org

Enhance Security in Multi-Clouds by Using Secret Sharing Algorithm

M. Tulasi Rama, A. Madhuri
(CSE, PVPSIT/ JNTUK, India)
(CSE, PVPSIT/ JNTUK, India)

Abstract: *Cloud computing is convenient and on-demand computing. Cloud computing provides Storing, retrieving and processing of resources and data in a cloud environment. Cloud computing provides several service models and deployment models. These features will help provide outsourcing the data with third party storage service providers. The storage provider must assure that the data stored by the user is secure. Data encryptions, hemimorphic encryption, secret sharing algorithms are the techniques extensively used as securing data outsourcing. Single cloud computing provides fast access to their applications and services. But due to some reason, that single cloud suffers from many security issues, users and customers are opting "multi-cloud" is also called inter-clouds" and "cloud of clouds". These multi-clouds are secured by using various techniques and algorithms. This paper applies secret sharing algorithm to secure data outsourcing.*

***Keywords**: Cloud computing, Data Encryption, Hemimorphic Encryption, Secret Sharing Algorithm, Single cloud, Cloud of Clouds, Inter-Clouds, Multi-Cloud, Techniques.*

I. Introduction

By using cloud computing accessing the applications and their utilities through the Internet. By using Cloud Computing create and configure, customize the applications in online. Cloud computing is a help to many organizations to maintain their business activates and improve their performing of the applications. Cloud computing is effectively and economically managing the activates of organizations. As per NIST cloud computing is convenient and on-demand computing the shared pool of computing resources like servers, storage, networks and applications. The third party is cloud Service Provider this improves security mechanisms in the cloud; this provides security to the sensitive data of the user or Organizations.

1.1 Cloud Computing Overview

These are Deployment and service models are working in cloud computing to feasible and accessible for end users.

1.1.1 Deployment Models

Deployment Models are explained which type of cloud will be accessed, i.e., how the cloud is located? Cloud is four types: Public, Private, Hybrid, and Community.

The resources of **public cloud** can be easily accessed by the public. Security of Public cloud very less compared to another type of clouds. Examples of public cloud are Google, Amazon, Microsoft, and Sales force.The resources of **private cloud** are used by within an organization because an organization gets the permissions to access resource for their private use. Private cloud is much secured The **community cloud** is almost same as private cloud. The resources of private cloud accessed one organization but community cloud resources are accessed by a group of the organization.The combination of public and private clouds is **Hybrid cloud**, in which private cloud performs the critical activities and public cloud performs the non-critical activities.

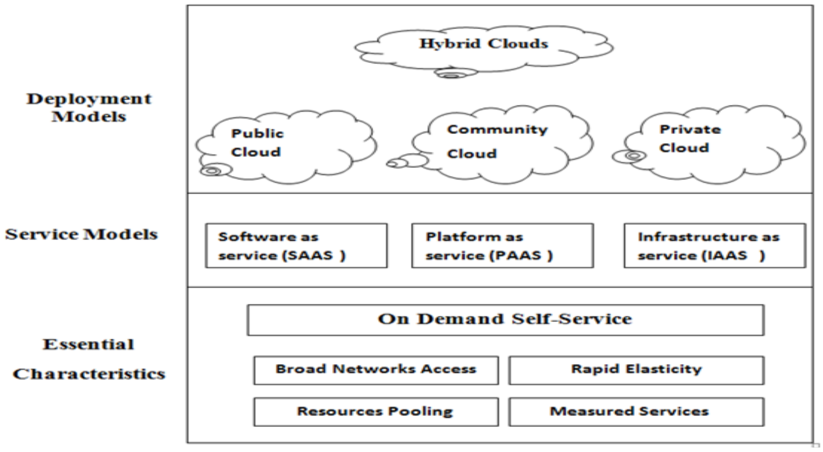

Fig1. Basic diagram of cloud computing

1.1.2 Service Models

Service models are basic models of Cloud computing. These are -

- In IaaS the user access the fundamental resources thus are physical, virtual machines, etc.
- Runtime environment is provided by PaaS for applications, development and deployment tools, etc.
- The end user accesses the software applications by SaaS model.

1.2 Single cloud Strategy

Cloud computing is another way of maintaining its infrastructure, applications of the organization. Users can interact with data over the Internet by delegating administrative tasks of maintenance to Cloud computing providers.

1.2.1 Security Issues in Single Cloud

Data Integrity: Data integrity is major security thread in cloud security. Data integrity means stored data may corrupt or loss during transition operation. Ex of data integrity is given bellow
In January 2009, servers Magnolia have loss of total data due to a failure; the loss of half a terabyte of it does not possible to recover the data, making the site dead

Data Intrusion: Another cloud security risk is data intrusion. If anyone accesses the password of any accounts, then they will be accessing the account's instances and resources, by using the stolen password the hacker to erase all the information user accounts and modify the data or even disable its services.
Service Availability: Another major issue in cloud computing is service availability. If we entrusted our data to store in a single cloud and it does not survey a backup solution or it store the data in a single platform or in a same geographical area they may increase the risk at downtime, and it impacts on customers. Ex is Amazon. Amazon underlines in its contract that a service may be cut down at any moment.

1.3 Multi-cloud Strategy

Multi-cloud means is the combination of two or more clouds. Multi-cloud overcomes the security risks in a single cloud. In Multi-cloud reduce the service unavailability, loss, and damage of data, loss of privacy. The service unavailability is occurred when hardware breakdown of software or system infrastructure. A multi-cloud strategy can also improve overall performance by reducing "vendor lock-in". The cost of using multiple clouds will be higher than compared to single clouds. A high-level design of clouds-of-cloud is presented.

1.3.1 Depsky system:

DepSky is better architecture design to overcome all the security risks of multi-clouds by eliminating the requirement of code execution in the storage clouds (servers). It is still effective as it requires only two communication round-trips for every operation. Also, it deals with data confidentiality and avoids the high amount of data stored in each cloud. Depsky uses an efficient set of Byzantine quorum protocols, cryptography, Shamir secret sharing, erasure codes and the diversity that comes from using several clouds. Several areas of cloud computing that will benefit by using this DepSky are discussed.

1.3.2 DepSky Architecture:

The DepSky model three parts: readers, writers, and four cloud storage providers, where readers and writers are the client‘s tasks. Arbitrarily fail the Readers example is for suppose readers fail by crashing, they can display any behaviour whereas, writers only fail by crashing As fig.2 shows it is a DepSky architecture which contains the combination of different storage cloud.

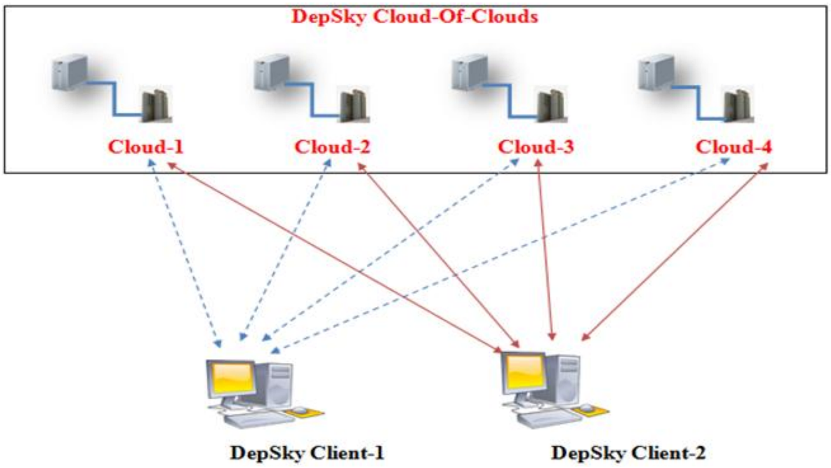

Fig2: Depsky Architecture

II. Secret Sharing Algorithm

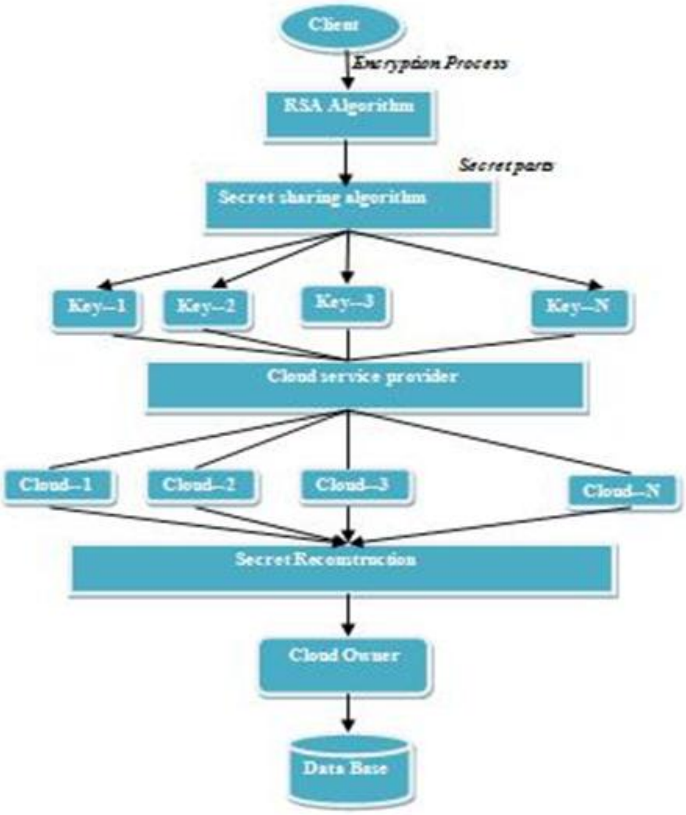

Fig3. Secret sharing algorithm work Flow

Fig3 represents the work flow diagram of this project. This secrete sharing algorithm aims to provide a better way to secure cloud database and assure the cloud computing community with a highly effective security measure. By using this algorithm to reduce the risk of data intrusion and service availability in the cloud.

2.1 Mathematical Definition:

The aim of this algorithm is to divide the data DATA into N pieces (DATA1, DATA2, DATA3, DATA4 …..DATA) so that,

1. Retrieving any k or more DATAq pieces makes DATA easily computable.
2. Retrieving any k-1 or fewer DATAq pieces leaves DATA thoroughly undetermined.

The above scheme is known as a threshold (k, N). if k=N, then all pieces are available for reconstruction of DATA.

2.2 Shamir's Approach

The secret is divided into pieces by considering an approximate degree polynomial

H (p)=a0+a1p1+a2p2+…………+ak-1pk-1

In which a0 = S, S1 = H (1), S2 = H (2), ………… , SN = H (N) and represent each share as a point

2.3 Example

Given example illustrates the algorithm. For understanding, integer arithmetic is used instead of any other vector or scientifically based arithmetic. Therefore the example provided does not ensure perfect secrecy and is not a perfect example of secret sharing scheme.

2.4 Encryption and Preparation

Consider 1999 as the secret data. Dividing it into 6 parts (N = 6). Parts required to reconstruct the secret is 3 parts (k = 3).

2 numbers are selected in random. Let it be 154 and 19. a1 = 154 and a2 = 19.

Our polynomials to produce shares are:

H(p) = 1999 + 154p + 19p2

6 parts are constructed from the polynomial.

(1, 2172) ; (2, 2383) ; (3, 2632) ; (4, 2919) ; (5, 3244) ; (6, 3607)

Different single point is given to each participant, both p and H(p).

2.5 Reconstruction

Any 3 points are enough to reconstruct the secret.
Assume: (r0, s0) : (2, 2383) ; (r1, s1): (4, 2919) ; (r2, s2) : (5, 3244)
Apply Lagrange basis polynomials:
I0 = r -r1/r0-r1 . r -r2/r0-r2 = 1/6r2- 3/2r +10/3
I1 = r -r0/r1-r0 . r -r2/r1-r2 = 1/2r2- 7/2r -5
I2 = r -r0/r2-r0 . r -r1/r2-r1 = 1/3r2- 2r +8/3
Therefore,
H(p) = j=2sj.Ij(p)
H(p) = 2383 (1/6p2 - 3/2p +10/3) + 2919 (1/2p2 + 7/2p – 5) + 3244 (1/3p2 – 2p +8/3)
H(p) = 1999 + 154p + 19p2

III. Solution Methodology

Cloud customers may expect on behalf of their past experience and requirements. But the best approach is to gather information about the best and efficient cloud service provider. Customers are also prescribed to ensure the level of security of these important characteristics of the cloud: Confidentiality, Integrity, and Availability (CIA). Security in Cloud computing is organized into different sections: security categories, security in service delivery models and security dimensions.

Security in cloud services is dependent on the following:

- Strong network security should be applied to the service delivery platform.
- Data Encryption.
- Authorization is given every Access.

IV. Conclusion

Now a day's Cloud computing usage is rapidly increases. Security is main issue in Cloud computing environment. Customers want privacy to their private information in the cloud. Many security mechanisms use in cloud environment for secure the users data, but the loss of service availability, data integrity, data intrusion has caused many problems to the large number of customers.This paper survey on single clouds and multi-clouds using secret sharing algorithm and to address the security risks and solutions by Shamir's Secret Sharing algorithm. These algorithms generate their own secret sharing humanisms and use secure keys to distribute shares among themselves. The Shamir's secret sharing scheme provide best abstract foundation and excellent framework to users application

References

[1]. (NIST), http://www.nist.gov/itl/cloud/.

[2]. I. Abraham, G. Chockler, I. Keidar and D. Malkhi, "Byzantine disk paxos: optimal resilience with Byzantine shared memory", Distributed Computing, 18(5), 2006, pp. 387-408.

[3]. H. Abu-Libdeh, L. Princehouse, and H. Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium on Cloud computing, 2010, pp. 229-240.

[4]. D. Agrawal, A. El Abbadi, F. Emekci and A. Metwally, "Database Management as a Service: Challenges and Opportunities", ICDE'09:Proc.25thIntl. Conf. on Data Engineering, 2009, pp. 1709-1716.

[5]. M.A. AlZain and E. Pardede, "Using Multi Shares for Ensuring Privacy in Database-as-a-Service", 44th Hawaii Intl. Conf. on System Sciences (HICSS), 2011, pp. 1-9.

[6]. Amazon, Amazon Web Services. Web services licensing agreement, October3,2006.

[7]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores", Proc. 14th ACM Conf. on Computer and communications security, 2007, pp. 598-609.

[8]. A. Bassani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc. 6thConf. on Computer systems, 2011, pp. 31-46.

[9]. K. Birman, G. Chockler and R. van Renesse,"Toward a cloud computing research agenda", SIGACT News, 40, 2009, pp. 68-80.

[10]. K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage", CCS'09: Proc. 16th ACM Conf. on Computer and communications security, 2009, pp. 187-198.

[11]. C. Cachin, R. Haas, and M. Vukolic, "Dependable storage in the Intercloud", Research Report RZ, 3783, 2010.

[12]. C. Cachin, I. Keidar and A. Shearer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.

[13]. C. Cachin and S. Tessaro, "Optimal resilience for erasure-coded Byzantine distributed storage", DISC:Proc. 19thIntl.Conf. on Distributed Computing, 2005, pp. 497-498.

[14]. M. Castro and B. Liskov, "Practical Byzantine fault tolerance", Operating Systems Review, 33, 1998, pp. 173-186.

[15]. G. Chockler, R. Guerraoui, I. Keidar and M. Vukolic, "Reliable distributed storage", Computer, 42, 2009, pp. 60-67.

[16]. Clavister, "Security in the cloud", Clavister White Paper, 2008.

BOOKS

[17]. 'Software Engineering',Roger.S.Pressman Mc.Graw Hill

[18]. 'The Unified Modeling Language User Guide', Grady Booch, James Rumbaugh, Ivar Jacobson.

[19]. 'Sotware Project Management'.Walker Royce.

WEBSITES

[20]. http://java.sun.com.

[21]. http://www.sourcefordgde.com.

[22]. http://www.networkcomputing.com/

[23]. http://www.roseindia.com/