An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds

Md Kausar Alam, Sharmila Banu K

School of Computing Science and Engineering, VIT University, Vellore, Tamil Nadu, India.

Abstract- Now a day's rapidly increased use of cloud computing in the many organization and IT industries and provides new software with low cost [1]. So the cloud computing give us lot of benefits with low cost and of data accessibility through Internet. The ensuring security risks of the cloud computing is the main factor in the cloud computing environment, for example sensitive information with cloud storage providers may be entrusted. But 'single cloud' providers is a less popular with customers due to risks service availability failure and possibly of malicious insiders in the 'single cloud'. A towards movement of 'multi clouds' or 'multiple clouds' or 'cloud-of-clouds' has emerged currently using Shamir's Secret Sharing Algorithm.

This paper surveys to many running research related paper to single cloud and multi clouds security using Shamir's Secret Sharing algorithm and addresses possible solutions and methodology. Main focus of this paper use of multi clouds and data security and reduce security risks and affect the cloud computing user using 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. If we're going to Count all participants to combine together the secret might be impractical, and therefore sometimes the threshold scheme is used where any 'k' of the parts are sufficient to reconstruct the original secret [7].

Index Terms- Shamir's Secret Sharing Algorithm, data integrity, cloud storage, data intrusion, service availability.

I. INTRODUCTION

The cloud computing is a cost-effective, service availability, flexible and on demand service delivery platform for providing business through the internet [2]. Cloud computing resources can be quickly extracted and effortlessly scaled with all the processes, services and applications provisioned on demand service despite the consequences of the user location or device. Hence, the opportunity for an organization to enhance their service deliverance efficiencies is achieved through cloud computing. The issues in cloud security series from substantial security of the cloud fixing and hardware infrastructure, through the architectural security of function and data deployments, to the actual security of the cloud framework in the presence of peripheral attacks and the mechanisms accessible to respond to and recuperate from these attacks [3]. The use of cloud computing Subashini and Kavitha argue services for many reasons including because this service provide fast access the applications and reduce service costs [6]. Cloud computing providers should address privacy and security as matter for higher and urgent priorities. The dealing with 'single cloud' providers is becoming less popular service with customers due to potential problems such as service availability failure for some time and malicious insider's attacks in the single cloud. So now single cloud move towards 'multi clouds', 'interclouds', or 'cloud of clouds'.

Aim of the paper the data security aspect of cloud computing, data and information will be shared with a third party without any hacks. Every cloud users want to avoid untrusted cloud provider for personal and important documents such as debit/credit cards details or medical report from hackers or malicious insiders is the importance. It supply secure cloud database that will prevent security risks. We apply multi clouds concept using Shamir's Secret Sharing algorithm that is reduce risk of data intrusion and loss of service availability for ensuring data.

II. OBJECTIVE

Cloud computing concept is relatively new concept but it is based on not so many new technologies. Many of the features that makes cloud computing attractive, however has to meet certain basic security criteria. In our paper, we have briefed on various measure ion cloud computing security challenges from single to multi clouds. While making a cloud secure, the following objectives are to be met:

- Understanding the cloud computing environment provided by the cloud service provider.
- The cloud computing solution should meet the basic security and privacy requirements of any firm deploying it.
- Maintain an account of the privacy of the cloud and data security and applications that are deployed in cloud computing environment.
- Data Integrity.
- Service Availability.
- The user runs customer applications using the service provider's resources

.

III. ALGORITHM USED

3.1 Shamir's Secret Sharing Algorithms:

Data stored in the cloud can be compromised or lost. So, we have to come up with a way to secure those files. We can

encrypt them before storing them in the cloud, which sorts out the disclosure aspects [7].However, what if the data is lost due to some catastrophe befalling the cloud service provider? We could store it on more than one cloud service and encrypt it before we send it off. Each of them will have the same file. What if we use an insecure, easily guessable password to protect the 2012 45th Hawaii International Conference on System Sciences file, or the same one to protect all files? I have often thought that secret sharing algorithms could be employed to good effect in these circumstances instead [8].

Mathemetical Definition given below:

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

1. The Knowledge of any k or more Di pieces makes D easily computable.
2. 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 k points to define a polynomial of degree $k-1$.

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

Choose at random $k-1$ coefficients $a_1,\cdots,a_{k-1}$ in F, and let $a_0 = S$. Build the polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{k-1}x^{k-1}$. Let us construct any n points out of it, for instance set $i = 1,\cdots,n$ to retrieve $(i, f(i))$. Every participant is given a point (a pair of input to the polynomial and output). Given any subset of k of these pairs, we can find the coefficients of the polynomial using interpolation and the secret is the constant term a_0 [27].

Shamir Approach:

We divide our secret into pieces by picking a random degree polynomial $q(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1}x^{k-1}$
in which $a_0 = S$ $S_1 = q(1), S_2 = q(2), \ldots, S_n = q(n)$
and represent each share as a point $(x_i, q(x_i) = y_i)$

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.

Preparation:

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 2 numbers: 166, 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 from the polynomial:
$$(1,1494);(2,1942);(3,2578);(4,3402);(5,4414);(6,5614)$$

We give each participant a different single point (both x and $f(x)$ [27].

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

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

$$= 1942\cdot\left(\frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}\right) + 3402\left(-\frac{1}{2}x^2 + \frac{7}{2}x - 5\right) + 4414\cdot\left(\frac{1}{3}x^2 - 2x + \frac{8}{3}\right)$$

$$= 1234 + 166x + 94x^2$$ [27].

IV. SOLUTION METHODOLOGY

Cloud customers may form their expectations based on their past experiences and organizations' needs. They are likely to conduct some sort of survey before choosing a cloud service provider. Customers are expected also to do security checks that

are centered on three security concepts: confidentiality, integrity and availability. On the other hand, cloud service providers may promise a lot to entice a customer to sign a deal, but some gaps may manifest later as overwhelming barriers to keep their promises. Many potential cloud customers are well aware of this, and certainly, still sitting on the sidelines. They will not undertake cloud computing unless they get a clear indication that all gaps are within acceptable limits. All relevant information are visualized into cloud computing security in a snapshot which is presented in Fig.1 [9]. We organized cloud computing security into three sections: security categories, security in service delivery models and security dimensions.

Security in cloud services is based on the following:

- Strong network security is possible around the service delivery platform
- Data encryption: for data in transit (particularly over wide area networks), and sometimes stored data, but it cannot be applied to data in use.
- Access controls to ensure that only authorized users gain access to applications, data and the processing environment and is the primary means of securing cloud-based services

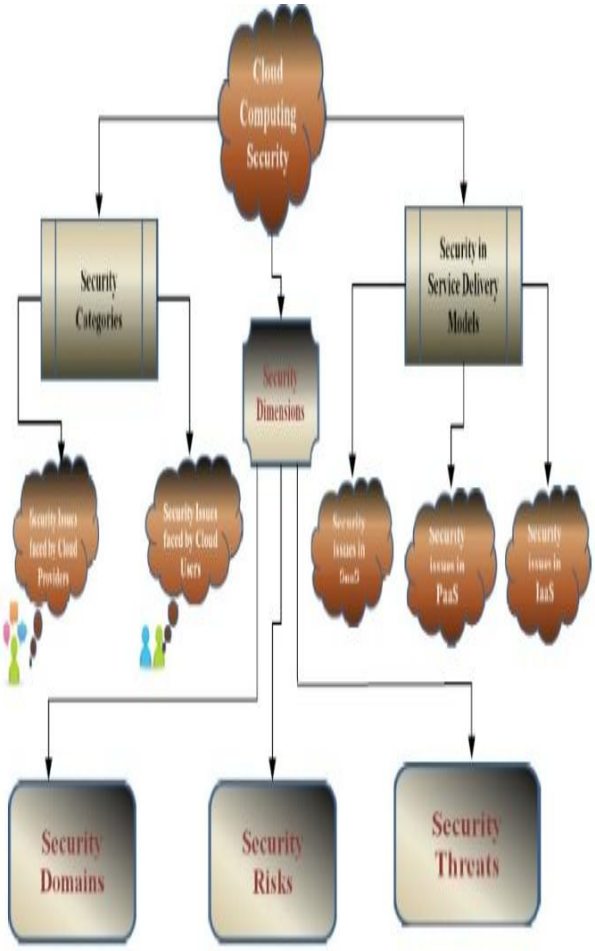

Figure 1: Graphical View of Cloud Computing Security [9]

.

- Service providers are able to inspect activity in their environment and provide reports to clients.

Logs need to be carefully constructed to appraisal the actions of their system administrators and other restricted users or risk producing reports that mix events relating to different customers of the service.

Both the organizations seeking cloud solutions and the service providers have to ensure cloud security is addressed [11]. Some of the measures to ensure security in cloud are good governance, compliance, privacy, Identity and Access Management (IAM), Data protection, Availability, Business Continuity and Disaster Recovery plans etc. The figure (fig 2) below depicts the above mentioned security measures in a snapshot:

Figure 2: Measures to ensure Security in Cloud [10]

V. IMPLEMENTATION

5.1 Data Integrity:

It is not an easy task to securely maintain all essential data where it has the need in many applications for clients in cloud computing. To maintain our data in cloud computing, it may not be fully trustworthy because client doesn't have copy of all stored data. But any authors don't tell us data integrity through its user. So we have to establish new proposed system for this using our data reading protocol algorithm to check the integrity of data before and after the data insertion in cloud. Here the security of data before and after is checked by client with the help of CSP using our "effective automatic data reading protocol from user as well as cloud level into the cloud" with truthfulness[8].

5.2 Data Intrusion:

The importance of data intrusion detection systems in a cloud computing environment. We find out how intrusion detection is performed on Software as a Service, Platform as a

Service and Infrastructure as Service offerings, along with the available host, network and hypervisor-based intrusion detection options. Attacks on systems and data are a reality in the world we live in. Detecting and responding to those attacks has become the norm and is considered due diligence when it comes to security[8].

5.3 Service Availability

Service availability is most important in the cloud computing security. Amazon already mentions in its licensing agreement that it is possible that the service might be unavailable from time to time. The user's web service may terminate for any reason at any time if any user's files break the cloud storage policy. In addition, if any damage occurs to any Amazon web service and the service fails, in this case there will be no charge to the Amazon Company for this failure. Companies seeking to protect services from such failure need measures such as backups or use of multiple providers [8][11].

5.4 DepSky System Model Architecture:

The DepSky system model contains three parts: readers, writers, and four cloud storage providers, where readers and writers are the client's tasks. Bessani et al. explain the difference between readers and writers for cloud storage. Readers can fail arbitrarily (for example, they can fail by crashing, they can fail from time to time and then display any behavior) whereas, writers only fail by crashing [8][14].

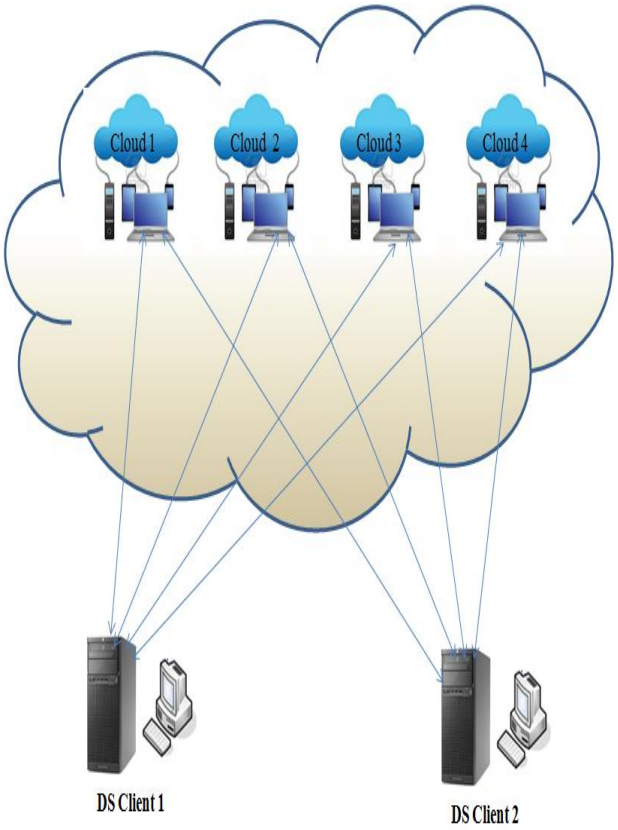

Figure 3: DepSky Architecture [14]

VI. RESULT AND DISCUSSIONS

In any cloud computing environment, the scope of activities can be divided into three major steps as: preliminary activities, initiating activities and concluding activities. The preliminary activities include a wide range of steps from identifying the security, privacy and organizational requirements to analyzing the security and privacy provided by the security provider and the levels of risks involved with respect to control objectives of the organization **.**Reliable distributed storage which utilizes a subset of BFT (Byzantine fault tolerance) techniques was suggested by Vukolic to be used in multi clouds or interclouds. One example for protocol of controls the multiple clouds HAIL (High Availability and Integrity Layer).HAIL is permits set of services to ensure that client's stored data is retrievable and integral and also provides a software layer to address availability and integrity of stored data in the intercloud.

We already discussed before, Bessani et a1 present a virtual storage cloud system called Depsky consisting of a combination of different clouds to build a cloud of clouds. Finally, the Depsky system presents an experimental evaluation with several clouds that is different from other previous work on multi clouds.

VII. CONCLUSION

The purpose of this work is to survey the recent research on single clouds and multi-clouds using secret sharing algorithm and to address the security risks and solutions using Shamir's Secret Sharing algorithm. These algorithms generate their own secret sharing schemes and use secure channels to distribute shares among themselves[7][8]. The Shamir's secret sharing scheme has a good abstract foundation which provides an excellent framework for proofs and applications [28].

We presented algorithms for performing addition, standard and scalar multiplication with shares. We are currently developing a secure computation platform based on a simple secret sharing scheme than Shamir's. 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[8][28]. We support the migration to multi clouds due to its ability to decrease security risks that is affect the cloud computing users.

ACKNOWLEDGMENT

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

REFERENCES

[1] Axel Buecker, Koos Lodewijkx, Harold Moss, Kevin Skapinetz, Michael Waidner, " Cloud Security Guidance", a red paper, January 2011.

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

[3] Neil Robinson, Lorenzo Valeri, Jonathan Cave and Tony Starkey (RAND Europe), Hans Graux (time.lex), Sadie Creese and Paul Hopkins (University of Warwick), "The Cloud: Understanding the Security, Privacy and Trust

Challenges", TR-933-EC, 30 November 2010, Prepared for Unit F.5, Directorate –General, Information Society and Media, European Commission.

[4] J. Archer, A. Boehm, "Security Guidance for Critical Areas of Focus in Cloud Computing", Cloud Security Alliance, December 2009.

[5] SNIA, Advancing Storage and Information Technology, "Cloud Storage for Cloud Computing", Storage Networking Industry Association, September 2009.

[6] S. Subashini, V.Kavitha, "A Surveys on Security and privacy Issues in Service Delivery Models of the Cloud Computing", Journal of Networks and Computer Applications, 34 (1),2011,pp1-11. .

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

[8] Cloud Computing Security: From Single to Multi-Clouds,2012 ,45th Hawaii International Conference on System Sciences.

[9] Md. Tanzim Khorshed, A.B.M. Shawkat Ali, Saleh A. Wasimi, "A surveys on gaps, threat remediation challenge, and some thoughts for proactive attack detection in the cloud computing", School of Information and Communication Technology, CQ University QLD 4702, Australia. Received 15 August 2011. Revised 11 January 2012. Accepted 18 January 2012. Available online 27 January 2012.

[10] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou, "Security and Privacy in Cloud Computing: A Survey" , Sixth International Conference on Semantics, Knowledge and Grids, August 2010.

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

[12] RedHat, https://rhn.redhat.com/errata/RHSA-2008-0855.html.

[13] S.L. Garfinkel, "Email-based identification and authentication: An alternative to PKI?", IEEE Security and Privacy, 1(6), 2003, pp. 20-26.

[14] A. Bessani, 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.

[15] 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.

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

[17] Ryan, Patrick S., Merchant, Ronak and Falvey, Sarah, "Regulation of the Cloud computing in India", Journal of Internet Law, Vol. 15, No.4, p.7, October 2011.

[18] T. Ferrari, L. Gaido, "Resources and Services of the EGEE Production Infrastructure", Journal of Grid Computing, pp. 1-15, May 2011.

[19] I.Foster, Y. Zaho, I.Raicu, S.Lu, "Cloud Computing and Grid Computing 360o Compared", November 2009.

[20] O. Arasatnam,S. Boardman, 2010, " Security for the Cloud and SOA" retrieved 8 April 2012, from

[21] D. Svantesson and R Clarke, "Privacy and Consumer Risks in Cloud Computing", Computer Law and Security Review, 26(4) (2010), pp.391-397.

[22] DMTF, "Interoperable Clouds", a white paper from Open Cloud Standards Incubator, January 2011

[23] B. Grobauer, T. Walloschek, E.Stocker, "Understanding Cloud Computing Vulnerabilities", IEEE Security and Privacy, March 2010.

[24] B. Schneier, M. Ranum, 2009, Face-off: "Assessing Cloud Computing Risks", retrieved 12thApril 2012,from http://searchcloudsecurity.techtarget.com/video/Face offAssessing-cloud-computing-risks.

[25] M.M.Boroujerdi, S.Nazem, "Cloud Computing: Changing Cogitation about Computing", World Academy of Science, Engineering and Technology, December 2009, p.58.

[26] ETSI, 2011, "Grid and Cloud Computing", retrieved 15 April 2012, from http://www.dmtf.org/standards/cloud.

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

[28] 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

AUTHORS

First Author – Md. Kausar Alam, Pursuing M.Sc-Computer Science-SCSE, VIT University, Vellore, Tamil Nadu,India,Email-kausaralam357@gmail.com

Second Author – Sharmila Banu K., Assistant Professor-SCSE, VIT University, Vellore, Tamil Nadu, India