International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 06 | June-2016 www.irjet.net p-ISSN: 2395-0072

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

Prof. Ms. A. A. Raipure, Dr. A. S. Alvi , Assistant Prof. Ms. P. P. Deshmukh

Prof Ms. A. A. Raipure, Dept. of Computer science & Engineering, Government Polytechnic Bramhapuri,Maharastra,India

Dr. A. S. Alvi, Dept. of Computer science & Engineering, Prof. Ram Meghe Institute Of Technology & Reserch Badnera ,Maharastra,India

Assistant Prof Ms. P. P. Deshmukh, Dept. of Computer science & Engineering, Prof. Ram Meghe Institute Of Technology & Reserch Badnera ,Maharastra,India

---*****---

Abstract-*These days rapid use of cloud computing in several IT industries and organizations offers new software at a reasonable cost. Cloud computing is an emerging technology that is at the top in the IT industry. Data is used, processed and stored in cloud environment all over the world. With, this there is unlimited benefits but the security risks are alarming in cloud computing environment. One of the main hurdlesis sharing sensitive data with cloud storage providers. However, single cloud providers are less popular among customers because of service availability feature and malicious insiders that exists in single cloud. For securing data outsourcing homomorhic encryption, data encryption and secret sharing algorithms are the techniques used extensively to secure data outsourcing. Managing CIA (Confidentiality, Integrity, and Availability) is a main issue and due to security issues, users are opting for multi cloud as these are secured with various techniques and one of these techniques is secret sharing algorithms. The paper applies Shamir's Secret Sharing Algorithm which will address possible methodologies and solutions to secure data outsourcing in multi clouds. The main focus of this paper will be on data security and reducing security risks.*

Keywords:Shamir's Secret Sharing Algorithm, data integrity, data security, cloud storage, data intrusion.

1. INTRODUCTION

Cloud computing is a low cost service availability technology that I highly scalable, flexible and offers service on demand delivery platform to provide business over the internet. The resources of cloud computing can be extracted fast and in an effortless way which can be scaled with diverse procedures, applications and services that are supplied on demand service in spite of the results that happen because of user location or device. Thus, through cloud computing organizations can improve their service deliverance efficiencies.

As per Subhashini and Kavitha they argue services on the basis of various reasons as the service provides quick access to applications and minimize the service costs. An important thing is that cloud service providers should give urgent priority to privacy and security. Single cloud service providers are less popular due to various issues with service availability failure and malicious insider's attack. Therefore, single clouds moves to interclouds or clouds of clouds.

The aim of this paper is data security aspect of cloud computing where data and security will be shared without any hacks with the third party. All the cloud users do not want to rely on cloud providers that can't be trusted for personal and important details like their credit or debit card or medical report from the malicious insiders and hackers is crucial. This will give a secured cloud database to avoid risks. Here we apply multi clouds concept making use of Shamir's Secret algorithm which will minimize the risk of data intrusion and loss of service availability to ensure data.

1.1 OBJECTIVE

Cloud computing is a new concept; however this is not based on the new technologies. Most of its features have made cloud computingappealing, but it needs to meet some basic security criteria. In this paper, several measures on cloud computing security challenges are highlighted from single to multi clouds. To make the cloud secure some of the objectives need to be met which are stated below:

- Understanding the working of the cloud computing environment by the cloud service provider
- Cloud computing solution must meet the basic criteria of security and privacy of a firm deploying it
- Maintaining an account of the privacy of the cloud and data, security and applications which are deployed in the cloud computing environment.
- Data Integrity
- Service Availability
- Using theservice provider's resources users run the customer applications

1.2 ALGORITHM USED 3.1 Shamir's Secret Sharing Algorithms: T

The SHAMIR'S SECRET SHARING ALGORITHM Data can be lost or compromised in the cloud. Therefore, it is important to keep the data secured in the cloud environment. For this, to secure the data in multi-cloud, Shamir proposed to store the data in more than one cloud and encrypt the same in the cloud before it is transferred and saved.

[1] MATHEMATICAL DEFINITION:

The aim of the algorithm is to divide the data in n pieces (DATA1, DATA2, DATA3, DATA4 ….. DATAn) so that,

1. Retrieving any **k or more DATA pieces will make DATA easily computable**.

2. Retrieving any **k-1 or fewer DATA pieces will leave the DATA completely undetermined**.

The above scheme is known as **threshold (k, n).**If k=n, then all the pieces are there for construction of DATA again. **The purpose of Shamir's secret sharing algorithm is that k points are enough to define a polynomial of degree k-1.[1]** Example, 2 points are enough to define a line.

Select an approximate k-1 coefficients **c 0 , c 1 , c 2 , c 3 ….c k-1 in H,** and let c0 = S, where S is the Secret data which will be stored in cloud. Build the polynomial **H(z) = c 0 + c1z 1 + c2 z2 +……+ck-1zk-1.** Then **n** points are defined, for example **set i=1,2….n** to retrieve **(i, H(i))** . A pair is formed with the input to the polynomial and output. Given any subset of k of these pairs, using the interpolation the coefficients of the polynomial which can be found and the constant term a0 is the secret.

Shamir's Algorithm Approach:

The secret is now divided into pieces by keeping into consideration the approximate degree polynomial which **is H(z) = c 0 + c1z 1 + c2 z2 +……+ck-1zk-1**

In this, c 0 = S, S1 = H(1), S2 = H(2),……., Sn = H(n) and represent every share as a point **(zi , G(zi) = yi)**

Example

The example stated below provides the algorithm. To understand, the integer arithmetic is used in place of a scientific based arithmetic or any other vector. Thus, the example illustrated does not ensure perfect secrecy, and is therefore not a perfect example of Shamir's scheme.

Encryption & Preparation

Take 1999 as the secret data. Dividing it in**6 parts (n = 6).** Parts that are needed to reconstruct the secret is **3 parts (k = 3).**

2 numbers are selected at random. Let them be 154 and 19. **c1 = 154 and c2 = 19**. Our polynomial to produce shares are: **H(z) = 1999 + 154z + 19z2**

6 parts are made from the polynomial.

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

The diverse single point is given to each participant, **both z and H(z).**

Reconstruction

Any 3 points are enough to reconstruct the secret.

Assume: (a0, b0) : (2, 2383) ; (a1, b1): (4, 2919) ; (a2, b2) : (5, 3244)

Now Lagrange basis polynomials will be applied:

l0 = a-a1/a0-a1 . a-a2/a0-a2 = 1/6a2 - 3/2a +10/3

l1 = a-a0/a1-a0 . a-a2/a1-a2 = 1/2a2 + 7/2a – 5

l2 = a-a0/a2-a0 . a-a1/a2-a1 = 1/3a2 – 2a +8/3

Thus,

H(z)= $H(z) = \sum_{j=0}^{2} bj - lj(z)$

2383 (1/6z² - 3/2z +10/3) + 2919 (1/2z² + 7/2z – 5) + 3244 (1/3z² – 2z +8/3)

H(z) = 1999 + 154z + 19z²

1.3 SOLUTION METHODOLOGY

Cloud customers expect on the basis of their past experiences and needs. However, thequality approach is to collect information about the reputed and effective cloud service provider. Customers must also make sure about the level of security of these vital characteristics of the cloud: Confidentiality, Integrity and Availability (CIA).

Security in Cloud computing is organized in different sections: security categories, security in service delivery models and security dimensions. Security in cloud services depends on powerful network security that should be applied in and around the service delivery platform. Secondly, it is encrypting the data and thirdly by accessing controls by authorization.

Logs must be strictly maintained and secured to note the activities of the system administrators and of other restricted users. Logs are useful to produce reports that mix events relating to different customers of the service. Security should be implemented and taken care of in both the organizations that are looking for cloud solutions and the service providers. Identity and Access Management (IAM), Good governance, compliance, Availability, privacy, Data protection, Business Continuity and Disaster Recovery plans etc. are some of the measures to ensure security in cloud.

2. IMPLEMENTATION

5.1 Data Integrity: This is not an easy task to maintain all the required data in a secured way and where it has the requirement in many applications for clients in cloud computing. To properly maintain the data in cloud computing, it cannot be completely trustworthy because the client doesn't have the copy of all the data that is stored. But any author does not tell about the data integrity through its user. Thus, we need to keep the new proposed system in place to use our data reading protocol algorithm and to check the integrity of data before and after data is inserted in the cloud. The security of data is checked here before and after by the client with the help of CSP using the "effective automatic data reading protocol from user and cloud level into the cloud" with integrity.

1.2 Data Intrusion:

The data intrusion detection systems in a cloud computing environment are valuable. We find out that how intrusion International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 4 ISSN 2250-3153 www.ijsrp.org detection is performed on the Software as a Service Platform as the service and Infrastructure as Service offerings with the available host, network and the hypervisor-based intrusion detection options. In the world we live, attacks on systems and data are a reality and it has become a norm and considered as a due diligence to detect and respond to those attacks.

1.2 Service Availability:

Service availability is quite important in the cloud computing security. This is stated by Amazon in its licensing agreement that there is possibility that the service might be unavailable from time to time. If any users file break through the webs service of the user will

be terminated for any kind of reason at any time. Moreover, if any damage is caused to the Amazon web service and if the service fails there will be no charge to the Amazon Company for this kid of failure. Companies that look to protect the services from such failures need measures like backups or use of multiple providers

1.3 DepSky System Model Architecture:

The DepSky system model consists of three parts who are the readers, writers, and four cloud storage providers. Here the readers and writers are the task of client. Bessani et al. explains the difference between the readers and and organizational requirements that helps to analyze security and privacy offered by the security provider and the risk level that is involved with respect to control objectives of the organization .Reliable distributed storage that makes use of the subset of BFT or Byzantine fault tolerance techniques is suggested by Vukolic to be used in multi clouds or interclouds. For example, for protocol of controls the multiple clouds HAIL (High Availability and Integrity Layer) and it is permits set of services that makes sure that client's stored data is retrievable and integral and this also offers a software layer to address the availability and integrity of stored data in the intercloud. As discussed earlier Bessani et a1 present a virtual storage cloud system called Depsky made of a combination of different clouds to build a cloud of clouds. Finally, the Depsky system presents the experimental evaluation with several clouds that differs from the previous work on the multi clouds.

3. CONCLUSION

The aim of this work is to study and secure the Multi-cloud with the help of secret sharing algorithm. This purpose is achieved implementing Shamir's secret sharing algorithm. This secret sharing scheme has a good foundation that offers an excellent platform for proofs and applications. Moreover, the disadvantages of single cloud and the benefits of multi cloud are addressed in this paper. Cloud computing is the present technology that is discussed everywhere and it contents the enterprise and its consumers by giving their requirements. However, the data of the consumer and the enterprise must be safe and it needs to be maintained as well as ensured by the writers for cloud storage. As per Bessani et al. the readers can fail arbitrarily like by crashing and they can fail from time to time and then display any behavior whereas, writers only fail by crashing.

2. RESULTS & DISCUSSIONS

In any kind of cloud computing environment, activity scope can be divided into three major steps like, preliminary activities, initiating activities and concluding activities. The preliminary activities comprises of a wide range of steps which is identifying the security, privacy

administrator. Migration to multi cloud is encouraged keeping in mind about its ability to minimize the breaches and other security problems.

REFERENCES

[1] Md Kausar Alam, Sharmila Banu K, An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds, School of Computing Science and Engineering, VIT University, Vellore, Tamil Nadu, India, Volume 3, Issue 4, April 2013

[2] R.Kishore Kumara , E. A. Mary Anita, Securing Multi-Cloud using Secret Sharing Algorithm, a Department of Computer Science and Engineering, S.A. Engineering College, Affiliated to Anna university, Chennai-600077,India, 2015

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

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

[5] 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.

[6]B. Schneier, M. Ranum, 2009, Face-off: "Assessing Cloud Computing Risks", retrieved 12thApril 2012,

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

[8]ETSI, 2011, "Grid and Cloud Computing", retrieved 15 April 2012

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

[10]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

[11]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

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

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

[14]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.

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

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

[17]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.

[18]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.

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

[20]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.