Enhanced Authorized Cloud Computing Security and Data Integrity using Multi-Cloud Technology, AES and MD5 Algorith

1.Dhage Meghna 2. Deshmukh Sayali 3. Gaje Reshma 4. Deshmukh Asmita

B.E. Comp,AVCOE,Sangmner ,India,
Prof. Sachin Thanekar,
M.E. Comp,AVCOE,Sangmner.India

ABSTRACT

Now a days most of the organization using cloud computing. To access data at low cost the cloud computing is beneficial. In the cloud computing keeping the security is major factor, as users keep sensitive and private information with cloud storage providers, but these providers may be untrusted. Clouds data storage redefine security issues targeted on customers outsource data. Level of customization can be achieved by providing, deciding security. In paper we define secure cost effective multi cloud storage model in cloud computing which contain distribution of data to provide clients service with data availability and secured storage. In studies we elaborate Multicloud storage model in cloud computing where we can provide data to user as data has store in data pieces .We define cost effective SCMCS model which is distribute data to all service providers available in market, to provide data availability with security.

Keywords: *Cloud computing, DepSky, Secret Sharing algorithm, LaGrange's basis polynomial, multi-clouds.*

1. Introduction

The end of this decade is marked by a paradigm shift of the industrial information technology towards a subscription based also known as pay-per-use service business model known as cloud Computing. This model provide list of advantage. Large amount of data being retrieved from different data sources and non-localized data handling requirement create changes as technological as well as business model. The best offered service in cloud computing is cloud data storage. Where user do not have store personal data on their server instead of data store in cloud service provider's server. In cloud computing, subscribers have to pay for provides for this storage service. This service provide reliability for data storage it's also provide benefit of only pay for used data which they need to save particular time without any storage mechanism maintaining issue. In addition with this benefit user can access their data from any geographical region where service provider's internet will be easily accessed.

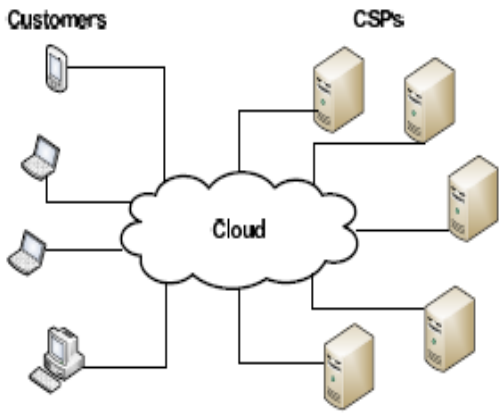


Fig. 1. Cloud computing architecture example

An example of the cloud computing is shown in Fig. 1. With these advantage cloud data storage define the security issues targeted on users outsource data. Cloud service provider having standered regulations and powerfull infrastucture to ensure users data privacy and provide availability.

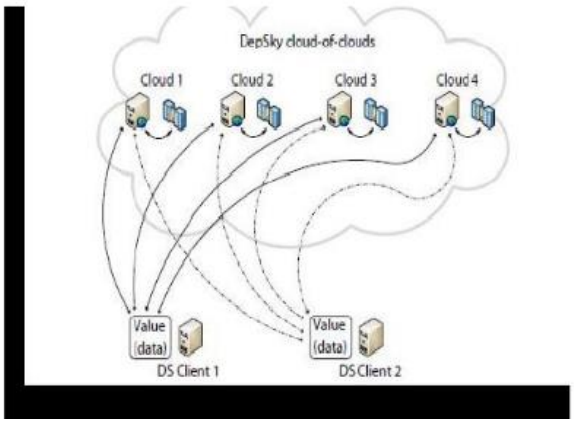
In this studies we observed that customers data is not very promising. Moreover, providing better privacy as well as ensure data availability, can be get by users data block divided into the data pieces and distribute them among service providers in such way less than service providers not able to achived users data block. Our approch will provide decision model to cloud computing users, will provide good security to distributed data over the cloud server in such a way that,no one Service provider can successfully access private information which is obtained from the data pieces which are allocated at their servers. Also, in addition, we can provide privacy to aavailable data by maintaining redundancy in data distribution.If one service provider not able to provide data in that case other service provider also retrieved data successful and provide to user. For the bussines cloud storage is subsciption service and highly data redundancy done hence user highly pay for the data storage. Inshort her we are trying to provide optimize the security for a given budget for the cloud data.

2. Literature Survey

Most critical security issues related to user data is Privacy preservation and data integrity [4]. In the most organization crucial part is their data and thus they try to get data security system. In cloud computing data will be stored on third business party they provide data storage as subscription service. The users can trust on SP for the privacy of data. In [7], the author define the importance of privacy issue of data storage in cloud computing and pointed that data can be accessed easily from third party than from main creator. Following the pattern of [7], the security policies are also evolved from the traditional cryptographic schemes applied in central and distributed data storage, for achieving the data privacy. In many approaches proposed that to secure the data privacy hiding data from the service providers [18] [19] [5]. In [19], the authors define scheme in which, the user's identity is also fetched from the data, and claim to provide public auditing of data. These types of approaches can work only for solo service provider and they are able to easily access service. In [14], the authors proved that sole cryptographic measures are lack of ensuring data privacy in cloud computing. They also define that hybrid model for keep the privacy in cloud storage. One more concern arrived in that scheme there is no proof for data privacy will stay secure on cloud from the service providers. Most of the time data can be decrypted to access information .Since, the user might not be availing the storage services from that service provider; he will be not having any idea of such a passive attack. The better the cryptographic scheme, the more complex for its implementation and hence the service provider demands for more cost. This could also lead to a monopoly over cloud services in the market. To users get chance to keep data secure in cloud storage with affordable cost, our model helpful for distributes the data pieces among more than one service providers, the conventional single service provider based cryptographic techniques does not seem too much promising service providers can access the data from the server in data pieces without getting others data pieces from another service providers. In [16], the authors explained distributing data over the multiple cloud or network it was advantage to not able to access from one specific network. Hence they cannot access the private data because multiple data pieces store in multiple cloud or network. Both work as remove centralized distribution of cloud data. If because of some causes a service outage in one of the data networks others network not able to access data. We propose to use a redundant distribution scheme, similar to[17], in which at least a threshold number of pieces of the data those are required out of the whole distribution range, for successful retrieval.

3. Proposed System

DepSky Model-The virtual cloud storage called DepSky Model. It address the issue like data integrity, availability in multi cloud.



Depsky architecture [3] consist four cloud and each cloud uses its own particular interfaces. As software library contact with cloud this algorithms available in client machine. We will describe our system model and the threat model. Then, formally to explain our problem statement we are going to study the paper, cloud storage and cloud data storage are interchangeable as service providers and cloud service providers interchangeable.

A. System Overview

We assumed that two entities involved in cloud data storage first is cloud users and second cloud service providers. Cloud storage service depend on two factor how much data stored on cloud server and how long time it will be stored. In our model, the assumption is that all the data is to be stored for similar period of time. We assumed N number of cloud service providers (SP), each available cloud service provider as associated with a QoS factor, along with its cost of providing storage service that is provided per unit of stored data (C). Every SP has a different level of quality of service (QoS) offered as well as a different cost associated with it. However the cloud user stored his data on different service providers according to required security level and budget.

B. Threat Model

Data will be stored at cloud service providers is open moral attack of many threat. In our work, we can consider two kinds of threat models. First is the single point of failure [9], [11], that will affect the data presence, that would occur if a server at the cloud service provider is failed or destroyed, which make it difficult for the client to retrieve his stored data from the server. Availability of data is also necessary issue which could be affected, if the cloud service provider (SP) runs out of business. A cloud service client cannot always totally rely upon a solo cloud service provider to confirm the storage of his vital data.

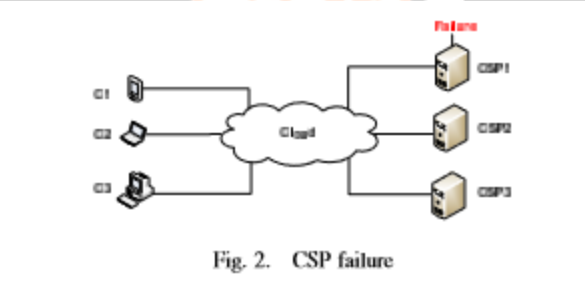


Fig. 2. CSP failure

Fig. 2. CSP failure to illustrate this threat we use an example in Fig. 2. Let us assume that three users stored their data on three different service providers respectively. Every customer is able to retrieve or get his own data from the cloud service provider who it has a contract with. If a failure occur at first service provider, due to internal problem with the server or some issues with the cloud service provider, all first level users' data which was stored on first service providers servers will be lost and cannot be retrieved. One solution for threat is that, the user can seek to store his data at multiple service providers to ensure better availability of his data.

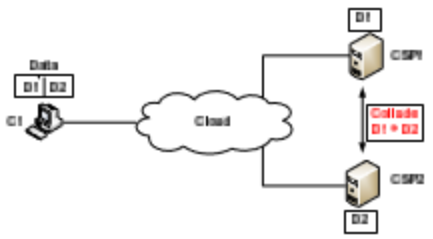


Fig. 3. Colluding cloud service providers

Fig. 3.The next threat discussed in this paper is the colluding service providers [6], in that to access user data all service providers colluding together. In [16]The author suggest that store data on two cloud server thus not able to access content of data, without having access to both the storage clouds. Data will be not secure against service provider's collusion such type of attacks are passive attack because the cloud user cannot search that his information will be retrieved or accessed by service providers without his consent. We illustrate the colluding service providers' threat in Fig. 3. Let's assume that user want to keep his data secure hence he select two service providers and will divide

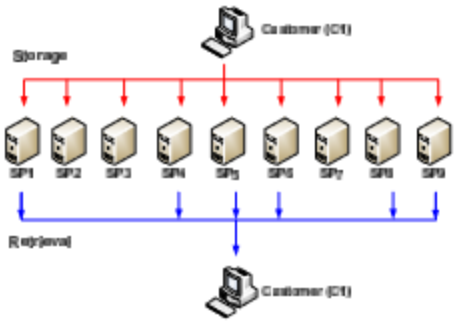


Fig. 4. Data Storage and Retrieval

Data Storage and Retrieval his data into two parts and distribute these parts on the two available two service providers. The ir two different service providers collude and exchange the available data which is stored in server by user and reconstruct data without detection by the user.

X. Problem Statement

In this section, we will formally state the definition of our problem that we are going to study. Given p number of cloud service providers (SPi : i ∈1 ,2,..,p). Each SP associated with a QoS factor (QSi ∈(0 ,1)) along with the cost of storing data units (Ci). The Secured Cost-effective Multi-Cloud Storage Model (SCMCS) seeks a distribution of customer's data pieces among the available SPs in such that, at least p number of SPs must take part in data retrieval, while minimizing the entire cost o f storage the data on SPs as well as to maximize the quality of service provided by the SPs.

To generate the hash value of the data we have used MD5 massage digest version 5 algorithm to generate the hash value of the user data. If there is any change in data occur the hash value of that data get changed. Md5 algorithm helps to ensure the data security.

We are using Advanced Encryption Standard (AES) algorithm to encrypt the data and then this data is storing on the cloud server. To add more security to it we are splitting the encrypted data into the parts and upload that data to the different proxy servers. A Permutation based image encryption approach for secure and efficient data security. Primary focus is on practical design of a pair of encryption and digestion of data schemes in such a way that it should achieve the security as well as detect the changes in the data.

4. CONCLUSION

In the paper we studied Multicloud storage in cloud computing which is how to keep secure and cost effective, and provide each user best storage model with consider the users budget as well as providing him with the best quality of service of availability and security offered by available cloud service providers. Our model has shown its ability of providing a customer with a secured storage under his affordable budget by dividing and distributing customers data.

REFERENCES

[1] Amazon.com, "Amazon s3 availablity event: July 20, 2008", Online at http://status.aws.amazon.com/s3-20080720.html, 2008.

[2] "A Mordern Language for Mathematical Programming", Online at http://www.ampl.com.

[3] M. Arrington, "Gmail Disaster: Reports of mass email deletions", Online at http://www.techcrunch.com/2006/12/28/gmail-disasterreports-ofmass- email-deletions/, December 2006.

[4] P. S. Browne, "Data privacy and integrity: an overview", *In Proceeding of SIGFIDET '71 Proceedings of the ACM SIGFIDET (now SIGMOD)*, 1971.

[5] A. Cavoukian, "Privacy in clouds", *Identity in the Information Society*, Dec 2008.

[6] J. Du, W. Wei, X. Gu, T. Yu, "RunTest: assuring integrity of dataflow processing in cloud computing infrastructures", *In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS '10)*, ACM, New York, NY, USA, 293-304.

[7] R. Gellman, "Privacy in the clouds: Risks to privacy and confidentiality from cloud computing", Prepared for *the World Privacy Forum*, online at http://www.worldprivacyforum.org/pdf/WPF Cloud Privacy Report.pdf, Feb 2009.

[8] The Official Google Blog, "A new approach to China: an update", online at http://googleblog.blogspot.com/2010/03/new-approach-to-chinaupdate. html, March 2010.

[9] N. Gruschka, M. Jensen, "Attack surfaces: A taxonomy for attacks on cloud services", *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, 5-10 July 2010.

[10] W. Itani, A. Kayssi, A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures," *Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, Dec 2009.

[11] M. Jensen, J. Schwenk, N. Gruschka, L.L. Iacono, "On Technical Security Issues in Cloud Computing", *IEEE International Conference on Cloud Computing, (CLOUD II 2009)*, Banglore, India, September 2009, 109-116.

[12] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors", Online at http://www.techcrunch.com/2008/-7/10/mediamaxthelinkup-closes-itsdorrs/, July 2008.

[13] B. Krebs, "Payment Processor Breach May Be Largest Ever", Online at http://voices.washingtonpost.com/securityfix/2009/01/ payment processor breach may b.html, Jan, 2009.

[14] M. Dijk, A. Juels, "On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing", *HotSec 2010*.

[15] P. Mell, T. Grance, "Draft NIST working definition of cloud computing", Referenced on June. 3rd, 2009, Online at http://csrc.nist.gov/groups/SNS/cloud-computing/index.html, 2009.

[16] P. F. Oliveira, L. Lima, T. T. V. Vinhoza, J. Barros, M. M´edard, "Trusted storage over untrusted networks", *IEEE GLOBECOM 2010*, Miami, FL.USA.

[17] A. Shamir, "How to share a secret", *Commun. ACM* 22, 11(November 1979).

[18] S. H. Shin, K. Kobara, "Towards secure cloud storage", *Demo for CloudCom2010*, Dec 2010.

[19] C. Wang, Sherman S.-M. Chow, Q. Wang, K. Ren, W. Lou, "Privacypreserving public auditing for secure cloud storage", in *InfoCom2010, IEEE*, March 2010.