Data Storage in Secured Multi-Cloud Storage in Cloud Computing

Archana Waghmare[1], Rahul Patil[2], Pramod Mane[3], Shruti Bhosale[4].

[1, 2,3,4] *S.V.P.M's COE Malegaon(Bk). Department Of Computer Engg.*

ABSTRACT

Now a day even though Cloud services offer flexibility, scalability, there have been proportionate concerns about security. As more data moves from centrally located server storage to the cloud storage. Security is the most important factor related to the cloud computing. As the users can stores his private data on cloud with the help of cloud service providers. Data stored on single cloud is risk of service availability failure due to attacker enters in single cloud.Our approach is to movement towards multi-clouds that is data stored on multi-cloud service providers. In this system we propose a secured cost-effective multi-cloud storage (SCMCS) model in cloud computing in which holds an economical distribution of data among the available cloud service provider (SP) in the market, instead of single cloud to provide the customers with advanced data availability as well as security. This work aims to encourage the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user. Our proposed model provides a better security for customer's data according to their available budgets from that they can choose cloud service provider.

KEYWORDS: *Cloud Networks , Service provider ,Multi- Cloud Storage ,Security, Cloud Services, Cloud Computing.*

I. INTRODUCTION

Cloud computing is nothing but rate server and internet based model .A huge amount of data being retrieved from geographically distributed data sources and non localized data handling requirements. The industrial information technology towards a subscription based or pay-per-use service business model known as cloud computing. One of the advantage of cloud computing is cloud data storage, in which users do not have to store his own data on their own servers [1], where instead their data will be stored on the cloud service provider's servers. For that reason users have to pay the service charge to service provider for this storage service. This service does not provide only flexibility and scalability for the data storage it also provides customers with the benefit of paying a charge only amount of data they need to store for particular time.To access this cloud services security and reliability we are using different modules like: 1) Using single cloud service provider. 2) Using multiple cloud service providers. The drawback of single cloud service provider is that it can be easily hacked by any attacker. In multiple cloud service provider model gives better security and availability of user private data.

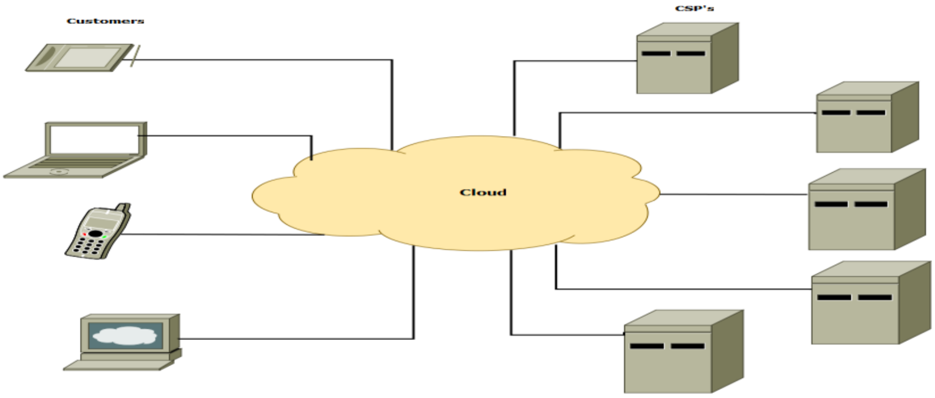

Fig 1: Cloud Computing Architecture

Data integrity and privacy of the data are the most critical issues in cloud storage. For that reason cloud service provider have standard techniques and hybrid model [4][3][5]. In this work we provide better privacy and availability of user's data can be achieved by dividing into block of data pieces and distributing them among the cloud service provider's in such way that for retrieving original data specific number of cloud service providers are required. Our proposed approach will provide the cloud computing users a decision model, That will provide a better security by distributing data over multiple cloud service providers in such a manner, none of the SP can successfully retrieve meaningful information from the data pieces allocated at their servers. Also in addition, we may provide user with better assurance of availability of their data.

II. BACKGROUND

We found these some existing system is related to our proposed system having their advantages and limitations. From these we can say that our proposed system is better than existing one.

	Existing System	Advantages	Limitations
1	Single Cloud Computing	i. Availability of data is maintained.	i. Require high cost. ii. Does not provide flexibility and scalability.
2	Data Storage only with Cryptography.	i. Due to encryption and decryption of data, confidentiality is achieved.	i. Only cryptography does not provide full security. ii. Cryptography does not provide integrity and availability.
3	Data Storage Over Untrusted Networks.	i. If Attacker hacks any one network still he does not retrieve any meaningful data.	i. Secret key get be shared with every user. ii. Losses of data.

In one of the above system we consider threat model which will losses data availability because of failure or crash of server of cloud service provider which makes difficult for customer to retrieve his stored data on the server [2]. Customer cannot depend on single cloud service provider to ensure the storage of confidential data. For understanding this threat model we take example in Fig 1. Let us consider three customers (customer1, customer2 and customer3) and stored their data on three different cloud service providers (CSP1, CSP2 and CSP3) respectively. Each customer can retrieve his own data from the cloud service provider who it has dealing with. If a failure occurs at CSP1, due to internal problem with the server all customer1 data which was stored on CSP1's servers will be lost and cannot be retrieved.

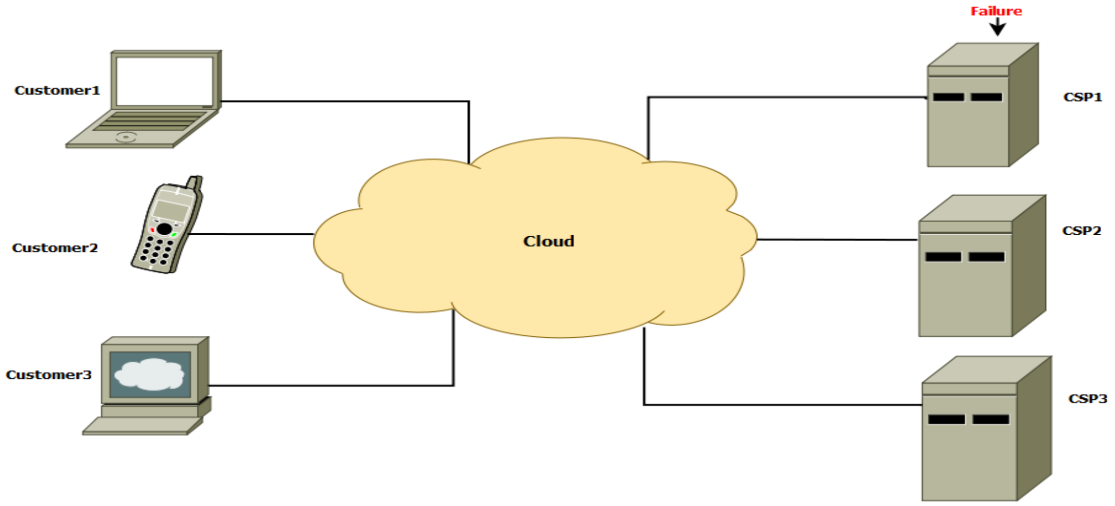

Fig. 3:CSP Failure

III. SYSTEM OVERVIEW

In our system, we are considering 1] Customer (C1): The person who has some files to store on the cloud (i.e. Cloud Server). 2] Cloud service provider (CSP): To manage Cloud Server, having considerable storage space and to provide effective services for data storage and maintenance.The cloud service provider priced to customers which is based on two factors, how much data is going to be stored on the cloud servers and for how long time the data is to be stored. In our system, we consider that specific number cloud service providers for data storage and retrieve. Hence, customer can store his private data on multiple clouds according his budgets.

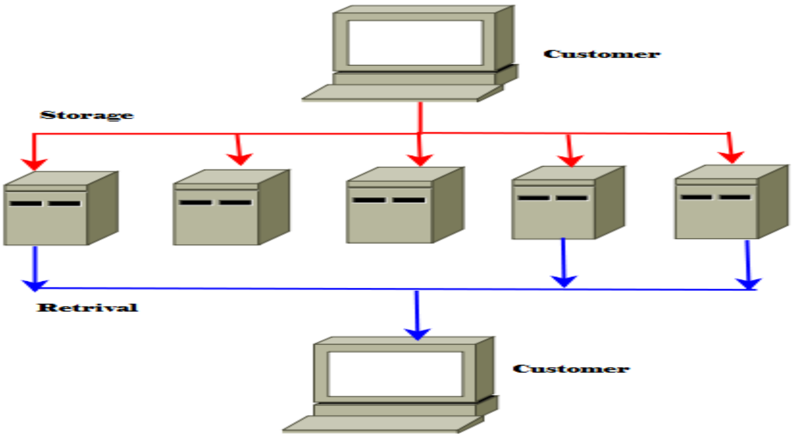

Fig 2: Data Storage And Retrieval

IV. PROPOSED MODEL

In this system, we proposed distribution of user's data among the available service providers in the market, to provide all the cloud users with data availability as well as better security of data storage. In our model, the customer divides his data among several CSP's available in the market, based on user available budget. Also we provide a choice for the customer, to choose different CSP. User may choose CSP to store or to access the data.

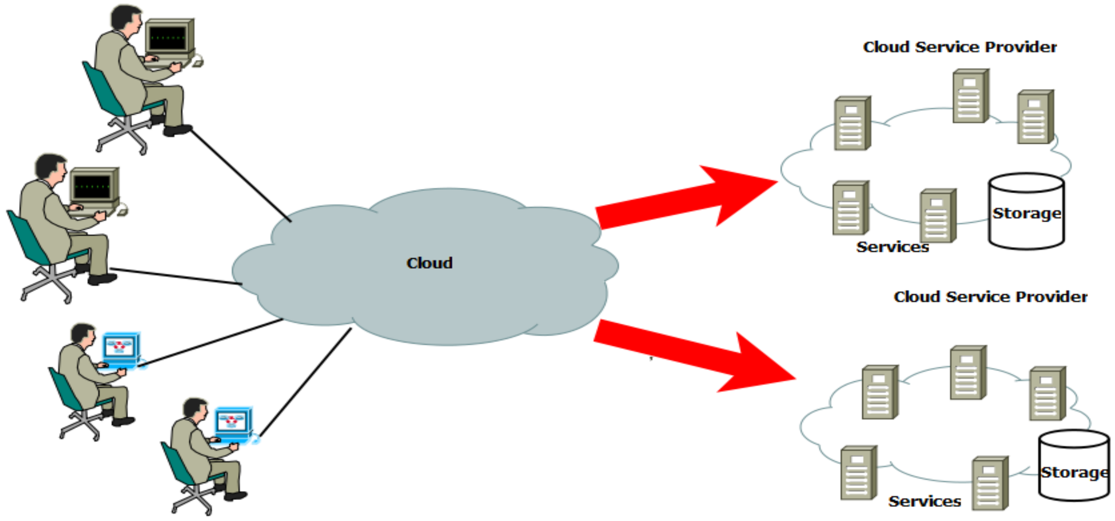

Fig. 4: Multi-Cloud Storage in Cloud Computing

Our proposed approach provides a better security by distributing the data over multiple cloud service providers in such a way that, none of the service provider can successfully retrieve meaningful data from the data stored at their own servers and provides better availability of data. If any hacker hacks any of the network still user can access his data by retrieving it from other cloud service providers.

3.1. Advantages

1) The system provides data Integrity, Availability, Confidentiality in short Security.
2) By using cryptography data is secured.
3) Less cost and cost based on client requirements.
4) Cloud data storage also redefines security issues targeted on customers outsourced data.
5) Easy to maintain large databases with security.
6) Avoid database losses.

3.2. Algorithms

The Algorithms to be used in our system:
1) Shamir Secret Sharing Algorithm

In cryptography, secret sharing refers to a method for distributing a ”secret” amongst a group of shares, each of them gets allocated a share of the secret. The secret can be only reconstructed when the shares are combined together; individual shares are of no use on their own. 2) Message Digest (MD5) This algorithm used for checking integrity of retrieved data. It takes as input a message of arbitrary length and produces as output a 128 bit fingerprint or message digest of the input. It is conjectured, so it is computationally infeasible to produce two messages having the same message digest intended, where such a large file should be compressed in a secure manner before being encrypted with a private key under a public-key crypto-system.

V. CONCLUSION

It is clear that although the use of cloud computing has rapidly increased, its security is still considered the major issue in the cloud computing environment. The customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, loss of service availability has caused many problems for a large number of customers. Furthermore, data intrusion leads to many problems for the users of cloud computing. The purpose of this work is to check the recent research on single clouds and multi-clouds to address the security risks and solutions.

REFERENCES

[1] 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.

[2] 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.

[3] J. Kincaid, ”MediaMax/TheLinkup Closes Its Doors”, Online at http://www.techcrunch.com/2008/-7/10/mediamaxthelinkupcloses-itsdorrs/, July 2008.

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

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

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

[7] 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.

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

[9] P. F. Oliveira, L. Lima, T. T. V. Vinhoza, J. Barros, M. Medard ”Trusted storage over untrusted networks”, IEEE GLOBECOM 2010, Miami, FL. USA.