Research Paper on A Secured Cost-Effective Multi-Cloud Storage in Cloud Computing

Prof. Rucha Dixit[1] Dipika Deshmukh[2] Priya Pokale[3] Niketan Tote[4] Surendra Tipre[5]
[1]Professor
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]JSPM's JSCOE, Pune, Maharashtra, India

Abstract— Now a days industries and business move towards the pay per use services also knows as the cloud computing. Cloud is very popular and useful because of pervasive nature of it. But security issues of customer outsourced data become the main overhead. We can observe that single cloud service provider is not sufficient to provide prominent security to the customer outsourced data. In this paper we address the security issue of customers outsourced. We provide the more privacy and availability to customer data by dividing customer data into the no of data pieces and distribute them to the available service providers and successful retrieval of data takes the participation of threshold no of service provider. In this paper we presents a secured cost-effective multi-cloud storage in cloud computing. Our model provides better security as well as availability of data with cost effective service.

Key words: Cloud, Cloud Computing, Cloud Service Provider, Customer outsourced

I. INTRODUCTION

Cloud computing means applications and services that runs on a distributed networks using virtualized resources and access by some common internet protocol standards and networking standards. Standard internet protocol means web service description language. cloud computing is distributed computing which is scalable. The end of this decade use cloud computing is increased due to the long list of features such as ubiquitous computing capabilities, resource pooling, flexibility etc. cloud provides the main three services, software as a service(SAAS), Platform as a service(PAAS), Infrastructure as a service(IAAS). One of the services named as cloud data storage provides flexibility to the customer to store their data remotely instead of storing on the local server. Customers have to pay for this subscription of storage service. Along with the flexible and scalable storage one more main benefit is that customers have to pay only for amount of data stored for a specific time period without worrying of storage and maintenance methods or mechanisms. Customer can access their data from any geographical location at any time by using network or internet. Along with the various advantages, it redefines the security issues and privacy issues related to the customer outsourced. Service providers have standard structure and rules to provide the better privacy and availability to customer data but still there are privacy problem and storage outage have been arrived in last few years. Depending upon single cloud is not sufficient for customers outsourced. There may be chances of single point failure or may be service outage. One cannot rely on one cloud service provider to satisfy the requirements of customers related to different geographic regions. So, what is required is an assimilated network of multiple clouds. Hence we are moving towards the multi-cloud concepts for achieving better security and availability of customers outsourced. Multi-cloud is latest technique which is also used by many popular social Medias like Gmail, Facebook etc. for maintaining their databases. So we can overcome drawbacks of single cloud into this paper by using multi-cloud concept by dividing the whole data file into no of parts and distributes to the available service provider and successful retrieval of whole data requires threshold no of service provider takes part into it.
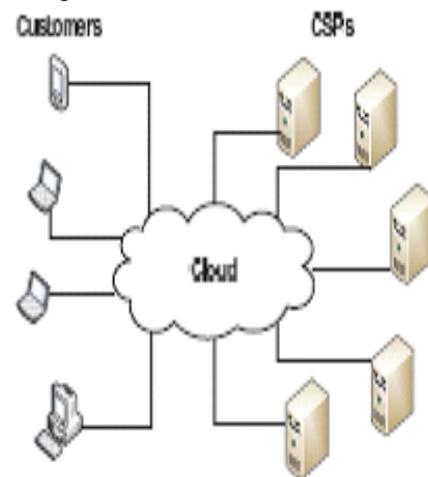

Fig. 1: Cloud Architecture
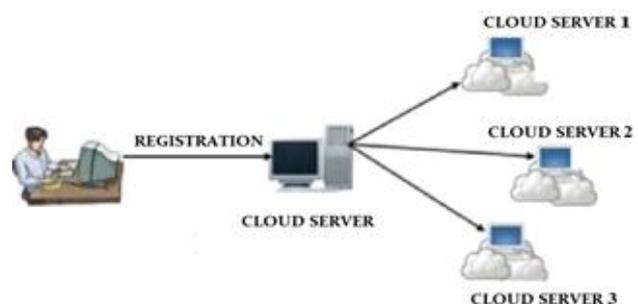
II. SYSTEM ARCHITECTURE

Fig. 2: System Architecture

Above system shows system architecture. In the system, we create Multi cloud Environment in which multiple service provider take part. It consists of client and multiple clouds service providers. Client can register to the system for accessing service of our system. Multiple clients can access the system at time for data storage. More than one client can upload their file on system for better security and as per their budget file will store on the available cloud service provider. Each service provider will store respective parts of encrypted file. Suppose we have use three service provider then CSP1 will store file.part1 and file.part3, CSP2 will store file.part2 and file.part1, CSP3 will store file.part3 and file.part2. File is partitioned based on cost and space. Similarly according to cost of cloud file will download and

combine. So we are Multi cloud Servers does the Jobs, we are identifying the best Service providers for the data storage. For the Cloud Computing process, we are implementing, Cloud computing as Software as a Service (SAAS).

III. EXISTING SYSTEM

In existing system we are using single cloud for customer outsourced data storage. Single cloud provide security to customer outsourced but still it is not sufficient. Customers rely upon single cloud for their data storage. But depending on single cloud for storage is not good practice for data storage. Single cloud has some drawbacks like single point failure, data outage, service unavailability etc. In previous system there are various cases of data losses and service outage. Hence we are moving towards the multi-cloud technique.
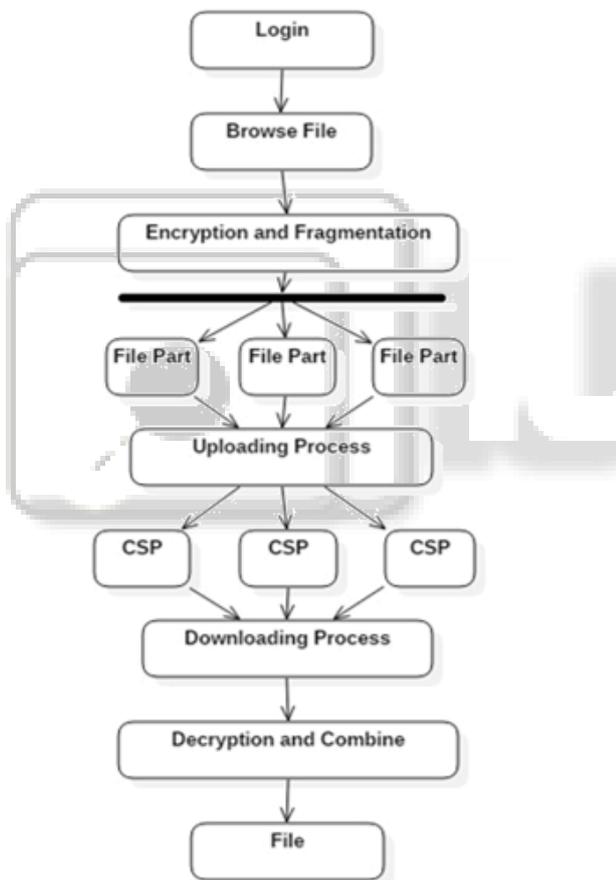
IV. PROPOSED SYSTEM ARCHITECTURE

Fig. 3: Proposed System

Proposed a secured cost effective multi cloud storage in cloud computing architecture divide into following parts:

A. Login

Module is designed for authentication purpose. A user first need to register to system for verification of user info is done through email verification after that user can login to the system by using unique username and password. Successful login leads to the further data storage operations.

B. Encryption

After successful user can browse file for uploading process. But for security reason we will encrypt the file before uploading it on cloud. File is encrypt by using AES (Advance Encryption Standard Algorithm) and fragmented into parts.

C. Upload

This module is developed for uploading process. Encrypted parts of file will distribute on the available service provider according to the size of file and cost parameter.

D. Decryption

This module is used for the decrypting file. This module will decrypt the encrypted parts of file and combine them into one file. AES algorithm is used for decryption process.

E. Download

This module is developed for downloading purpose. User can download the any file which he has uploaded. Successful downloading of file will done only when threshold no of service provider takes part into it.

V. RESULT

A. Login

This screen shot shows the login page where user can login into the system by using unique id and password.

Fig. 4: Login page

B. Uploading

This screen shows the successful uploaded file. File is divided into no of parts and successfully uploaded.

Fig. 5: Uploading page

C. Downloading

This file shows successful downloaded file.

Fig. 6: Download screen

VI. CONCLUSION

This paper presents a secured cost effective multi-cloud storage in cloud computing system which provides storage to customer outsourced. This paper provide decisional model for customer outsourced data with better security, privacy, availability and as per their budget.

REFERENCES

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

[2] "A Modern 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-of-mass- 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-china- update.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.