International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 3, March-2014, pp: (300-306), Impact Factor: 1.252, Available online at: www.erpublications.com

A Proposed Secured Cost-Effective Multi-Cloud Storage in Cloud Computing

Ganesh Yewale[1], SagarGunjal[2], Vaibhav Kadam[3]

[1,2,3]Department of Computer, Parvatibai Genba Moze College of Engineering, Wagholi (Pune)
Pune, Maharashtra, India

Abstract: The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data. Ensuring that security is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be untrusted. Dealing with "single cloud" providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. A movement towards "multi-clouds", or in other words, "interclouds" or "cloud-of-clouds" has emerged recently. This paper surveys recent research related to single and multi-cloud and addresses possible solutions. It is found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community than as the use of single clouds. This work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user.

Keywords: Cost-effective, multi storage, cloud service provider, cloud computing.

I. INTRODUCTION

The end of this decade is marked by a paradigm shift of the industrial information technology towards a pay-per-use service business model known as cloud computing. Cloud computing is internet based computing where virtual shared servers provide software, infrastructure, platform, devices and other resources and hosting to customers on a pay-as-you-use basis. Cloud data storage redefines the security issues targeted on customer's outsourced data. The term "Cloud Computing" is same like as "Internet". Pay-per-use service business model paradigm provides users with a long list of advantages, like as broad, heterogeneous network access; resource pooling and rapid elasticity with measured services [15].Huge amounts of data being retrieved from geographically distributed data sources, and non-localized data-handling requirements, creates such a change in technological as well as business model. One of the prominent services offeredin cloud computing is the cloud data storage, in which; subscribers do not have to store their data on their own servers, where instead their data will be stored on the cloud service provider's servers. In cloud computing, subscribers have to pay the service providers for this storage service.It also provides facilities for consumer to develop and manage their own applications on the cloud, which enhance the concept of virtualization of resources. Through virtualization the resources are managed itself. The best example of cloud computing is Google docs where any document can be accessed using a browser and it can be shared on thousands of computer through the Internet.

In addition to these benefits, customers can easily access their data from any geographical region where the Cloud Service Provider's network or Internet can be accessed. Along with these unprecedented advantages, cloud data storage also redefines the security issues targeted on customer's outsourced data (data that is not stored/retrieved from the costumers own servers). Since cloud service providers (SP) are separate market entities, data integrity and privacy are the most critical issues that need to be addressed in cloud computing. Even though the cloud service providers have standard regulations and powerful infrastructure to ensure customer's data privacy and provide a better availability, the reports of privacy breach and service outage have been apparent in last few years[1][3][12] and [13].Also the political influence might become an issue with the availability of services [8].In previous work we observed that, from a customer's point of view, relying upon a solo SP for his outsourced data is not very promising.

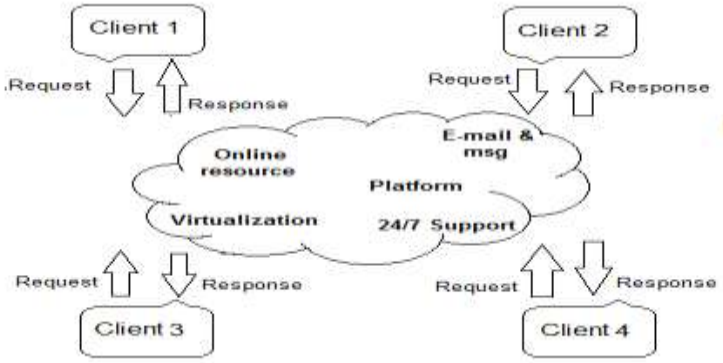

Fig: 1: Basic Cloud Computing Architecture

In addition, providing better privacy as well as ensure data availability, can be achieved by dividing the user's data block into data pieces and distributing them among the available SPs in such a way that no less than a threshold number of SPs can take part in successful retrieval of the whole data block.To address these issues in this paper, we proposed an economical distribution of data among the available SPs in the market, to provide customers with data availability as well as secure storage. In our model, the customer divides his data among several SPs available in the market, based on his available budget. Also we provide a decision for the customer, to which SPs he must chose to access data, with respect to data access quality of service offered by the SPs at the location of data retrieval. This not only rules out the possibility of a SP misusing the customers' data, breaching the privacy of data, but can easily ensure the data availability with a better quality of service.

II. LITERATURE SURVEY

A. Related work:

Privacy preservation [10] and data integrity are two of the most critical security issues related to user data [4]. In conventional paradigm, the organizations had the physical possession of their data and hence have an ease of implementing better data security policies. But in case of cloud computing, the data is stored on an autonomous business party that provides data storage as a subscription service. The users have to trust the cloud service provider (SP) with security of their data. In [7], the author discussed the criticality of the privacy issues in cloud computing, and pointed out that obtaining information from a third party is much easier than from the creator himself. Following the pattern of paradigm shift, the security policies also evolved from the conventional cryptographic schemes applied in centralized and distributed data storage, for enabling the data privacy. Many of the cryptographic approaches have been proposed for hiding the data from the storage provider and hence preserving data privacy [18][19][5], we proposed a scheme in which, the user's identity is also detached from the data [19], and claim to provide public auditing of data. These approaches concentrate on one single cloud service provider that can easily become a bottleneck for such services. One bigger concern that arises in such schemes of cloud storage servicesis that, there is no full-proof way to be certain that the service provider does not retain the user data, even after the user opts out of the subscription. With enormous amount of time, such data can be decrypted and meaningful information can be retrieved and user privacy can easily be breached. Since the user might not be availing the storage services from that service provider, he will have no clue of such a passive attack. The better the cryptographic scheme, the more complex will be its implementation and hence the service provider will ask for higher cost. This could also lead to a monopoly over cloud services in the market. To provide users with better and fair chances to avail efficient security services for their cloud storage at affordable costs, our model distributes the data pieces among more than one service providers, in such a way that no one of the SPs can retrieve any meaningful information from the pieces of data stored on its servers, without getting some more pieces of data from other service providers. Therefore, the conventional single service provider based cryptographic techniques does not seem too much promising. In [16], the authors discussed distributing the data over multiple clouds or networks in such a way that if an adversary is able to intrude in one network, still he can't retrieve any meaningful data, because it's complementary pieces are stored in the other network. Our approach is similar to this approach, because both aim to remove the centralized distribution of cloud data. Although in their approach, if the adversary causes a service outage even in one of the data networks, the user data can't be retrieved at all. This is why in our model, we propose to use a redundant distribution scheme, such as in [17], which at least a 1threshold number of pieces of the data are required out of the entire distribution range, for successful retrieval.

B. Existing system

Cloud computing offers many benefits, but it also is vulnerable to threats. As the uses of cloud computing increase, it is highly likely that more criminals will try to find new ways to exploit vulnerabilities in the system. There are many underlying challenges and risks in cloud computing that increase the threat of data being compromised. To help mitigate the threat, cloud computing stakeholders should invest heavily in risk assessment to ensure that the system encrypts to protect data; establishes trusted foundation to secure the platform and infrastructure; and builds higher assurance into auditing to strengthen compliance. Security concerns must be addressed in order to establish trust in cloud computing technology.

III. SYSTEM MODELS

We will describe our system model and the threat model. Then, we will describe our problem statement we are going to study in this paper.

A. System Overview

We consider the storage services for cloud data storage between two entities, cloud users (U) and cloud service providers (SP). The cloud storage service is generally priced on two factors, how much data is to be stored on the cloud servers and for how long the data is to be stored. In our model, we assume that all the data is to be stored for same period of time. We consider p number of cloud service providers (SP); each available cloud service provider is associated with a QoS factor, along with its cost of providing storage service 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. Hence, the cloud user can store his data on more than one SPs according to the required level of security and their affordable budgets.

B. Threat Model

Customers' stored data at cloud service providers is vulnerable to various threats. Previous studies in [9], [11] discussed in detail that a cloud service provider can be a victim to Denial of service attacks or its variants. In our work, we consider two types of threat models. First is the single point of failure [9], [11], which will affect the data availability, that could occur if a server at the cloud service provider failed or crashed, which makes it harder for the costumer to retrieve his stored data from the server. Availability of data is also an important issue which could be affected, if the cloud service provider (SP) runs out of business. Such worries are no more hypothetical issues; therefore, a cloud service customer can not entirely rely upon a solo cloud service provider to ensure the storage of his vital data. To illustrate this threat we use an example in Fig. 2. Let us assume that three customers (C1, C2 and C3) stored their data on three different service providers (CSP1, CSP2 and CSP3)respectively. Each customer can retrieve his own data from the cloud service provider who it has a contract with.

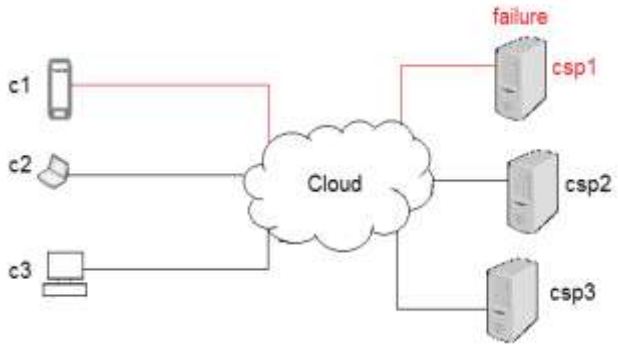

Fig.2. CSP failure

If a failure occurs at CSP1, due to internal problem with the server or some issues with the cloud service provider, all C1's data which was stored on CSP1's servers will be lost and cannot be retrieved. One solution for this threat is that, the user will seek to store his data at multiple service providers to ensure better availability of this data. Our second threat discussed in this paper is the colluding service providers [6], in which the cloud service providers might collude together to reconstruct and access the user stored data. In [16] the authors provide the idea for distributing the data among two storage clouds such that, an adversary cannot retrieve the contents of the data without having access to both the storage clouds.

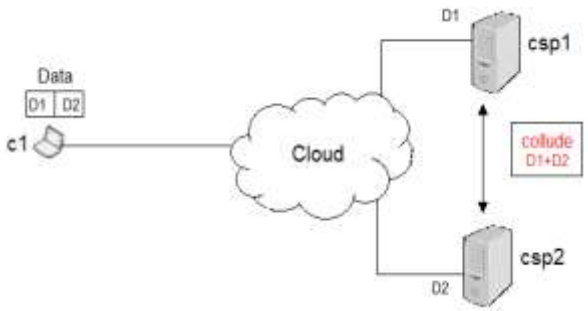

Fig: 3. Colluding cloud service providers

Relying entirely upon a couple of service providers for the storage and retrieval of data might not be secured against colluding service providers. Such an attack scenario is entirely passive, because the cloud user cannot detect that his information has been collectively retrieved from the service providers without his consent. We illustrate the colluding service providers' threat in Fig. 3. Let us assume that two cloud service Providers are available for customer (C1),who wants to store his own data securely.

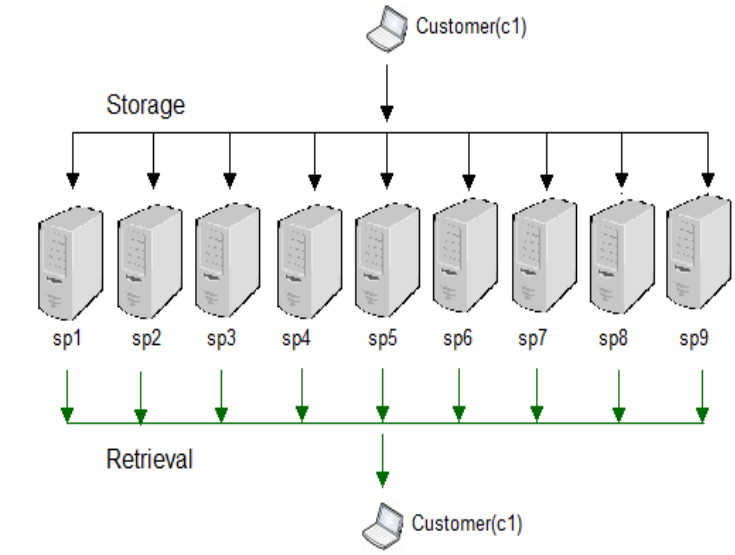

Fig.4. Data Storage and Retrieval

Here he will divide (Fig. 4. Data Storage and Retrieval)his data into two parts (D1 and D2) and distribute these partson the two available CSPs (CSP1 and CSP2) respectively. Thetwo cloud service providers might collude with each other, andexchange the parts of data that the customer has stored on theirserver and reconstruct the whole data without being detectedby the user.

IV. PROPOSED SYSTEM

In this work, to mitigate the threats facing cloud storage, we extended the cloud data storage to include multiple serviceproviders, where each cloud storage represents a differentservice provider. Our motivation behind such an extension isthat, the adversary, similar to any other cloud user, is abstractedfrom the actual clouds of servers implemented by different cloud service providers.

IV.I Implementation Details

Step1:- Select the data (any type of data).
Step2:- Calculate hash value by using Hash algorithm.
Step 3:- Encrypt the data by using AES Algorithm.

Step4:- Divide the data into number of parts
This can be uploaded on different CSP's.
Step5:- Select the data for downloading purpose which is uploaded by same user.
Step6:- Decrypt the data by using AES algorithm.
Step7:- Calculatehash value and compare with the first hash value if match occurs then data which is downloaded is original.

IV.II Parameters

1. Data
   Text,Images, Video,Audio, Pdf.
2. Hash Algorithm

A hash value is a numeric value of a fixed length that uniquely identifies data. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures. You can sign a hash value more efficiently than signing the larger value. Hash values are also useful for verifying the integrity of data sent through insecure channels. The hash value ofreceived data can be compared to the hash value of data as it was sent to determine whether the data was altered. Finding similar records

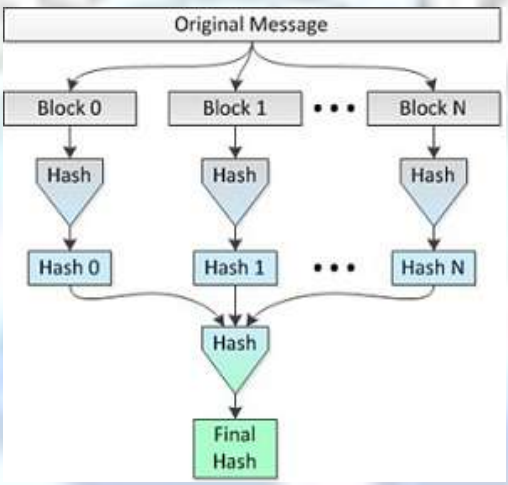

Fig 5: Hash value generation

To hash a message M the following steps are performed:

1. M is paddedwith '1' as many 0's as needed (up to 512)and the original length of M encoded in 64 bits, such that the length of the padded message pad(M) is Divisible by 512.
2. Pad(M) is divided into nblocks of 512 bits, i.e.,pad(M) = m1,m2, . . . ,mn.
3. The 128-bit chaining value h0 is initialized.
4. For i = 1, 2. . .n, hi = H (hi−1,mi) (the compressionFunction is applied).
5. The output is hn.

3. AES Algorithm

AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block sizeof 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits. AES operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field.

High-level description of the algorithm

1. Key Expansion: Round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
2. Initial Round
    1. Add Round Key—each byte of the state is combined with a block of the round key using bitwise xor.
3. Rounds
    1. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
    2. ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
    3. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
    4. AddRoundKey
4. Final Round (no MixColumns)
    1. SubBytes
    2. ShiftRows
    3. AddRoundKey.

V. ADVANTAGE'S

1. Large amounts of data storage.
2. Cloud data storage also redefines the security issues targeted on customer'soutsourced data.
3. Using cryptography technology for data base security
4. Less cost and cost based on client requirements.
5. Easy to maintains large databases with security
6. Avoid database losses.

VI. CONCLUSION

So, we proposed a secured cost-effective multicloud storage in cloud computing, which seeks to provide each customer with a better cloud data storage decision, with considering the user budget as well as provide them the best quality of service (Security and availability of data) offered by available cloud service providers. By dividing and distributing customer's data, our model has shown its ability of providing a customer with a secured storage under his affordable budget.

ACKNOWLEDGMENT

This research was supported by department of computer engineering of Parvatibai Genba Moze College of Engineering Wagholi, Pune University.

REFERENCES

[1]. Amazon.com, "Amazon s3 availability event: July 20, 2008", online athttp://status.aws.amazon.com/s3-20080720.html, 2008.
[2]. "A Modern Language for Mathematical Programming", online athttp://www.ampl.com.
[3]. M. Arrington, "Gmail Disaster: Reports of mass email deletions", Online at http://www.techcrunch.com/ 2006/12/28/gmaildisaster reports-ofmass-email-deletions/, December 2006.
[4]. P. S. Browne, "Data privacy and integrity: an overview", in Proceeding ofSIGFIDET '71 Proceedings of the ACM SIGFIDET (now SIGMOD), 1971.
[5]. A. Cavoukian, "Privacy in clouds", Identity in the Information Society, Dec2008.
[6]. J. Du, W. Wei, X. Gu, T. Yu, "RunTest: assuring integrity of dataflowprocessing in cloud computing infrastructures", In Proceedings of the 5thACM 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 confidentialityfrom cloud computing", Prepared for the World Privacy Forum, onlineat 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 oncloud services", Cloud Computing (CLOUD), 2010 IEEE 3rd InternationalConference on, 5-10 July 2010.
[10]. W. Itani, A. Kayssi, A. Chehab, "Privacy as a Service: Privacy-AwareData Storage and Processing in Cloud Computing Architectures," EighthIEEE International Conference on Dependable, Autonomic and SecureComputing, Dec 2009.
[11]. M. Jensen, J. Schwenk, N. Gruschka, L.L. Iacono, "On Technical SecurityIssues in Cloud Computing", IEEE International Conference on CloudComputing, (CLOUD II 2009), Bangalore, India, September 2009.
[12]. J. Kincaid,"MediaMax/The Linkup Closes Its Doors",Online athttp://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 /security fix/2009/01/payment processor breach may b.html, Jan, 2009.
[14]. M. Dijk, A. Juels, "On the Impossibility of Cryptography Alone forPrivacy-Preserving Cloud Computing", HotSec 2010.
[15]. P.Mell, T. Grance, "Draft NIST working definition ofcloud computing", Referenced on June. 3rd, 2009, onlineathttp://csrc.nist.gov/groups/SNS/cloudcomputing/index.html, 2009.
[16]. P. F. Oliveira, L. Lima, T. T. V. Vinhoza, J. Barros, M. M´edard, "Trustedstorage over untrusted networks", IEEE GLOBECOM 2010, Miami, FL.USA.
[17]. A. Shamir, "How to share a secret", Common. ACM 22, 11(November1979).
[18]. S. H. Shin, K. Kobara, "Towards secure cloud storage", Demo forCloudCom2010, Dec 2010.
[19]. C. Wang, Sherman S.-M. Chow, Q. Wang, K. Ren, W. Lou, "Privacypreservingpublic auditing for secure cloud storage", in InfoCom2010, IEEE,March 2010

AUTHOR'S PROFILE

1]

Ganesh Manaji Yewale, BE Computer, University of Pune-412207

2]

Gunjal Sagar Sharad, BE Computer, University of Pune-412207

3]

Kadam Vaibhav Vasant, BE Computer, University of Pune-412207