IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 4, Issue 1, Feb - March, 2016
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

Data Partitioning From Homomorphism Identification With Dynamic Data

Sangeetha.R, Saranya.A, Anitha.V

**Computer Science & Engineering, GKM College of Engineering & Technology,
Chennai, Tamil Nadu-600 063, India**

Abstract

Cloud computing is also on-demand computing is a kind of internet based computing that provide shared processing resources with the technical support by services providers. To meet the high demands, 'IaaS – Infrastructure as a service' a service is imported which deals with cloud servers and storage. Ensuring the security, relying upon single service provider is not promising. Better privacy can be achieved by dividing the data into blocks and distributing among available servers. The data can be accessed with the help of key provided to the customer. We analyze the performance by performing extensive experiments. The results show that multi cloud obtained in addition of data privacy is very secure in accessing.

Keywords*: Service Provider, Data privacy, Multi cloud, Infrastructure.*

1. Introduction

The use of cloud computing has expanded rapidly in many organizations. Cloud computing provides many benefits in terms of low priced and accessibility of data. Ensuring the security is a major factor in the cloud computing environment, as users continuously save sensitive information with cloud storage providers but these providers may be non-assuring. The "single cloud" leads to failure among customers due to risks of service connection failure and the instance of malicious insiders in the single cloud. A steps forward towards "multi-clouds",has appeared recently. This paper says that recent research related to single and multi-cloud security and tackles possible solutions. It is found that the use of multi-cloud providers to maintain immunity has received less attention from the research community than usage of single clouds. This specialize target to put forward the use of multi-clouds due to its ability to reduce security problems which affects the cloud user. The provable Multiple copy Dynamic data possession in cloud computing deals with stored data in Dynamic way to cloud server. In this the file owner will upload the data in cloud server which automatically splits into three equal parts and stored in the form of encrypted data in three separate servers to avoid server overloading. For this **Key gen** algorithm is used for generation of key. **Key generation** is the process of propagating keys in **cryptography.** A key is used to encode and decode whatever data is being encrypted/ decrypted.

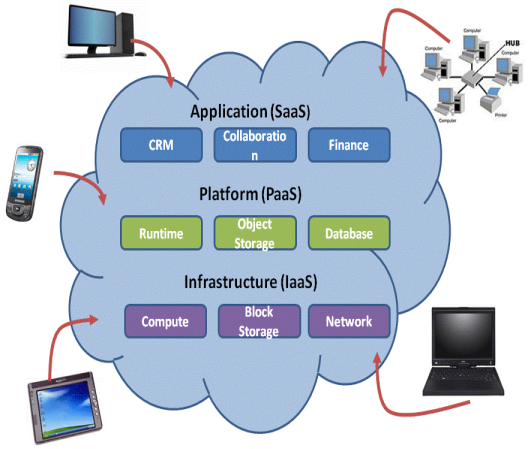

Fig 1: cloud computing architecture

2. Related work

In the cloud computing, the data is stored on a business party provides data storage as a contribution

service. The users have to confide the cloud service provider (SP) with privacy of their data. Following the pattern of shift, the security policies also derived from the typical cryptographic schemes applied in distributed data storage, for easing the data confidentiality. The user's identity is also isolated from the data, and claim to provide public accounting of data. These approaches concentrate on one single cloud service provider that can efficiently become a bottleneck for such services. The sole cryptographic measures are insufficient for ensuring data confidentiality in cloud computing. In cloud storage requires a hybrid model of privacy implementation, appropriated computing and complicated trust ecosystems. To provide the customer with better and fair chances to avail well-organized security services for their cloud storage at affordable costs, our simulation distributes the data pieces between more than one service providers, in such a way that no one of the Service providers can retrieve any consequential information from the pieces of data stored on its servers, without obtaining some more pieces of data from other service providers. Therefore, the single service provider based cryptography does not seem too much promising.

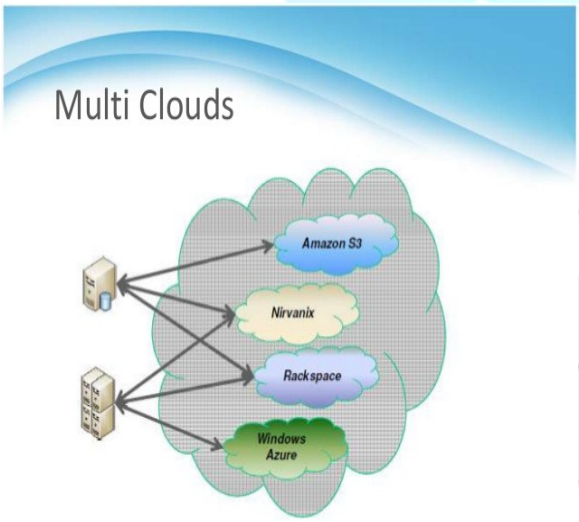

Fig 2: example multi clouds

3. Our contribution

In our system, we use multiple copy dynamic data possession which is deployed in multi – cloud infrastructure. As well as ensure data accessibility, can be achieved by splitting the user's data into pieces and distributing them among the possibility service providers in such a way that no less than a inception number of service providers can take part in successful recovery of the whole data block to address this issues in this paper, we proposed an economical distribution of data among the possible service providers in the market, to provide customers with data accessibility as well as secure storage. In our model, the customer splits his data among several service providers applicable in the market, based on his achievable budget. Also we provide the customer the decision to which service providers he must choose to access data and quality of service offered by the service providers at the location of data recovery. This not only rules out the possibility of a service provider misusing the customers' data, breaching the privacy of data, but can easily ensure the data accessibility with a better quality of service. In addition the data is stored in the encrypted format and decrypted only if the authorized user can access the data. This leads to better privacy than previous system.

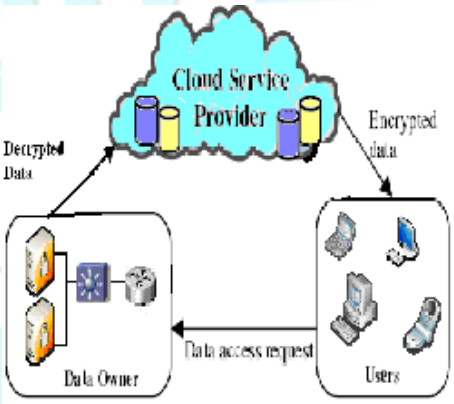

Fig 3: cloud service provider

4. Overview

We first describe the system model consisting of set of cloud service provider, admin has to verify the details of the users who are registering.

4.1 Service provider

Cloud Service provider will provide the service to user. User registers to service provider before uploading the file. After user registration admin verify the user profile and accept the user request. Admin may reject the unauthorized profile details.

4.2 User transmitting with key generation

After verifying the user details by admin, user has to upload the file to cloud server.While uploading the file, data are encrypted and stored in three servers in order to avoid hacking. Key gen algorithm used in data uploading and encrypting. While uploading the data, it is converted into zip file in order to reduce space.

4.3 File requisition

Authorized users are those users only can download the file. The user has to send the file request to admin. User may share their files to another user. Shared user will send the file request to file owner and automatically same request is sent to admin. Then the admin verify with the server and provide the key from file owner. After file owner sends the temporary key to shared user.

4.4 File retrieval and summary

If shared users download the shared file, the temporary key will automatically expire. If the user delete any file, can recover the deleted files from file server. It is very useful to all cloud users.Admin has to generate the reports that how many users register in the cloud.

5. Secured Cost Effective Multi-Cloud Storage

Privacy preservation and data rectitude are two of the most critical security problems related to user data. In conventional prototype, the organizations had the physical possession of their data and hence have an inertness of implementing better data privacy policies. But in case of cloud computing, the data is stored on an independent business party that provides data storage as a pledge service. The users have to trust the cloud service provider (SP) with immunity of their data. Following the pattern of prototype shift, the security policies also evolved from the conservative cryptographic methods applied in centralized and distributed data storage, for enabling the data security. Many of the cryptographic methods have been proposed for veiling the data from the storage provider and hence conserving data privacy. In, the authors projected a method in which, the user's identity is also detached from the data, and profess to provide public accounting of data. These approaches concentrate on one single cloud service provider for such services can easily become a hold in. In, the authors studied and proved that sole cryptographic measures are lacking for ensuring data security in cloud computing. They also argued that the security in cloud storage needs a fusion model of privacy implementation, distributed computing and complex trust ecosystems. One more big concern that arises in such methods of cloud storage services is that, there is no way to be certain that the service provider does not maintain the user data, even after the user prefers out of the pledge. With enormous amount of time, such data can be decoded and eloquent information can be retrieved and user privacy can easily be breached. Since, the user might not be gaining the storage services from that service providers, he will have no clue of such an unreceptive attack. The better the cryptographic pattern, the more complex will be its implementation and hence the service provider will ask for peak cost. This could also head to a monopoly over cloud services in the market. To provide customers with better and fair chances to gain effectual security services for their cloud storage at affordable costs, our model allots the data parts among more than one providers, in such a way that no one of the SPs can retrieve any eloquent information from the parts of data stored, without getting some more parts of data from other service providers. Therefore, the conservative single provider based cryptographic techniques does not seem too much promising. In, the authors discussed distributing the data over multiple networks in such a way that if an opponent is able to interfere in one network, still he cannot reclaimany eloquent data because it's correlative parts are stored in the other network. Our approach is unique to this approach, because both aim to remove the inner more distribution of cloud data. Even though in their approach, if the opponent causes a service outage even in one of the data linkages, the user data cannot be reclaimed at all. This is why in our model we propose to use a surplus distribution pattern, such as

in, in which at least a threshold number of pieces of the data are required out of the whole distribution range, for successful reclaim.

6.Conclusion

Cloud computing is an ongoing technology that allows users to utilize on-demand computation, storage, data services from around the world. In this paper, secured cost-effective multi cloud storage (SCMCS) in cloud computing is proposed, which investigates to provide the customers with a better cloud data storage, taking into consideration the users budget as well as providing the best quality of service offered by possible cloud service providers. By splitting and distributing customer data, our model has shown the customers with a secured storage under his affordable budget.

References

[1] A. Fox, M. Armbrust, M. Grifth, A. V. Joseph, R. Katz, B. Konwinski, C. Lee, L. Patterson, C. Rabkin, I. Stoica, and M. Zaharia, A view of cloud computing, University of California , February 2009.

[2] C.S.Yeo, D. Buyya, S. Venugopal, J. Broberg, and I. Brandic. Cloud computing: Vision, 2009.

[3] N. Dhawas, V. Pranali, “A Multi cloud storage in cloud computing”, Singhad Institute of tech, may 2013.

[4] Cavoukia’s, “Privacy in clouds”, Dec 2008.