ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

MULTICLOUD STORAGE USING LINEAR PROGRAMMING

Karishma Dharmavat*, Apoorva Paygude, Prof. M. K. Nivangune
* Dept.of Information technology, SAE,Kondhwa,pune-48.
Dept.of Information technology, SAE,Kondhwa,pune-48.
Dept.of Information technology, SAE,Kondhwa,pune-48.

ABSTRACT

in our work we are going to use the concept of multi-cloud storage. These multi clouds will be different according to their quality of Service (QOS). That is each one will have different efficiency. the user will upload the file which he wish to, then the file will be uploaded with the help of network in the auditor which will store the data in encrypted form using linear programming in parts which will have unique hash key for each part. Third Party Administrator (TPA) will send the data to the cloud based on its quality of service (QOS) and at this time the user will be kept on waiting. Providing better privacy as well as ensuring data availability.

Auditor will also save the encrypted data in the database too when user wish to download the desired file the auditor. It will match the hash key of the file with the cloud and will send it to user.

KEYWORDS: cloud,multicloud,security,storage,thirdparty administrator(TPA)

INTRODUCTION

In the current scenario usage of cloud computing technique has intensely increased. Huge amount of data being retrieved from geographically distributed from many different sources and non-localize data handling requirements, creates many changes in technological as well as business model. One of the best services offered in cloud computing are cloud data storage in which subscribers data will be stored on the cloud service provider's servers. In cloud computing, subscribers should pay for storing the data on cloud server. This service doesn't only provides flexibility and scalability of data storage but it also provides customer with the benefit to pay only for the amount of data they needs to store for a particular period of time, without any issues with large amounts of data storage. As the technique is widely used there are certain flaws occurring in it such as less security, file integrity, storage problems. In this report, we model the sequence of operations in multi-cloud storage process using linear programming. We are going to use the algorithms such as AES, SHA for the encryption and decryption purpose and for hashing purpose. The third party administrator (TPA) is going to conduct the process of file uploading and downloading. The application is usefull for security and storage purpose.

In our project we are going to use the concept of multi-cloud storage. These multi clouds will be different according to their quality of Service (QOS). That is each one will have different efficiency. the user will upload the file which he wish to, then the file will be uploaded with the help of network in the auditor which will store the data in encrypted form using linear programming in parts which will have unique hash key for each part. Third Party Administrator (TPA) will send the data to the cloud based on its quality of service (QOS) and at this time the user will be kept on waiting. Providing better privacy as well as ensuring data availability.

Auditor will also save the encrypted data in the database to when user wish to download the desired file the auditor. It will match the hash key of the file with the cloud and will send it to the user.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

LITRATURE SURVEY

Privacy preservation and data integrity are two of the most critical security issues related to user data [1]. In conventional paradigm, the organizations had possession of their data and thus had an ease of implementing better data security options. But in case of cloud computing, the data is stored on a business party that provides data storage as a subscription service. The users need to trust the Third party administrator (TPA) for security of their data. In [3] this author Has discussed the criticality of the privacy issues in cloud computing and shown that obtaining an information from a third party is much more 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 [8] [9] [2]. The authors have proposed a scheme which the user's identity is also detached from the data and claim to provide public auditing of data [9]. These approaches concentrate on one single cloud service provider that can easily become a bottleneck for such services. The authors studied and proved that sole cryptographic measures are insufficient for ensuring data privacy in cloud computing [4]. They also argued that the security in cloud storage needs a hybrid model of privacy enforcement distributed computing and complex trust ecosystems. One more issue that arises in such schemes of cloud storage services is that there is no full-proof way to be certain that the service provider does not retains the user data even after the user operates 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 servers/clouds in such a way that no one of the server/cloud can retrieve any meaningful information from the pieces of data stored on its servers without getting some more pieces of data from other servers. Therefore the conventional single service provider based cryptographic techniques does not seem too much promising. In [6], 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 cannot retrieve any meaningful data, because its 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 cannot be retrieved at all. This is why in our model we propose to use a redundant distribution scheme, such as in [7] in which at least a threshold number of pieces of the data are required out of the entire distribution range for successful retrieval.

REQUIREMENT ANALYSIS

Requirements analysis is the process of determining user expectations for a new or modified product.

FUNCTIONAL REQUIREMENT

Functional requirement determines what the system must do. Functional requirement can represent various functions performed by system or work-flows performed by the system. Functional requirement gives a detailed description of what the system is supposed to do and what must the system do.

NON-FUNCTIONAL REQUIREMENT

The non-functional requirement identifies and determines the requirements that should work to assist the project to accomplish its goal. A non-functional requirement determines certain attribute that can be used to judge the operation of a system, which is totally different than judging only the specific behaviour of the system. A non-functional requirement gives a detailed description of what the system shall do. The non-functional requirements for the current system are:

1) Security one of the most important features of any system is its security attribute. There should be one or more requirements about protection of your system and its data. These measurements can be expressed in a different ways (effort, skill level, time) to break into the system. As the proposed system ensures the authentication process before any clustering process begins.
2) Performance there are lots of attribute to determine the performance of the system which includes requirements about resources required, response time, transaction rates, throughput, specifications.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

RESOURCE REQUIREMENT

1) Language:
   Java and JDK Java would be the required as language for development of the project. JDK is the development kit used to compile java programs.
2) IDE: NetBeans
   Just like visual studio provides development environment for VB and .Net, NetBeans provides an integrated development environment (IDE) for Java.
3) Operating system: Window XP or greater

MODELS

Firstly, we would like describe about our system model and the threat model. Next, we would be describing about our problem statement that is to be studied in this paper. Specifically, in this paper the terms cloud server and third party administrator are interchangeable, the terms cloud storage and cloud data storage are interchangeable, not only these, the terms user and customer are also interchangeable.

We would be considering the storage for third party administrator for cloud data storage between two entities; normally one is *cloud users* and *third party administrator*. The *cloud storage service* is generally categorized on the basis of p two factors one is how much data is to be stored on the cloud servers and another is for how long the data is to be stored. In this particular model, we need be assuming that all the data is to be stored for same period of time. We consider *p* number of *third party administrator*, each of them is associated with a *quality of service* factor, along with its cost of providing storage service per unit of stored data (*C*). Every *third party administrator* has a various level of *quality of service* (*QoS*) provided as well as a different cost associated with it. Hence, the *cloud users* can store their data on multiple *TPA*s according to the required level of security and their affordable budgets.

MATHMATICAL MODEL

SET THEORY:

Let s (be a main set of) ≡ {SDB, LDB, C, A, S, MR, AO}
Where, SDB is the copy of the server database. This database is responsible for storing user information related to cloud interactions.

LDB is a set of local database that a user owns. It consists of data tables having data items related to the products and their sales transactions.

C is a set of all clients using the server database and mining services from the server. And (c_1 , c_2 , c_3, ...c_n) Є C.

A is a set of algorithms applied on the input data to get mining results.

S is the server component of the system. The server is responsible for registering, authenticating and providing associations to the end user.

MR is a set of mining rules that are applied on the input dataset provided by the client from his LDB. And (mr_1 , mr_2 , mr_3, ...mr_n) Є MR

AO is a set of associations that are extracted from the input and a form the output of the system.

FUNCTIONALITIES :

SDB' = RegisterUser (uid, password, fullname, address, country, contact, email);
password = SHA1(input_password);
U = AuthenticateUser(uid, password, SDB');
LDB1 = ManageProducts(pid, product name, cost);
LDB2 = ManageBilling(transactions, items);
LDB = LDB1 + LDB2
ED(Encoded data) = EncodeTransactions(LDB2, EncodingAlgorithm(EA));

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

```
UPLOAD(ED);
AO = Apply Mining(ED);
Results = Decode(Download(AO));
```

MULTICLOUD STORAGE

Our proposed approach will provide the a decision model to the cloud computing users, which provides a better security by distributing the data over multiple cloud using third party administrator in such a way that, none of the TPA can successfully retrieve meaningful information from the data pieces allocated at their servers. For maintaining redundancy in data distribution, we can provide the user with better assurance of availability of data. In this case, if a service provider service outage or goes bankrupt, then user still can access their data by retrieving it from other cloud servers. From the business point of view, multi cloud data storage is a payment service, higher the data redundancy, the higher will be the cost which paid by the user. Thus, we can provide an optimization system to handle the cost that a cloud computing user is willing to pay to get a particular level of security for his data. In other words, we can provide a scheme which is used to maximize the security of the cloud data in given budget. The authors discussed distributing the data over multiple clouds servers or networks in such a way that if an antagonist is able to interrupt in one network, still he cannot retrieve any meaningful data; because it's corresponding are stored in other network. Our approach is similar to this approach, because both plan to remove the centralized distribution of cloud data. Although, in their approach, if the antagonist causes a service outage even in one of the data networks, then user data cannot be retrieved at all. This is why in our model, we offer to use a redundant distribution scheme, such as , in which at smallest amount a threshold number of pieces of the data are required out of the entire distribution series, for successful retrieval. We consider the storage services for cloud data storage between two entities, cloud users (U) and third party administrator (TPA). The multi cloud storage service is generally based on two factors, how much data is to be stored on the cloud servers or networks and for how long the data is to be stored on that cloud server. In our model, we assume that the entire the data is to be stored for same period of time. we consider n number of cloud server, and there is one third party administrator(TPA), each available cloud server is associated with a QoS factor, along with its cost of providing storage service per unit of stored data (C). Every cloud server has a different level of quality of service (QoS) ordered as well as a different cost associated with it. Hence, the cloud user can store his data on more than one cloud server according to the required level of security and their adorable budgets.

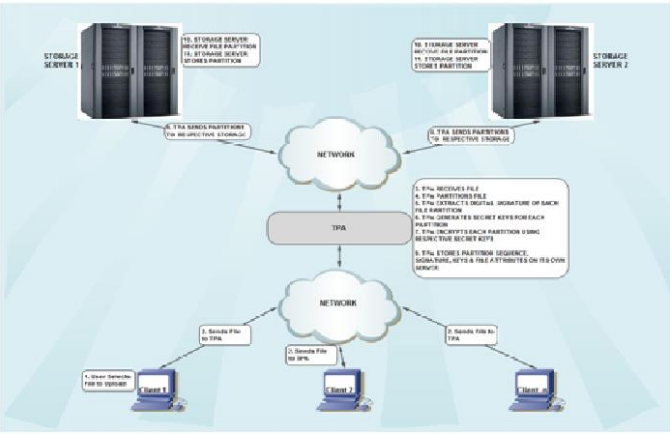

Fig. 1

CONCLUSION

In this paper, we proposed a secured cost-effective multicloud storage (SCMCS) in cloud computing, which seeks to provide each customer with a better cloud data storage decisions, taking into consideration the user budget as well as providing him with the best quality of service (Security and availability of data) offered by available cloud service providers.

REFERENCES

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

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

[2] A. Cavoukian, "Privacy in clouds", Identity in the Information Society, Dec2008.
[3] R. Gellman, "Privacy in the clouds: Risks to privacy and confidentiality from cloud computing", Prepared for the World Privacy Forum, online at /WPF Cloud Privacy Report.pdf,Feb 2009.Online at payment processor breach may b.html, Jan, 2009.
[4] M. Dijk, A. Juels, "On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing", HotSec 2010.
[5] 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.
[6] 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.
[7] A. Shamir, "How to share a secret", Commun. ACM 22, 11(November1979).
[8] S. H. Shin, K. Kobara, "Towards secure cloud storage", Demo for CloudCom2010, Dec 2010.
[9] C. Wang, Sherman S.-M. Chow, Q. Wang, K. Ren, W. Lou, "Privacypreserving public auditing for secure cloud storage", in InfoCom2010, IEEE, March 2010.