MULTI CLOUD STORAGE USING SPLIT ALGORITHM

Mr P.Madhavan[1], M.Anitha [2], P.M.Dhravya [3] , N.Keerthana[4]
Assistant Professor, Department of Computer Science & Engineering, Sri Krishna College of Technology, Kovaipudur, Coimbatore, India[1]

U.G Scholar,Department of Computer Science & Engineering, Sri Krishna College of Technology, Kovaipudur, Coimbatore, India[2,3,4]

ABSTRACT –

In the cloud storage, it is very important to check the Remote Data Integrity. It can make the clients verify whether the data in the cloud is kept intact without downloading their whole data. By using ID-DPDP Protocol the clients store their data in multi cloud storage. It is more efficient in data integrity and flexible.The data is encrypted using private key and stored in multi cloud storage. In the proposed model, large amount of data is also stored by using split algorithm and the modifications made by new users are stored in the database.The users can decrypt the data and are able modify based on their usage.

Index Terms Remote Data Integrity, Encryption, Decryption, private key, Identity-Based Distributed Provable Data Possession in Multi cloud Storage.

I INTRODUCTION

It gives an introduction about the cloud computing and its real time applications. The main idea behind this project is to improve security in accessing the data in the cloud in an efficient manner. Cloud computing is a computing paradigm, where a large pool of systems are connected to private or public networks, to render scalable infrastructure for application, data and file storage. With the arrival of this technology, the expenditure of computation, application hosting, content storage and delivery is reduced significantly. Cloud storage service (e.g. Dropbox, Skydrive, Google Drive, and AmazonS3) is becoming more and more popular in recent years. The objective of the project is Identity-based public key cryptography which can eliminate the complicated certificate management. In provable data possession protocol, it needs public key credentials distribution and management. It will incur considerable overheads since the verifier will check the certificate when it verifies the remote data integrity. In addition to the heavy certificate verification, the system also suffers from the other complex certificates management such as generation of certificate, delivery, revocation, renewals, etc. In cloud computing, most verifiers only have low computing capacity. Identity-based public key cryptography can get rid of the complicated certificate management. In order to increase the performance, identity-based provable data possession is more attractive. They considered multiple cloud service providers to store data in cooperative fashion. A definitional framework and efficient constructions for dynamic provable data possession(DPDP) was used, which extends the PDP model to support provable updates to stored data.

II LITERATURE REVIEW

A. EFFICIENT REMOTE DATA POSSESSION CHECKING IN CRITICAL INFORMATION INFRASTRUCTURES ENSURING DATA STORAGE SECURITY IN CLOUD COMPUTING

1) Cloud computing has been visualized as the on-demand self-service, ubiquitous network access, location independent resource organization, rapid resource elasticity, usage-based pricing and transference of risk. Technical research works focus on Remote data possession Checking protocols license to check that a remote server can access an uncorrupted file with the help of third party verifiers. Seb´e et al.'s protocol is modified to support efficient remote data possession checking in critical information infrastructure without the help of a third party auditor. This design allows users to audit the cloud storage with cipher communication and computation cost. In addition, the auditing result not only ensures strong cloud storage correctness guarantee at the same time achieves fast data error localization, i.e., the identification of misconducting remote server. The design further supports secure and

cost-efficient dynamic operations on outsourced data, including block modification, deletion, and append.

B. IDENTITY-BASED REMOTE DATA POSSESSION CHECKING IN PUBLIC CLOUDS

1) Checking remote data possession is of crucial value in public cloud storage. It enables the users to check that their outsourced data have been kept intact without downloading the primary data. The active remote data possession checking (RDPC) protocols have been designed in the PKI (public key infrastructure) setting. The cloud server has to authorize the users certificates before storing the data download by the users in order to prevent spam. This incurs considerable costs since numerous users may frequently upload data to the cloud server. This paper deals with model of identity-based RDPC (ID-RDPC) protocols. We present the first ID-RDPC protocol proven to be secure assuming the hardness of the standard computational Diffie-Hellman (CDH) problem. In addition to the structural benefit of elimination of certificate management and verification.The ID-RDPC protocol also outperforms RDPC protocols in the PKI setting in terms of computation and communication.

III SCOPE OF RESEARCH

The cloud storage is to store and compute the data in the cloud.The problem is that the modifications made by the users are not stored.It may leads to loss of the owner's data.The large amount of data takes more time to store and retrieve.It takes the information processing as a service, such as storage, computing, Public Key Infrastructure(PKI) is used to check the integrity of the data.

Existing system suffers from many limitations. They are as follows:

- It will incur considerable expense since the verifier will check the certificate when it checks the remote data integrity.
- It is less flexible besides the lower efficiency.

IV PROPOSED METHODOLOGY

A. USER INTERFACE DESIGN

To link with server, user must give their username and password and they can link to the server. If the user already exits they can directly login to the server else user must enrol their details such as username, password, Email id, City and Country into the server. Database will generate the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter to a specific page. It will search the query and display the result.

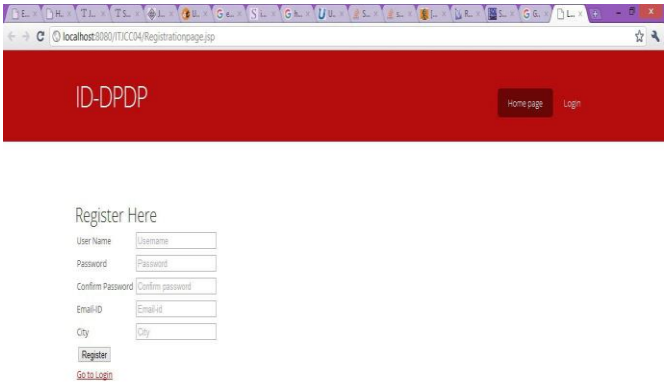

Fig. 1. **User registration**

B. CLIENT MODULE

This module is used to help the cloud owner to view details and upload files with the security. The individual cloud owner contains the key. The Cloud owners view the user
searching details and the counting of file request details. Which has massive data to be stored on the cloud for maintenance and computation, can be either individual consumer or corporation.

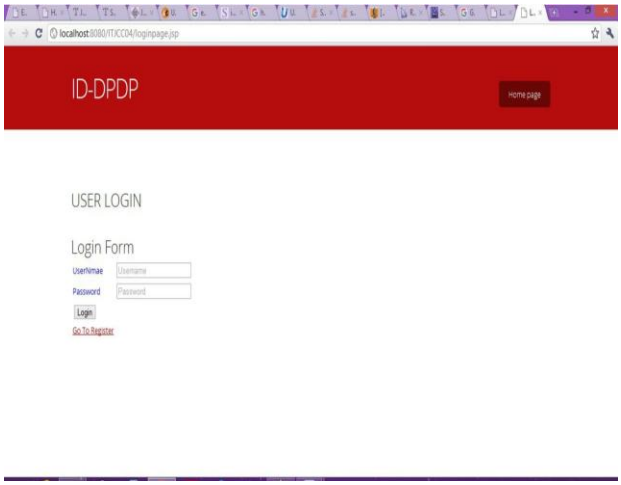

Fig 2.User login

C. PRIVATE KEY GENERATOR

In this module is used to help the Key Generator to generate keys to the cloud owners data and check their data is in safe also provide protection to the data. Because of providing private key any unknown persons are not easily identify our data. when receiving the identity, it outputs the corresponding private key.

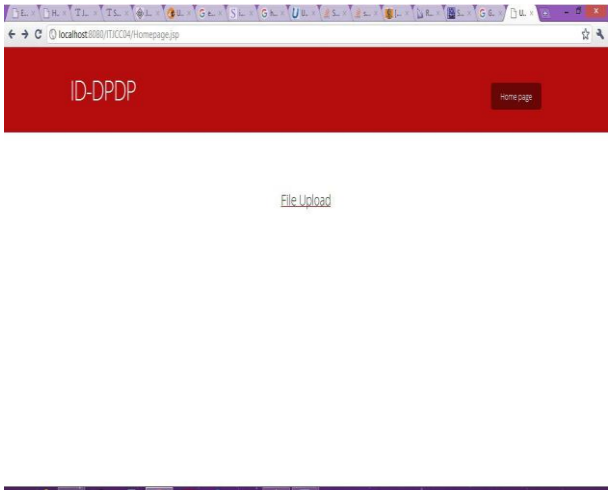

Fig 3.File upload

D. COMBINER

Combiner an entity, which receives the storage request and issues the block-tag pairs to the corresponding cloud servers. When receiving the challenge, it cleave the challenge and issues them to the different cloud servers. When accepting the effect from the cloud servers, it combines them and sends the combined response to the verifier.

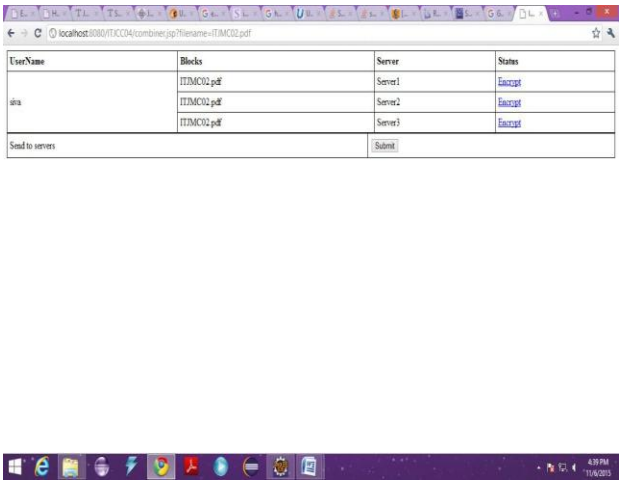

Fig 4.Encrypted files

E. CLOUD SERVER

This module is used to help the cloud server which is managed by cloud service provider, has essential storage space and computation resource to preserve the clients' data. Cloud Servers reside in our world-class data centers , with memory, and fully redundant networking and power all the way to the Client.

F. USER INTEGRATED OUTPUT

This module has developed an efficient method to outsource the policy updating to the cloud server, which can satisfy all the requirements. We have also proposed a sensitive attribute-based access control scheme for big data in the cloud, and depicted policy updating algorithms for different types of access policies.

V RESULT

Thus, it is used for quick upload of the files as it has multi-server as the files are stored in the three clouds. It stores a large amount of files in an encrypted format using private key. The files in the server is downloaded in an decrypted format by using the private key. The combiner combines the files and provide to the users.

VI TECHNIQUES

A. ATTRIBUTE-BASED ACCESS CONTROL

Attribute-based access control (ABAC) defines an access control model whereby access rights are given to users through the use of policies which combine attributes together. The policies can use any type of attributes like user attributes, resource attributes, object, environment attributes etc. This model help Boolean logic, in which rules include "IF, THEN" statements about who is devising the request, the resource, and the action. Unlike Role-Based Access Control (RBAC), which employs pre-defined roles that carry a specific set of advantages associated with them and to which subjects are allocated, the key difference with ABAC is the concept of policies that explicit a complex Boolean rule set that can evaluate various attributes. Attribute values can be set-valued or atomic-valued. Set-valued attributes comprise more than one atomic value. Some of the examples are role and project. Atomic-valued attributes comprise only one atomic value. Examples are clearance and sensitivity. Attributes can be related to static values or to one another, thus authorizing relation-based access control.

B. FILE SPLITTING AND CLUBBING MODULE

In Proposed system, the file is split into different portions then encode and store it on various cloud. Meta data necessary for decrypting and moving a file will be kept in metadata management server. File can stick with another file.The basic plan is to use many clouds at constant time to reduce the risks of malicious knowledge influence, disclosure, and method meddling. This design changed target's confidentiality of knowledge and process logic. The idea of this design is that the applying logic must be divided into small-grained components and these components area unit dispersed to distinct cloud. In coding technique, the user translates the information together with his public key and transfer the cipher texts to the Cloud. The cloud will individually figure on the encrypted knowledge to get an encrypted result, that only the user will decode. The user (or a little trusty non-public cloud) controls the keys and performs the coding operations, whereas the huge computation on encrypted knowledge is processed by an untrusted public cloud.

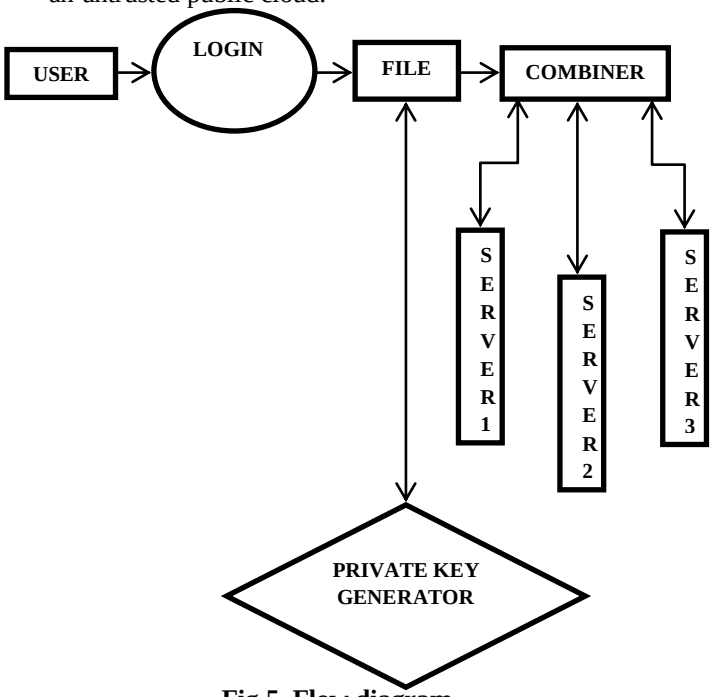

Fig 5. Flow diagram

VII CONCLUSION

In the multi cloud storage the formalized security model is used to provide efficient security and the proposed model is flexible to store a large amount of data. By using split algorithm, the data can be split and stored in three cloud servers. The combiner is integrated within the module which performs both encryption and decryption. The private keys are generated for each cloud server which will keep the data more intact.

VIII REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner,Z. Peterson, and D. Song, ‘‘Provable Data Possession atUntrusted Stores,’’ in Proc. CCS, 2007, pp. 598-609.

[2] G. Ateniese, R. DiPietro, L.V. Mancini, and G. Tsudik, ‘‘Scalableand Efficient Provable Data Possession,’’ in Proc. SecureComm,2008, pp. 1-10.

[3] C.C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,‘‘Dynamic
Provable Data Possession,’’ in Proc. CCS, 2009,pp. 213-222.

[4] F. Sebe´, J. Domingo-Ferrer, A. Martı´nez-Balleste´, Y. Deswarte,and J. Quisquater, ‘‘Efficient Remote Data Integrity Checkingin Critical Information Infrastructures,’’ IEEE Trans. Knowl.Data Eng., vol. 20, no. 8, pp. 1034-1038, Aug. 2008.

[5] H.Q.Wang. (2013, Oct./Dec.). Proxy Provable Data Possession inPublic Clouds. IEEE Trans. Serv. Comput. [Online]. 6(4), pp. 551-559. Available.

[6] Y. Zhu, H. Hu, G.J. Ahn, andM. Yu, ‘‘Cooperative Provable DataPossession for Integrity Verification in Multicloud Storage,’’IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231-2244,Dec. 2012.

[7] Y. Zhu, H.Wang, Z. Hu, G.J. Ahn, H. Hu, and S.S. Yau, ‘‘EfficientProvable Data Possession for Hybrid Clouds,’’ in Proc. CCS, 2010,pp. 756-758.

[8] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, ‘‘MR-PDP:Multiple-

Replica Provable Data Possession,’’ in Proc. ICDCS,2008, pp. 411-420.

[9] A.F. Barsoum and M.A. Hasan, ‘‘Provable possession andreplication of data over cloud servers,’’ Centre Appl. Cryptogr.Res., Univ. Waterloo, Waterloo, ON, Canada, Rep. 2010/32.

[10] Z. Hao and N. Yu, ‘‘A Multiple-Replica Remote Data PossessionChecking Protocol with Public Verifiability,’’ in Proc. 2nd Int.Symp. Data, Privacy, E-Comm., 2010, pp.
84-89.