CLIENT ORIENTED DATA ACCESSING IN PUBLIC CLOUD WITH ENHANCED SECURITY.

[1] Janarthanan.R [2] Badialekhya, [3] Srimathi.S, [4] Sujatha.D

[1] Hod [2] Asst.Professor [3][4] UG Student, Department of Computer Science and Engineering

T.J.S Engineering College

[1] hodcse@tjsenggcollege.com, [2] alekhyareddy1@gmail.com, [3]srimathisankar1996@gmail.com,[4] sujathacse2013@gmail.com

***Abstract*-The cloud security is one of the important role in cloud. New security problems have to be solved in order to help more clients to process their data in public cloud. In our system we are using advanced encryption standard(AES) for encryption to enhance the security. Users login to their account then they upload their files. That files will be stored into the cloud storage and also the content will be encrypted in cloud server. If anyone try to hack at the cloud end, is not possible to break the two different blocks .They need to first decrypt the file and also want to combine the file from three different locations. This is not possible by any one. If anyone want to download the file they want to get the permission from the file owner.**

***Index Terms*- cloud computing, advanced encryption standard,hyper splitting technique.**

I.INTRODUCTION

As the rapid full of computer networks, multi-server architecture has been distributive in many network environments.Along with the rapid development of computing and communication technique, a great deal of data are generated. These massive data needs more strong computation resource and greater storage space. Over the last years, cloud computing satisfies the application requirements and grows very quickly. Essentially, it takes the data processing as a service, such as storage, computing, data security, *etc*. By using the public cloud platform, the clients are relieved of the burden forstorage management, universal data access with independent geographical locations, *etc*. Thus, more and more clients would like to store and process their data by using the remote cloud computing system. In public cloud computing, the clients store their massive data in the remote public cloud servers. Since the stored data is outside of the control of the clients, it entails the security risks in terms of confidentiality, integrity and availability of data and service.

A.MOTIVATION

More and more client would like to store their data to PCS (PUBLIC CLOUD SERVERS).Along with the rapid development of cloud computing.the main motive of our project is to implement multi-server architecture in cloud.the data can be upload and split by three then it can be stored into multi-server.by this way we can achieve secure and efficiency. To enhance the security we are using advanced encryption standard (AES).to split the file we are using hyper splitting technique.in this project we are introducing two more steps.the first step is to split the file into three. And the second step is to encrypt the each splitted file by using AES algorithm.and then the each splitted file is uploaded to the each cloud server.if the file owner is not a mutual user ,then they want to register in a private registerationcentre.else,the file owner is a mutual user ,then they can directly upload the file.

Existing system

In previous, the single server architecture is used to achieve this method. But here security is less, deduct high computation and communication costs, having limited resource management and migration has been occurred.along with the rapid development of cloud computing. New security problems have to be solved in order to help more clients process their data in public cloud. When the client is restricted to access PCS, he will delegate its proxy to process his data and upload them. On the other hand, remote data integrity checking is also an important security problem in public cloud storage. It makes the clients check whether their outsourced data is kept intact without downloading the whole data. From the security problems, we propose a novel proxy-oriented data uploading and remote data integrity checking model in identity-based public key cryptography: ID PUIC(identity-based proxy-oriented data uploading and remote data integrity checking in public cloud). We give the formal definition, system model and security model. Then, a concrete ID-PUIC protocol is designed by using the bilinear pairings. The proposed ID-PUIC protocol is provably secure based on the hardness of CDH (computational Diffie-Hellman) problem. Our ID-PUIC protocol is also efficient and flexible. Based on the original client's authorization, the proposed ID-PUIC protocol can realize private remote data integrity checking, delegated remote data integrity checking and public remote data integrity checking. An efficient distributed scheme with data in the cloud is been made. Here we are using the erasure code technique for distribute the data to cloud locations and access the data from cloud. User can register and login into their account. Provided a option to store, share and access the data from cloud storage. Here we are using the double ensurity scheme for storing data into the cloud. First isyour data or file splited into multiple parts and it will store into different cloud server locations. Each and every file generates the key-code for auditing. Then second is each and every splited file will encrypt before store into different locations. The shared users can edit the file in the cloud with file owner's permission. That file eligible of own public auditing.

Existing Architecture

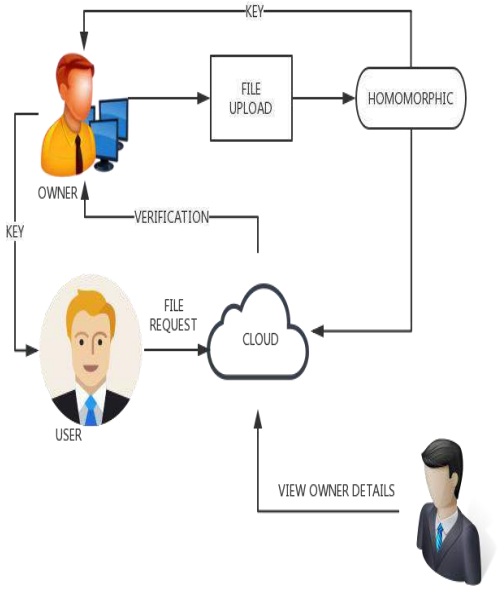

Figure : Existing System

PROPOSED SYSTEM

An efficient distributed scheme with data in the cloud is been made. Here we are using the erasure code technique for distribute the data to cloud locations and access the data from cloud. User can register and login into their account. It Provideda option to store, share and access the data from cloud storage. Here we are using the double ensurity scheme for storing data into the cloud. First is your data or file splited into multiple parts and it will store into different cloud server locations. Each and every file generates the key-code for auditing. Then second is each and every splited file will encrypt before store into different locations. The shared users can edit the file in the cloud with file owner's permission. That file eligible of own public auditing. Search and download the files, at the time of download user should use the security key. As a authentication success it will be decrypt and combine to get the original data from cloud. Moreover, we design a novel public verifiable authenticator, which is generated by a couple of keys and can be regenerated using partial keys. Thus, our scheme can completely release data owners from online burden. In addition, we randomize the encode coefficients with a pseudorandom function to preserve data privacy. Extensive security analysis shows that our scheme is provable secure under random oracle model and experimental evaluation indicates that our scheme is highly efficient and can be feasibly integrated into the regenerating code- based cloud storage.

Proposed Architecture

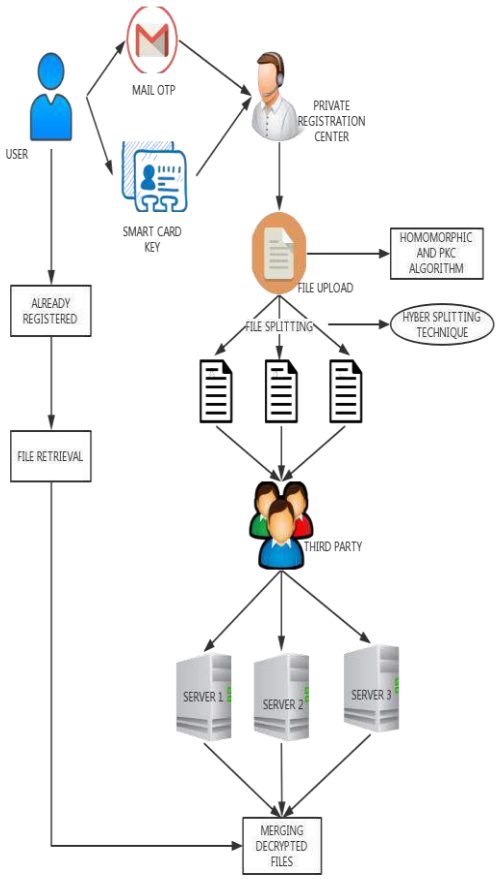

Figure : Proposed system

Literature reviews

A proxy signature scheme is a method which allows an original signer todelegate his signing authority to a designated person, called a proxy signer. Up tonow, most of proxy signature schemes are based on the discrete logarithm problem.In this paper, we propose a proxy signature scheme and a threshold proxy signature[1].we propose afine-grained and heterogeneous proxy re-encryption (FHPRE)system to protect the confidentiality of data owners'cloud data. By applying the FH-PREsystem in cloud, dataowners' cloud data can be securely stored in cloud andshared in a fine-grained manner. Moreover, the heterogeneitysupport makes our FH-PRE system more efficient thanthe previous work. Additionally, it provides the secure datasharing between twoheterogeneous cloud systems, which are equipped with different cryptographic primitives[2].Inorder to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper aflexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded data. It moves the applicationsoftware and databases to the centralized large data centers, where the management of the data and services may not be fullytrustworthy. This unique paradigm brings about many new security challenges, which have not been well understood. This workstudies the problem of ensuring the integrity of data storage in Cloud Computing[3]. In particular, we consider the task of allowing a thirdparty auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPAeliminates the involvement of theclient through the auditing of whether his data stored in the cloud are indeed intact, which can beimportant in achieving economies of scale for Cloud Computing[4].In addition, a practicalDPDP scheme is proposed and implemented for the specificregenerating code, while preserving the combined properties ofdefault data integrity protection, efficient dynamic data updating,fault tolerance and repair traffic saving. Our DPDP scheme isbased on the new *Memory Adversary* model specifically broughtby dynamic operations. It allows different parameters to be finetunedfor the performance-security tradeoff. We implement andevaluate the overhead of our DPDP[5].

References

1.B. Chen, H. Yeh, "Secure proxy signature schemes from the weilpairing", *Journal of Supercomputing*, vol. 65, no. 2, pp. 496-506, 2013

2. P. Xu, H. Chen, D. Zou, H. Jin, "Fine-grained and heterogeneous proxy re-encryption for secure cloud storage", *Chinese Science Bulletin*, vol.59,
no.32, pp. 4201-4209, 2014.

3.C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou, "Toward secure and dependable storage services in cloud computing," *IEEE Transactionson Services Computing*, vol. 5, no. 2, pp. 220-232, 2012.

4.Q. Wang, C. Wang, K. Ren, W. Lou, J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing", *IEEETransactions on Parallel And Distributed Systems* , vol. 22, no. 5, pp.
847-859, 2011

5..P. Xu, H. Chen, D. Zou, H. Jin, "Fine-grained and heterogeneous proxy re-encryption for secure cloud storage", *Chinese Science Bulletin*, vol.59,
no.32, pp. 4201-4209, 2014.

Conclusion

The main purpose of this paper is to use multi-server architecture to enhance the security in public cloud.