HYBRIDCLOUDSTORAGEAPPROACH FOR SECURE AUTHORIZATION AND INFORMATION HIDING

M.Jyothi, S.Kanthimathi, Dr.G.Aravind Swaminathan,M.E.,Ph.D.,
Department of CSE, Department of CSE, Professor/CSE,
Francis Xavier Engineering College.Francis Xavier Engineering College.Francis Xavier Engineering College.
jothipatil17@gmail.comsujithasankar9@gmail.comaravindcse2010@gmail.com

Abstract—With the increasing popularity of cloud data services, data owners are highly motivated to store their huge amount of sensitive personal data files on remote servers in encrypted form. Clients who are in need of retrieving those kind of files can query over the encrypted database while protecting privacy of both the queries and the database, by allowing some reasonable leakage information.Cloud Computing uses the internet to maintain data and applications. Users can store their data to the cloud. The cloud file might contain some sensitive information. Encrypt the whole file.A Sanitizer is used to sanitize the data blocks. The File stored in the cloud able to be shared and used by other.This paper provide more secure and authorized encryption scheme.Our solutions are highly compact, practical and flexible compared to previous schemes.

Index Terms—Hybrid cloud, Encrypted database, dynamic update, cloud computing.

I.INTRODUCTION

Cloud computing means storing and accessing data over internet. Instead of computer's hard drive. Maintenance of cloud computing applications is easy. It is also used as a core technology. User can access emails by mobile or computer from any corner of the world. Many organizations would like to store their data in the cloud. The Data owner upload the data in the cloud. The user can share the data. The shared data stored in the cloud might contain some sensitive information. The Data owner upload the data in the cloud. The user can share the data. The shared data stored in the cloud might contain some sensitive information.In the cloud computing paradigm, providing database-as-a-service (DaaS) allows a third party service provider to host database as a service, providing its customers mechanisms to create, store, and access databases at cloud with requisite storage resource, convenient data access and reduced management and infrastructure costs.

II.RELATED WORK

In previous studies, several authors encrypt the whole file and generate the signature. They proposed an encoding approach which allows identification of files

tomatch the general multi-keyword queries on the basis of data identifier vectors(DIVs). For sanitizing the data blocks, a sanitizer is used. The Sanitizer stores the files into information system and upload in the cloud. Then the user can download the file. The Filethat is stored in the cloud able to be shared andcan be used by others based on the condition.

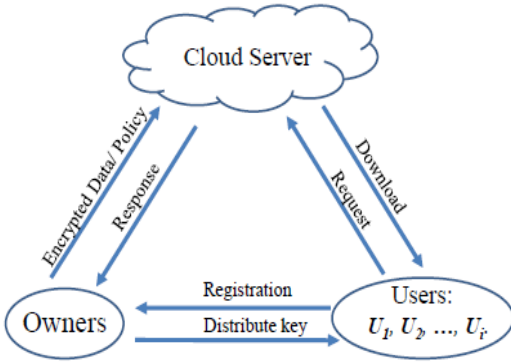

Fig2.1:Workflow of existing system

III.PROPOSED SYSTEM

Our proposed system provides Key aggregate cryptosystem for public key encryption along with Nth degree truncated polynomial ring units. In this process,the secret key holder can release a constant size aggregate key. It is then decrypted with constant size decryption key. After that decryption, sharing of the outsourcing record is done.

NTRU

Nth degree truncated polynomial ring units (NTRU) is the first public key cryptosystem which was founded in 1996. This mechanism helps in speeding up the process. The objects in a truncated polynomial ring is calculated by using the formula,

R=Z[X]/(X^N-1)

The following figure shows the workflow diagram of the proposed system in which the user data is encrypted and send to the cloud and then it is decrypted at the retriever ‘s end.

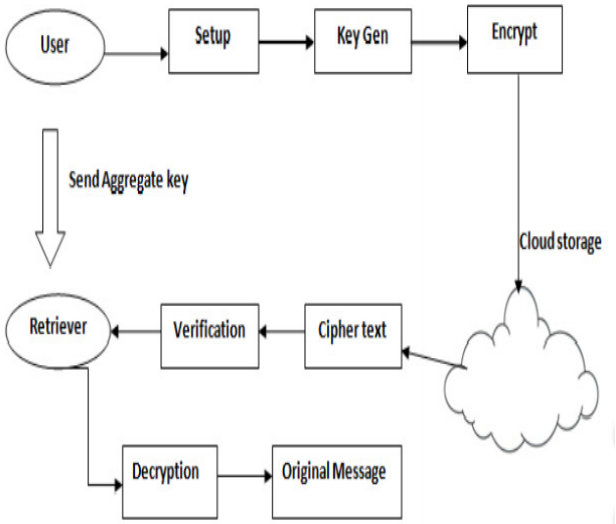

Fig3.1:Workflow of proposed system

A.Aggregate key generation

This process is executed by the data owner to randomly generate a public/master-secret key pair. This key executed by the single person, in case the retriever itself share the key to others it does not work. This key generated for each user by the data owner as well as it does not maintained by the cloud service provider. This key should be managed by individual, the cloud service provider stores the key for authentication purpose only.

B.User account creation

User is the data owner he/she generates the data and upload to cloud and generates key for retriever. All the data's should be encrypted while file uploading process. This encryption process is executed by anyone who wants to encrypt data. On input a public-key PK, an index I denoting the cipher text class, and a message m, it outputs a cipher text. But in our project this process for the user.

C.Receiver

This process is executed by the data owner to setup an account on an untrusted server. On input a security level parameter and the number of cipher text classes n (i.e., class index should be an integer bounded by 1 and n), it outputs the public system parameter, which is omitted from the input of the other algorithms for brevity.

D.Setup

The retriever is the person who wants to view the uploaded data. The data is associated with attributes so the authenticated retrievers only view the original data. To authenticate the retriever we have verification phase in that retriever credentials are verified. After that while the retriever searching and view the data they should have corresponding aggregate key.

IV.EXECUTION AND RESULT

In previous studies, the out sourcing record does not have any prior permission. There is no option to outsource the permitted records. In the proposed system, getting permission is easy and outsourcingis allowed only forthe permitted records.This paper provide more secure and authorized encryption scheme which is more efficient than previously existing systems.

V.CONCLUSION

In this paper, we used NTRUpublic key cryptosystem scheme for processing queries over large-scaled encrypted databases. By using this, the query efficiency and query privacy, with flexible query functionalities. Due to its strong security analysis and security model, it provides more security of the files stored in cloud.

V.REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *IEEE Internet Comput.*, vol. 1 6, no. 1, pp. 69–73, Jan. 2012.

[2] G. Atenieseet *al.*, "Provable data possession at untrusted stores," in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, 2007, pp. 598–609.

[3] A. Juels and B. S. Kaliski, Jr., "Pors: Proofs of retrievability for large files," in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, 2007, pp. 584–597.

[4] H. Shacham and B. Waters, "Compact proofs of retrievability," *J. Cryptol.*, vol. 26, no. 3, pp. 442–483, Jul. 2013.

[5] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," *IEEE Trans. Comput.*, vol. 62, no. 2, pp. 362–375, Feb. 2013