# SECURE DATA RETRIEVAL IN CLOUD USING LINEAR SECRET SHARING MESSAGE AUTHENTICATION

S.Jananee[1], D.Anne Priya[2], K.Malini[3]
[1,2,3]Assistant Professor , C. Abdul Hakeem College of Engineering& Technology

**Abstract**
**Cloud computing is a technology which provides on-demand self-services to store and retrieve large amount of data through internet services. Due to the nature of cloud computing (multi tenancy) and the volume of data stored on the cloud, the data security capability is more important for future cloud. This technology also faces some challenges in encrypting the data and securing the data, where data owner stores confidential data in an untrusted cloud server, where stored data can be used for sharing. When the fine -grained access control is used, it requires huge computation for key distribution and data management. When the counter mode of encryption is used, it can encrypt the data at high speed but it cannot provide message authentication and protection against bit-flipping attacks. Galois counter mode of encryption is used to overcome these problem by sharing the confidential information by sharing the secret key and it can be achieved with the help of Linear Secret Sharing scheme(LSSs). Secret key is shared only if authorized subset of parties are available to reconstruct the secret. The proposed scheme will overcome the problem of computation complexity and provides confidentiality along with privacy and also it avoids re-encrypting the sensitive data.**

**Keywords: cloud computing, counter mode, Linear secret sharing, message authentication.**

## I. INTRODUCTION

Cloud computing is a technology that provides on demand computing services, and it is mainly used for data storage. But practically, data stored in the cloud is not safe, and there is a chance of data missing, therefore we don't have any physical backup or local backup. So, cloud becomes insecure. To provide security in cloud, we use some techniques that provide confidentiality to the stored data.

Firstly, the data is to be encrypted with proper encryption method. Here, we are using Galois Counter mode with AES encryption. This Galois counter mode operates by using block cipher mode which uses universal hashing over binary Galois. This field provides the authenticated encryption and implemented in the hardware to achieve high speeds and reduces the cost and latency. This mode should admit parallelized and pipelined implementations and have the computational latency at the minimum rate for the usage of high data rates.

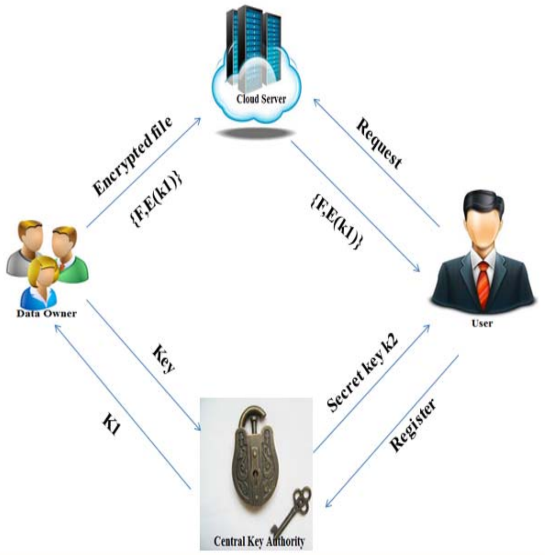
The best method for high-speed encryption is Counter mode because it satisfies those requirements and therefore there may not be a suitable standard message authentication algorithm. Due to this fact there occurs a situation which we can decrypt at high speed, but cannot provide message authentication that can keep up the cipher. This lack is especially conspicuous since counter mode provides no protection against bit-flipping attack. Only GCM meet these needed criteria but others are not meeting these criteria.

The data stored in the cloud should be made secured with the help of a secret key. There are many techniques available for generating the secret key but choosing the correct method for providing data privacy and security is most important. Yu Fang et al proposed that in the Cipher text-Policy Attribute-Based Encryption(CP-ABE), the user's private key contains cipher text and a set of attributes, which specifies the access policy for the attributes within the system in which the user will be able to decrypt a cipher text to obtain the original data.

But, the problem is, if the user leaves the system, the entire data has to be re-encrypted which results in time complexity. To overcome this, we are using a technique called Linear Secret Sharing scheme (LSSS).Secret Sharing scheme is established with the owner, who has a secret data with a set of parties. The information is shared by the Data owner to the parties only if they are available in subsets.

A secret sharing scheme will be linear if the distribution function is linear (i.e.), for any piece of every party, there will be a 'constant' such that for any r and s where r is a random vector and s is the secret key. GCM mode of encryption and LSSS are used to achieve the privacy and confidentiality. This privacy and confidentiality makes the cloud user to effectively store and retrieve the data from the cloud, and prevent it from the data loss and makes the data to be more secured from the attackers.

## II. SYSTEM ARCHITECTURE:



**Architecture of Counter Mode Encryption**

The system model consists of four entities such as, Cloud server, Data owners, user and the central key authority. Data owners stores the confidential information in cloud in an encrypted form along with the secret key. By using GCM mode of AES encryption, secret key will be generated and it is provided to the key authority. By using the Central key authority the secret key is splitted into two parts. One part of the key will be attached with the encrypted file and the other part of the key will be with the key authority.

The data owner sends the encrypted information along with secret key {F, E(K1)} which will be stored in the cloud servers. This information will be provided to the user after receiving their request and by checking their reputation. Data user is solely responsible for accessing the encrypted file and it can be decrypted with the secret key. But the user will receive only a part of the secret key and to get the second part of the secret key K2, the user has to register with the central key authority. The key authority checks for the valid user. If it is a valid user the secret key will be provided and the user can decrypt the file and access the whole information from the file. If it is an invalid user the request will be dropped.

## III. COUNTER MODE SECRET SHARING SCHEMA:

This schema is implemented by using an algorithm to efficiently retrieve the data stored on the cloud systems. The data owner stores the confidential information on the cloud, secrecy can be achieved by encrypting the data using the Galois counter mode of Advanced Encryption Standard (AES). This GCD mode of encryption will encrypt the data and generates the key. This secret key is sent to the central key authority. The key authority will split the secret key and sends a part of the key to the data owner. The data owner will in turn send the key along with the encrypted file to the cloud server.

The data user has to request cloud server before accessing the data. Once the request is sent to the cloud server it checks for the valid user. If it is a valid user the server provides the requested users service. If it is not a valid user the server will rejects the particular user request. Once the valid user request is accepted the encrypted file is received from the server, the user requires another key to decrypt the data. To get another part of the secret key the user has to register it with the central key authority. This authority will provide the key to the user to decrypt the original data.

| S.NO | SYMBOL | DESCRIPTION |
|---|---|---|
| 1 | DO | Data Owner |
| 2 | CKA | Central Key Authority |
| 3 | CS | Cloud Server |
| 4 | DU | Data User |
| 5 | K | Secret key |
| 6 | E(F) | Encrypted File |
| 7 | E(K) | Encrypted Key |

Table 3.1 Description of symbols

## IV. ALGORITHM FOR COUNTER MODE SECRET SHARING:

Data owner shares the data with the central key authority and cloud server.

DO $\xrightarrow{\text{secret key}}$ CKA

Central key authority splits the key into two parts as K1 and K2.

CKA $\xrightarrow{\text{secret key 1}}$ DO

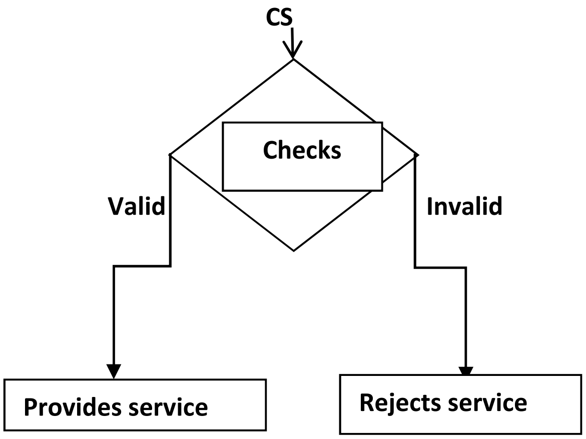
Data owner shares the encrypted data along with the secret key to cloud server.

DO $\xrightarrow{\{E(F),E(K1)\}}$ CS

Data user can access the encrypted file by requesting the cloud server.

DU $\xrightarrow{\text{Request}}$ CS

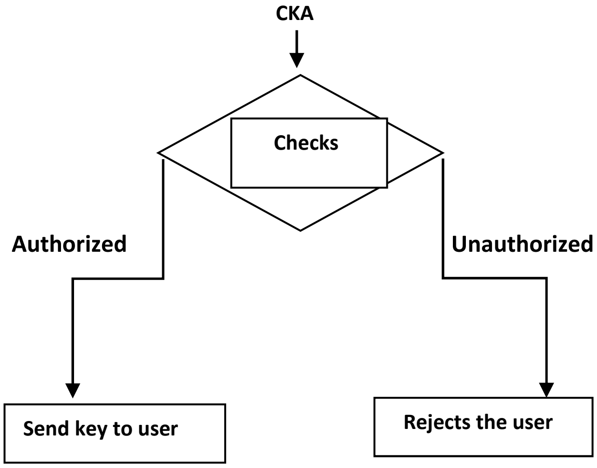
Cloud server will accept the request and checks whether a valid user or not.



Data user will get the encrypted information along with secret key k1. But, it needs another secret key k2 to decrypt the information. Data user has to register to the central key authority to get the second key.

DU $\xrightarrow{\text{Register}}$ CKA

Central key authority checks with the data owner whether he is an authorized user or not.



Now, the data user will get the secret key k2 and with the help of this key the user can decrypt the encrypted file.

## V. SECURITY ANALYSIS:

The CTR mode does not provide integrity which means message integrity will not be provided by this encryption.

The cipher text by a MAC is accompanied whenever there is a need for message integrity. The CBC mode will be more effective than MAC which is strongly required for CTR. This is the major concern because it is wrong that mode will be providing the meaningful integrity. It propagates the error, when a block of cipher text contains some bit-flip errors. But it is irrelevant because whenever the detection or correction of errors is needed.

Another drawback will be stateful encryption. the sender is stateful but when we looks at the CBC mode, the sender is also stateful this is because when the block is enciphered and also at the same state we should respect statefulness and this is called as stateful encryption.

The value used for counter in CTR mode is reused then all the security will be lost because the sensitivity to the user will be one of the disadvantages. Another disadvantage in CTR mode is that when the attacker obtains the pairs of plaintexts then it would be facilitating in the differential crypt analysis. But it is not correct mode to compensate the weakness in CTR mode. There is no integrity, error propagation, stateful encryption, sensitive to usage error, interaction with weak cipher are also some of the disadvantages. We overcome all these bottlenecks in our paper by implementing counter mode secret sharing algorithm.

## VI CONCLUSION:

The counter mode secret sharing algorithm can be implemented for two or more systems. This method provides more confidentiality and privacy to the cloud storage systems for the efficient data storage and retrieval of data. This method overcomes error propagation, stateful encryption, sensitive to usage error, interaction with weak cipher and integrity propagation.

## VII FUTURE WORK

In this paper, we have implemented the counter mode secret sharing algorithm for two systems. As a future work, we can extend to a group of systems which can be created as a network . For this network we can implement the algorithm to acquire more privacy and confidentiality.

## REFERENCES:

1. Waters B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography (PKC'11), May 6−9, 2011, Taormina, Italy. LNCS 6571. Berlin, Germany: Springer-Verlag, 2011: 53−70

2.Yang K, Jia X, Ren K. Attribute-based fine-grained access control with efficient revocation in cloud storage systems. Proceedings of the 8th ACM SIGSAC International Symposium on Information, Computer and Communications Security (ASIACCS'13), Mar 8−10, 2013, Hangzhou, China. New York, NY, USA: ACM, 2013: 523−528

3.Yang K, Jia X. Security for cloud storage systems. New York, NY, USA: Springer, 2014: 39−58

4.Hur J, Noh D K. Attribute-based access control with efficient revocation in data outsourcing systems. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(7): 1214−1221

5.J.-M. Do, Y.-J. Song, and N. Park, Attribute based proxy re-encryption for data condentiality in cloud computing environments, in Proceedings of the 1st International Conference on Computers,Networks, Systems and Industrial Engineering. Los Alamitos, USA: IEEE Computer Society,2011, pp. 248-251.

6. M. Nabeel, N. Shang and E. Bertino, Privacy preserving policy based content sharing in public clouds. IEEE Transactions on Knowledge and Data Engineering, Vol. 25 (11), 2012, pp. 2602-2614.

7. B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography, ser. Lecture Notes in Computer Science, vol. 6571. Springer, 2011, pp. 53–70.

8. A. B. Lewko and B. Waters, "Decentralizing attribute-based encryption," in EUROCRYPT, ser. Lecture Notes in Computer Science, vol. 6632. Springer, 2011, pp. 568–588.

9. Z. Liu, Z. Cao, Q. Huang, D. S. Wong, and T. H. Yuen, "Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles," in ESORICS, ser. Lecture Notes in Computer Science, vol. 6879. Springer, 2011,pp. 278–297.

10. A. B. Lewko and B. Waters, "New proof methods for attribute-based encryption: Achieving full security through selective techniques," in CRYPTO , ser. Lecture Notes in Computer Science, vol. 7417. Springer, 2012, pp. 180–198.

11. Z. Liu, Z. Cao, and D. S. Wong, "White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures," IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 76–88, 2013.

12. Y. Rouselakis and B. Waters, “Practical constructions and new proof methods for large universe attribute-based encryption,”in ACM Conference on Computer and Communications Security. ACM, 2013, pp. 463–474.

13. Z. Liu, Z. Cao, and D. S. Wong, “Blackbox traceable CP-ABE: how to catch people leaking their keys by selling decryption devices on ebay,” in ACM Conference on Computer and Communications Security. ACM, 2013, pp. 475–486.

14. Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak," Decentralized access control with anonymous authentication of data stored in cloud" in IEEE transactions on parallel and distributed systems, vol-25,No.2,2014.

15. Song Lingwei, Yu Fang, Zhang Ru, Niu Xinxin "Method of secure, scalable and fine-grained data access control with efficient revocation in untrusted cloud" April 2015, 22(2): 38–43.