International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

# Providing High Securtiy for Encrypted data in cloud

**Aswin kumar S[1], Kirubakaran A[2], Mothish A[3], Venkatesan V[4], Anitha M[5]**

[1,2,3,4]*UG Scholar, Department of Computer Science Engineering, Kingston Engineering College, Tamilnadu, India.*
[5]*Assistant Professor, Dept. of Computer Science & Engineering, Kingston Engineering college, Tamilnadu , India.*

---

**Abstract -** *Secure pursuit strategies over encoded cloud information enable an approved client to inquiry information documents of enthusiasm by submitting scrambled question catchphrases to the cloud server in a protection safeguarding way. The practically speaking, the returned question results might be mistaken or deficient in the exploitative cloud condition. we outline a protected, effectively incorporated, and fine-grained question comes about confirmation instrument, by which, given an encoded inquiry comes about set, the question client not exclusively can check the rightness of every information record in the set yet in addition can additionally check what number of or which qualified information documents are not returned if the set is inadequate before unscrambling. The check plot is free coupling to concrete secure inquiry procedures and can be effectively coordinated into any safe question conspire. We accomplish the objective by building secure check question for scrambled cloud information. Topography can exacerbate the effects of pollutants, trapping them inside a limited area or making it easy for pollutants to settle instead of being swept away by winds. Load balancing in the cloud computing environment has an important impact on the performance.*

***Key Words***: Cloud computing, Trapdoor key, Decryption, AES Algorithm, Object verification.

## 1. INTRODUCTION

Cloud computing means storing the data, and accessing the data in remote. When you upload the files in cloud, you will be able to access or download the file anytime and anywhere and from any device. An example of a cloud computing provider is Google's Gmail and Drive.

By using the concept of cloud computing this project includes some advanced level security by using the three private keys. Data user, Data owner plays a major role. First data owner wants to login/register, then they are allowed to upload the files in the cloud and allows to verifies the data users to give permission to access their files. Data user also need to login/register, then only they are able to search or request file that can be uploaded by the data owner. The cloud can be verify the data owner. Once the data owner verifies the data user, the three keys will be provided to data user the registered mail id. The three keys namely trapdoor key, file decryption key, object verification key. By using three keys only the data user can be able to access the files in the cloud. The files can be uploaded by the data user in the cloud, it can be uploaded after the encryption. AES algorithm can be used to encrypt the file. That file can't be read without decrypting it. Third key called object verification key, this key consists of two keys. The two key is mainly provided for checking whether any hacker/attacker are tried to access the data. If hackers try to overcome these process, one of the object verification key will be automatically changed. By seeing the changes in object verification key, data owner have to know that the data can be tried to access by some unauthorized person.

## 2. ANALYSIS OF PREVIOUS METHOD

Our understanding about previous method, it only matter of public concern is how to guarantee the security of data that is outsourced to a remote cloud server and breaks away from the direct control of data owners. Encryption on private data before outsourcing is an effective measure to protect data confidentiality. However, encrypted data make Effective data retrieval a very challenging task. First introduced the concept of searchable encryption and proposed a practical technique that allows users to search over encrypted data through encrypted query keywords. Later, many searchable encryption schemes were proposed based on symmetric key and public-key setting to strengthen security and improve query efficiency with the growing popularity of cloud computing, how to securely and efficiently search over encrypted cloud data becomes a research focus. Some approaches have been proposed based on traditional searchable encryption schemes.

In existing system, the cloud server may return erroneous or incomplete query results once they behaves dishonestly for illegal profits. A latent space with lower-dimensionality while preserving important discriminative features amongst users. To learn an effective latent representation, we simultaneously incorporate prior knowledge, such as temporality of wellness features and heterogeneity of users. They first present the notations and then formally define the problem of representation learning of longitudinal data.

## 3. PROPOSED SYSTEM

A secure and fine-grained query results verification scheme by constructing the verification object for encrypted outsourced data files. When a query ends, the query results set along with the corresponding verification object are returned together, by which the query user can accurately verify: 1) the correctness of each encrypted data file in the

results set; 2) how many qualified data files are not returned and 3) which qualified data files are not returned. Furthermore, our proposed verification scheme is lightweight and loose-coupling to concrete secure query schemes and can be very easily equipped into any secure query scheme for cloud computing. Just as possibly tampering or deleting query results, the dishonest cloud server may also tamper or forget verification objects themselves to make the data user impossible to perform verification operation. Specially, once the cloud server knows that the query results verification scheme is provided in the secure search system, this information may leak query user's privacy and expose some useful contents about data files. More importantly, this exposed information may become temptations of misbehavior for the cloud server.

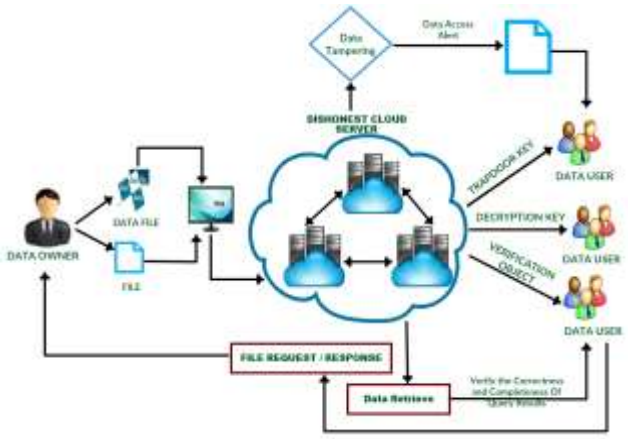


**Fig-1** : Proposed diagram

## 4. MODULES

### 4.1. QUERY RESULTS VERIFICATION

The query result verification mechanism allows the data user to verify the results. In this project, we designed a safe, easy to integrate Fine-grained query results validation mechanism, by giving a given query result set, the query user can not only verify The correctness of each data file in the collection can also be further checked if the collection does not return how many or which qualified data files

### 4.2. OUTSOURCING ENCRYPTED FILE

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction. The data owner will outsource the encrypted file to the cloud server, automatically three different keys will be generated for the file.

We propose a secure, easily integrated, and fine-grained query results verification scheme for secure search over encrypted cloud data. Different from previous works, our scheme can verify the correctness of each encrypted query result or further accurately find out how many or which qualified data files are returned by the dishonest cloud server. A short signature technique is designed to guarantee the authenticity of verification object itself. Moreover, we design a secure verification object request technique, by which the cloud server knows nothing about which verification object is requested by the data user and actually returned by the cloud server. Performance and accuracy experiments demonstrate the validity and efficiency of our proposed scheme.

### 4.3. VERIFICATION OBJECT CONSTRUCTION

To maximize reduce storage and communication cost and achieve privacy guarantee of the verification objects. Trapdoor key, verification object key and decryption key is automatically constructed. The trapdoor key is basically differentiate the data owner and hacker.

### 4.4. VERIFICATION OBJECT SIGNATURE AND AUTHENTICATION:

When a query ends, the query results set and corresponding verification object are together returned to the query user, who verifies the correctness and completeness of query results based on the verification object. Our proposed query results verification scheme not only allows the query user to easily verify the correctness of each encrypted data file in the query results set, but also enables the data user to efficiently perform completeness verification before decrypting query results.

### 4.5. UNAUTHORIZED DATA ACCESS ALERT

When the cloud server or unauthorized person gains the access of the information or data which is stored by the user. The data user will get alert whenever anyone try to access the data or information. We can prevent from accessing the user information or data by verifying the verification object.

### 4.6. UNAUTHORIZED DATA ACCESS ALERT

When the cloud server or unauthorized person gains the access of the information or data which is stored by the user. The data user will get alert whenever anyone try to access the data or information. We can prevent from accessing the user information or data by verifying the verification object.

## 5. Conclusion:

We propose a secure, easily integrated, and fine-grained query results verification scheme for secure search over encrypted cloud data. Different from previous works, our scheme can verify the correctness of each encrypted query result or further accurately find out how many or which qualified data files are returned by the dishonest cloud server. A short signature technique is designed to guarantee the authenticity of verification object itself. Moreover, we design a secure verification object request technique, by which the cloud server knows nothing about which verification object is requested by the data user and actually returned by the cloud server. Performance and accuracy experiments demonstrate the validity and efficiency of our proposed scheme.

## 6. REFERENCES

[1] N. Park and D. J. Lilja, "Characterizing datasets for data dedupli- cation in backup applications," in Proc. IEEE Int. Symp. Workload Characterization (IISWC), 2010, pp. 1–10.

[2] A. ODriscoll, J. Daugelaite, and R. D. Sleator, "Big data, hadoop and cloud computing in genomics," J. Biomed. Inform., vol. 46, no. 5, pp. 774–781, 2013.

[3] P. C. Zikopoulos, C. Eaton, D. DeRoos, T. Deutsch, and G. Lapis, Understanding Big Data. New York, NY, USA: McGraw-Hill, 2012.

[4] M. Dong, H. Li, K. Ota, and H. Zhu, "HVSTO: Efficient privacy preserving hybrid storage in cloud data center," in Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), 2014, pp. 529–534.

[5] J. Li, Y. K. Li, X. Chen, P. P. Lee, and W. Lou, "A hybrid cloud approach for secure authorized deduplication," IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 5, pp. 1206–1216, May 2015.

[6] M. Dutch. (2008, Jun.). SNIA: Understanding Data De-Duplication Ratios [Online]. Available: http://www.snia.org/sites/default/files/ Understanding_Data_De-duplication_Ratios-20080718.pdf

[7] M. Dong, H. Li, K. Ota, L. T. Yang, and H. Zhu, "Multicloud-based evacuation services for emergency management," IEEE Cloud Comput., vol. 1, no. 4, pp. 50–59, Nov. 2014.

[8] J. Long, A. Liu, M. Dong, and Z. Li, "An energy-efficient and sink- location privacy enhanced scheme for WSNS through ring based rout- ing," J. Parallel Distrib. Comput., vol. 81, pp. 47–65, 2015.

[9] M. Wen, R. Lu, K. Zhang, J. Lei, X. Liang, and X. Shen, "PaRQ: A privacy-preserving range query scheme over encrypted metering data for smart grid," IEEE Trans. Emerging Topics Comput., vol. 1, no. 1, pp. 178–191, Jun. 2013.