Achieving Universal Assured Fine-Grained Query Result Verification for Secure Search Scheme over Encrypted Cloud Data

Mrs.N.Haripreethi[#1], Mr.V.Gnanasekar,M.E[*2] ,Mr.K.Sathish,M.E[#3].

*[#1]Pursuing M.E. Computer Science and Engineering, [*2]Head of the Department of Computer Science and Engineering, [#3]Assistant professor in Department of Computer science and Engineering, Gojan School of Business and Technology, Redhills, Chennai, 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. In any case, practically speaking, the returned question might be mistaken or deficient in the exploitative cloud condition. For instance, the cloud server may deliberately preclude some qualified outcomes to spare computational assets and correspondence overhead. In this manner, a well-working secure inquiry framework need to provide a question comes about check system that permits the knowledge client to verify comes about. In this paper we outline a protected, efficiently included, and fine-grained question comes about corroboration instrument, by which, given an prearranged inquiry comes about set, the query client not wholly can check the rightness of every in order record in the set yet in addition can as well 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 may be effectively coordinated into any safe question conspire. We accomplish the target by building secure check question for scrambled cloud information. Moreover, a short mark strategy with greatly little stockpiling cost is proposed to ensure the credibility of confirmation protest and a check question ask for method is introduced to enable the inquiry client to safely get the coveted check protest. Execution assessment demonstrates that the proposed plans are down to earth and proficient.*

I. INTRODUCTION

In a process of searching, for a query that has returned in which the result may contain various data of encrypted form, in such cases the user has to verify each and every data files for the correctness or he has to check which appropriate files are not returned on earth if the cloud server intentionally omits some query results. These information can be regarded as a hard evidence to punish the cloud server.

This is challenging to realize the fine-grained verifications since the query and verification are enforced within the encrypted environment. We proposed 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. our proposed verification scheme is lightweight and loose-coupling to concrete secure query schemes and can be easily equipped into any secure query scheme for cloud computing.

More importantly, in the dishonest cloud environment, the scheme suffers from the following two important security problems: 1) 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, he may return in veracious verification object to escape responsibilities of misbehavior. 2) When a data user wants to obtain the desired verification object, some important information will be revealed such as which verification objects are being or have been requested before frequently, etc. More importantly, these exposed information may become temptations of misbehavior for the cloud server.

The objective of the paper is that the secure keyword search issues in cloud computing have been adequately researched which aim to continually improve search efficiency, reduce communication and computation cost, and enrich the category of search function with better security and privacy protection. A common basic assumption of all these schemes is that the cloud is considered to be an ”honest-but-curious” entity as well as always keeps robust and secure software/hardware environments. As a result, the user can easily identify the datas that are tampered or damaged so that particular file can be modified and identified which does not lead to overall crashing of data.

II. RELATED WORK

Qian Wang [1] proposed enabling public audit ability and data dynamics for storage security in cloud computing which deliberately explains Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centers, where the management of the info and services might not be fully trustworthy. This unique paradigm brings about many new security challenges, which haven't been well understood. This work studies the matter of ensuring the integrity of knowledge storage in Cloud Computing. Foremost thing is to analyse the challenges faced in the security issues based on dynamic data updates during the direct extension which paves in building chic verification scheme for the seamless integration of those two salient features in our protocol design.

Peng Xu, Hai Jin [2] proposed Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack that Public-key encryption with keyword search (PEKS) is a versatile tool.It allows a unknown user to open the encrypted file by getting trapdoor keyword without decrypting the data or known to that keyword. However, it's shown that the keyword are going to be compromised by a malicious third party under a keyword guess attack (KGA) if the keyword space is during a polynomial size. A malicious searcher cannot learn the precise keyword to be searched albeit the keyword space is little. We propose a global change over that transform any incognito identity-based encryption (IBE) into a safe PEFKS scheme. Observing the generic establishment, we express the primary PEFKS scheme that is very much safe during the polynomial size of the keyword space.

Wenhai Sun, Bing Wang [3] proposed that demonstrable Privacy-Preserving Multi-Keyword Text Search in the Cloud behind Similarity-Based Ranking With the growing fame of cloud compute, huge amount of documents are outsourced to the cloud for reduced organization cost and simple access. Even though encryption helps in ensuring the security of user data, it omits the good working that sensibly efficient search methods over a encrypted file is a exigent problem. we present a verifiable privacy-preserving multi-keyword text search (MTS) scheme with similarity-based ranking to deal with this problem. To help in multiple keyword searching and ranking of a particular search, we establish the index search supported factor and that the vector space design with cosine similarity ensure to achieve greater correctness in query result.

Multi-Tier Cloud Systems proposed by Jyotiska Nath Khasnabish, Mohammad Firoj Mithani[4] based on Tier-centric that IT service delivery and fulfil, in which the cloud paradigm has initiated the IT resource for over-provisioning by fast automation of practical IT operations. Based on the flexibility of cloud computing, this upcoming completes up by unique that decrease the important advantage, results in the cost-budgeting of cloud adoption for Cloud Service Consumers (CSC). Similarly, detecting and eliminating such over provisioning without affecting the quality of service (QoS) is extremely difficult for Cloud Service Providers (CSPs) since they have no visibility into the appropriate presentation of economical service only into the IT fields. we have increased analytics to deal with the numerical and to move with virtual cloud adoption for large enterprises only in the context of meeting economical service level objectives (SLOs) and reduce the cloud payment cost (OpEx) for the commerce.

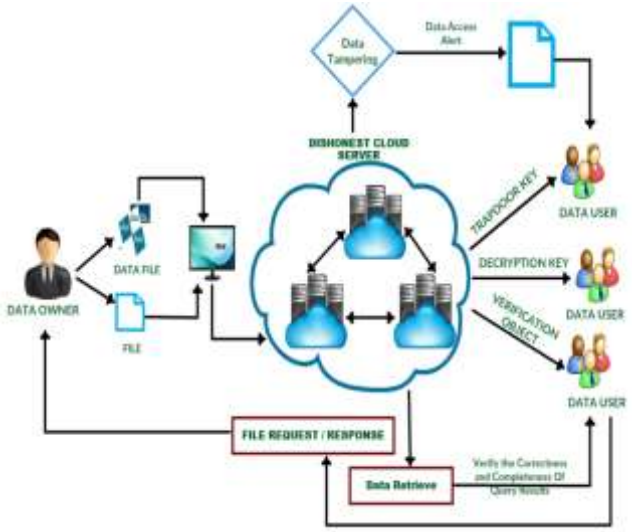
Semantic demonstration of Cloud Patterns and armed forces with automatic way of thinking to support Cloud Application Portability by Beniamino Di Martino, Antonio Esposito and Giuseppina Cretella [5] future that During the history existence the Cloud Computing offer has exponentially grown, with new Cloud providers, stage and services being introduce in the IT Market. The extreme sort of services, often providing non uniform and incompatible interfaces, makes it hard for patrons to make a decision the way

to develop, or maybe worse to migrate, their own application into the Cloud. This situation can only worsen when customers want to take advantage of services from different providers, due to the portability and interoperability issues that always arise. In our proposal we suggest propose a stable, incorporated, machine-readable representation of cloud platforms, patterns, applications and their compositions. We focuses mainly on upgrading the emerging applications in the Cloud environment, using defined patterns and reflexive reasoning to strengthen portability and interoperability when several platforms are in the ground. Mainly, the implemented reasoning procedure allow us to work on discovery of Cloud services and Appliances and mapping the agnostic and creator based Cloud models and Services; that usually shows the uniqueness.

III.PROPOSED WORK

A secure and fine-grained question outcome confirmation scheme by construct the confirmation 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. 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.

IV.ARCHITECTURE DIAGRAM



Above figure shows the proposed architecture of secured search scheme involves majorly of three phases as data owner, cloud admin and a data user. The data owner first register with the cloud admin to allocate some space and uploads a n number of files. Now the admin maintains the files. When an user needs to access to such files he has to register to the admin where the admin ensures the three level of security keys.

V.PROPOSED MODULES

***A.QUERY RESULT VERIFICATION*: The** query result verification mechanism allows the data user to verify the results. In this project, we designed a secure , easy to integrate Fine-grained query results validation mechanism, by giving a given query result set, the query user can't 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

***B.OUTSOURCING ENCRYPTED FILE* :** Cloud computing is a model for enabling universal,

co-operative, on-demand network access for a common source for configurable cloud computing resources such as links, servers, memory, and services that will be fatly furnished and outraged with lower management or lower network provider communication. The data owner will outsource the encrypted file to the cloud server; automatically three different keys will be generated for the file.

***C.VERIFICATION OBJECTS CONSTRUCTION*:** To maximize reduce storage and message cost and achieve solitude assurance of the confirmation objects. Trapdoor key, verification object key and decryption key are automatically constructed. The trapdoor key is basically differentiate the data owner and hacker

D.VERIFICATION OBJECT AUTHENTICATION AND SIGNATURE: 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

E.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 tries to access the data or information. We can prevent from accessing the user information or data by verifying the verification object.

***F.FILE RECOVERY*:** Data recovery may be a process of salvaging (retrieving) inaccessible, lost, corrupted, damaged or formatted data from auxiliary storage, removable media or files, when the info stored in them can't be accessed in a normal way. Even the hacker will access the data or even hacker does the tampering we can still recover the whole document.

VI.ALGORITHM

A. AES ALGORITHM

The encryption process uses a group of specially derived keys called round keys. These are applied, along side other operations, on an array of knowledge that holds exactly one block of knowledge, the info to be encrypted. This array we call the state array.
You take the subsequent as steps of encryption for a 128-bit block:

1. Derive the set of round keys from the cipher key
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the ultimate state array out because the encrypted data (cipher text).

VII. 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 every encrypted query result or further accurately determine what percentage or which qualified data files are returned by the dishonest cloud server.

A short signature technique is meant to ensure 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 info user and truly returned by the cloud server. Presentation and correctness experiment show the soundness and competence of our future system.

VIII. FUTURE ENHANCEMENT

In future of outsource data -Search method is not efficient since the cloud needs to search through the whole database, which is very inefficient. In future we have some work in this line that will be enhancements for efficient verification for large-scale outsourced data. This system works on semi trusted cloud but in future it'll be extended up to all or any sorts of cloud environment and may provide better security. Furthermore in future we will extend our search scheme to use auxiliary storage more carefully while maintaining privacy.

IX. 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 preserv- ing 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.