Enabling Fine Grained Multi Keyword Search in Cloud for Secure Data Transmission by Trapdoor Encryption.

[1]P.Saroja, [2]Dr. GV.Padmaraju
[1,2]Dept. of CSE, SRKR Engineering College, Bhimavaram, A.P, India

Abstract
Cloud service suppliers offer user's economical and ascendible knowledge storage services with lower price than ancient approaches, with the behavior of low maintenance cloud computing offers an inexpensive along with cost-effective decision as partition cluster resource with distinctive cloud end users. To provide privacy to the data, we encode effective info antecedently uploading into the cloud. Sadly, sharing the info and searching the info is extremely complex during multi-owner manner. To address this issue, we are proposing a new scheme for developing the fine-grained multi-keyword search by encoded cloud info. For the Encryption part we are using advanced encryption standard. The main goal of our planned theme is to offer the safety for documents that are transferred within effective Cloud and to inquire the reports based on the fine grained multi-keyword search scheme. For the safety reason we are using the 128 bit Advanced Encryption Standard, Hash Search operation and Sub directories techniques.

Keywords
Encryption, Hash Search, Sub Directories.

I. Introduction

Cloud computing is recognized as an alternate to ancient data technology due to genuine resource distribution and low allowance aspects. In cloud computing, the Cloud Service Providers (CSPs) like Amazon, Google Drive, Apple iCloud, Amazon Cloud drive and the Hybrid services like Drop box, Sugar sync will allow users to store their information in large amounts.

Cloud computing, the long held dream of computing as a utility, has a potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way the IT industry is designed and purchased. Cloud computing provides facilities by which users can access the applications as utilities, over the internet. It can also refer to the delivery of computing resources over the internet. Cloud computing allows users to manipulate, configure and access online applications. Cloud can provide services over internet that is on public networks like WAN, LAN or VPN. There are three service modules on which the cloud computing is based. They are Infrastructure as a Service (Iaas), Platform as a Service (PaaS) and Software as a Service (SaaS). IaaS provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc. PaaS provides the runtime environment for applications, development and deployment tools, etc. SaaS model allows using software applications as a service to the end users. Content delivery networks are based on the Network as a Service (NaaS).

The advantages of the cloud computing unit are to increase storage, to reduce the cost and to provide more mobility. We can be able to search the data that was present in the cloud by using the technique called hash based multi keyword search. All the hash based keywords are stored in database.

The data will place her data into the cloud for convenient and reliable data access to the corresponding search users. To protect the data privacy, the data owner encrypts the original data through symmetric encryption. To improve the search efficiency, the data owner generates some keywords for each outsourced document. Here we address that owner has a permission to add the files and appropriate keywords. He will add the keywords based on the category of files and internally every file consists of unique public key for maintaining security over the cloud. The corresponding index is then created according to the keywords and a secret key. After that, the data owner sends the encrypted documents and the corresponding indexes to the cloud, and sends the secret key to search users.

Whereas the hunt users wish to approach the communal info, then he can pick a few suited keywords also delegate the cipher text of the picked keywords to the cloud remote server. The cloud remote server later requires a decrypted key for the cipher text to meet the encoded keywords and it returns the files that are matched with the keywords of the search user. To find the identical search ability along with attention on encoded data like multi grained keyword search, we perform searching based on the hashing disclosed to cloud suppliers and attackers.

II. Related work

Multi keyword search is used to achieve the improved search results compare to the previous methods over the cloud data.

N. Cao, C. Wang [1] proposed that the information house holder can place their info from their native places to the business public cloud because of their excellent resilience along with commercial reserves. To maintain information privacy, sensitive information ought to be encoded since deploying. Thus encoded cloud information quest utility has dominant priority. In consideration of the massive range regarding information end-users and reports within the cloud, it is significant to grant more than one keywords within the search request and the reports will come within the regulation of their suitable keywords. The searchable cryptography targets individual keyword hunt or Boolean keyword hunt. For the primary time, we admit a habit to outline and work out the difficult drawback about Fine Grained Multi Keyword Search Scheme (FGMSE). We have a tendency to authorize an assembly of tough confidentiality necessities being such a protected cloud information usage system. With various multi keyword definitions, we have decided the practical closeness measure of "correlative matching," that is as various matches as attainable to catch the relevant reports to the hunt inquiry.

N. Cao, S. Yu, Z. Yang [2] proposed that with the expanding acceptance of cloud for knowledge repository, in particulars of knowledge exactness and availableness has-been dominant. Whereas redundant information becomes difficult with the pay based on the usage of cloud standard that have to be resolved for both fraud disclosure and knowledge reconstruction. Previous shared repository systems supported deletion codes or complex writing approaches that accept either/or huge secret writing process value for knowledge users or an excessive amount of burden for information repair and being on-line for data homeowners. Here, we design a secure cloud storage service which addresses

the reliability issue with near-optimal overall performance. By allowing a third party to perform the public integrity verification, data owners are significantly released from the onerous work of periodically checking data integrity.

S. Kamara and Lauter [3] proposed that the complication of constructing protected cloud repository service above the universal cloud framework, where the customer will not completely will not completely trust the service provider. We describe at the high level, several architectures that combine recent and non standard cryptographic primitives in order to achieve our goal. We survey the benefits of such architecture would provide to both customers and service providers then give an overview of recent advances in cryptography motivated specially by cloud storage. All the hash based keywords are stored in the database.

A. Singhal [4] proposed that for thousands of years people have realized the importance of achieving and finding information. With the usage of computers, it became possible to store large amounts of information and finding useful information from such collections became a necessity. The field of Information Retrieval (IR) was born in 1950's out of this necessity. Over the last forty years, the fields have matured considerably. Several IR systems are on use every day basis by a wide variety of users. It will give a brief overview of the key advances in the field of information retrieval and the description of where state of the art is at the field.

III. Problem statement

Previously in order to meet the search requirements, the encrypted data have to support three functions. First is to introduce the connection scores and preference factors upon keywords that precise keyword search and personalized user experience. Second is to develop a sensible and really economical multi keyword search scheme. The search scheme will support difficult logic search with mixed "AND", "OR" and "NO" operations on keywords. Third is to use the classified sub dictionaries technique to attain higher potency on index building, trapdoor generating and query. Lastly, we have a tendency to analyze the protection of the planned schemes in terms of confidentiality of documents, privacy protection of index and trapdoor and unlinkability of trapdoor. But it is complex approach and is difficult to perform all operations for encryption and decryption using AND, OR and NOT operations and it will take more time for searching.

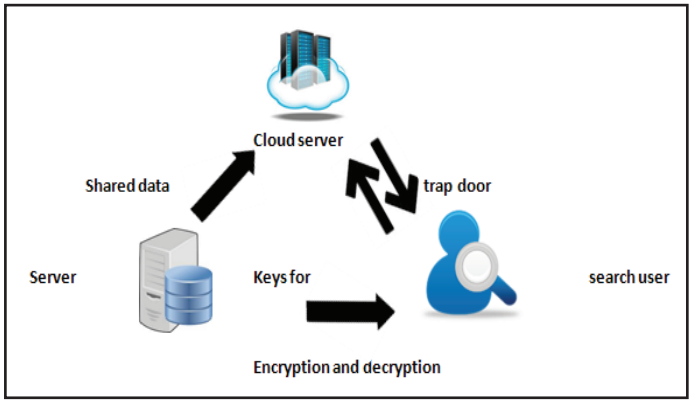

Fig. 1: Proposed Architecture

IV. Proposed Methodology

The above issue for searching and storing the data which have been located in the cloud is solved by the following.

For the searching we are using the multi grained hash technique and for the security purpose we are using symmetric key encryption. It is a sensible and really economical multi keyword search scheme. The planned scheme will support for Hash search operations on keywords and then we use classified sub-dictionaries technique to realize higher potentiality on index building, trapdoor generating and query. The main goal of our planned theme is to give safety for the documents that are uploaded within the cloud. We are using Advance Encryption Standard (AES) for providing the security. It will take less time to search over the encrypted data.

V. Result Analysis

We have implemented the previous and existing methods on different algorithms and different search techniques. In the search techniques we are using multi grained hashing approach to search the data based on hash index. These results are stored in the database (we are using MySql) and storing the shared data with the usage of public key is for providing the security over the cloud. In the encryption phase we are using 128 bit symmetric key encryption technique called as Advanced Encryption Standard.

The high level description for AES

1. **Key Expansion:** Round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
2. **Initial Round:**

(i). **AddRoundKey:** Each byte of the state is combined with the round key using bitwise XoR.

(ii). **Rounds:**

- Sub-Bytes: It is a non-linear substitution step where each byte is replaced with another according to a lookup table.
- Shift rows: It is a transposition step where each row of a state is shifted cyclically a certain number of steps.
- Mix columns: It is a mixing operation which operates on the column of the state, combing the four bytes in each column.
- Add round key

(iii). Final Round (no mix columns):

- Sub bytes
- Shift rows
- Add round key

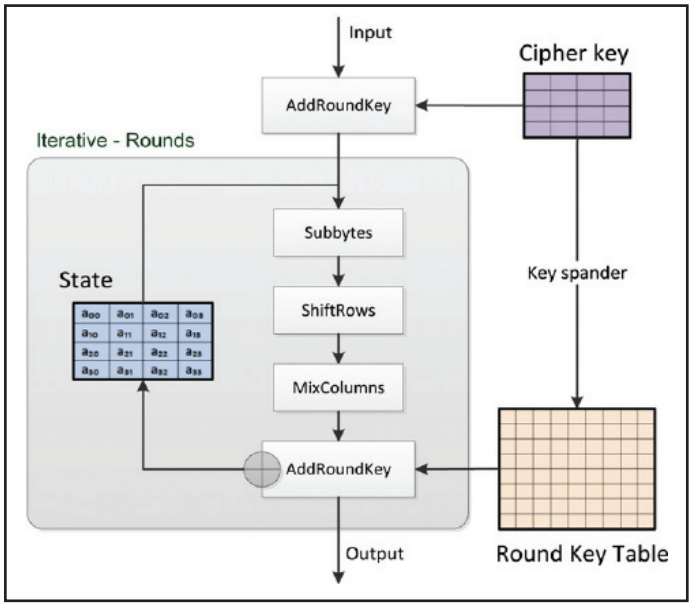

Fig. 2: Advanced Encryption Algorithm

VI. Conclusion and Future Work

We proposed the confidentiality of outsourced documents that are provided by the info owners are kept within the cloud server, if they match the search keywords then they will be send to the

search user. Thanks to the privacy of documents, the data can only be accessed by the info owner and the authorized search users. Privacy protection for the index and the trapdoor keys are provided by the Advanced Encryption Standard. The hash based indexing and the trapdoor is primarily created based on the document keywords and the search keywords respectively. If the cloud server identifies the content of index or trapdoor, he can deduce any association between keywords and encrypted documents.

References

[1] N. Cao, C. Wang, M. Li, K. Ren, W. Lou,"Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," [Online] Available: http://digital.cs.usu.edu/~mingli/papers/Cao_INFOCOM11.pdf

[2] N. Cao, S. Yu, Z. Yang, W. Lou, Y. Hou,"LT Codes-Based Secure and Reliable Cloud Storage Service," [Online] Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.714.3863&rep=rep1&type=pdf

[3] N. Cao, C. Wang, M. Li, K. Ren, W. Lou,"Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," [Online] https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/crypto-cloud.pdf

[4] A. Singhal,"Modern Information Retrieval: A Brief Overview Data," [Online] Available: http://singhal.info/ieee2001.pdf

[5] I.H. Witten, A. Moffat, T.C. Bell,"Managing Gigabytes: Compressing and Indexing Documents and Images" [Online] Available: https://sigmodrecord.org/publications/sigmodRecord/0406/RB2.Nagaraj.pdf

[6] D. Song, D. Wagner, A. Perrig,"Practical Techniques for Searches on Encrypted Data," [Online] Available: https://people.eecs.berkeley.edu/~dawnsong/papers/se.pdf

[7] E.-J. Goh,"Secure Indexes," Cryptology ePrint Archive, A. Singhal, "Modern Information Retrieval: A Brief Overview Data," [Online] Available: http://singhal.info/ieee2001.pdf

[8] Y.-C. Chang, M. Mitzenmacher,"Privacy Preserving Keyword Searches on Remote Encrypted Data," [Online] Available: https://eprint.iacr.org/2004/051.pdf

[9] R. Curtmola, J.A. Garay, S. Kamara, R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," [Online] Available: http://web.cs.ucla.edu/~rafail/PUBLIC/74.pdf