ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 11, November 2017

Attaining Multi-Keyword Search in Cloud Data using Logical Conditions

[1] Aranganathan.k, [2] Mr.V.Parthipan
[1] [2] Department Of Computer Science EngineeringSaveetha School of Engineering,Saveetha University, Chennai, India.

Abstract: **: The major use of the distributed computing is when the users can store their data in any form on remote server cloud while these data accessibility is also permitted for the authorized users. Since the secured data and the personal information are inclined to changing of data, these are highly protected in the cloud servers. This is done by the process of encoding of the data. The data must be secured in terms of how they could be transformed easily if they aren't encrypted. This project aims at addressing this issue by working on the fine grained multi word data sets in the information that is encoded. This is hence achieved by a three-fold process. Initially, we present the importance scores and inclination elements upon watchwords which empower the exact catchphrase look and customized client experience. Second, we add to a viable and exceptionally productive multi-watchword look plan. The proposed plan can bolster convoluted rationale seek the blended "AND", "OR" and "NO" operations of watchwords. Third, we advance utilize the arranged sub-word references method to accomplish better productivity on file building, trapdoor creating and question. Ultimately, we dissect the security of the proposed plans as far as classification of records, security insurance of file and trapdoor, and unlink capacity of trapdoor. The security investigation and the results that prove to be explanatory show that the plans proposed can accomplish a level of security which is different from the present levels and also provides with a useful and productive output as required and expected.**

Keywords- **:** logical conditions, secured, multi keyword, cloud data, trapdoor, secured data transfer, keywords search, fine grained logics.

I. INTRODUCTION

Computing is generally, taken to be as a utility source, according to the cloud computing where the computing storage strategies and capabilities are rented out publicly to the individuals. This brings feasibility for the data owner to stock all the data into the owner's database which would be available for outsourcing of data. This then makes the data to be available for public viewing and access through the cloud server. This enables a cost effective and highly efficient cloud server which acts as a medium for the sharing of information. Thus, it is affirmative to mostly all the petty enterprises.

There may be sensitive private information in the data that is outsourced. It is better to encrypt the user data before transmission of the data to the cloud server. The result of the data encryption would bring about a change in the stored loads of data wherein there would be difficulty in searching for the data from the stored encrypted data. For example, the Google Search Engine uses Secure Sockets Layer (SSL) which encrypts the connection between the user and the server while the search results appear onto the screen. These can be documents, emails or any other source of representation which has information.

II. Strategies Proposed

2.1. Basic Existing Framework

The distributed computing regards registering as a utility and rent out the processing and capacity abilities to people in general person. In such a system, the individual can remotely store her information on the cloud server, in particular information outsourcing, and afterward make the cloud information open for free through the cloud server. This speaks to a more versatile, ease and stable route for open information access on account of the adaptability and high proficiency of cloud server, and subsequently is positive to little ventures. The outsourced information might contain delicate protection data. Simply scrambling the information might in any case cause other security concerns. The information encryption, in any case, would essentially bring down the convenience of information because of the trouble of looking over the encoded in format.

2.2. Schemes Proposed

This paper there goes an investigation on the FMS – Fine grained Multi keyword Search technique with regards to the encrypted data in cloud and there are hence, two different schemes proposed in terms of FMS. FMS-I contains the relevant

document information and also the results based on preferences of the different keywords used. This helps in getting a precise and to the point search result and hence, increases the efficient experience of the user. On the other hand, the FMS-II sets up a search that is very secured which has logical functions in them- 'AND' condition, 'OR' condition, and 'NO' condition. The primary security properties of the proposed plans are broken down into simpler parts. Specifically, the examination of this process concentrates on how the proposed plans can accomplish classification of reports, security insurance of record and trapdoor, and unlink capacity of trapdoor.Using the broad investigations utilizing this present reality dataset, the execution of the proposed plans are being accepted. Both the security examination and exploratory results exhibit that the proposed plans can accomplish the same security level contrasting with the current ones and better execution as far as usefulness, question unpredictability and productivity. The aggregate lexicon as a typical sub-lexicon and numerous expert sub-lexicons are ordered by using the different advancements in the proposed reference algorithm FMSCS – Fine grained Multi Keyword search scheme that supports the sub-dictionaries that are classified. The mission to reduce the communication and computation process to a greater extent is achieved. This helps in unlinking the abilities of trapdoor and the protection security of the different documents in the stored database in the cloud server. Also efficient searching techniques are improvised using the FMS-II algorithm strategies.

III. Modules

3.1. Model of the System

3.1.1. Data Proprietor

The information proprietor outsources her information to the cloud for helpful and solid information access to the relating seek clients. To secure the information protection, the information proprietor encodes the first information through symmetric encryption. To enhance the hunt effectiveness, the information proprietor creates some catchphrases for each outsourced record. (Fig 1) The relating list is then made by watchwords and a mystery key. After that, the information proprietor sends the encoded reports and the relating files to the cloud, and sends the symmetric key and mystery key to hunt clients.

3.1.2. The Cloud Server

The cloud server is a middle of the road element which stores the encoded archives and comparing lists that are gotten from the information proprietor, and gives information get to and seek administrations to hunt clients. At the point when a data seeking client sends a catchphrase trapdoor to the cloud server, it would give back a gathering of coordinating records in view of specific operations.

Fig 1. Architecture of the cloud server system process

3.1.3. Public Users Search

A pursuit client inquiries the outsourced records from the cloud server with taking after three stages. In the first place, the inquiry client gets both the mystery key and symmetric key from the information proprietor. Second, as per the pursuit watchwords, the inquiry client utilizes the mystery key to create trapdoor and sends it to the cloud server. Last, the client gets the coordinating record accumulation from the cloud server and decodes them with the symmetric key.

3.2. The Menace Model and the security requisites

The cloud server is thought to be "straightforward however inquisitive", in the threat menace model, which is the same as most related chips away at secure cloud information look. In particular, the cloud server sincerely takes after the assigned convention detail. Be that as it may, the cloud server could be "interested" to induce and break down information (counting record) in its capacity and message streams got amid the convention in order to learn extra data. Two risk models are being considered relying upon the data accessible to the cloud server.

3.2.1. Known Cipher content Model

The cloud server can just know scrambled report gathering C and file accumulation I, which are both outsourced from the information proprietor. This makes the cloud server to contain huge amount of data that can be retrieved easily from the search results of the user's data search graph.

3.2.2. Known Background Model

The cloud server can have more learning than what can be gotten to in the known figure content model, for example, the connection relationship of trapdoors and the related factual of other data, i.e., the cloud server can have the measurable data from a known equivalent dataset which bears the comparable nature to the focusing on dataset.

3.3. Scheme of Fine grained Multi Keyword Searching Strategy

A Fine-grained Multi catchphrase Search plan supporting Classified Sub-lexicons (FMSCS), which groups the aggregate word reference as a typical sub-lexicon and numerous expert sub-word references. This would probably altogether lessen the calculation and correspondence overhead.

3.3.1. Lexicon Updating

In the searchable encryption plans with word reference, word reference overhaul is a test issue since it might bring about to redesign gigantic files outsourced to the cloud server. When all is said in one word reference based inquiry plots, the overhaul of lexicon will prompt re-era of all files. In our FMSCS plans, when it needs to change the sub-lexicons or include new sub-word references, just the information proprietors who utilize the relating sub-lexicons need to upgrade their lists, most other information proprietors don't have to do any redesign operations. Such word reference upgrade operations are especially lightweight. The measurement development strategy is used to actualize the proficient word reference extension. Such strategy can likewise be incorporated into our word reference overhauling process. What's more, our plan can even be more effective in spite of the fact that does not have to re-produce all files, but rather the comparing developed operations on all lists are fundamental. In examination, the plans just need to broaden the records of halfway information proprietors.

3.4. Analytic Thinking phase – Security

So as to effectively exhibit our plan calculation overhead, we examination our plan from every stage.

3.4.1. Secrecy of Documents

In our plans, the outsourced reports are scrambled by the customary symmetric encryption calculation (e.g., AES). Furthermore, the mystery key sk is produced by the information proprietor and sent to the pursuit client through a protected channel. Subsequent to the AES encryption calculation is secure, any substance can't recuperate the scrambled archives without the
mystery key sk. Thusly, and the privacy of encoded archives can be accomplished.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 11, November 2017

IV. System Study

4.1. Feasibility Study

The practicality of the framework is dissected in this stage and business proposition is advanced with an extremely broad arrangement for the venture and some expense gauges. Amid framework examination the possibility investigation of the proposed framework is to be completed. This is to guarantee that the proposed framework is not a weight to the organization. For plausibility investigation, some comprehension of the real necessities for the framework is vital.

Three key contemplations included in the possibility investigation are

- Economic Feasibility
- Technical Proficient Feasibility
- Societal Feasibility

4.1.1 Economic Feasibility

This study is completed to check the monetary effect that the framework will have on the association. The measure of asset that the organization can fill the innovative work of the framework is limited.(Fig 2) The consumptions must be defended. In this way the created framework too inside of the monetary allowance and this was accomplished on the grounds that the greater part of the advancements utilized are openly accessible. Just the modified items must be acquired.

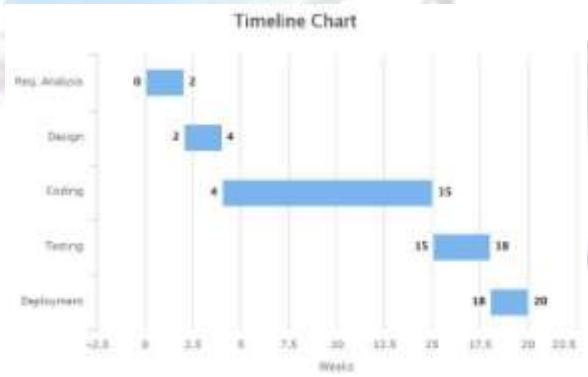

Fig 2. Gantt chart for the server system process

4.1.2. Technical Proficient Feasibility

The technical requirements of the secure system in cloud storage is checked using this feasible system. Not all systems that are developed have a proficient feasibility. Similarly, not all the systems developed from these sources would contain the proficient requirements in the system that is required. So this would definitely lead to a high demand in the technical resources for the system's use. Hence, there would be a pressure that is carried upon the client or the user's side with demands being high. The system developed must have a minimal change in the implementations that would be required for the system.

4.1.3. Societal Feasibility

The part of study is to check the level of acknowledgment of the framework by the client. This incorporates the procedure of preparing the client to utilize the framework proficiently. The client must not feel debilitated by the framework, rather should

acknowledge it as a need. The level of acknowledgment by the clients exclusively relies on upon the techniques that are utilized to teach the client about the framework and to make him acquainted with it. The client's level of certainty must be raised so that the client is additionally ready to make some useful feedback, which is invited, as he is the last client of the framework.

V. References

[1] Zhang Yaling, Jia Zhipeng ; Wang Shangping. A Multi-user Searchable Symmetric Encryption Scheme for Cloud Storage System

[2] Jyun-Yao Huang; I-En Liao, "A searchable encryption scheme for outsourcing cloud storage," Communication, Networks and Satellite (ComNetSat), 2012 IEEE International Conference on, pp. 142-146, 12-14 July 2012.

[3] S. Kamara, C. Papamanthou, T. Roeder, "Cs2: A searchable cryptographic cloud storage system", Technical Report MSR-TR-2011-58, Microsoft, 2011.

[4] Koletka, R.; Hutchison, A., "An architecture for secure searchable cloud storage," Information Security South Africa (ISSA), 2011, pp. 1-7, 15-17 Aug. 2011.

[5] Yanjiang Yang, "Towards Multi-user Private Keyword Search for Cloud Computing," Cloud Computing (CLOUD), 2011 IEEE International Conference on, pp. 758-759, 4-9 July 2011.

[6] Yanjiang Yang; Haibing Lu; Jian Weng, "Multi-User Private Keyword Search for Cloud Computing", Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on, pp. 264-271, Nov. 29 2011-Dec. 1 2011.

[7] S. Kamara; K. Lauter, "Cryptographic cloud storage", in Proceeding of Financial Cryptography: Workshop on Real-Life Cryptographic Protocols and Standardization 2010, Tenerife, Canary Islands, Spain, January 2010, pp. 136-149.

[8] Dan Boneh; Eyal Kushilevitz; Rafail ostrovsky; William E; Skeith III, "Public Key Encryption That Allows PIR Queries", 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, pp. 50-67.

R. Curtmola; J. A. Garay; S. Kamara; R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions", CCS'06 Proceedings of the 13th ACM conference on Computer and communicatons security, New York, USA, 2006, pp. 79-88.

[10] Yevgeniy Dodis; Nelly Fazio, "Public Key Broadcast Encryption for Stateless receivers", ACM CCS-9 workshop, DRM 2002, Washington, DC, USA, pp. 61-80, November 18, 2002.

[11] Dan Boneh; Matt Franklin, "Identity-Based Encryption from the Weil Pairing",21st Annual International Cryptology Conference, Santa Barbara, Califonia, USA, August 19-23, 2001 Proceedings, pp. 213-229.

[12] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovskey, Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions. Proc. ACM Conference on Computer and Communications Security, CCS'06, pp. 79-88, 2006. (Pubitemid 47131358)

[13] S. Kamara and K. Lauter, Cryptographic Cloud Storage. Proc. Financial Cryptography 2010.

[14] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, 2009.

[15] D. Song, D. Wagner, and A. Perrig, Practical Techniques for Searches on Encrypted Data. Proc. IEEE Symposium on Security and Privacy, S&P'00, pp. 44-55, 2000.