International Journal of Research in Engineering, Science and Management
Volume-2, Issue-6, June-2019
www.ijresm.com | ISSN (Online): 2581-5792

Implementation of Fast Phrase Search in Storage of Encrypted Cloud Environment

G. Jyothi Sree[1], Ch. Mastan Chowdary[2], P. Ganga Bhavani[3]

[1]M.Tech. Student, Dept. of Computer Science and Engineering, Chirala Engineering College, Chirala, India
[2]Assistant Professor, Dept. of Computer Science and Engineering, Chirala Engineering College, Chirala, India
[3]Associate Professor, Dept. of Computer Science and Engineering, Chirala Engineering College, Chirala, India

***Abstract*: Cloud computing greatest advancement in the current technological world began a new era in the community of research being a good evolution. There are so many advantages even it consists of alarming security and privacy problems. Flexibility in ease of access to classified data and storage has been recognized as one of the major issues in the present situation. To be specific many researchers are hardly trying to find solutions to look for encrypted documents which are basically stored on remote cloud servers. Where proposed solutions has to perform search based on keyword, search giving less attention on more focused searching methodologies. Implementation of a phrase search technique based on filters that are faster and have a better storage and communication efforts. This immense functionality we use is a series of filters. Providing a trade-off between storage and transfer rate and is capable to protect against different attacks.**

***Keywords*: Fast phrase search, Cloud, filters.**

1. Introduction

Most firms, organizations, enterprises, industries, are more continuously use cloud technologies, with the increase in day-to-day use of cloud technologies there are number of security and privacy issues of accessing their personal and confidential information over the Internet. Breaches in recent and continuing data will emphasize the importance for more secure cloud storage systems. Encryption is the need for those problems; cloud providers will enhance the encryption and preserve the private keys in its place of the data owners. That is, the cloud can read any format data it desired, providing no privacy to its users. Private keys can be stored and data can be encrypted by the cloud provider, it is also problematic in case of data breach. For handling this situation, researchers have actively been importing different solutions for secure storage on private and public clouds; private keys are the part of data owners. Keys are in the hands of data owners.

For quick response times than the existing systems response time we can represent the phrase scheme. This method is very trustworthy and easy to implement also scalable, that means we can simply add and remove documents in the corpus. Making some small changes to the scheme we can reduce the storage cost to low cost and we can protect the cloud providers with statistical knowledge. Although phrase searches are processed separately using filter technique, they are characteristically a specialized function in a keyword search scheme, where the main function is to provide keyword based searches.

2. Literature survey

Paper 1: major aim of this project suggested a scheme for preferred search over encrypted data (PSED) that can take search preferences of users' into consideration for the search over encrypted data. In the assumed search process, they have ensured the confidentiality of not only keywords but also quantified preferences related with them. PSED constructs its encrypted search index using Lagrange coefficients and employs secure inner-product calculation for both search and relevance measurement. The property dynamism and scalability of cloud computing is also considered in PSED.

Paper 2: Enterprises outsourcing their hardware as well as software and databases to the cloud and giving authorization to multiple users for access that represents a typical use scenario of cloud storage services in deep. In such a case of usage of database outsourcing, data encryption is a good approach that enabling the data owner to keep holds of its control over the outsourced data. Encryption Searchable is a cryptographic primitive allowing for private keyword supported search over the encrypted database

Paper 3: Ranked search really enhances system usability by returning the identical files in a ranked order about to certain relevance criterion (e.g., keyword frequency keyword matching, deduplication), thus making one step closer towards realistic deployment of privacy-preserving data hosting services in Cloud Computing. They suggested a straightforward yet ideal construction of ranked keyword search in the state-of-the-art searchable symmetric encryption (SSE) security definition, and exhibit its inefficiency.

Paper 4: a natural way to form privacy-preserving data outsourcing Oblivious storage (OS), where a client, Alice, stores sensitive data at server, Bob. solution show that Alice can hide both the data and the pattern in which she accesses her data, by high probability, using a method that achieves O(1) amortized rounds of communication between alice and Bob for each data access. Alice and Bob exchange small chunks of messages, of size O ($N^{1/c}$), for some constant c≥2, in a single

Table 1
Study of methods

S. No.		PAPER DETAILS
1	Bloom th filter	It is a space-efficient probabilistic data structure that supports set membership queries. The data structure was conceived by Burton H. Bloom in 1970. Bloom filters are space-efficient probabilistic data structure used to test whether an element is a member of a set. A Bloom filter contains m bits, where k hash functions, Hi(x), are used to map elements to the m-bits in the filter. The Bloom filter is initially set to all zeros. To add an element, a, to the filter, we compute Hi(a) for i = 1 to k, and set the corresponding positions in the filter.
2	a keyword search scheme	a keyword-to-document index and a location/chain index to map keywords to documents and match phrase
3	Conjunctive keyword search protocol	To provide conjunctive keyword search capability, each document, Di , was parsed for a list of keywords kwj. A Bloom filter of size m was initialized to zeros. Each keyword was hashed using a secret key to produce Hkc(kwj) and passed into k Bloom filter hash functions to set k bits in the Bloom filter. This results in a 1-gram Bloom filter for each document: B1Di= {b1, b2, ...bm} where bi∈{0, 1}. The document collection, D = {D1, D . . . ,Dn}, was encrypted and uploaded along with the Bloom filters to the cloud server. The Bloom filters are then prepared into a matrix with the first row containing the filter B1D1 for the first document and the last row containing B1DN. Its transpose was stored as a Bloom filter index IBF where each row corresponds to a bit in the Bloom filters.
5	Symmetric Key Algorithm	Two symmetric key algorithms.they are AES is to encrypt the document and triple DES is to encrypt the keywords with base 64 hashing technique
6	TRIPLE DES (Data Encryption Standard)	•Triple Data Encryption Standard (DES) is a symmetric key encryption technique where block cipher algorithms are applied three times to each data block. •The key size is increased in Triple DES to guarantee additional benefit security through encryption capabilities. •Each block contains 64 bits of data. Three keys are referred to as bundle keys with 56 bits per key.
7	AES(Advanced Encryption Standard)	•Advanced encryption standard is a block cipher intended to replace DES for commercial applications. •It uses a 12~-bit block size and a key size of 128, 192 or 256 bits.
8	Nth gram filter	N-gram indexing is a powerful method for getting fast, “search as you type” functionality like iTunes. It is also useful for quick and effective indexing of languages such as Chinese and Japanese without word breaks. N-grams refers to groups of N characters... bigrams are groups of two characters, trigrams are groups of three characters, and so on. Whoosh includes two methods for analyzing N-gram fields: an N-gram tokenizer, and a filter that breaks tokens into N-grams.

round, where N is the size of the data set that` Alice is storing with Bob. Alice has a private memory of size $2 N^{1 /c}$

3. Conclusion

This paper presented an overview on fast phrase search in storage of encrypted cloud environment.

References

[1] K. Cai, C. Hong, M. Zhang, D. Feng, and Z.Lv, “A secure conjunctive keywords search over encrypted cloud data against inclusion-relation attack,” in IEEE International Conference on Cloud Computing Technology and Science, 2013, pp. 339–346.

[2] Y. Yang, H. Lu, and J. Weng, “Multi-user private keyword search for cloud computing,” in IEEE Third International Conference on Cloud Computing Technology and Science, 2011, pp. 264–271.

[3] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” in International Conference on Distributed Computing Systems, 2010, pp. 253–262.

[4] M. T. Goodrich, M. Mitzenmacher, O. Ohrimenko, and R. Tamassia, “Practical oblivious storage,” in Proceedings of the Second ACM Conference on Data and Application Security and Privacy, 2012, pp.13–24.

[5] C. Hu and P. Liu, “Public key encryption with ranked multi keyword search,” in International Conference on Intelligent Networking and Collaborative Systems, 2013, pp. 109 – 113.

[6] F. Kerschbaum, “Secure conjunctive keyword searches for unstructured text,” in International Conference on Network and System Security, 2011, pp. 285 – 289.

[7] H. Tuo and M. Wenpin g, “An effective fuzzy keyword search scheme in cloud computing,” in International Conference on Intelligent Networking and Collaborative Systems, 2013, pp. 786 – 789.