© 2017 IJSRST | Volume 3 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X

National Conference on Advances in Engineering and Applied Science (NCAEAS)
16th February 2017
In association with
International Journal of Scientific Research in Science and Technology

A Review on Search Scheme over Cloud Data

Akshay Shirbhate[1], Aniket Waghmare[2], Prof. P. H. Govardhan[3]

[1,2]Students, Department of Computer Science and Engineering, Priyadarshini Institute of Engineering and Technology, Nagpur, Maharashtra, India
[3]Assistant Professor, Department of Computer Science and Engineering, Priyadarshini Institute of Engineering and Technology, Nagpur, Maharashtra, India

ABSTRACT

Organizations are showing great interest in storing data on cloud. This could be the result of the unprecedented growth of data stored in the last few years. However for the security of sensitive data, it should be encrypted before outsourcing, which performs traditional data utilization based on plaintext keyword search. Because of the several numbers of data owners and documents in the cloud, it is required to allow multiple keywords in the search request and retrieve documents in the order of their relevance to these keywords. So far, several works have been studied to achieve various search functionality, such as single keyword search, multi-keyword Boolean search, ranked search, multi-keyword ranked search, etc. Among them, multi key word ranked search found more efficient to sort the search results.

Keywords : Sensitive Data, Single Keyword

I. INTRODUCTION

Currently we have a tendency to square measure in associate degree information explosion era wherever perpetually getting new hardware, software and coaching IT skilled is turning into a nightmare for virtually each IT person. Coincidentally, we square measure witnessing associate degree enterprise IT design that shifted to a centralized, more powerful computing paradigm famous as Cloud Computing, in which enterprise's knowledge bases and applications square measure stirred to the servers within the massive data centres (i.e. the cloud) managed by the third-party cloud service providers (CSPs)a in the web. Cloud computing has been recognized as the most momentous turning purpose within the development of data technology throughout the past decade. People square measure attracted by the advantages it offers, such as personal and versatile access, on-demand computing resources configuration, considerable capital expenditure savings, etc. Therefore, many firms, organizations, and individual users have adopted the cloud platform to improve their business operations, research, or everyday needs. With the remunerative option of pay-asyou- use, general and private knowledge square measure outsourced by several individual users and organizations to 3rd party CSPs. A knowledge owner will source their knowledge to the cloud and either he will question on it outsourced data or will attest a shopper to perform question.

II. LITERATURE SURVEY

2.1 Secure and privacy preserving keyword search

Qin Liuy [1] proposed in this paper that the search provides keyword privacy, data privacy and linguistics secure by public key coding. CSP is involved in partial decoding by reducing the communication and machine aerial in secret writing method for finish users. The user submits the keyword trapdoor encrypted by users private key to

cloud server firmly and retrieve the encrypted documents. But the communication and machine price for encryption and secret writing is much higher.

2.2 Secure and Efficient Ranked Keyword Search

Cong Wang [2] proposed stratified search that will increase system usability by sanctioning search result connection ranking instead of causing uniform results, and further guarantees the file retrieval accuracy. Specifically, they explore the statistical live approach, i.e. relevance score, from information retrieval to build a secure searchable index, and develop a one-to-many order-preserving mapping technique to properly secure those sensitive score information. The resulting style is in a position to facilitate economical server-side ranking while not losing keyword privacy. But it will not perform multiple keyword searches.

2.3 Efficient and Secure Multi-Keyword

Search on Encrypted Cloud Data This proposed technique by C. Orensik has defined and resolved the drawback of effective however safe and sound hierarchal keyword search over Encrypted cloud knowledge [2]. Ranked search greatly enhances system usability by returning the matching files in a hierarchal order concerning to bound vital criteria (e.g. keyword frequency) thus creating one step nearer towards wise consumption of secure knowledge hosting services in Cloud Computing. These pers has defined and resolved the difficult drawback of privacy protective and economical multi keyword hierarchalsearch over encrypted cloud knowledge storage (MRSE), and establish a set ofstrict privacy requirements for such a otected cloud knowledge utilization system to become a reality. The proposed ranking technique proves to be economical to go back extraordinarily relevant documents admire submitted search terms. But it lacks dynamic updation and deletion of the document from the cloud.

2.4 A Secure and Dynamic Multi keyword

Ranked Search Scheme over Encrypted Cloud Data This proposed methodology [4] by Z. Xia suggest a secure tree-based search theme over the encrypted cloud storage, which supports multi keyword hierarchal search on with dynamic operation on document assortment obtainable at server. The vector space model and term frequency (TF) × inverse document frequency (IDF) model area unit jointly used in the development of index and generation of question to supply multi keyword hierarchal search output. To obtain high search potency results, author construct a tree-based index structure and proposed a Greedy Depth-first Search algorithmic program based mostly on this index tree. Because of this special structure of treebased index, the proposed search themeill flexibly accomplish sub linear search time and will effectively handle the deletion and insertion of documents. The kNN algorithm is applied to write in code the index and question vectors, and till then guarantee correct connection score alculation between encrypte index and question vectors.

III. TECHNIQUES AND ALGORITHMS

Some of the models, techniques and algorithms being used within the existing system are mentioned and summarized as follows.

3.1 Vector area Model

This model is used to represent the text by a vector of functions. The terms are the words and phrases. If words are thought of as terms, every word becomes associate freelance dimension in a terribly high dimension vector area. If term represents a text, it gets a non- zero value n the text-vector on the dimension like the term. Text vectors are terribly area and no term is allotted a negative worth.

3.2 Searchable secret writing rule

An rule that consists of the polynomial time randomized algorithms. They are: eyGen(s) - s is a security parameter taken and wont to generate a key pair either public or personal. PEKS (Apub, w) - Apub may be a public key and w is a word which square measure wont to manufacture a searchable secret writing.

Trapdoor (Apriv, w) - Apriv may be a private key and w is a word that square easure wont to manufacture a trapdoor Tw.

3.3 Term Weight

Term weighting is a technique that depends upon the higher estimation of assorted chances. The main three factors play in term weight formulation is: Term Frequency - Words that repeat multiple times in a document. Document Frequency - Words that appear in several documents square measure thought of common. Document Length - hen assortment have documents ofvariable lengths, longer documents influence to score higher since they contain additional words and more repetition.

3.4 Cipher Text Security

It is a method that's wont to provide security for the encrypted knowledge. A cipher text attacker might simply break linguistics security by rearrangement the keywords and submitting the ensuing cipher text for secret writing. A standard technique is employed to interrupt this and this system is termed the cipher text security.

3.5 Non-Public Key Searchable Encoding

A model called non-public key searchable encoding is used to look on a personal key encrypted knowledge. The user himself encrypts data, so as to organize in Associate in Nursing impulsive manner. 3.6 Public Key Searchable encoding Public key searchable cypherion is a model that permits user to encrypt knowledge and send it to the server. The owner provides decryption key might be completely different.

IV. CONCLUSION

In this review paper, we have summarized totally different reasonably looking out techniques for the encrypted information over cloud. A systematic study on the privacy and data utilization problems is roofed here for numerous looking out techniques. Some of the important roblems to be handled by the looking out technique for providing the information utilization and security area unit keyword privacy, Data privacy, Fine-grained Search, Scalability, Efficiency, Index privacy, Query Privacy, Result ranking, Index confidentiality, Query confidentiality, Query Unlinkability, semantic security and Trapdoor Unlink ability. The limitations for all the searching techniques mentioned during this paper area unit mentioned in addition. From the above survey, we will conclude that multi-keyword stratifiedb search theme provides the economical, secure and dynamic search results.

V. REFERENCES

[1]. Qin Liuy, Guojun Wangyz, and Jie Wuz, ”Secure and privacy preserving keyword searching for cloud storage services”, ELSEVIER Journal of Network and computer Applications, March 2011

[2]. Cong Wang et al., ”Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data”, IEEE Transactions on parallel and distributed systems, vol. 23, no. 8, August 2012

[3]. C.Wang, N. Cao, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over outsourced cloud data,”Parallel and Distributed System, IEEE Transction on ,vol.23,no. 8,pp.1467-1479,2012

[4]. Zhihua Xia, “A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data”, IEEE Transactions on parallel and distributed systems, vol: pp no: 99 year 2015