Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 8759 - 8763
Received 05 March 2021; Accepted 01 April 2021.

Challenges in implementing Encrypted Keyword Search Techniques over Cloud and Feasible Solution

D. Naga Swetha[1], Dr. Savadam Balaji[2]
[1]Research Scholar, Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation, Deemed to be University, Hyderabad,
Telangana-500075.
[2] Professor, Associate Dean, Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation, Deemed to be University, Hyderabad,
Telangana-500075.
E-Mail: mailsforswetha@klh.edu.in, balajis@klh.edu.in

Abstract – In Cloud Computing, search-theme-maintained on phrases where Bloom varies that is substantially faster than the current methods, necessitating merely one round of correspondence and Bloom filter confirmations. With Advanced Forward and Secure Conjunctive Keyword Search Encryption technique, fast verification, storage cost and computational cost for all types of applications is made practical by using a Bloom filter index only. This even can accommodate its facilities as much efficient as CKS technique detects the matched documents much faster. Customizing filter sizes for effective usage of Bloom filter indexes and overcoming resource-limited client problem also. To avoid the server from restoring undesirable results and prevent the blooms filter false positive probability, an encoded index for every keyword is to be stored in the server. All these issues are to be resolved by designing and implementing Framework for Forward Secure Connective Keyword Search (FS-CKS) Encryption technique to attain low redundant storage in Cloud.

Keywords – Cloud Computing, Connective Keyword Search, Encryption, Computational Cost, Bloom Filters.

I. Introduction

Cloud computing is a trending stand to the traditional IT sectors as it delivers the smallest amount of attempt and "pay-as-you-go" facility based on to registration facilities and managements on demand. Governments, and enterprises, relocated their entire or the greater part of the IT framework into the cloud. Framework mists guarantee a vast number of points of interest when contrasted with on-start settled foundation. These crucial points incorporate on-request asset accessibility, pay as you go alleging, better equipment usage, no in-house devaluation misfortunes, and, no assistance overhead [1]. These days companies use cloud technologies and with this practice, there can be a defense and secrecy concerns of reclaiming private and classified knowledge over the Net [2]. The newest and on-moving data violations emphasize the necessity for further reliable cloud storage areas. Cloud sources frequently operate the encryption and maintain the private keys instead of the data owners as it is essential [4]. The storing of private keys and encoded data by the cloud provider is also difficult w.r.t. data crack. Therefore, investigators have keenly been encountering declarations for reliable storage on private and public clouds where private keys are under control of data owners. The phrase proposal is very consistent, accessible to execute [7]. Even though phrase search techniques are handled separately, its typical for a function in a keyword search scheme to offer connective keyword searches.

An advanced phrase-search-proposal-theme-maintained Bloom alters that is considerably faster than current techniques, demanding exclusively authentications of Bloom filter processing. Constructing Advanced Forward Search Connective Keyword Search Encryption technique using a Bloom filter index facilitates quick confirmation and achieves a reduced storage cost and computational cost for all different categories of purposes [3]. Advanced Forward Secure Connective keyword search technique supported Bloom filters provides with improvised storage and communication cost as CKS technique distinguishes the corresponding documents much quicker, performing lesser operations than distinct filter authentication, this functionality is helpful to FS-CKS technique[3]. In sight of lessening high cost in storage and computational cost, a trade-off between latent period and storage cost may be made by using t sets of filter sizes where just one of the document set would conform to the most important filter size used, efficiently delivering Bloom filter indexes. Server Usage keyword search framework uses two parties: the knowledge owner and an untrusted cloud server.

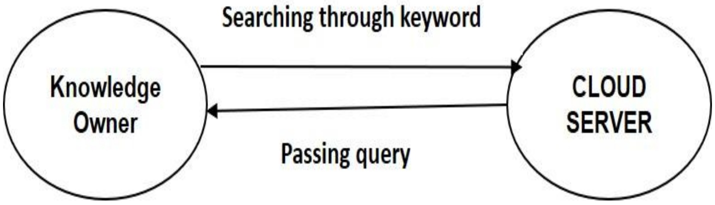

Fig. 1: Standard Process for Keyword Search

During this process, the knowledge owner generates the specified encryption keys for hashing and encryption operations. Then, all documents within the database are parsed for keywords [3]. Bloom filters tied to hashed keywords and n-grams are attached [1]. The documents are then evenly encrypted and uploaded to the cloud server [9]. To feature files to the database, the knowledge owner analyzes the files as in setup and uploads them with Bloom filters attached to the cloud server. to get rid of a file from the information, the knowledge owner simply sends the request to the cloud server, who removes the file together with the attached Bloom filters [6]. To perform a groundwork, the knowledge owner calculates and transmits a trapdoor encryption of the queried keywords to the cloud to instruct a protocol to look for the demanded keywords within the corpus. Ultimately, the cloud reacts to the knowledge owner with the identifiers to the demanded documents [2].

II. Thematic and Methodological Observations on Encrypted Keyword Search Techniques (EKST)

The intention of A Secure and Dynamic Multi Keyword Ranked Search Scheme over encrypted is to determine the problem of multi-keyword hierarchical search over encrypted cloud knowledge (MRSE) at the time of protective actual technique wise privacy within the cloud computing construct[1]. Knowledge holders' unit inspired to source their tough knowledge management systems from native sites to the business public cloud for giant flexibility and monetary savings. Except for defending knowledge privacy, sensitive knowledge ought to be encrypted before outsourcing, which operates basic knowledge consumption endorsed plaintext keyword search [2]. Therefore, permitting Associate in Nursing encrypted cloud knowledge search service is of great importance. Visible of the large range of data users and documents within the cloud, it's essential to permit many keywords within the search demand and are available back documents within the order of their acceptable to those keywords [9]. Related mechanism on searchable cryptography makes centre on single keyword search or Boolean keyword search, and sometimes type the search results [4]. within the center of varied multi-keyword linguistics, deciding the well-coordinated similarity live of coordinate matching, it means as several matches as doable, to capture the acceptable knowledge documents to the search question. notably, we consider inner product similarity i.e., the quantity of question keywords shows in an exceedingly document, to approximate such match up live that document to the search question [6]. Through the index construction, each document is connected with a binary vector as a sub-index wherever equally indicates whether or not matching keyword is contained within the document [10].

In Privacy-Preserving Multi-keyword Ranked Search Over Encrypted Cloud Data [5], the development in cloud computing has encouraged the information owners to outsource their data managing system from local sites to profitable public cloud for unnecessary tractability and cost-effective reserves. But people can take advantage of cloud computing, if we are ready to report very real secrecy and safety measures concerns that include loading sensitive personal information [8].

Consenting an encrypted cloud data search facility is of great significance. A secure index could be a system that enables a queried with a trapdoor for a word x to check in O(1) time providing the index contains x[10]. The index reveals no knowledge about its subjects without valid trapdoors, and trapdoors can only be produced with a secret key. Secure indexes are a natural extension of the matter of building data structures with privacy guarantees like those provided by oblivious and record unbiased data structures [4].

III. Addressing Gaps in EKST from Thematic and Methodological Observations

In the basic methodology that is FS-CKS technique, the client must store up and verify a bloom filter locally, which is able to be a waste away of storage and computation resources for a resource-limited client. Moreover, as there's false positive probability within the membership test of a bloom filter, the essential scheme may make mistakes within the Search protocol [11]. On the server side, it resumes some redundant indexes in an execution of the Search protocol, which can increase the communication overheads [2]. To stop the server from returning redundant results and avoid the false positive probability of bloom filter, an encrypted index for every keyword is to be stored within the server. But this might lead to waste of storage.

3.1 Trends and Patterns identified in EKST over Cloud

Concentrating on the considerable scenarios of present systems, w.r.t FS-CKS technique, (1) The client must store up and local verification of bloom filter is necessary (2) Consumption of storage and computation resources for a resource-limited client are high. (3) Additionally, as there's false positive probability within the membership test of a bloom filter, the fundamental scheme might commit errors within the Search protocol. (4) On the server side, it returns some unwanted indexes in an execution of the Search protocol, which can rise the communication costs.

3.2 Innovative approaches in finding Feasible Solution for EKST issues in Cloud

A bloom filter on the client side to test the survival of keywords in every file makes comfortable to scrap and get into locality instead of on the server side [5]. By this way, it can avoid the false positive probability of the bloom filter and decrease the unnecessary search results, frame work are often improved by utilizing secret-key inner-product encryption to attain sub-linear efficiency and one round communication within the search protocol. As this process is limited to forward secure single-keyword searchable encryption scheme, the subsequent step to get could be a Connective-keyword one [6].

The practice of a Bloom filter index involves the filters to be of the identical length in keeping with the version of basic methodology. A customized filter size is safer and secure in terms of identity protection and storage. Employing a small number of hash functions greatly develops the execution time since the computational cost is proportional to the amount of hash function utilized. In routine, the amount of hash functions, k, needed to scale back false positive rate is never used, because there's little improvement in false positive rate as we improve the amount of hash functions past a specific threshold limit. More highly in real time scenarios, it might be the biggest document within the corpus. All other minor documents would display below required false positive rate. However, this method incorporates a high cost in storage. In corpuses, where there’s an oversized variance in document sizes, much of the storage is wasted. Longer phrases even have a low probability of existence and yield less matches. Consequently, even with a precision rate of fifty, is never seen over one false positive for an enquiry query of longer phrases.

The framed Innovative Approaches are listed below:

1. To design a framework for FS-CKS encryption technique by enhancing Bloom’s Filter

technology.

2. To implement Bloom's technology for searching multiple documents using encrypted keywords.
3. To create and develop customized filters and offer filter size ratio for protecting the file's identity to reduce computational costs.

The following is the area of research where Keyword Searching and Security plays a major role:

- Enhancing Search Protocols.
- Designing a customized filter size to guard the file's identity.
- Identifying one document that gives the accuracy but the focusing is on enhancement of Keyword identification in multiple documents.
- Long phrase searching by attaining at lower storage and computational costs in cloud.
- Enhancement in usage of Encryption techniques.

IV. Reviewing and Analyzing methodology applied for Formed and Future Developing Frameworks of EKST

Currently EKST Framework searching technique: Search technique with Conjunctive keyword mechanism supported Bloom filters providing with better results in storage and communication cost. This CKS technique uses a series of n-gram filters to sustain system functionality. This scheme does not require sequential verification and is parallelizable having an applied storage requirement. This method can detect the matched documents much faster, performing fewer operations than individual filter verification. This result in only some rows being separated for identical one. To perform a sequential keyword search with phrases, the knowledge owner must first perform the Bloom filter hash computation of the pair, to characterize the set bits within the query filter if the phrase comprises of more than one keyword.

Enhanced version of search technique consists of: (a) Enhancing Search Protocols. (b) Designing a customized filter size to guard the file's identity. (c) Identifying one document that gives the accuracy but the focusing is on enhancement of Keyword identification in multiple documents. (d) Long phrase searching by attaining at lower storage and computational costs in cloud. (e) Enhancement in usage of Encryption techniques.

V. Conclusion

Based on the real time scenarios considered, currently in many Software organizations and Cyber Intelligence departments, employees are facing complexity in searching multiple documents using encrypted keywords. This problem can be overcome by our proposed AFSC Keyword search technique developed on AWS platform. And now it's time to focus on achieving Advanced Forward Secure Connective Keyword Search Technique(AFSC Keyword Search Technique) by enhancing Bloom's Filter technology, for searching multiple documents using encrypted keywords and develop customized filters and offer filter size ratio for safeguarding the file's identity to cut back computational costs.

References

[1] Chengyu Hu, Xiangfu Song, Pengtao Liu, Yue Xin, Yuqin Xu, Yuyu Duan, And Rong Hao, "Forward Secure Conjunctive-Keyword Searchable Encryption", IEEE-2019.

[2] Yunyun Wu, Jingyu Hou, Jing Liu, Wanlei Zhou, (Senior Member, Ieee), And Shaowen Yao, "Novel Multi-Keyword Search on Encrypted Data in the Cloud", IEEE-2019.

[3] D. Naga Swetha, "Conjunctive Keyword Search (CKS) technique using Series of N-gram filters for Security and Privacy in Cloud" Journal of Adv Research in Dynamical & Control Systems,

Vol. 10, 07-Special Issue, 2018.

[4] H. Poon and A. Miri, “An efficient conjunctive keyword and phrase search scheme for encrypted cloud storage systems,” in IEEE International Conference on Cloud Computing, 2015.

[5] “A low storage phrase search scheme based on bloom filters for encrypted cloud services,” to appear in IEEE International Conference on Cyber Security and Cloud Computing, 2015.

[6] Z. Fu, X. Sun, N. Linge, and L. Zhou, “Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query,” IEEE Transactions on Consumer Electronics, vol. 60, pp. 164–172, 2014.

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

[8] 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, pp.13–24, 2012.

[9] M. Ding, F. Gao, Z. Jin, and H. Zhang, “An efficient public key encryption with conjunctive keyword search scheme based on pairings,” in IEEE International Conference on Network Infrastructure and Digital Content, pp. 526–530, 2012.

[10] Y. Tang, D. Gu, N. Ding, and H. Lu, “Phrase search over encrypted data with symmetric encryption scheme,” in International Conference on Distributed Computing Systems Workshops, pp. 471– 480, 2012.

[11] 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, pp. 253–262, 2010.

Authors Profile

D. Naga Swetha[1], pursuing Ph.D., under esteemed guidance of Dr. S. Balaji, Professor, Associate Dean in Koneru Lakshmaiah Education Foundation, Deemed to be University, Hyderabad. Her areas of interest include Cloud Computing, Network Security and Computer Networks.