International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 03 Issue: 09 | Sept -2019 ISSN: 2590-1892

A NOVEL IMPLEMENTATION OF FAST PHRASE SEARCH FOR ENCRYPTED CLOUD STORAGE

PALAKURI SUDHA RANI (PG SCHOLAR)
COMPUTER SCIENCE AND ENGINEERING.
SREEYAS INSTITUTE OF ENGINEERING &TECHNOLOGY

A SWATHI (ASSOCIATE PROFESSOR)
COMPUTER SCIENCE AND ENGINEERING.
SREEYAS INSTITUTE OF ENGINEERING &TECHNOLOGY

ABSTRACT: Cloud computing has generated much interest in the research community in recent years for its many advantages, but has also raise security and privacy concerns. The storage and access of confidential documents have been identified as one of the central problems in the area. In particular, many researchers investigated solutions to search over encrypted documents stored on remote cloud servers. While many schemes have been proposed to perform conjunctive keyword search, less attention has been noted on more specialized searching techniques. In this paper, we present a phrase search technique based on Bloom filters that is significantly faster than existing solutions, with similar or better storage and communication cost. Our technique uses a series of n-gram filters to support the functionality. The scheme exhibits a trade-off between storage and false positive rate, and is adaptable to defend against inclusion-relation attacks. Adesign approach based on an application's target false positive rate is also described.

INTRODUCTION

AS organizations and individuals adopt cloud technologies, many have become aware of the serious concernsregarding security and privacy of accessing personal andconfidential information over the Internet. In particular, therecent and continuing data breaches highlight the need formore secure cloud storage systems. While it is generallyagreed that encryption is necessary, cloud providers oftenperform the encryption and maintain the private keys instead of the data owners. That is, the cloud can read anydata it desired, providing no privacy to its users. The storageof private keys and encrypted data by the cloud provider isalso problematic in case of data breach. Hence, researchershave actively been exploring solutions for secure storage onprivate and public clouds where private keys remain in thehands of dataowners.

Bonehetal.proposed one of the earliest works onkeyword searching. Their scheme uses public key encryption to allow keywords to be searchable without revealingdata content. Waters et al. investigated the problem forsearching over encrypted audit logs. Many of the earlyworks focused on single keyword searches. Recently, researchers have proposed solutions on conjunctive keywordsearch, which involves multiple keywords. Otherinteresting problems, such as the ranking of search resultsand searching with keywords that might contain errors termed fuzzy keyword search, have alsobeen considered. The ability to search for phrases was alsorecently investigated. SomehaveIn this paper, we present a phrase search schemewhich

Achieves a much faster response time than existing solutions. The scheme is also scalable, where documents canexamine the security of the proposed solutions and, whereflaws were found, solutions were proposed.

EXISTING SYSTEM

1.Boneh et al. proposed one of the earliest works on keyword searching. Their scheme uses public key encryption to allow keywords to be searchable without revealing datacontent.

2. Waters et al. investigated the problem for searching over encrypted audit logs. Many of the early works focused on single keywordsearches.

3. Recently, researchers have proposed solutions on conjunctive keyword search, which involves multiplekeywords.

4. Other interesting problems, such as the ranking of search results and searching with keywords that might contain errors termed fuzzy keyword search, have also been considered. The ability to search for phrases was also recentlyinvestigated.

5. Some of the existing system hasexamined the security of the proposed solutions and, where flaws were found, solutions were proposed.

DISADVANTAGES OF EXISTING SYSTEM

1. The cloud can read any data it desired, providing no privacy to its users. The storage of private keys and encrypted data by the cloud provider is also problematic in case of databreach.

2. By recognizing the almost exponential distribution of keywords, the entries in the keyword location tables are split into pairs to achieve normalization without the high cost of storing unused random data. However, the use of encrypted indexes and the need to perform client-sideencryption

and decryption may still be computationally expensive in certain applications.

3. Its space-efficiency comes at the cost of requiring a brute force location verification during phrase search. Since all potential locations of the keywords must be verified, the amount of computation required grows proportionally to the file size. As a result, the scheme exhibits a high processing time.

PROPOSEDSYSTEM

1. In this paper, we present a phrase search scheme which achieves a much faster response time than existing solutions. The scheme is also scalable, where documents can easily be removed and added to the corpus. We also describe modificationsto the scheme to lower storage cost at a small cost in response time and to defend against cloud providers with statistical knowledge on storeddata.

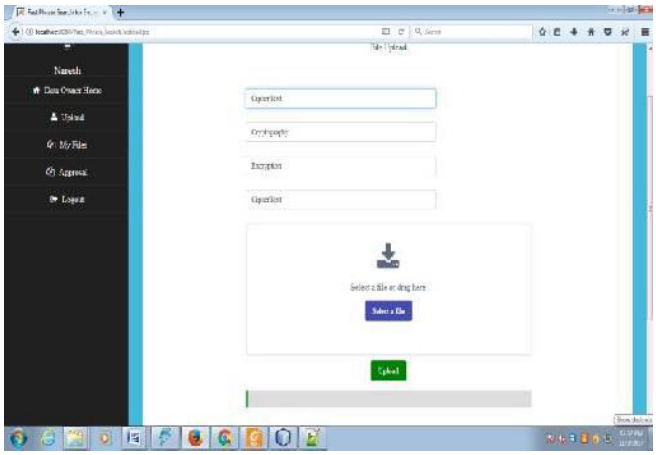
2. Although phrase searches are processed independently using our technique, they are typically a specialized function in a keyword search scheme, where the primary function is to provide conjunctive keyword searches. Therefore, we describe both the basic conjunctive keyword search algorithm and the basic phrase search algorithm along with designtechniques.

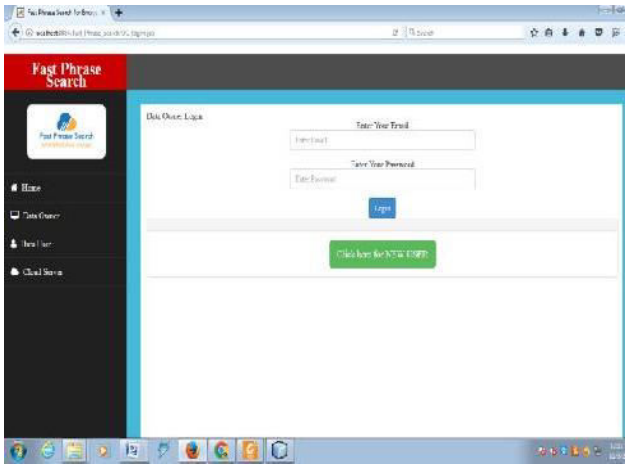
ADVANTAGES OF PROPOSED SYSTEM

1. Our framework differs from some of the earlier works, where keywords generally consist of meta-data rather than content of the files and where a trusted key escrow authority is used due to the use of Identity basedencryption.

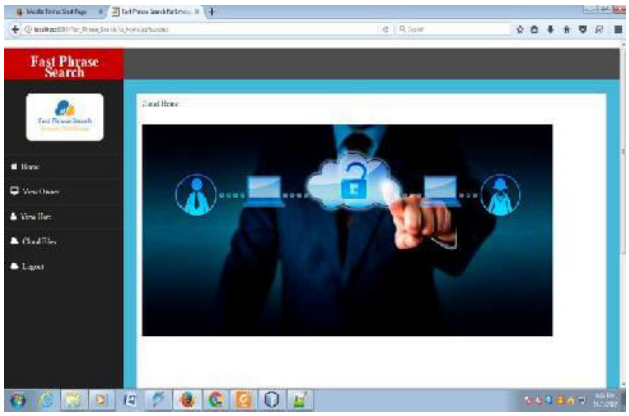
2. When compared to recent works, where an organization wishes to outsource computing resources to a cloud storage provider and enable search for its employees, where the aim is to return properly ranked files. Most other recent works related to search over encrypted data have considered similar models such as, where the client acts as both data owner and user**.**

Fig.1: System Architecture

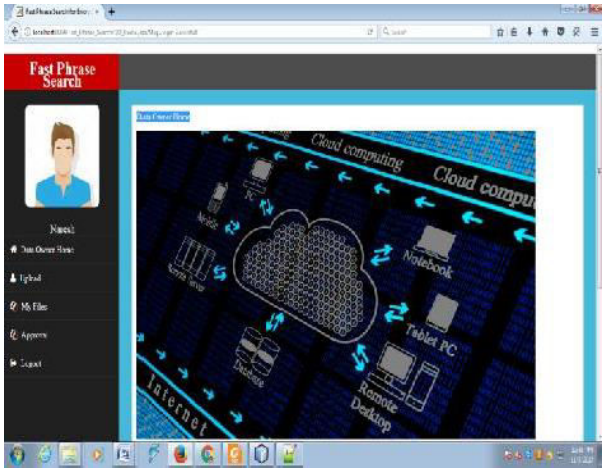


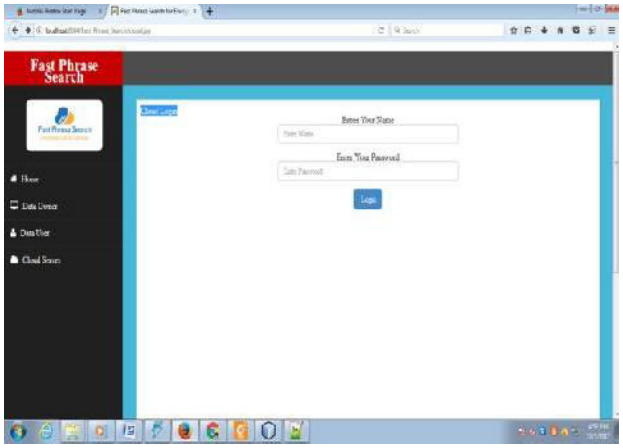


Data Owner Home File Upload



Home Page Data Owner Login





CONCLUSION

In this paper, we presented a phrase search scheme based on Bloom filter that is significantly faster than existing approaches, requiring only a single round of communication and Bloom filter verifications. The solution addresses the high computational cost noted in by reformulating phrase search as n-gram verification rather than a location search or a sequential chain verification. Our schemes consider only the existence of a phrase, omitting any information of its location. Our schemes do not require sequential verification, is parallelizable and has a practical storage requirement. Our approach is also the first to effectively allow phrase search to run independently without first performing a conjunctive keyword search to identify candidate documents. The technique of constructing a Bloom filter index enables fast verification of Bloom filters in the same manner as indexing. According to our experiment, it also achieves a lower storage cost than all existing solutions except where a higher computational cost was exchanged in favor of lower storage. While exhibiting similar communication cost to leading existing solutions, the proposed solution can also be adjusted to achieve maximum speed or high speed with a reasonable storagecost depending on the application. An approach is also described to adapt the scheme to defend against inclusion-relation attacks. Various issues on security and efficiency, such as the effect of long phrases and precision rate, were also discussed to support our design choices

REFERENCES

[1] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in In proceedings of Eurocrypt, 2004, pp. 506–522.

[2] B. Waters, D. Balfanz, G. Durfee, andD. K. Smetters, “Building an encrypted and searchable audit log,” in Network and Distributed System Security Symposium, 2004.

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

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

[5] C. Hu and P. Liu, “Public key encryption with ranked multikeyword search,” in International Conference onIntelligent