IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 14-16

Fast phrase search scheme in cloud computing for encrypted keyword

Mr.T.Ragupathi.M.E., Assistant Professor,
Department Of Cse.,Mailam Engineering College,Mailam.

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

I. Introduction

AS organizations and individuals adopt cloud technologies, many have become aware of the serious concerns regarding security and privacy of accessing personal and confidential information over the Internet. In particular, the recent and continuing data breaches highlight the need for more secure cloud storage systems. While it is generally agreed that encryption is necessary, cloud providers often perform the encryption and maintain the private keys instead of the data owners. That is, 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 data breach. Hence, researchers have actively been exploring solutions for secure storage on private and public clouds where private keys remain in the hands of data owners. Boneh et al. [1] proposed one of the earliest works on keyword searching. Their scheme uses public key encryption to allow keywords to be searchable without revealing data content. Waters et al. [2] investigated the problem for searching over encrypted audit logs. Many of the early works focused on single keyword searches. Recently, researchers have proposed solutions on conjunctive keyword search, which involves multiple keywords [3], [4]. Other interesting problems, such as the ranking of search results [5], [6], [7] and searching with keywords that might contain errors [8], [9] termed fuzzy keyword search, have also been considered. The ability to search for phrases was also recently investigated [10], [11], [12], [13]. Some [14] have examined the security of the proposed solutions and, where flaws were found, solutions were proposed [15]. 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 H.T. Poon and A. Miri are with the Department of Computer Science, Ryerson University, Toronto, Ontario, Canada E-mail: hoiting.poon@ryerson.ca, samiri@scs.ryerson.ca easily be removed and added to the corpus.We also describe modifications to the scheme to lower storage cost at a small

cost in response time and to defend against cloud providers with statistical knowledge on stored data. We begin by presenting the communication framework in section 2 and various backgrounds including related works in section 3. 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 in section 4 along with design techniques in section 4.3. Performance analysis and experimental results are included in section 5 and 6.

II. Existing System

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 data content. Waters et al. investigated the problem for searching over encrypted audit logs. Many of the early works focused on single keyword searches. Recently, researchers have proposed solutions on conjunctive keyword search, which involves multiple keywords. 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 recently investigated. Some of the existing system has examined the security of the proposed solutions and, where flaws were found, solutions were proposed

Disadvantage Of Existing System

- 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 data breach.
- 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-side encryption and decryption may still be computationally expensive in certain applications.
- 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.

III. Proposed System

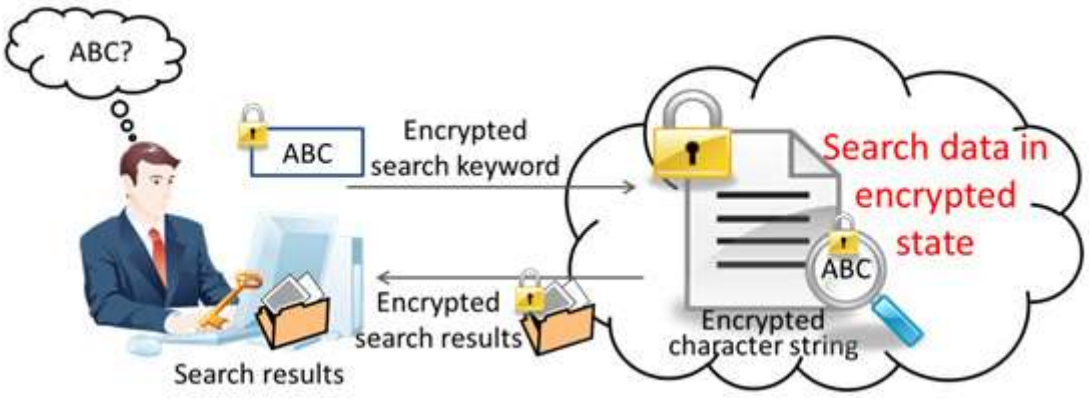
In this paper, we present a phrase search scheme which achieves a much faster response time than existing solutions. The scheme is also scalable, where documents can easily be removed and added to the corpus. We also describe modifications to the scheme to lower storage cost at a small cost in response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

Advantage Of Proposed System

- 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 based encryption.
- 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.

.

IV. Architecture Diagram



V. Conclusion

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 introduced in section 4.2 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 [13], 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 storage cost 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, and D. 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 scheme based 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.