Fast Phrase Search For Encrypted Cloud Storage

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. A design approach based on an application's target false positive rate is also described.

EXISTING SYSTEM

- In this paper, we present a phrase search scheme which achieves a much faster response time than existing solu-tions. 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 us-ing our technique, they are typically a specialized function in a keyword search scheme, where the primary function is to provide conjunctive keyword searches

DISADVANTAGES

- Serious concerns regarding security and privacy of accessing personal and confidential information over the Internet

PROPOSED SYSTEM

- 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. Unlike , our schemes consider only the existence of a phrase,omitting any information of its location. Unlike, our schemes do not require sequential verification, is paralleliz-able and has a practical storage requirement. Our approach is also the first to effectively allow phrase search to run inde-pendently without first performing a conjunctive keyword search to identify candidate documents.

ADVANTAGES

- According to our proposed system, it also achieves a lower storage cost than all existing solutions except.

HARDWARE REQUIREMENTS

System	: Pentium IV 2.4 GHz.
Hard Disk	: 40 GB.
Floppy Drive	: 1.44 Mb.
Monitor	: 15 VGA Colour.
Mouse	: Logitech.
Ram	: 512 Mb.

SOFTWARE REQUIREMENTS

- Operating system : Windows XP/7.
- Coding Language : ASP.net, C#.net /java

CONCLUSION

- 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. Unlike [our schemes consider only the existence of a phrase,omitting any information of its location. Unlike , our schemes do not require sequential verification, is paralleliz-able and has a practical storage requirement. Our approach is also the first to effectively allow phrase search to run inde-pendently without first performing a conjunctive keyword search to identify candidate documents.

REFERENCE

- [1] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in In proceedings of Euro-crypt, 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