Abstract

Cloud computing has emerged as a new technology that aims to provide unlimited virtualized resources to clients and enterprises. As services and huge sensitive data are being moved to the cloud server, a new challenge arises as to how to use the migrated data in a way that preserves privacy. Due to privacy concerns, important data should be encrypted before uploading onto cloud servers, so that only authenticated clients can access the data. Searchable encryption techniques allow the clients to search the encrypted data. Public key encryption with keyword search (PEKS) is a scheme of searchable encryption using a public key solution. In our scheme, we present a novel public key encryption with the 'fixed and short length' keyword search which reduce the size of the keyword space and get keywords with a fixed and short length. Further, we employe the Bloom filters (BFs), which can accelerate the search process with a large amount of keywords. We also analyse the security of our construction in the random oracle model.

References
without Random Oracles. Advances In Cryptology-Eurocrypt 2004, LNCS 3027, pp. 223- 238,
Springer-Verlag.
Issue 7.
Ranked Search over Encrypted Cloud Data, in: IEEE transactions on parallel and distributed
systems, Vol. 25, No. 1.
253-262.
Oard, D., W., Confidentialitypreserving rank-ordered search, in: Proceedings of the 2007 ACM
7-12.
Public-key Searchable Encryption with Strong Privacy Guarantee, in: INFOCOM, 2015
Proceedings IEEE, pp. 2092-2100.
preserving multi-keyword text search in the cloud supporting similaritybased ranking, in:
Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and
over encrypted cloud data with ranking, in Springer Distributed and Parallel Databases, pp. 119-
160.

Index Terms

Computer Science

Security
Keywords

Cloud Computing, Searchable Encryption, Public key encryption, Bloom filter, Bilinear pairing