User verifiable multiple keyword search scheme using the merkle tree for outsourced data in the cloud

Devi Thiyagarajan, author

Abstrak

Cloud computing has revolutionized the IT industry by offering huge storage for data outsourcing and also for computation. Various security issues concerned with security and privacy of data arise in the context of data outsourcing. The framework enables clients to outsource encrypted data to the cloud, enables users to retrieve preferred documents using multiple keywords and allows the user to verify the response from the server. The strength of the proposed model relies on the discrete logarithmic problem of Hyper Elliptic Curve Cryptography (HECC) and the security of Merkle trees. The paper proposes a user verifiable multi-keyword search scheme, which focuses on: (i) construction of inverted index for the documents with keywords; (ii) index and document encryption by HECC; (iii) index and document authentication by the Merkle tree; and (iv) verification of the accuracy of response from server by top hash or root hash value of the Merkle tree. Security analysis and results demonstrate the correctness of proposed multiple keyword search (MKS) scheme. The search algorithm combined with the hash value verification process by the Merkle tree is strong enough to provide data security, privacy, and integrity. The proposed model reduces the storage overhead on both the client’s and user’s side. As the number of documents increases, the retrieval time is less, which reduces the storage overhead on both sides.