Private Searching on Encrypted Data in Cloud

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 165
Number 7

Year of Publication: 2017

Authors:
Huda M. Saleh, Hameed A. Younis

Abstract

Cloud computing appeared as the most common paradigm in the time being that provides calculations and storage resources by when used – pay method. Users can exploit cloud resources from anywhere at any time without maintenance cost. Flexibility in resource allocation enabled cloud services to be effective in delivering with reasonable cost. However, transfer data to cloud make it vulnerable to leakage, and loss of privacy. Therefore, data security in cloud considered as the primary hurdle of cloud adoption. Many users prefer prior protection for their data using data encryption, which determine cloud popularity, since most searches process are not carry out on encrypted data directly. This paper build secure and effective system for searching over encrypted images in cloud environment and propose public-key image encryption algorithm from RSA and Paillier algorithms. The proposed image encryption algorithm achieved higher security and appropriate processing time, which evaluated by PSNR, Entropy, NPCR, UACI and processing time. We used Scale Invariant Feature Transform algorithm (SIFT) algorithm for image feature extraction, locality sensitive hashing (LSH) to secure sensitive images and build index, and Euclidean distance as similarity metric.
References

Index Terms

Computer Science  Security

Keywords

Cloud Computing, RSA, Paillier, Searchable Encryption, LSH, SIFT