Framework Design for Secured Local Cloud Data Query Processing Analysis


Abstract

Cloud computing is a vastly growing technology that enables more users and organizations to transfer their services to the cloud. With the exploitation of public cloud computing infrastructures, the usage of clouds to provide data query services is becoming an attractive solution due to its numerous benefits on scalability and cost-minimizing. The cloud services especially the database-as-a-service have tended to encrypt sensitive data before the migration over the cloud. Encrypting data would facilitate protecting private information from any violation by the service provider. Several studies have addressed the handling of cloud query processing by providing approaches to maintain the privacy of the data stored within the cloud. During their studies, researchers have proposed different types of encryption methods, each encryption method provides a specific level of security which comes with an opposite level of efficiency. This research is focused on framework design to evaluate cloud data query processing locally using two encryption methods namely AES and RSA. The parameters chosen are time consumption for encryption and decryption along with secrecy or the strength of the encryption and decryption. © 2019 IEEE.

SciVal Topic Prominence

Topic: Cryptography | Cloud computing | Encrypted cloud

Prominence percentile: 98.682

Author keywords

decryption, encryption, local cloud data query

Indexed keywords

Engineering controlled terms: Cloud computing, Data handling, Query processing

Engineering uncontrolled terms: Attractive solutions, Cloud data, Database as a service, decryption, Encryption and decryption, Encryption methods, Framework designs, Private information