Enhancement of security in cloud computing is challengeable when big data such as medical and government confidential information involves in a cloud environment. The managing key for individual user participated in the mobile cloud will be the problem when big data is handled without efficient security key management. Especially, mobile cloud nodes where users handle their data can be anywhere else in the cloud environment. So, managing keys for random users and finding correct locations of users’ nodes and their identities are interesting areas for the research. To solve this problem related to key management, cloud services need efficient key management that employs quantum cryptography using Grover’s algorithm. Moreover, in this research, we introduce effective authentication technique in order to improve the level of security (with minimum complexity) In this paper, theoretical model, Grover’s algorithm and quantum cryptography with the PairHand protocol are considered as methodologies. As summarized results, security levels of users and services providers are considered to verify the services used in a cloud environment. In spite of same quantum properties characterize the light, data security issues are still not matured with the light technology. Hiding the big data in
the light through this research methodology will be the conclusion of the future security.

References


Index Terms

Computer Science Security

Keywords

Big data security; PairHand protocol; Key Management; Quantum cryptography; Cloud services