Abstract

Cloud plays the vital role in internet world. Cloud provides storages, platforms which improves the functionality. Cloud storage shows how securely and flexibly we can store and share our data. With the help of keys user can easily and securely share their data over cloud. This introduces Key Aggregate Cryptosystem in which an aggregate key is created using which user can share their data partially over cloud and it provides a constant size ciphertext. In spite of traditional cryptographic key generation techniques, this technique possesses unique cryptographic key aggregate cryptosystem which is helpful for secure cloud and privacy preserving key generation process. We propose access level policy structure such as Public and Private Access level to improve the data access mechanism in the data sharing cloud.
mechanism process. We are using algorithm such as Blowfish algorithm which results in higher security and faster execution when compared to AES (Advanced Encryption standard) and DES (Data Encryption Standard). Also the blowfish algorithm is unpatented and no license is required.

References

Patient Controlled Encryption using Key Aggregation with Blowfish Algorithm


Index Terms

Computer Science
Algorithms

Keywords

Virtual Machine Key Aggregate Encryption Ciphertext Attribute Based Encryption Aggregate Keys

Extraction