Abstract

Cloud has become very important 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. This technique introduces a special type of encryption called as key-aggregate cryptosystem which allows user to share their data partially across cloud and which produces constant size ciphertext. In this technique user provide a constant-size aggregate key for different ciphertext classes in cloud storage, but the other encrypted files outside the class remain confidential. We also compare this technique with existing one. We implemented this cryptosystem for public-key patient-controlled encryption system.

References

Patient Controlled Encryption using Key Aggregation

- S. S. M. Chow, J. Weng, Y. Yang, and R. H. Deng, "Efficient Unidirectional

Index Terms
Computer Science
Security

Keywords
Virtual machine Key aggregate encryption ciphertext Attribute based Encryption Aggregate keys Extraction