Abstract

Data owner encrypt their data before outsourcing into the cloud for the purpose of privacy preserving. Additionally, the attribute based encryption method is used to enhance the confidentiality and access control. Delegation is a process which is performed by the users who are containing the less computing power. They delegate their decryption process to the cloud server to reduce the computation cost. This time the cloud server may change the given cipher text and sends the modified one to the data user for malicious attack. This time the access control cannot be malleable. To enhance the access control, we propose a circuit cipher text-policy attribute-based hybrid encryption with verifiable delegation method. For the authentication purpose, mac mechanism is added with the symmetric encryption technique. By this mechanism, we can certify the confidentiality of data, accuracy of the delegated computing results and enhance the access control. Our paper uses the k-multi linear Decisional Diffie-Hellman algorithm to improve the security to the encrypted data. This scheme takes only less computational and communication cost so it will be done at practically.


Index Terms

Computer Science

Distributed Systems

Keywords

Attribute based encryption, data sharing, verifiable delegation, authentication, confidentiality.