Abstract

The notion of attribute-based encryption (ABE) was proposed as an economical alternative to public-key infrastructures. ABE is also a useful building block in various cryptographic primitives such as searchable encryption. For ABE, it is not realistic to trust a single authority to monitor all attributes and hence distributing control over many attribute-authorities is desirable. A multi-authority ABE scheme can be realized with a trusted central authority (CA) which issues part of the decryption key according to a user’s global identifier (GID). However, this CA may have the power to decrypt every cipher text, and the use of a consistent GID allowed the attribute-authorities to collectively build user’s attributes. Decentralized ABE scheme can eliminate the burden of heavy communication and collaborative computation. It is observed that privacy-preserving decentralized key-policy ABE scheme has claimed to achieve better privacy for users and is provably secure in the standard model. However, after carefully revisiting the scheme, it is observed that existing system cannot resist the collusion attacks, hence fails to meet the basic security definitions of the ABE system. This paper proposes a solution without the trusted CA and without compromising users’ privacy, thus making ABE more usable in practice. The privileged users are the users who will exactly match policy attributes with decentralized authority. To the best of our knowledge this framework of privileged users enhances the access control mechanism by avoiding the collusion. Collusion attack occurs
when more than one user try to occupy same resource at a time. Proposed system resists collusion attack at every execution. After some encryption and decryption there can be load on the system. This load can be reduced using this system in terms of processing speed. When system load is increased backup server will be initialized to reduce system load and speedup the processing of cryptography. The message privacy is therefore enhanced with load balancing using attribute based encryption (LB-ABE), as it provides an added support of rebalancing which inherently supports optimally more user work-load.

References


Index Terms

Computer Science  Distributed Systems
Keywords
Attribute-based Encryption  Global Identifier  Privacy  Decentralized Authority  Access Control.