Abstract

In Ciphertext-Policy Attribute Based Encryption (CP-ABE), attributes are attached to the user's secret key and access policy is attached to the ciphertext. If attributes in the secret key of a user satisfy the policy then only the user can decrypt the ciphertext. However, such scenario also necessitates periodic updating of the secret key with the changing attributes. According to our observations, the existing attempts at doing so are not efficient. In this paper, we propose a new approach to add, update or delete the value of a particular attribute efficiently without the knowledge of the other attributes.
References

- Nanxi Chen, Mario Gerla Dynamic Attributes Design in Attribute Based Encryption. Annual Conference of ITA (ACITA), University of Maryland University College, September. 2009.
toolkit.

Index Terms

Computer Science Security

Keywords

Attribute Attribute Based Encryption Dynamic Attributes Network Security