A Dynamic Multi-Group Secure Data Sharing Scheme for Cloud

Md Azharul Islam

ABSTRACT
The need for secure data sharing has become more important than ever before as privacy is a big concern in content sharing via cloud, social media or online blogs. All the previous work in secure group data sharing were primarily focused on single group setting. But in real life, organizations that are potential users of cloud based data sharing platforms are mostly multi-group in nature and single group setting based schemes essentially fail to provide any practical solution for them. In this paper, we provide the first solution for secure cloud data sharing in multi-group setting. Towards our solution, we combine ciphertext-policy attribute-based encryption (CP-ABE) scheme with Tree-based Group Diffie-Hellman (TGDH) protocol. Our solution is distributed and scalable in nature which is preferable for cloud platforms. In our approach, entire user domain is divided into multiple independent groups based on the affiliations of the users and group administrative task is equally distributed among admins of different groups. Unlike most of the previous CP-ABE based data sharing schemes, current users do not need to change their secret keys in our scheme when an existing user leaves group or new user joins in. Our performance assessment shows that our solution is highly efficient when compared with others and also meets the necessary security requirements.