246. ANONYMOUS AUTHENTICATION IN CLOUD USING IBE AND RSA

Mrs A.Revathi[1], M. Sharmil nisha[2],
Department of Computer Science and Engineering, Peri Institute of Technology
Chennai
Email id: sharmilnisha@gmail.com

Security and privacy are very important issues in the cloud computing, We propose a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. By using this scheme, cloud server helps to identify the user as an authorized one, without knowing the user identity before storing the data. In addition, the scheme has an added feature of access control which means authorized users can access the data. There are three users: creator, reader & writer. Creator receives a token from a trustee i.e. organization after giving ID to the trustee. There are multiple Key Distribution Centers (KDC) which can be scattered. A creator gives their token to one or more KDC's then creator receives keys for encryption & decryption and for signing from KDC's. The message is encrypted under access policy which means it decides who can access the data stored in the cloud. Creator decides on a claim policy to prove her authenticity and signs the message under this claim. The cipher text is sent to the cloud. The cloud verifies the signature and stores the cipher text. When a reader wants to read, the cloud sends cipher text. If the user has attributes matching with access policy, it can decrypt and get back original message. The proposed design allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server.

ISBN 978-81-904760-6-5