

**CHENNAI – PONDICHERRY**

**KEY-POLICY ATTRIBUTE-BASED ENCRYPTION WITH**

**EQUALITY TEST IN CLOUD COMPUTING**

**Abstract:**

The privacy of users must be considered as the utmost priority in distributed networks. To protect the identities of users, attribute-based encryption (ABE) was presented by Sahai et al. ABE has been widely used in many scenarios, particularly in cloud computing. In this paper, public key encryption with equality test is concatenated with key-policy ABE (KP-ABE) to present KP-ABE with equality test (KP-ABEwET). The proposed scheme not only offers fine-grained authorization of ciphertexts but also protects the identities of users. In contrast to ABE with keyword search, KP-ABEwET can test whether the ciphertexts encrypted by different public keys contain the same information. Moreover, the authorization process of the presented scheme is more flexible than that of Ma et al.'s scheme. Furthermore, the proposed scheme achieves one-way against chosen-ciphertext attack based on the bilinear Diffie-Hellman (BDH) assumption. In addition, a new computational problem called the twin-decision BDH problem (tDBDH) is proposed in this paper. tDBDH is proved to be as hard as the decisional BDH problem. Finally, for the first time, the security model of authorization is provided, and the security of authorization based on the tDBDH assumption is proven in the random oracle model.