

**CHENNAI – PONDICHERRY**

**IMPROVING PRIVACY-PRESERVING AND SECURITY FOR DECENTRALIZED KEY-POLICY ATTRIBUTED-BASED ENCRYPTION**

**Abstract:**

Decentralized attribute-based encryption(ABE) is an efficient and flexible multi authority attribute-based encryption system, since it does not requires the central authority and does not need to cooperate among the authorities for creating public parameters. Unfortunately, recent works show that the reality of the privacy-preserving and security in almost well-known decentralized key policy ABE(KP-ABE) schemes are doubtful. How to construct a decentralized KP-ABE with the privacy- preserving and user collusion avoidance is still a challenge problem. Most recently, Y.Rahulamathavam et al. proposed a decentralized key-policy(KP) ABE scheme to try avoiding user collusion and preserving the user’s privacy. However, we exploit the vulnerability of their scheme in this paper at first and present a collusion attack on their decentralized KP-ABE scheme. The attack shows the user collusion can not be avoided. Subsequently, a new privacy-preserving decentralized KP-ABE is proposed. The proposed scheme avoids the linear attacksat present and achieves the user collusion avoidance. We also show that the security of the proposed scheme is reduced to decisional bilinear Diffie-Hellman(DBDH) assumption. Finally, numerical experiments demonstrate the efficiency and validity of the proposed scheme.