

**CHENNAI – PONDICHERRY**

**NON-REPUDIABLE PROVABLE DATA POSSESSION SCHEME WITH DESIGNATED VERIFIER IN CLOUD STORAGE SYSTEMS**

**Abstract:**

In cloud storage systems, users can upload their data along with associated tags (authentication information) to cloud storage servers. To ensure the availability and integrity of the outsourced data, provable data possession (PDP) schemes convince verifiers (users or third parties) that the outsourced data stored in the cloud storage server is correct and unchanged. Recently, several PDP schemes with designated verifier (DV-PDP) were proposed to provide the flexibility of arbitrary designated verifier. A designated verifier (private verifier) is trustable and designated by a user to check the integrity of the outsourced data. However, these DV-PDP schemes are either inefficient or insecure under some circumstances. In this paper, we propose the first non-repudiable PDP scheme with designated verifier (DV-NRPDP) to address the non-repudiation issue and resolve possible disputations between users and cloud storage servers. We define the system model, framework and adversary model of DV-NRPDP schemes. Afterward, a concrete DV-NRPDP scheme is presented. Based on the computing discrete logarithm assumption, we formally prove that the proposed DV-NRPDP scheme is secure against several forgery attacks in the random oracle model. Comparisons with the previously proposed schemes are given to demonstrate the advantages of our scheme.