

**CHENNAI – PONDICHERRY**

**EFFICIENT PRIVACY-AWARE AUTHENTICATION SCHEME FOR MOBILE CLOUD COMPUTING SERVICES**

**Abstract:**

With the exponential increase of the mobile devices and the fast development of cloud computing, a new computing paradigm called mobile cloud computing (MCC) is put forward to solve the limitation of the mobile device's storage, communication, and computation. Through mobile devices, users can enjoy various cloud computing services during their mobility. However, it is difficult to ensure security and protect privacy due to the openness of wireless communication in the new computing paradigm. Recently, Tsai and Lo proposed a privacy-aware authentication (PAA) scheme to solve the identification problem in MCC services and proved that their scheme was able to resist many kinds of existing attacks. Unfortunately, we found that Tsai and Lo's scheme cannot resist the service provider impersonation attack, i.e., an adversary can impersonate the service provider to the user. Also, the adversary can extract the user's real identity during executing the service provider impersonation attack. To address the above problems, in this paper, we construct a new PAA scheme for MCC services by using an identity-based signature scheme. Security analysis shows that the proposed PAA scheme is able to address the serious security problems existing in Tsai and Lo's scheme and can meet security requirements for MCC services. The performance evaluation shows that the proposed PAA scheme has less computation and communication costs compared with Tsai and Lo's PAA scheme.