

**CHENNAI – PONDICHERRY**

**CLOAK: A STREAM CIPHER BASED ENCRYPTION PROTOCOL FOR MOBILE CLOUD COMPUTING**

**Abstract:**

Mobile device and its applications have revolutionized the way we store and share data. It is becoming a warehouse of users personal information. Unluckily, most of these data are stored in an unencrypted format, prone to security threats. In this paper, we propose a lightweight, computationally efficient protocol, called CLOAK, for the mobile device. CLOAK is based on stream cipher and takes the help of an external server for the generation and distribution of cryptographically secure pseudo-random number (CSPRN). In order to enhance the security of our protocol, we use the concept of symmetric key cryptography. We present three versions of the protocol referred as s-CLOAK, r-CLOAK and d-CLOAK, varying on the basis of the key selection procedure. In CLOAK, the core encryption/decryption operation is performed within the mobile devices to secure data at its origin. The security of CSPRN is ensured using deception method. In CLOAK, all messages are exchanged securely between mobile and the server with mutual identity verification. We evaluate CLOAK on Android smart phones and use Amazon Web services for generating CSPRN. Additionally, we present attack analysis and show that the brute force attack is computationally infeasible for the proposed protocol.