

**CHENNAI – PONDICHERRY**

**ENHANCED INSTANT MESSAGE SECURITY AND PRIVACY PROTECTION SCHEME FOR MOBILE SOCIAL NETWORK SYSTEMS**

**ABSTRACT:**

Instant messaging (IM) systems can be considered the most frequently used applications in mobile social networks. Nowadays, people are becoming increasingly concerned about data security and privacy protection with IM applications. Therefore, a comprehensive enhanced secure IM scheme was proposed in this paper, which is based on the elliptic curve cryptosystem and the advanced encryption standard algorithm. An offline key agreement process between users was designed under the computational Diffie-Hellman (CDH) assumption by updating the ephemeral key periodically. The proposed scheme supports denial of replaying attack and denial of forgery attack by utilizing timestamps and the elliptic curve digital signature algorithm. It supports multiple types of messages (such as document and multimedia messages) and prevents privacy leakage by storing sent and received messages with ciphertext. We proved the security of the proposed scheme under the elliptic curve discrete logarithm assumption and the CDH assumption. The comparison results of the proposed scheme with other schemes and the results of an experiment show that it is a comprehensive secure scheme with high security and good practicability.practicability.