**ABSTRACT**

Identity-Based Encryption (IBE) is an alternative to public key encryption which simplifies the public key at Public Key Infrastructure (PKI). However, the only drawback of IBE is the overhead computation at Private Key Generator (PKG) during revocation of user. In traditional PKI setting efficient revocation has been well studied, but the cumbersome management of private keys is precisely the burden that IBE strives to alleviate. In this paper, objective to tackle the critical issue of identity revocation, we introduce outsourcing computation into IBE for the propose to reduce the overburden at PKG. Our scheme offloads most of the key generation related operations during key-issuing and key-update processes to a Key Update Cloud Service Provider, leaving only a constant number of simple operations for PKG and users to perform locally. This goal is achieved by using KU-CSP: we employ a hybrid private key which is a combination of identity component and time component for each user.

**Project Title: IDENTITY-BASED ENCRYPTION USING KEY UPDATE-CSP**

**Name: Prabhunath Yadav**

**Reg No: 1031210334**

**Name: Ashish jangu  
Reg No: 1031210332**

**Project Guide: Mr. M. RAJASEKARAN**