**IDENTITY-BASED ENCRYPTION USING KEY UPDATE-CSP**

**SRM University**

**Department of Computer Science and Engineering**

**Kattankullathur, Chennai , Tamil Nadu 603203  
  
  
Name: Prabhunath Yadav**

**Reg No: 1031210334**

**Branch:CSE  
Name:Ashish Jangu**

**Reg No: 1031210332**

**Branch: CSE**

**Under the guidance of Mr. M. RAJASEKARAN**

**(Assistant Professor)**

**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.

**EXISTING SYSTEM**

As far as we know, though revocation has been thoroughly studied in PKI, few revocation mechanisms are known in IBE setting. In Boneh and Franklin suggested that users renew their private keys periodically and senders use the receivers’ identities concatenated with current time period. But this mechanism would result in an overhead load at PKG. It requires that PKG is online and the secure channel must be maintained for all transactions, which will become a bottleneck for IBE system as the number of users grows. It requires that PKG is online and the  
secure channel must be maintained for all transactions, which will become a bottleneck for IBE system as the number of users grows. For this reason,a challenge on how to design a secure revocable IBE scheme to reduce the overhead computation at PKG with an untrusted CSP is raised.