

A privacy Control System in Cloud Computing Environment using Identity based Encryption and Signature (IBE and IBS)

Cho Cho Kyaw

University of Computer Studies, Yangon

star90.cck@gmail.com

Abstract

Privacy protection play a vital role to build up the cloud computing environment. This system intends to implement secure cloud privacy system using Identity based Encryption (IBE) and Identity based Signature (IBS) algorithms, that do not have to generate the keys itself. IBE and IBS systems allow any party such as cloud provider, cloud user and trusted third party to generate a public key from a known unique identity value. Private Key Generator (PKG) generates the corresponding private keys. This system generates public key and private key of cloud service provider (CSP) and cloud users by PKG using IBE and IBS for each group. When data sent from server to client, first data is encrypted using public key of user. Data is signed using the private key of server for the authentication of sender. This system implements a cloud server and cloud clients where cloud server stores client data in its data center.