Cryptology ePrint Archive: Report 2011/169

Identity-Based Cryptography for Cloud Security

Hongwei Li, Yuanshun Dai, Bo Yang

Abstract: Cloud computing is a style of computing in which dynamically scalable and commonly virtualized resources are provided as a service over the Internet. This paper, first presents a novel Hierarchical Architecture for Cloud Computing (HACC). Then, Identity-Based Encryption (IBE) and Identity-Based Signature (IBS) for HACC are proposed. Finally, an Authentication Protocol for Cloud Computing (APCC) is presented. Performance analysis indicates that APCC is more efficient and lightweight than SSL Authentication Protocol (SAP), especially for the user side. This aligns well with the idea of cloud computing to allow the users with a platform of limited performance to outsource their computational tasks to more powerful servers.

Category / Keywords: public-key cryptography / identity-based cryptography

Date: received 3 Apr 2011

Contact author: hongwei uestc at gmail com