Abstract: Broadcast-Based Anonymous Authentication for Distributed Systems

Jongseok Choi, Howon Kim*
Information Security and System LSI Laboratory,
Computer EngeneeringEngineering Department,
Pusan National University,
Busandaehak-ro 63beon-gil,
Geumjeong-gu, Busan, Korea
Tel: +82-51-510-1010
Fax: +82-51-517-2431
Jschoi85@pusan.ac.kr, howon@pusan.ac.kr

Abstract

Cloud computing system has been actively reviewed by a number of researchers. Unfortunately, most researchers have not considered the security of the cloud computing system. Two problems for cloud computing exists: one on the side of client, and one on the side of the server. On the client side, it involves private security of the clients, and on the server side, the problem is related to server compliance of the server. Unfortunately, Identity-Based Encryption has to reveal client IDs to maintain data confidence. In this paper, we propose a scheme which protects the anonymity of users. The scheme is based on pairing operations, since pairing makes the cloud computing system use public key cryptography with a non-PKI framework. The proposed scheme forms a hierarchical model and partially broadcasts the messages for anonymity. Our scheme has three advantages: 1) it ensures anonymity, 2) it does not use SSL Authentication Protocol (SAP), and 3) its traffic is lower than that of general broadcasting.

Acknowledgement

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (No.2010-0026621).