عنوان مقاله:

An Efficient Identity-based Storage and Computation Auditing Protocol in Cloud Computing

محل انتشار:

هفتمین کنفرانس بین المللی فناوری اطلاعات، کامپیوتر و مخابرات (سال: 1398)

تعداد صفحات اصل مقاله: 11

نویسندگان:

Maryam Rahabzadeh Asaar - *Department of Electrical and Computer Engineering, Islamic Azad University, Science and Research Branch, Tehran*

Niloufar Vatanara - *Department of Electrical and Computer Engineering, Islamic Azad University, Science and Research Branch, Tehran*

خلاصه مقاله:

Cloud computing is a paradigm to achieve reliable computational and storage capabilities for cloud users. Cloud security provides storage and computation security in way that cloud users can trust on the correctness of stored data and computation result. In 2014, the first privacy cheating discouragement and secure computation auditing protocol using designated verifier signatures named as SecCloud was proposed by Wei et al. In this paper, we modified the protocol to be more efficient and secure in this way it will be pairing-free and also session keys will be fresh for each message. Then, to guarantee that it is uncheatable and can satisfy privacy cheating discouragement, we show that underlying designated verifier signature is existentially unforgeable against adaptively chosen-message and identity attack under Computational Diffie-Hellman Problem (CDHP) in the random oracle model.

کلمات کلیدی:

Secure auditing, designated verifier signature, batch verification, cloud computing.