Cryptology ePrint Archive: Report 2011/158

Enhancing Data Privacy in the Cloud

Yanbin Lu and Gene Tsudik

Abstract: Due to its low cost, robustness, flexibility and ubiquitous nature, cloud computing is changing the way entities manage their data. However, various privacy concerns arise whenever potentially sensitive data is outsourced to the cloud.

This paper presents a novel approach for coping with such privacy concerns. The proposed scheme prevents the cloud server from learning any possibly sensitive plaintext in the outsourced databases. It also allows the database owner to delegate users to conducting content-level fine-grained private search and decryption. Moreover, our scheme supports private querying whereby neither the database owner nor the cloud server learns query details. Additional requirement that user's input be authorized by CA can also be supported.

Category / Keywords: applications / Cloud, Privacy

Date: received 31 Mar 2011

Contact author: yanbinl at uci edu