Abstract

Outsourcing data in the cloud environment has recently gained special attention. However, data privacy remains one of the top concerns for users in cloud outsourcing scenarios. In this paper, we propose a privacy preserving query protocol based on proxy re-encryption schemes. The proposed protocol protects data privacy of all users in a multi-user cloud setting. Data privacy is preserved against honest but curious adversary model.

References

2. Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Trans. Inf. Syst.
Privacy-Preserving Protocol in Multi-User Cloud

4. Fangquan Cheng, Qian Wang, Qianwen Zhang, and Zhiyong Peng. Highly efficient
   indexing for privacy-preserving multikeyword query over encrypted cloud data. In Web-Age
5. Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano
   Paraboschi, and Pierangela Samarati. Keep a few: Outsourcing data while maintaining
   confidentiality. In Computer Security - ESORICS 2009, 14th European Symposium on Research
6. Ernesto Damiani, S. De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano
   In Proceedings of the 2005 ACM Workshop on Storage Security and Survivability, StorageSS ’05,
7. Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and
   Pierangela Samarati. Encryption policies for regulating access to outsourced data. ACM Trans.
8. Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, Gerardo Pelosi, and
   Pierangela Samarati. Efficient and private access to outsourced data. In 2011 International
   Conference on Distributed Computing Systems, ICDCS 2011, Minneapolis, Minnesota, USA,
9. Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, and Pierangela
    computation on the cloud via multikey fully homomorphic encryption. Cryptology ePrint Archive,
    ACM Symposium on Operating Systems Principles 2011, SOSP 2011, Cascais, Portugal,
16. Stephen Tu, M. Frans Kaashoek, Samuel Madden, and Nickolai Zeldovich. Processing
    analytical queries over encrypted data. Proceedings of the VLDB Endowment, PVLDB,
17. Li Xiong, Subramanyam Chitti, and Ling Liu. Preserving data privacy in outsourcing data

Index Terms
Keywords

Privacy-Preserving Protocol, Data Privacy, Cloud Computing, Multi-User