Cryptology ePrint Archive: Report 2011/185

Efficient and Secure Data Storage Operations for Mobile Cloud Computing

Zhibin Zhou and Dijiang Huang

Abstract: Cloud computing is a promising technology, which is transforming the traditional Internet computing paradigm and IT industry. With the development of wireless access technologies, cloud computing is expected to expand to mobile environments, where mobile devices and sensors are used as the information collection nodes for the cloud. However, users' concerns about data security are the main obstacles that impede cloud computing from being widely adopted. These concerns are originated from the fact that sensitive data resides in public clouds, which are operated by commercial service providers that are not trusted by the data owner. Thus, new secure service architectures are needed to address the security concerns of users for using cloud computing techniques.

In this paper, we present a holistic security framework to secure the data storage in public clouds with the special focus on lightweight wireless devices store and retrieve data without exposing the data content to the cloud service providers. To achieve this goal, our solution focuses on the following two research directions: First, we present a novel Privacy Preserving Cipher Policy Attribute-Based Encryption (PP-CP-ABE) to protect users' data. Using PP-CP-ABE, light-weight devices can securely outsource heavy encryption and decryption operations to cloud service providers, without revealing the data content and used security keys. Second, we propose an Attribute Based Data Storage (ABDS) system as a cryptographic access control mechanism. ABDS achieves information theoretical optimality in terms of minimizing computation, storage and communication overheads. Especially, ABDS minimizes cloud service charges by reducing communication overhead for data managements. Our performance assessments demonstrate the security strength and efficiency of the presented solution in terms of computation, communication, and storage.

Category / Keywords:

Date: received 10 Apr 2011

Contact author: zhibin zhou at asu edu