Cryptology ePrint Archive: Report 2011/668

Re-Encryption-Based Key Management Towards Secure and Scalable Mobile Applications in Clouds

Piotr K. Tysowski and M. Anwarul Hasan

Abstract: Cloud computing confers strong economic advantages, but many clients are reluctant to implicitly trust a third-party cloud provider. To address these security concerns, data may be transmitted and stored in encrypted form. Major challenges exist concerning the aspects of the generation, distribution, and usage of encryption keys in cloud systems, such as the safe location of keys, and serving the recent trend of users that tend to connect to contemporary cloud applications using resource-constrained mobile devices in extremely large numbers simultaneously; these characteristics lead to difficulties in achieving efficient and highly scalable key management. In this work, a model for key distribution based on the principle of dynamic data re-encryption is applied to a cloud computing system in a unique way to address the demands of a mobile device environment, including limitations on client wireless data usage, storage capacity, processing power, and battery life. The proposed cloud-based re-encryption model is secure, efficient, and highly scalable in a cloud computing context, as keys are managed by the client for trust reasons, processor-intensive data re-encryption is handled by the cloud provider, and key redistribution is minimized to conserve communication costs on mobile devices. A versioning history mechanism effectively manages keys for a continuously changing user population. Finally, an implementation on commercial mobile and cloud platforms is used to validate the performance of the model.

Category / Keywords: cryptographic protocols / key management

Date: received 9 Dec 2011

Contact author: pktysows at uwaterloo ca