Secure Dropbox

Gu Juntao, M.Sc.

University of Dublin, Trinity College, 2013

Supervisor: Tewari Hitesh

Recently there have been increasing requirements about utilizing cloud technology for data maintaining and management especially when reliable, stable data storage and remote data access required. Since the cloud storage service is usually designed to be available to users over the Internet, it essentially facilitates the data sharing as well. However, security concerns are growing as the most commonly cited reason why users, particularly those enterprise users who are information confidentiality critical, are not interested in SaaS, of which cloud storage services like Dropbox or Google Drive are typical instances. The use of those cloud storage service is actually exposing the sensitive data to the service vendors and government agencies.

This research project aims to investigate the feasibility of solving the data exposing issue and achieving the goal of secure data sharing via encryption approaches. It was decided to develop an application to explore this topic. A client end encryption tool would be implemented based on Python and Python accredited cryptography related modules. What is more, a key management system (KMS) with features of file encryption management, user profile management and sharing information management would be deployed to realize the function of everywhere use and secure data sharing. Dropbox would be selected as the instance of SaaS cloud storage service for demonstration purpose so that Dropbox core API would be used.

The result of the project indicated the idea of the hybrid application of symmetric and asymmetric cryptography algorithm could effectively protect the data stored on Dropbox and potentially could be implemented. The user testing session at the end of the project also strongly indicated that the encryption tool Secure Dropbox could tremendously gain users' confidence in terms of storing their confidential data on a cloud storage service like Dropbox.