Secure P2P cloud storage with a reputation point scheme and sharing

Bence Bakondi, Péter Burcsi, Péter Györgyi, Dávid Herskovics, Péter Ligeti*, Dániel A. Nagy, Viktória Villányi

Eötvös Loránd University, ELTECRYPT Research Group†

Abstract

This paper describes a scheme for a peer-to-peer based storage system with additional features. The main motivation for such systems is to provide the functionality of cloud storage without having to rely on central servers or large datacenters, i.e. having to trust a central entity (both from a security and safety point of view). Users of a P2P cloud storage system offer their own drive space for storing other users' files and vice versa. The system motivates fair behavior by using reputation points.

Decentralized storage has been in use for more than a decade now, e.g. by KaZaA or BitTorrent. In classical file sharing services however, the required content usually need not be encrypted and usually belongs to or can be read by several users. More recently, P2P storage software for securely storing private user files is also available by a few enterprises. Wuala addresses reliability issues by using a hybrid storage system: they provide storage space for money or in exchange for the user's space. One's files are then stored on servers and on other users' machines. Symform has a similar scheme. Neither of these schemes are known to handle selfish behavior of users storing the data of others. Space Monkey sells dedicated devices (external hard drives equipped with their software) that implements the storage system in a P2P manner. They still rely on servers for handling user connections.

It seems that to date no fully decentralized free cloud storage system is available. We propose such a system and address several potential risks. First, unauthorized data access should be impossible. This can be achieved by using secure encryption schemes before uploading data to the P2P network. But sometimes we would like to provide access to another user or to a group of other users, so we combine encryption with secret sharing. Second, data safety (availability) is needed. We propose a reputation point scheme for this. Similar ones exist for classical file sharing services, but as the users' goals are different here, we have to analyze the scheme carefully against selfish behavior.

*The author was partially supported by the grant OTKA PD-100712.

†The research was carried out as part of the EITKIC_12-1-2012-0001 project, which is supported by the Hungarian Government, managed by the National Development Agency, financed by the Research and Technology Innovation Fund and was performed in cooperation with the EIT ICT Labs Budapest Associate Partner Group. (www.ictlabs.elte.hu)