UNIVERSITY OF BERGAMO

School of Doctoral Studies

Doctoral Degree in Engineering and Applied Sciences

XXXII° Cycle

SSD: ING-INF/05

Protecting Resources and Regulating Access in Centralized and Decentralized Cloud Storage

– short summary –

Advisor

Prof. Stefano Paraboschi

Doctoral Thesis

Enrico BACIS

Student ID 1006904

Academic year 2018/2019

The low costs and high reliability guarantees associated with cloud storage, led many IT organizations to offload their data to cloud service providers. Yet, this also raises new challenges to manage access control and data confidentiality in these environments.

The first part of this doctoral thesis analyzes centralized cloud storage providers. In this setting, the servers are considered honest-but-curious: they always comply with users' requests, but they might access unprotected data. A possible defense is to encrypt the data; however, standard encryption modes would introduce relevant overheads when performing access revocation. To address this problem, we present an approach that relies on a resource transformation that provides strong mutual inter-dependency in its encrypted representation. To revoke access on a resource, it is then sufficient to update a small portion of it.

The second part studies how these guarantees can be extended to the decentralized cloud storage environment. In this case, the data is sharded and offloaded in a peer-to-peer network, in which nodes might not be honest, and might try to ignore users' deletion and access revocation requests in order to maximize their revenue. We propose a solution that addresses both availability and security guarantees, and enables resource owners to tune these settings to their needs.

When dealing with decentralized networks, an important aspect is how to detect misbehaving nodes, to stop paying for their service and migrate the data to new peers. This process has to happen without the need of the data owner presence and without imposing trust or honesty assumption on any of the involved parties. To address this problem, in the third part of this thesis, we detail a novel way of deploying self-releasing time-locked secrets. The use of such a technique can be used to realize delegated challenge-response protocols that, in turn, can be used to guarantee data confidentiality and retrievability properties without the need of trusted third parties. Our solution leverages smart contracts and economic incentives to regulate a game among the mutually distrusting users that compose a blockchain, thus removing the need of any trusted party.