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 Systems

– *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 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 (CSP). In this setting, the CSP is considered honest-but-curious: it always complies with users' requests, but it 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 be dishonest and try to disobey users' deletion and access revocation requests 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 work even when the data owner is offline 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. This technique can be used to implement delegated challenge-response protocols that, in turn, can guarantee data confidentiality and retrievability properties in fully distributed systems. 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.

The technologies detailed in this thesis push the state of the art as regards resource protection and access regulation in centralized and decentralized cloud storage systems. The implementations have been released under open-source licenses and can be readily integrated with real systems.