

Project consortium



UNIVERSITÀ
DEGLI STUDI
DI MILANO

Università degli Studi
di Milano



British Telecom



EMC Corporation



IBM Research - Zurich



SAP SE



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Technische Universität
Darmstadt



UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Università degli Studi
di Bergamo



Wellness Telecom



Project title

Enforceable Security in the Cloud to Uphold Data Ownership

Project acronym

ESCUDO-CLOUD

Funding scheme

H2020-ICT-2014

Topic

ICT-07-2014

Project duration

January 2015 - December 2017 (36 months)

Total cost

Euro 4,822,750

Requested EC funding

Euro 3,827,000

Project website

www.escudo-cloud.eu

Contact

Pierangela Samarati, pierangela.samarati@unimi.it



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644579. This work is supported in part by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract No 150087.

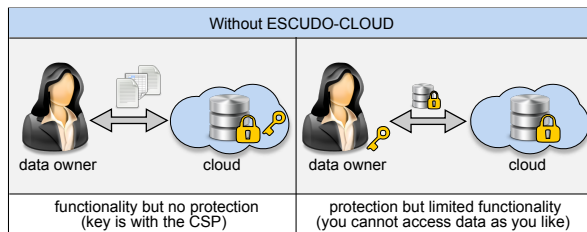
ESCUDO-CLOUD

Enforceable Security in the Cloud
to Uphold Data Ownership

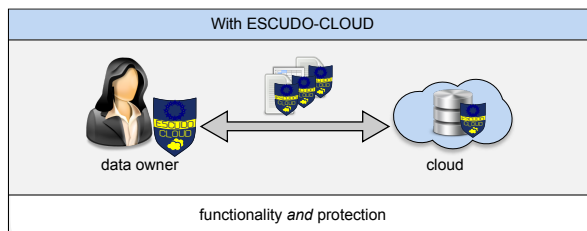


Vision

Today, users placing data in the cloud need to put complete trust that the Cloud Service Providers (CSPs) will correctly manage the outsourced information. As a matter of fact, all CSPs apply security measures in the services they offer, but these measures either give full trust to the CSP and allow it to have full access to the data, or greatly limit the flexibility the CSP is able to offer in accessing the outsourced data.



ESCUDO-CLOUD aims at empowering data owners as first class citizens of the cloud. ESCUDO-CLOUD will provide effective and deployable solutions allowing data owners to maintain control over their data when relying on CSPs for data storage, processing, and management, without sacrificing on functionality.



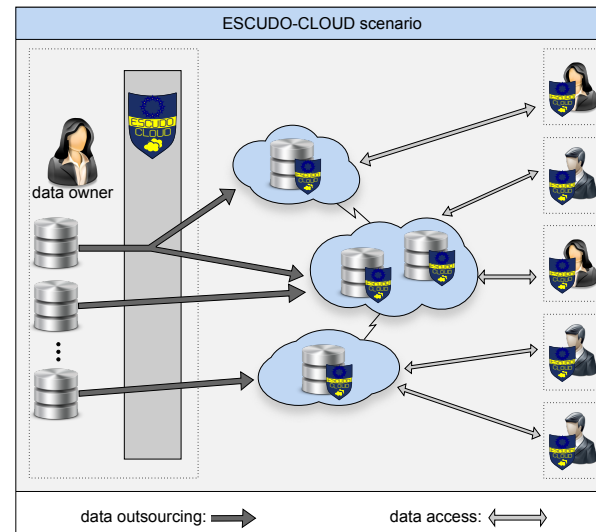
ESCUDO-CLOUD will provide enforceable security by means of techniques wrapping the data to provide a layer of protection to the eyes of the storing/processing CSP itself, setting the trust boundary at the client side, that is, assuming correct and trusted behaviour only by the client.

Use cases

OpenStack cloud platform
Secure enterprise-data management in the cloud
Federated secure cloud storage
Elastic cloud services

Scenario

Cloud computing is increasingly a necessary strategic ICT infrastructure component for European companies to successfully compete in the world-wide economy. The advantages of renting ICT infrastructures, platforms, and services, with easy access to scalability and elasticity, are driving an ever accelerating transfer toward the cloud of data and applications. Unfortunately, such a convenience comes at the price of the data owners losing control over their own data.



ESCUDO-CLOUD will enable data owners to outsource their data while maintaining control over them, with support of fine-grained data retrieval and with the ability to regulate access to them and share them with other users in a selective way and with assurance that their data will remain protected from the CSPs.

Work dimensions

Security properties

Confidentiality, Integrity, Availability

Sharing requirements

Owners only, Selective sharing

Access requirements

Upload/download, Fine-grained retrieval, Write

Cloud architectures

Single cloud, Multi and Federated cloud

Beneficiaries

ESCUDO-CLOUD will be beneficial for both data owners and CSPs.

Data owners will be enabled to outsource their data while maintaining control over them, with the ability to regulate access to them and share them with other users in a selective way and with assurance that their data will remain protected from the CSPs. Data owners will then be able to rely on CSPs and use their services for a wider range of applications. This will benefit both companies as well as individual users.

CSPs will significantly benefit, in addition to the increased market penetration that robust data ownership would provide, from reduced regulatory risks, audit costs, and general security threats that they would have to face in the absence of such protection. CSPs will be free from the worries of protecting data, allowing them to even handle the data outside their own control. For instance, a CSP would be able to rely on other services for outsourcing storage and computation, behaving as a broker providing a virtualised cloud service, without worrying about improper exposure of user information, guaranteed to be self-protected. This will benefit both larger and smaller players in the market.

Key takeaways

ESCUDO-CLOUD:

- sees the participation of major industry players in the cloud market
- enables strong exploitation and impact of innovative solutions in strategic use cases
- empowers data owners to maintain full control over their data in the cloud
- supports a variety of security properties, sharing requirements, access requirements, and cloud architectures
- ensures self-protection of data
- enables secure and private information sharing
- provides modular middleware, offering practical applicability and compatibility with current techniques
- operates with client-side trust boundary
- supports fundamental data protection rights of citizens in modern societies