Project number: **609611**
Project website: **www.practice-project.eu**
Project start: **1 November, 2013**
Project duration: **3 years**
Total costs: **EUR 10.465.059**
EC contribution: **EUR 7.550.000**

PRACTICE

Privacy-Preserving Computation in the Cloud

The PRACTICE consortium is well-positioned to achieve its objectives by bringing together a team of leading industrial and research companies, a research-oriented SME as well as respected European universities. These 18 project partners from 11 different countries form a complete chain stretching from basic research and service design, via applied research, up to end-user oriented service providers.

Technikon Forschungs- und Planungsgesellschaft mbH (Villach/Austria)

SAP AG (Walldorf/Germany)

Technische Universität Darmstadt (Darmstadt/Germany)

Alexandra Instituttet A/S (Aarhus/Denmark)

Arçelik A.Ş. (Istanbul/Turkey)

Bar Ilan University (Ramat-Gan/Israel)

Cybernetica AS (Tallinn/Estonia)

Julius-Maximilians Universität Würzburg (Würzburg/Germany)

Intel GmbH (Munich/Germany)

Katholieke Universiteit Leuven (Leuven/Belgium)

Inesc Porto – Instituto de Engenharia de Sistemas e Computadores do Porto (Porto/Portugal)

Aarhus Universitet (Aarhus/Denmark)

Technische Universiteit Eindhoven (Eindhoven/Netherlands)

University of Bristol (Bristol/United Kingdom)

Distretto tecnologico aerospaziales S.c.a.r.l. (Brindisi/Italy)

Universita degli studi di Milano (Milan/Italy)

Partisia APS (Aarhus/Denmark)

Georg-August-Universität Göttingen Stiftung öffentlichen Rechts (Göttingen/Germany)

Mission of PRACTICE:

- Is to design cloud computing technologies that allow computations in the cloud thus enabling new business processes while keeping the used data secret.
- Is to prevent cloud providers and other unauthorized parties from obtaining secret or sensitive information.

Motivation:

Information processed by businesses, government organizations and individuals often comes with confidentiality and integrity requirements. As a result, data processors must deploy security controls for their ICT infrastructure, protecting it against external as well as internal attackers.

Cloud services promise great benefits in terms of financial savings, easy and convenient access to data and services, as well as business agility. Organizations and individuals therefore choose to outsource their data to the cloud, where an untrusted party is in charge of storage and computation. A major concern for the adoption of cloud computing is the inability of the cloud to build user trust.

A comprehensive solution for securing the cloud computing infrastructure is based on cryptographic mechanisms of secure computation. These mechanisms allow for distributed computation of arbitrary functions of private (secret) inputs, while hiding any information about the inputs to the functions.

PRACTICE will address all of these settings:

- Hiding user data from other users of the same cloud service.
- Hiding user data from the cloud provider.
- Securing computation between several servers.
- Securing computation between untrusting parties.

Objectives:

The PRACTICE project aims to build a secure cloud framework that allows for the realisation of advanced and practical cryptographic technologies providing sophisticated security and privacy guarantees for all parties in cloud computing scenarios.

The goals of the PRACTICE project are:

- Data confidentiality and integrity
- Computation on encrypted data
- Flexible architecture and tools

The PRACTICE project will:

- enable European customers to save costs by globally outsourcing to the cheapest providers, while still maintaining guaranteed security and legal compliance.
- deliver a Secure Platform for Enterprise Applications and Services providing application servers and automatic tools enabling privacy-sensitive applications on the cloud.
- protect user data from cloud providers and other users.

The project aims to develop various fundamental technologies:

- Secure Multiparty Computation (MPC)
- Fully Homomorphic Encryption (FHE)
- Domain-Specific Development Tools
- Formal Methods

Technical Approach:

The work plan for the PRACTICE project is structured into three loosely coupled activity lines and tightly integrated work packages:

Activity 1 “Specification, Design and Implementation of Protocols”

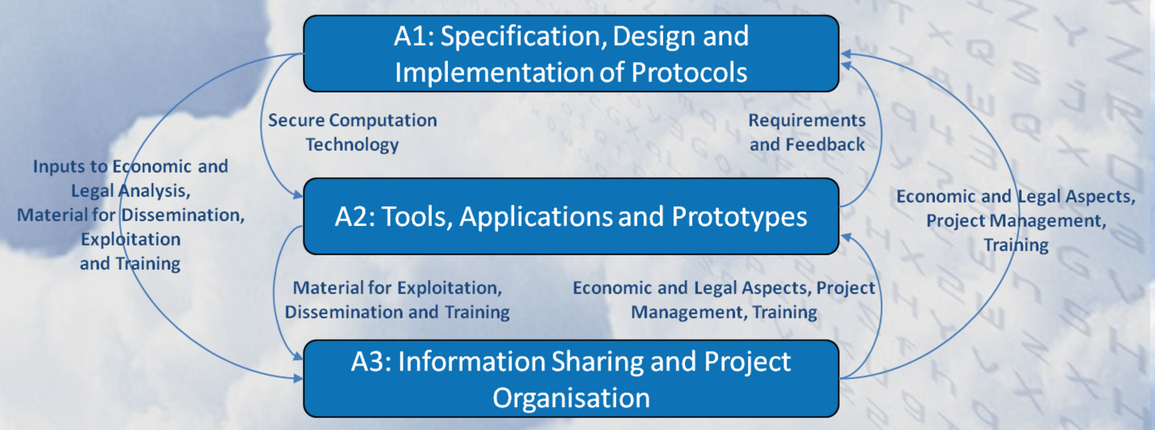
It is responsible for analysing existing techniques to build the application and protocol specifications to design algorithms and protocols.

Activity 2 “Tools, Applications and Prototypes”

It is concerned with the design, implementation, evaluation and demonstration of tools and applications of algorithms and protocols developed in Activity 1.

Activity 3 “Information Sharing and Project Organisation”

It is mainly responsible for wide and effective dissemination as well as the proper programme management that ensures timely and high-quality delivery of all results while mitigating emerging conflicts and risks.



Project Results:

- PRACTICE provides modern and novel technologies for secure computation on encrypted data, allowing the data owners to fully utilize the economies of scale.
- PRACTICE creates a secure cloud framework allowing for the realisation of advanced but practical cryptographic technologies that are integrated in virtualised environments.
- PRACTICE develops models to quantify the return on investment for security investment for the deployment of secure computation algorithms.
- PRACTICE evaluates the legal aspects related to the outsourcing of data and of computation to the cloud beyond national and European boundaries, and establish guidelines.

Contact:

Project Coordinator

Dr. Klaus-Michael Koch
Technikon Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a
9500 Villach
Austria
Tel.: +43 4242 233 55-71
E-mail: coordination@practice-project.eu

Technical Leader

Dr. Florian Kerschbaum
SAP AG
Dietmar-Hopp-Allee 16
69190 Walldorf
Germany
Tel: +49 6227 7-52577
E-mail: florian.kerschbaum@sap.com

Scientific Leader

Prof. Dr. Ahmad-Reza Sadeghi
Technische Universität Darmstadt
Karolinenplatz 5
64289 Darmstadt
Germany
Tel: +49 6151 16-75560
E-mail: ahmad.sadeghi@trust.cased.de

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no [609611].