PRACTICE

Privacy-Preserving Computation in the Cloud

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**

Project is co-financed by the European Commission (under Seventh Framework Programme)

Mission of PRACTICE:

The 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. Unlike today – where insiders can access sensitive data – PRACTICE will 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 that the processing party must adhere to. As a result, data processors must deploy security controls for their ICT infrastructure, protecting it against external as well as internal attackers. This is relatively easy when this infrastructure is local and controlled by the processing party, but much harder when it is provided by an external service provider.

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 in the information security measures deployed in cloud services. Common computing techniques cannot be applied on encrypted data, and therefore the data and the programs that compute on the data must be decrypted before being run on the cloud infrastructure.

A comprehensive solution for securing the cloud computing infrastructure can be 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. Put differently, these mechanisms support **computation on encrypted data.** We identify several settings where secure computation in the cloud is needed. 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 realization of advanced and practical cryptographic technologies providing sophisticated **security and privacy** guarantees for all parties in cloud-computing scenarios.

An advanced and comprehensive framework represents a key factor for the achievement of the following PRACTICE project goals:

- **data confidentiality and integrity,** eliminating need for users to trust cloud providers;
- **computation on encrypted data,** preventing even insiders from disclosing secrets or disrupting the service;
- **flexible architecture and tools** allowing seamless migration from execution on unchanged clouds today towards new platforms while gradually adding levels of protection.

This will open new markets, increase their market share, and possibly lead to the acquisition of foreign markets where reach has been limited due to confidentiality and privacy concerns. 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, **supporting cloud-aided secure computations** by mutually distrusting parties.

Fundamental Technologies:

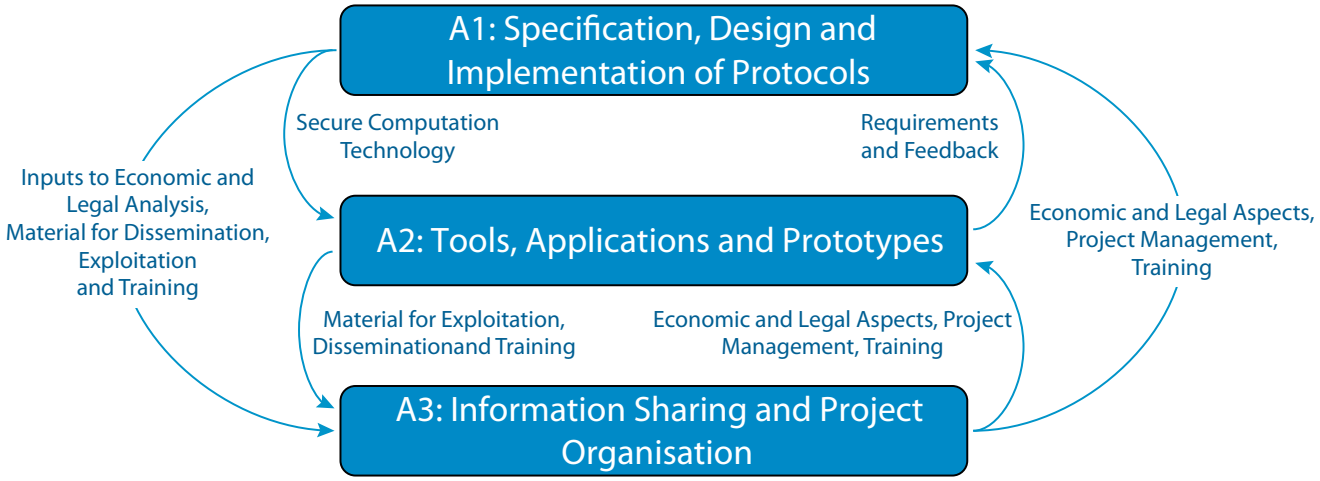
The project aims to develop various fundamental technologies and then to build upon them with distinct, but complementary developments. The fundamental technologies we aim to investigate are:

- **Secure Multiparty Computation** (MPC)
- **Fully Homomorphic Encryption** (FHE)
- **Domain-Specific Development Tools,** and the application of
- **Formal Methods** to verify relevant properties of resulting systems.

These will be investigated in a holistic manner, by developing all these fundamental technologies simultaneously via the deployment technologies. New programming languages and tools will be developed to support applications in using a combination of underlying technologies such as secure multiparty computation and homomorphic encryption. In addition we believe that research on hardware support in one fundamental technology can be utilized in another.

PRACTICE

PRACTICE Programme Structure



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

- **Activity 2 "Tools, Applications and Prototypes"** 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"** 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:

- Provide **modern and novel** technologies for **secure computation on encrypted** data, allowing the data owners to fully utilize the economies of scale provided by cloud computing while protecting their data from cloud provider insider attacks.

- Create a **secure cloud framework** allowing for the realisation of advanced but practical cryptographic technologies that are integrated in virtualised environments to provide efficient and sophisticated security and privacy guarantees for users and providers of cloud-based services while reducing trust in the cloud provider to the utmost extent.

- Develop models and techniques to quantify the **return on investment for security investment** for the deployment of secure computation algorithms. The model will allow for computing the risk landscape associated with outsourcing data and computation, and simulate different scenarios where both the investment in security and the required security level associated with the data can be changed.

- **Evaluate the legal aspects** related to the outsourcing of data and of computation to the cloud beyond national and European boundaries, and **establish guidelines.**

PRACTICE

Contact:

Project Coordinator
Dr. Klaus-Michael Koch
Technikon Forschungs- und
Planungsgesellschaft mbH
Burgplatz 3a
9500 Villach
Austria
Tel.: +43 4242 233 55 – 0
Fax: +43 4242 233 55 – 77
E-mail: coordination@practice-project.eu
Web: www.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
Fax: +49 6151 16 - 72135
E-mail: ahmad.sadeghi@trust.cased.de

Consortium

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 well 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.

1 **Technikon Forschungs- und Planungsgesellschaft mbH (Villach/Austria)**

2 **SAP AG (Walldorf/Germany)**

3 **Technische Universität Darmstadt (Darmstadt/Germany)**

4 **Alexandra Instituttet A/S (Aarhus/Denmark)**

5 **Arcelik A.S. (Istanbul/Turkey)**

6 **Bar Ilan University (Ramat-Gan/Israel)**

7 **Cybernetica AS (Tallinn/Estonia)**

8 **Julius-Maximilians Universität Würzburg (Würzburg/Germany)**

9 **Intel GmbH (Munich/Germany)**

10 **Katholieke Universiteit Leuven (Leuven/Belgium)**

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

12 **Aarhus Universitet (Aarhus/Denmark)**

13 **Technische Universiteit Eindhoven (Eindhoven/Netherlands)**

14 **University of Bristol (Bristol/United Kingdom)**

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

16 **Universita degli studi di Milano (Milan/Italy)**

17 **Partisia APS (Aarhus/Denmark)**

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