PRACTICE - Privacy-Preserving Computation in the Cloud

Newsletter

December 2016 - Issue 5

PRACTICE potential impact and use

Secure computation and secure computation services for the cloud have a potential of being a disruptive technology that will **change the economics of technology development and deployment**. The ability to provide cryptographic and more general secure computation services in the cloud, combined with the tools and applications that are adapted for using this **secure computation framework**, can bring forth new economic and technological opportunities for Europe, and new efficiencies from which multiple sectors of industry in Europe will benefit.

The project can **open new markets**, the 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. This is something not yet provided by any existing commercial cloud service.

While the project does not provide a universal "one size fits all" toolbox for secure cloud computation, the solution architecture and set of available components are **suitable for real world use cases**, which has been demonstrated by mini-clusters of consortium members. This is a good starting point towards sustainable exploitation of the project results and a good example how various PRACTICE framework components can and should be used to solve secure cloud computation problems.

PRACTICE has been a very well managed project with **strong technical leadership** and effective project management. All Work Packages have shown good handling of the activities and research challenges, both from the execution and planning point of views.

Message from the coordinator

The PRACTICE project successfully finalized all objectives and work plans during the third and final project period. There have been numerous events and achievements since the last issue of the PRACTICE newsletter. The project partners participated in various workshops, meetings and conferences dedicated to the dissemination of PRACTICE, as well as to support progress of the project (https://practice-project.eu/project-results/publications). Among the main events were the technical meeting in Tel Aviv, Israel in April 2016 and the technical, General Assembly and Advisory Board meeting in Porto, Portugal in September 2016. Partners were immersed in vivid discussions about the technical progress and further planning of PRACTICE beyond the project lifetime. It is with great pleasure to announce that the objectives targeted in PRACTICE were reached and the project successfully ended in October 2016. Knowledge and technology gained within the project will help to maintain and further increase competitiveness of the cloud computing market, as well as of the project industry partners.

Results and ongoing activities

During the third project year the PRACTICE team worked carefully on the following deliverables:

D13.2 - Efficient verifiability and precise specification of secure computation functionalities describes the results of the activities carried out wrt efficient verifiability solutions.

D13.3 - The full set of new protocols has short descriptions of protocols that were already published in D13.1 and a detailed description of protocols that were designed in the last year of the project.

D13.4 - Prototype implementation of key protocols describes the LibSCPAI software library which is C++ library for secure computation.

D14.3 - Protocol implementations documents on the implementation of secure computation protocols from theoretical work of WP13.

D14.4 - Validation Report validates the work on the PRACTICE platform implementations done in WP14.

D21.3 - Application architecture for secure computation describes the general architecture for applications using secure multiparty computation.

D24.5 - Prototypes assessment describes the analysis of real MRO performance and of demand satisfaction in consumer good industry highlights the industrial motivation for collaborate SCM.

D31.3 - Evaluation and integration and final report on legal aspects of data protection contains the final report on the current legal framework regulating storage and processing the data on the cloud.

D32.3 - Final dissemination, standardisation, exploitation and training report reports on the project's activities in the area of dissemination, standardisation, exploitation and training which have been executed since M25 until the project end in M36.

Key Data:

Start Date:	1 November 2013
End Date:	31 October 2016
Duration:	36 months
Project Reference:	609611
Project Costs:	€ 10.465.059
Project Funding:	€ 7.550.000

Consortium:	18 partners (11 countries)
Project Coordinator:	Dr. Klaus-Michael Koch coordination@practice-project.eu
Technical Leader:	Dr. Florian Kerschbaum florian.kerschbaum@sap.com
Scientific Leader:	Prof. Dr. Ahmad-Reza Sadeghi ahmad.sadeghi@trust.cased.de
Project Website:	www.practice-project.eu

FOLLOW US ON twitter

https://twitter.com/FP7_PRACTICE

PRACTICE - Privacy-Preserving Computation in the Cloud

Newsletter

December 2016 - Issue 5

Technical challenges

According to the work plan the project was mostly concerned with **architecture/design** and **implementation** of this design. The natural challenges in any large-scale software development project arise. We used the communication plan and many additional informal exchanges in order to ensure integration of the components leading to a **unified framework.** Furthermore, the initial investment of PRACTICE in order to provide **early demos** and **prototypes** paid off in order to avoid any unpleasant surprises. In any engineering project there are inherent trade-offs between the objectives. In PRACTICE this is mostly **security versus performance**. We used a principled design approach following the description of work. For components, such as secure computation protocols, where performance is critical, the design work provided **better than expected results**. For components, such as order-preserving encryption, where security is critical, the design work provided **clear improvements**. Hence, PRACTICE seems to be able to address the inherent trade-offs for its technology basis. After the foundations of the technologies have been addressed it was important to **provide the necessary tooling** for deployment in the cloud. We followed the reviewers' helpful suggestions and developed (or started the development) of many important tools to **ease cloud deployment**. The integration into an existing development infrastructure still remains somewhat challenging (also due to the continued progress of the non-secure infrastructure), but significant advances have been made within PRACTICE.

PRACTICE Final Review Meeting

The PRACTICE consortium executed successfully the final review meeting on 19-20th December 2016 in Brussels. The project was assessed with excellent progress, so we fully achieved our objectives and technical goals for the period and have even exceeded expectations. According to the reviewers and the EC the original objectives of the project are still relevant in the current, evolved market condition, and have been achieved within the time and resources available to the project. Ultimately, PRACTICE delivers excellent potential for further exploitation of its results, both from scientific and commercial point of view.

Summary of the final prototypes & main project results

The PRACTICE project yielded the targeted outcomes. The **harmonization** regulatory, organizational, and user **requirements** for data access became possible because of the unifying and verifiable framework that is provided as a set of security services. Such requirements are easier to formulate because it was necessary to adapt them to each application and each environment. Harmonized requirements greatly improve the economics of providing services.

Organizations have **access to much more information** about their business environment than ever before and are able to make **better decisions** to drive their work forward. This is possible without violating anyone's privacy.

Secure computation services increase the **openness in society**, by encouraging the **fair exchange of information** and enforcing fundamental rules of security and privacy in distributed environments under the control of multiple unconnected providers.

PRACTICE developed **a comprehensive framework**, bringing secure computation to practice. The application framework allows the creation and deployment of secure computation applications by providing interfaces to client applications. The interface to the framework allows its users a **clear and simple method** of choosing between the available options of deploying the computation, and their relative tradeoffs. The project combined state-of-the-art cloud technologies (such as virtualization and optimized distributed computation) with novel cryptographic techniques and established a framework that provides an application interface for secure computation and storage in the cloud.

The project demonstrates a clear drive towards the **application**, **demonstration** and **future exploitation** of its framework. PRACTICE used its framework to built two applications for secure statistics and supply chain management in the cloud. The applications provided direct feedback from industrial end users (ARC and DTA) which are described in D24.5 "Prototypes assessments".

Contact:

PRACTICE Project Coordination Team
Dr. Klaus-Michael Koch
Technikon Forschungs – und Planungsgesellschaft mbH
Burgplatz 3a, A-9500 Villach
Tel.: +43 4242 23355 - 71
Fax.: +43 4242 23355 - 77
E-Mail: coordination@practice-project.eu
Website: www.practice-project.eu

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