Publishable Summary

Project number:	609611
Project acronym:	PRACTICE
Project title:	PRACTICE: Privacy-Preserving Computation in the Cloud
Start date of the project:	1st November 2013
Duration:	36 months
Programme:	FP7/2007-2013

Date of the reference Annex I:	05.09.2013
Periodic report:	Publishable Summary (as part of D33.3 "2nd periodic report according to EC regulations of the model contract")
Period covered:	01.11.2014 – 31.10.2015
Activities contributing:	All
Due date:	October 2015 – M24
Actual submission date:	2nd March 2016, V1.1

Project Coordinator:	Dr. Klaus-Michael Koch Technikon Forschungs- und Planungsgesellschaft mbH (TEC)
Tel:	+43 4242 233 55
Fax:	+43 4242 233 55 77
E-mail:	coordination@practice-project.eu
Project website:	www.practice-project.eu

Chapter 1 Publishable Summary

Project name: **PRACTICE** *Start date*: 1st November 2013
Grant Agreement: **609611** *Duration***:** 36 months
Project website: http://www.practice-project.eu/
Contact: coordination@practice-project.eu

Mission of PRACTICE: *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.*

The PRACTICE project aims to:

- 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 realization of advanced but practical cryptographic technologies that are integrated in virtualized 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.

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. 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.

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.

Description of the work performed and results in the second project period

The PRACTICE project started in November 2013 and is set to run for 36 months. During the second project phase, corresponding to the second project year, the focus was to support works on all project topics including defining application and protocol specifications, as well as developing various architecture designs and secure platforms. All work packages produced altogether 15 Deliverables and 2 Milestones throughout the second project year. The progress achieved by all work packages within the second project year is in line with the initial plan and can be summarized as follows.

WP11 (Analysis of Existing Techniques) is responsible for a theoretical analysis of existing protocols for secure computation, in both the two-party and the multi-party settings. The analysis is with respect to generic protocols and to specialized protocols that solve specific problems with particular interest. Relevant key technologies are protocols for secure two-party computation based on the Yao and GMW techniques and their variants, protocols for multi-party computation based on the GMW and BGW techniques and their variants, protocols with a pre-processing step that have a very efficient online step, such as the BDOZA and SPDZ protocols, specialized protocols for specific problems such as private set intersection, and methods for enduring universal verifiability of the protocols. The WP members conducted a study, based on scenarios in WP12, of different techniques for secure computation, with an emphasis for the Yao and BMR techniques. Further the effect of different improvements to the basic building blocks of Yao's protocol was investigated. The partners also continued their studies on protocols for secure outsourcing and of computational secret sharing with applications to MPC. The partners worked also on the implementing of advanced variations of the Yao protocol with optimized performance and security against malicious adversaries.

WP12 (Applications Specifications) is responsible for the specification of application scenarios that benefit from secure computation technologies. Furthermore, the work package provides adversary, trust, communication and system models based on those scenarios. Another objective of WP12 is the application of formal verification techniques to application scenarios which require the establishment of strict correctness and security guarantees for critical components. The application scenarios were compiled in the D12.1 “Application scenarios and their requirements”. For each use case scenario an animation was created and published on the project website. Adversary, trust, communication and system models were described in D12.2 “Adversary, trust, communication and system models”. Requirements for formal verification were summarized in D12.3 “Formal verification requirements”. All work anticipated for this work package has been completed.

WP13 (Protocol Specification and Design) is responsible for designing new protocols for secure two-party and multi-party computation, and for designing efficient verifiability solutions for secure computation. This work builds upon the analysis of the state of the art by WP12, with the goal of designing new solutions where the existing protocols are insufficient. The tasks on this WP are ongoing and span until almost to the end project. In the first year, initial work started on the design of new protocols. In the second year, the protocol development work was largely based on the results of WP12 in D11.2, which identified shortcomings in the state-of-the-art in secure computation, mostly in terms of the scalability of existing solutions. Most of the results that are achieved in this WP have been published in multiple research papers at top-tier academic conferences.

In ***WP14 (Final Implementation)*** we design and develop a platform for secure computation. The platform will allow industrial and research users to quickly implement new secure computation solutions and validate the attributes of the solution. Either by benchmarking against other solutions, which are build on the platform, or by clearly seeing the value of the solution in practice. The platform will be flexible and support multiple applications, scenarios and secure computation methods. The development of the architecture and an implementation of this architecture were done in this period resulting in D14.1 “Architecture” and D14.2 “Platform for Secure Computing” respectively. The architecture was developed in close coordination with WP21, in order to align the architecture with that of D21.2 “Unified architecture for programmable secure computations” on the general architecture for secure computation applications and services.

WP21 (Architecture and Integration) is responsible for making sure that the secure computation technologies in PRACTICE fit together and are usable in real-world information systems. The consortium has brought together the world’s leading experts in deploying real-life secure computation applications, The WP started by collecting all that knowledge and compiling an architectural analysis of current deployments. This resulted in the D21.1 “Deployment models and trust analysis for secure computation services and applications” – a useful document for planning future deployments in an outside of PRACTICE. In follow-up work, D21.2 “Unified architecture for programmable secure computations” describes the SPEAR and DAGGER frameworks of PRACTICE and shows how to apply PRACTICE technologies to build real-world systems. WP21 has also performed continuous validation of the architecture by building prototypes and integrating with other work packages. For example, WP14 is closely collaborating with WP21 to ensure alignment. One of the most impressive achievements to date is the cloud-powered tax fraud detection system that is one of the largest secure multi-party computation applications ever built. Its evaluation on the Amazon cloud also showed that there is a strong synergy between secure computing and the cloud – as the cloud was the key component for increasing the performance of the Sharemind secure computing platform used for the prototype. Second, the survey system developed in collaboration with WP23 and demonstrates how the SPEAR/DAGGER architecture allows a secure cloud service to be built on two competing PRACTICE technologies.

In ***WP22 (Tools)*** a set of tools is designed and implemented, that allow application developers to utilize secure computation techniques for their applications without expert knowledge in cryptography. In the first year period, the consortium analysed the state of the art resulting in deliverables D22.1 “State-of-the-art analysis” and D22.2 “Tools design document”. In contrast, in the second year the consortium started to implement novel tools and to extend and enhance existing tools with novel approaches. These efforts resulted in several prototypical tools for secure computation, privacy preserving databases and formal verification. In the final third year these tools will be further improved and extended.

WP23 (Secure Statistics Prototype) focus on developing software for secure statistics tailored for various applications such as online questionnaires (surveys), relative performance evaluation (benchmarking) and descriptive statistics in a more broad sense. The primary focus has been on developing the Secure Survey prototype that uses Secure Multiparty Computation (MPC) to keep answers to surveys confidential and only reveal aggregated statistics e.g. in the form of frequency diagrams. The Secure Survey application is the first prototype in PRACTICE and based on input from the other WPs. In particular, we show how this prototype is a first step towards the general SPEAR & DAGGER approach described in WP21. The Secure Survey system utilizes the flexibility of the SPEAR & DAGGER architecture to allow the secure survey system to run on two different secure multiparty computation engines: Sharemind and Fresco/SPDZ. Hereby, the system offers different security levels and addresses furthermore a potential market risk from vendor lock-in. After the delivery of the survey in April 2015, the survey system has been improved with new features and used in a real-life survey as part of WP24 as well as an upcoming

employment satisfaction survey in Estonia. The Secure Survey system also promotes exploitation as showcase of the technology and secure statistics. In parallel, work on describing and developing the two applications for D23.2 “Secure financial and medical prototypes” has been conducted. In particular the prototype for secure credit rating has been improved and made ready for a second round of end user test before finalizing the prototype.

WP24 (Supply Chain Prototype): In the first project year, the aero-fleet management, focused on the maintenance, repair and overhaul service in the engine segment of the aeronautic industry, and the manufacturing planning in the global consumer goods industry were analysed. In both cases, the collaboration in demand forecasting, service and manufacturing planning and inventory management is obstacle by the need of confidential data from many conflicting participants. New collaborative supply chain models and computing algorithms, responding to the business challenges, were developed and customized. The identified risks associated with data leakage events involving insiders are: reduction of competitive advantage and reduction of negotiation power, depending by the participants involved. During the second year, 4 more objectives were achieved: 1) definition of supply chain models and algorithms, 2) measurement of data protection levels required by industries, 3) identification of benefits of collaborative supply chain management and 4) preparation of the prototype cloud system. The algorithms for the fleet management case are: Aggregated service demand forecasting, spare parts management, engine service scheduling, service capacity planning. Based on the actual MRO servicing processes, they involve many confidential data (engine efficiency status, MRO current and planned process and penalties are only the most relevant) belonging to different participants. They provide more accurate demand forecasts, more realistic plans and enable a more cost effective inventory management policy. With respect to the consumer goods case, the Vendor Management Inventory model was customized on the specific ARC case. A supply chain optimization model was developed leading to a short-term inventory plan computation algorithm, based on the aggregation of business data (order and holding costs, penalties, inventory policies among others) from a number of local and competing retailers. Data protection levels were measured through two surveys assessing the importance of the impacts of the risky events (data leakage events). The results of the surveys validate and complete the qualitative risk analysis. In the aeronautic case, the impact of the collaborative SCM system on four business areas (customer, process, inventory and finance) was explored and a set of metrics were developed. These metrics will lead the evaluation of the pilot case. By leveraging achieved results of WP24, WP21 and WP22, the architecture, the encryption scheme and deployment strategy of the supply chain cloud prototype were designed and the implementation of the prototype started. In the next period, the prototype will be completed and some industrial pilot cases will be run in order to test the system from a security and business point of view.

The goal of ***WP31 (Business Implications and Risks)*** is twofold: reporting on the current legal framework regulating. The protection of data stored and processed on the cloud from one side and developing a risk assessment methodology for data sharing in cloud-based services, on the other side. The WP aims to provide an overview of the current legal framework regulating data protection in the European Union. Since the legal framework is changing, the WP discusses the EU Data Protection Directive currently in force and the proposals for the forthcoming General Data Protection Regulation (GDPR), highlighting their relevance to the processing of personal data on the cloud. The WP introduces also a new methodology supporting the risk-aware deployment of secure computation, aiming to provide the analysis and the quantitative evaluation of risks related to privacy and confidentiality breaches during the execution of a multi-party business process on the cloud. Techniques for the estimation of the probability of information disclosure among colluding partners are discussed in detail, introducing also a new possible approach, based on the analysis of the micro-economics underlying the business process and the information’s value. Furthermore, a web-based tool is presented, allowing the modelling and the simulation of the business processes executed on the cloud.

Within ***WP32 (Dissemination, Standardisation, Exploitation and Training)*** the early established robust IT infrastructure (web site, SVN repository including web access, mailing lists including mailing list archives) was regularly updated. PRACTICE has also been advertised by web pages, press releases and internal partners' newsletters. Hardcopies of the PRACTICE project flyers have been distributed by partners at various events. The project is visible on twitter and LinkedIn. Several newsletter has been published and distributed, amongst others, to industrial partners contacted in the context of the project results. The project is represented in an EU year book. Dissemination activities are announced via http://practice-project.eu/news. A list of dissemination activities has been compiled and updated periodically. Details regarding dissemination activities can be found in D32.2 "Intermediate dissemination, standardisation, exploitation and training report" which includes all dissemination, standardisation and training activities that were performed by the PRACTICE consortium. Further, a detailed exploitation report of all partners is included.

WP33 (Project Management) was responsible for the effective organization of the project and covered all relevant management components. Some of the main achievements so far have been: the organization of meetings (e.g. GA, AB Meetings), monthly EB Telcos, monitoring of the work plan (Interim Management Reporting), supporting partners in everyday issues (handling day2day requests), etc.

Expected final results and their 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. A few improvements that could follow the development and deployment of PRACTICE technologies are listed below.

- **Harmonization** of regulatory, organizational, and user **requirements** for data access will become possible because of the unifying and verifiable framework that is provided as a set of security services. Such requirements will also be easier to formulate because it will not be necessary to adapt them to each application and each environment. Harmonized requirements greatly improve the economics of providing services.
- Organizations will have **access to** much **more information** about their business environment than ever before and will be able to make **better decisions** to drive their work forward. This will be possible without violating anyone's privacy.
- Secure computation services can 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.

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.

PRACTICE Disclaimer

All public information will be marked with the following PRACTICE project disclaimer: *"The PRACTICE project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement number ICT-609611".*