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

PRACTICE

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 D33.4 "3rd periodic report according to EC regulations of the model contract")
Period covered:	01.11.2015 – 31.10.2016
Activities contributing:	All
Due date:	October 2016 – M36
Actual submission date:	30th January 2017, V2.0

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

The **Mission of PRACTICE** *was 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 prevents cloud providers and other unauthorized parties from obtaining secret or sensitive information.*

The PRACTICE project:

- Provides 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.
- Created 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.
- Developed models and techniques to quantify the return on investment for security investment for the deployment of secure computation algorithms. The model allows 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.
- Evaluated 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 identified several settings where secure computation in the cloud is needed. PRACTICE addressed 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 developed various fundamental technologies and built upon them with distinct, but complementary developments. The fundamental technologies we investigated 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 were investigated in a holistic manner, by developing all these fundamental technologies simultaneously via the deployment technologies. New programming languages and tools were developed to support applications in using a combination of underlying technologies such as secure multiparty computation and homomorphic encryption. In addition we believed that research on hardware support in one fundamental technology can be utilized in another.

Description of the work performed and results since the beginning of the project

The PRACTICE project started in November 2013 and ended after 36 months in October 2016. During the first project year, the focus was placed on the analysis of existing techniques, application specifications and security requirements. During 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. Within the third project period (M25-M36) the prototypes have been ready and results of secure computation were verified. A general architecture for applications that use secure computation and protocols have been finalized and tested.

WP11 (Analysis of Existing Techniques) was responsible for a theoretical analysis of existing protocols for secure computation, in both the two-party and the multi-party settings. The analysis was 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) was responsible for the specification of application scenarios that greatly benefit from secure computation technologies. Furthermore, the WP provided adversary, trust, communication and system models based on those scenarios. Another objective of WP12 was the application of formal verification techniques to application scenarios that require the establishment of strict correctness and security guarantees for critical components. The application scenarios were compiled in 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 planned for this WP was completed successfully.

WP13 (Protocol Specification and Design) was responsible for designing new protocols for secure two-party and multi-party computation, and for designing efficient verifiability solutions for secure computation. This work built 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 in this WP spanned until the end of the 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 “An evaluation of current protocols based on identified model”, which identified shortcomings in the state-of-the-art in secure computation, mostly in terms of the scalability of existing solutions. In the third year, more advanced protocols were developed. 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)*** work was performed to design and develop a platform for secure computation. The goal of this platform is to allow industrial and research users to quickly implement new secure computation solutions and validate the attributes of the solution. A main aim of the platform is to be flexible supporting multiple applications, scenarios and secure computation methods. As such the platform should support the implementation of both new secure computation methods and applications utilizing the implemented methods. As part of this work we have developed a general architecture for secure computation frameworks supporting the overall goals of the platform resulting in D14.1 “Architecture”. An example implementation of the framework architecture was presented in D14.2 “Platform for Secure Computing”. 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 computation” on the general architecture for secure computation applications and services. Additionally, we have worked to implement new secure computation methods, resulting from the theoretical work in WP13, into the platform. Thus allowing secure computation based applications to take advantage of these new methods. This work resulted in D14.3 “Protocol implementations” describing a number of the implemented secure computation protocols. The platform has been validated partially by supporting the protocol implementations and integration described above, and partially by supporting the development of a number of prototypes addressing real world scenarios throughout the PRACTICE project. These validation activities were reported in D14.4 “Validation report”.

WP21 (Architecture and Integration) was responsible to ensure 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 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. D21.2 presents several architectural patterns for building PRACTICE applications of a certain kind (e.g., enterprise Java applications, web services). This work is then continued in D21.3 “Application architecture for secure computation” that gives more detailed guidelines on how to integrate PRACTICE technologies with both new and legacy user interfaces.

WP21 has also performed continuous validation of the architecture by building prototypes and integrating with other WPs. 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. To conclude, this work package has been coordinating integration throughout the project, with other work packages often presenting their pilots and demonstrators and prototypes aligned with the common architecture.

In ***WP22 (Tools)*** a set of tools was designed and implemented, that allow application developers to utilize secure computation techniques for their applications without expert knowledge in cryptography. In the first year, the consortium analysed the state of the art resulting in 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 as reported in deliverable D22.3 “Software development kit and tools prototype (1st version)”.

In the final year these tools were further improved and extended as described in deliverable D22.4 “Software development kit and tools (final version)”: Among the results are *new functionalities* such as NoSQL support, private function evaluation and tools for verifying the secure computation engines as well as *further improvements* like runtime optimizations, simplified deployment phases and comprehensive documentation. The final result of this WP is a variety of tools covering the entire SPEAR/DAGGER architecture developed within PRACTICE in WP21.

WP23 (Secure Statistics Prototype) focused on developing software for secure statistics tailored various applications such as online questionnaires (surveys), relative performance evaluation (benchmarking), DNA analysis and descriptive statistics in a more broad sense. A number of prototypes have been developed and improved during the course of the project. All applications use Secure Multiparty Computation (MPC) to keep input data (answers to surveys, sensitive company data, DNA profiles etc.) confidential at all time.

The initial Secure Survey application was the first prototype in PRACTICE and based on input from the other WPs – D23.1 “Platform for secure surveys”. 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. The Survey System has been used in several real-life surveys and improved accordingly during the course of the project.

As oppose to the generic survey system, the next two prototypes developed in WP23 and described in D23.2 “Secure financial and medical prototypes”, was tailored financial risk assessment and DNA analysis. Both applications addresses concrete business cases where secure statistics adds value directly. Also, a large number of stakeholders have been involved in designing and testing the prototypes to ensure that the solutions solve real problems. Both prototypes have been improved and extended in the final deliverable. This includes a combined use-case, where encrypted answers from the survey system are input to financial risk assessment.

D23.3 “An online portal providing secure computation capabilities” includes a large number of improvements and extensions of the three prototypes mentioned above as well as a Secure Computation Cloud Orchestrator service. This service aims at easing the uptake of MPC by simplifying the development and deployment of MPC applications.

WP24 (Supply Chain Prototype) was aimed at developing and evaluating supply chain management prototype systems**.** Firstly, new collaborative supply chain models and computing algorithms, responding to the identified industrial business challenges, were developed and customized, resulting in functional requirements for prototypes. The application of these models introduces confidential data leakage risks, i.e. reduction of competitive advantage and reduction of negotiation power. To focus that issue, required data protection levels were measured, resulting in validated security requirements.

Successively the analysis of real industrial cases identified the troubles in case of innovative business models application. In the aeronautic case, the large and unstable turn-around-time is a relevant negative performance in case of performance-based contract model. The causes of that are the scarce resource planning capabilities and the shortage in spare parts inventory (due to missing engine health status data from engine operators), both causes are positively affected by more accurate demand forecasts in term of demand in future time slots, and of engine components requiring services. Instead, ARC is not able to satisfy the product demand, due to differences between demand forecasts and actual demand. Indeed, demand forecasts are based on the pre-orders of customers that are not enough accurate and focused mainly on obtaining future economic benefits.

The test on the prototype applications, completed in the third project year, provided the following results. The aeronautic application is able to analyse the encrypted engine health status database and to identify which of them will need service in a future time slots. The consumer goods prototype, instead, aggregates encrypted pre-orders provided by several customers for the same products and deliver the result to the OEM. The prototype

applications satisfy the industrial functional and security requirements. The computing performances (i.e. time required by computation) are aligned to standard industrial applications.

The simulation of supply chain costs incurred applying the secure cloud supply chain management system showed a cost reduction as high as 10% for some engine components, depending on their demand properties, and as high as 8% in two product categories of ARC.

The goal of ***WP31 (Business Implications and Risks)*** was 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 aimed to provide a complete 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 introduced also a new methodology supporting the risk-aware deployment of secure computation and provided 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 possibilistic approach, based on the analysis of the micro-economics underlying the business process and the information's value. Furthermore, a web-based tool was 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 (website, SVN repository including web access, mailing lists and mailing lists archives) was updated regularly. PRACTICE has also advertised by web pages, press releases and newsletters were published and distributed, amongst others, to industrial partners contacted in the context of the project results. Hardcopies of the PRACTICE project leaflet were distributed by partners at various events. To summarize, the achievements and work towards the project goals during the third project year for dissemination and standardisation include: 19 peer-reviewed scientific publications, 27 presentations in conferences or organized events (workshops, winter/summer schools) with an international audience and very good feedback, contributions to privacy and cloud technology standards in international standardisation bodies. The project is visible on twitter and LinkedIn. Newsletters have been published and distributed, amongst others, to industrial partners contacted in the context of the project results. A list of dissemination activities has been compiled and updated periodically. All details regarding dissemination, exploitation and standardisation activities can be found in D32.3.

WP33 (Project Management) was responsible for the effective organization of the project and covered all relevant management components, including risk and innovation management.

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 follow the development and deployment of PRACTICE technologies are listed below.

- **Harmonization** of 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 not 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.

The PRACTICE Consortium brought together 18 partners from 11 different countries: leading industrial and research companies, a research-oriented SME as well as well respected European universities. All partners are experts in their field. This partnership of experienced professionals resulted in a successful project.