



D12.1 Application Scenarios and their Requirements

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

Deliverable type:	Report
Deliverable reference number:	ICT-609611 / D12.1 / 1.0
Activity and Work package contributing to deliverable:	Activity 1 / WP 12.1
Due date:	April 2014 – M6
Actual submission date:	30 th April, 2014

Responsible organisation:	TUDA
Editor:	Stefan Katzenbeisser, Niklas BÜscher
Dissemination level:	Public
Revision:	1.0 (r-2)

Abstract:	Application scenarios that can greatly benefit from secure computation technology are identified. Moreover, their requirements, the participating parties and attacker models are described.
Keywords:	Applications, Scenarios, Requirements, Analysis

Editor

Stefan Katzenbeisser, Niklas Büscher (TUDA)

Contributors (orderd according to beneficiary numbers)

Georg Hafner, Mario Münzer, (TEC)

Ferdinand Brassler, (TUDA)

Janus Dam Nielsen, Peter Sebastian Norholdt (ALX)

Dan Bogdanov, Riivo Talviste, Liina Kamm, Marko Jõemets (CYBER)

Meilof Veenigen, Niels de Vreede (TUE)

Antonio Zilli (DTA)

Kurt Nielsen (PAR)

Disclaimer

The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 609611.

Executive Summary

In this deliverable applications scenarios that greatly benefit from secure computation are identified and described. The presented scenarios originated four different areas, namely *joint business applications*, *joint studies applications*, *location sharing applications* and *end user applications*. The first area joint business applications involves multiple business partners that are interested in optimizing their joint operations without revealing internal sensitive company data. Secure multi-party computation (SMC), can be used to operate on the partners data without revealing the data itself. In the second area joint studies applications, studies on sensitive data of individuals are discussed. These applications profit from SMC by protecting the participants privacy as well as removing legal barriers. Moreover, the location sharing applications profit from SMC by protecting the location of individuals or objects while still allowing to detect proximities. Finally, end user applications aim towards increasing the user's privacy when using cloud services for personal purposes.

A special focus of this work package and deliverable is set on identifying the application scenarios requirements. These are an important factor for the solution development during the further course of PRACTICE. Therefore, the here presented scenarios are analyzed regarding their security goals, e.g. data privacy, their technical constraints, e.g. should run on cloud commodity hardware, and the possible attacker models, e.g. active and passive adversaries.

Disclaimer

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose subject to any liability which is mandatory due to applicable law. The users use the information at their sole risk and liability.

Contents

1	Introduction	1
2	Scenario Description and Background	4
2.1	SMC - Attacker Models	5
2.2	SMC Party Roles	6
2.3	Verification by external parties	6
2.4	Scenario Animations	7
3	Application Scenarios	8
3.1	Joint Business Applications	9
3.2	Joint Studies Applications	16
3.3	Location Sharing Applications	21
3.4	End User Applications	24
4	Conclusion	28
5	List of Abbreviations	29
	Bibliography	29

Chapter 1

Introduction

For decades, secure computation has been seen to be a powerful theoretical concept but also has been considered to be unusable for practical applications due to its high computational and communication requirements. This has changed in recent years and today there is interest in the technology of secure computation from industry, governments, and security agencies all around the world (e.g. DARPA's PROCEED, IARPA' SPAR, Partisia's Auctions-as-a-Service) [Gre11, SPA, BCD⁺09].

A major goal of PRACTICE is to provide privacy and confidentiality for computations in the cloud. To accelerate the process of making secure cloud computing a tool that is used in practice, we identify applications and application scenarios where secure computation is most needed. Furthermore, both, the scenarios and their technical requirements are elaborated. Gathering the individual scenario requirements enables a focussed development of solutions for the different applications during the further course of PRACTICE. Thus, this document aims towards providing a common ground of application scenarios for all PRACTICE work packages. Yet, it is important to mention that the process of identifying scenarios and their requirements is bidirectional. Since many scenarios are part of other work packages, results from these contributed to the here compiled list as well.

Deploying secure cloud computing concepts and techniques in applications involves the close cooperation between industry and science. Because of this, partners from both sides are needed to achieve a well rounded view on possible application scenarios. Partners from industry observe their customers demand for privacy preserving applications in their daily business. Critical input from the scientific community helps to identify needs that can be answered by current technology and novel technologies that will be developed in the coming years. The identified scenarios that result the joint work are compiled into a list and summarized in the next section.

Application Scenarios

This deliverable contains thirteen scenarios grouped thematically into four different areas. These areas are *joint business applications*, *joint studies applications*, *location sharing applications* and *end user applications*. A short overview of all scenarios and areas is given in this section, the scenarios are analyzed in detail and illustrated in Chapter 3 as well as in the referenced work packages.

The first area *joint businesses applications* involves companies that are interested in a cooperate without revealing internal sensitive company data. In scenarios from this area, secure computation can be used to jointly evaluate calculations, e.g. supply chain optimization, based on sensitive company data without revealing the data itself. *Joint business applications* that are investigated in this deliverable are:

- **Aeroengine Fleet Management:** A portal that enables the optimization of the maintenance repair and overhaul process for the engine sector of the aeronautic supply chain. Maintenance plans can be calculated without revealing the participating companies data. This use case is also analyzed in depth and implemented in Work Package (WP) 24.
- **Consortium Gathering Information from Its Members:** A Consortium would like to gather information from its members, e.g. benchmarking economic results. Secure computation enables competing companies to contribute their data to the consortium without risking a privacy breach of the individual data.
- **Platform for Auctions:** Multiple parties negotiate auctions without revealing their bids. Exemplary markets are spectrum and electricity auctions.
- **Platform for Benchmarking:** A privacy preserving platform for benchmarking between business partners enables a trustworthy assessment. Partners can evaluate each other regarding different factors, i.e. credit card rating, without losing sensitive company data. A prototype is implemented in WP 23.
- **Tax Fraud Detection:** Detecting tax frauds is one of the cases where state entities are interested in analyzing precise financial data of companies. With the help of secure computation, a precise analysis of money flows can be executed without the necessity to reveal the companies' sensitive financial data to the revenue office.

In the second area, namely *joint studies applications*, sensitive data of many individuals or entities is used for studies and statistics without exposing the individuals data at any time. In this area we discuss the following scenarios:

- **Joint Statistical Analysis Between State Entities:** In some cases the law forbids the compilation of so-called super-databases between different state entities. To enable a joint study between different entities, secure computation can be used to join data bases in a privacy preserving manner that fulfils the legal requirements.
- **Privacy Preserving Genome Studies Between Biobanks:** Biobanks from different countries can perform a joint genome-wide association study using each other's data without breaching the donors' privacy, when using secure computation.
- **Privacy Preserving Personal Genome Analyses and Studies:** Similar to the service offered by 23andMe [23a], donors can submit their genome data and enter their phenotype data to receive feedback on genetic associations with specific illnesses and disorders. Secure computation can be used to circumvent any mishandling of the donors' data.
- **Surveys on Sensitive Data:** A cloud portal that provides a platform for surveys. A survey creator submits a survey to the platform that is then filled with opinions from invited participants. Using secure cloud computing, the survey is evaluated and only the result is sent back to the creator. Thus, with the help of secure computation, the participants' input data can be protected. This scenario is elaborated further in WP 23.

Privacy preserving *location sharing* is of relevance in the following two scenarios:

- **Location Sharing with Nearby Contacts:** Location information of smart phone users is sensitive, yet useful for social activities where contacts meet. With the help of secure computation, proximities can be calculated without revealing actual location data.
- **Privacy Preserving Satellite Collision Detection:** Different countries wish to detect collisions between their satellites without revealing the exact location and trajectory of their satellites.

The last area are *end user applications*. These scenarios aim towards increasing the end user's privacy when using cloud services for personal purposes. The applications in this area are:

- **Key Management:** With the increasing number of devices an end user uses, cryptographic keys need to be shared more often between different platforms. To avoid a centralized trusted third party, i.e. key server, a solution based on secure computation is preferable
- **Mobile Data Sharing:** This scenario provides privacy preserving data sharing between different mobile devices through the cloud. Shared data should not be visible to the cloud service provider.

Chapter 2

Scenario Description and Background

A major goal of this deliverable is to provide a structured and uniform overview of the different identified application scenarios. Therefore, a tabular representation of each scenario is used. We begin by giving an overview of the template before describing the used definitions and notations. The template is presented below in Table 2.1 and structured as follows.

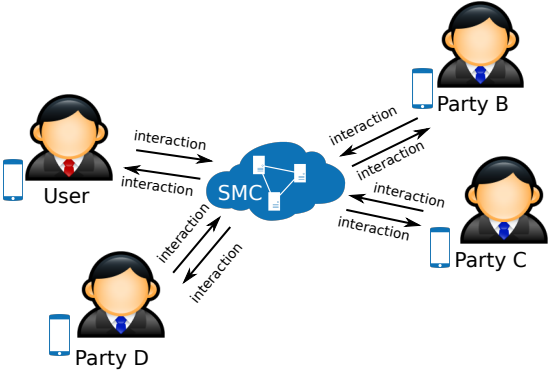
Scenario: Name of the scenario																					
Summary: A short description of the scenario																					
Scenario Illustration: 	Participants: The participating parties and their roles. <ul style="list-style-type: none"> • $P1$: < Party 1 > – \mathcal{I} (e.g.) • $P2$: < Party 2 > – \mathcal{IC} • $P3$: < Party 3 > – \mathcal{R} • ... 																				
Security Goals: <ul style="list-style-type: none"> • A list of security goals for the participating parties. • ... 	Attacker Model: <table border="1"> <thead> <tr> <th>Party</th> <th>trusted</th> <th>semi-ho.</th> <th>covert</th> <th>malicious</th> </tr> </thead> <tbody> <tr> <td>$P1$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P2$</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>$P3$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> </tbody> </table>	Party	trusted	semi-ho.	covert	malicious	$P1$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P2$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	$P3$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Party	trusted	semi-ho.	covert	malicious																	
$P1$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																	
$P2$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																	
$P3$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																	
Architectural Constraints: <ul style="list-style-type: none"> • Examples for architectural constraints are: • Execution time (CPU), latency, bandwidth, synchronization • ... 																					
Workpackage References: WP <xx.x>	Literature References: [1][2][3]																				

Table 2.1: The template to describe an application scenario.

Each scenario is motivated and described in a short summary. It is further illustrated by a figure that shows the interaction and communication behaviour between the different participants. The participants are also separately listed to show their assigned roles in the Secure multi-party computation (SMC) model. The different roles are introduced in the following sections. Furthermore, multiple security, privacy and verification goals are informally described for

each scenario. To analyze the behavior of possible adversaries, an attacker model for every participant is defined. A detailed description of the attacker models is also given in the next sections. Moreover, the technical requirements, e.g. hardware and network limitations, are listed. Finally, references to other work packages and literature are given, if available.

The technical notations and definitions that are used for each scenario are described in the remainder of this section. We begin by discussing common attacker models in SMC, before introducing the SMC role definitions. Finally, we clarify the notions used for verification requirements.

2.1 SMC - Attacker Models

In the setting of SMC, multiple parties with private inputs wish to jointly compute a functionality of their inputs. Informally speaking, the security requirements of such a computation are that nothing is learned from the protocol other than the output (privacy), the output is distributed according to the prescribed functionality (correctness), and parties cannot make their inputs depend on other parties' inputs [AL07]. Multiple technical solutions and frameworks for SMC have been developed in the past. A detailed overview is given in Deliverable D22.1 and here beyond the scope.

The security requirements in the setting of multi-party computation must hold even when some of the participating parties misbehave. Cryptographic tools have been proven to withstand strong adversarial behavior. However, the computational performance of the computation crucially depends on the adversaries strength. Therefore, an analysis of the attacker model is of importance when describing an application scenario.

Aumann and Lindell [AL07] distinguish three adversary models that are used to describe the attacker model in each scenario:

- *Malicious adversaries* are adversaries that may behave arbitrarily and are not bound in any way to follow the instructions of the specified protocol. Protocols that are secure in the malicious model provide a very strong security guarantee for the user.
- *Covert adversaries* have the property that they may deviate arbitrarily from the protocol specification in an attempt to cheat, but do not wish to be “caught” doing so. Protocols secure in the covert model guarantee that an adversary is caught cheating with at least a defined probability ϵ .
- *Semi-honest adversaries* correctly follow the specified protocol, yet they may attempt to learn additional information by analysing the transcript of messages received during the execution. Security in the presence of semi-honest adversaries provides a weaker security guarantee, yet might already be sufficient if the adversary is given limited access to the computation, e.g. through defined interface or framework.

We also annotate some parties as trusted parties which do not ‘attack’. A *Trusted third party (TTP)* is a party that is not in control of the honest party (user) but is assumed to behave according the protocol specifications without any semi-honest behavior.

2.2 SMC Party Roles

The participants in each scenario can be assigned with a SMC role. In the article [BKLPV13], Bogdanov et al. introduce three fundamental roles to describe an SMC system—the input party \mathcal{I} , the computation party \mathcal{C} and the result party \mathcal{R} . Input parties collect and send data to the SMC system. The SMC system itself is hosted by computation parties who carry out the SMC protocols on the inputs and send results to result parties in response of queries.

For the scenarios description in this deliverable we use the following notation. Let $\mathcal{I}^k = (\mathcal{I}_1, \dots, \mathcal{I}_k)$ be the list of input parties, $\mathcal{C}^m = (\mathcal{C}_1, \dots, \mathcal{C}_m)$ be the list of computing parties and $\mathcal{R}^n = (\mathcal{R}_1, \dots, \mathcal{R}_n)$ be the list of result parties.

In the following, \mathcal{ICR} refers to a party that fills all three roles, similarly, \mathcal{IC} refers to a party with roles \mathcal{I} and \mathcal{C} . We use superscripts ($k, m, n \geq 1$) to denote that there are several parties with the same role combination in the system. Real world parties can have more than one of these roles assigned to them. Thus, Bogdanov et al. argue that all deployments of SMC can be expressed using the combinations where all three roles are present. See Table 1 of [BKLPV13] for examples of typical SMC deployment models inspired by published research on SMC applications.

In conclusion, the three roles are sufficient to describe the tasks of each participant in the SMC model. Because of this, all participants in the scenario descriptions are annotated with a subset of the three fundamental roles $\mathcal{I}, \mathcal{C}, \mathcal{R}$.

2.3 Verification by external parties

Although typical mechanisms for secure computation outsourcing guarantee correctness, they do not guarantee verifiability. That is, although the parties involved in the computation are sure the results they obtain are correct, they may not have the means to prove this to others. In particular, to an outsider, all secure computations look the same regardless of the data that have been used. In fact, this property is used to show that secure outsourcing mechanisms meet certain privacy criteria. If the secure computations would look different, an (outside) attacker could derive information about the inputs of participants.

However, in various application scenarios, it is relevant for parties to be able to prove the correctness of a computation result. In particular, this is the case if outsiders who did not participate in the computation, nonetheless have an interest in its results. This may be a particular, known, set of outsiders; the set of outsiders may be unknown at the time of the computation; or it may be relevant that *anybody* can check the result of the computation, “for the common good”. A classical example of this latter type is e-voting. Also, parties that did participate in the computation may wish to be able to prove to an external authority that they are using the correct result of the computation. Here, one may consider medical researchers who publish statistical analysis results on patient data and want to prove correctness to an external referee.

Hence, in such cases, a securely outsourced computation should be *verifiable*, meaning that a party that was not involved in the computation can check that it was performed correctly. We distinguish between *universal verifiability* (also known as *public verifiability*), meaning that anybody can perform this check; and *designated verifiability*, meaning that only a specific set of parties appointed before the computation can perform the check. Note that, in its strongest form, the requirement of verifiability goes beyond the trust assumptions that parties in the computation place in each other: the verifier should be sure that, even if all parties involved

in the computation may attempt to cheat, the computation was still correctly performed.

The parties which verify a proof of correctness are said to take on the role of verifier. Although the role of verifier may overlap with that of result party, it is explicitly included for clarity. In the application scenario descriptions, parties that take on the role of verifier are indicated by the symbol \mathcal{V} in addition to their regular party roles.

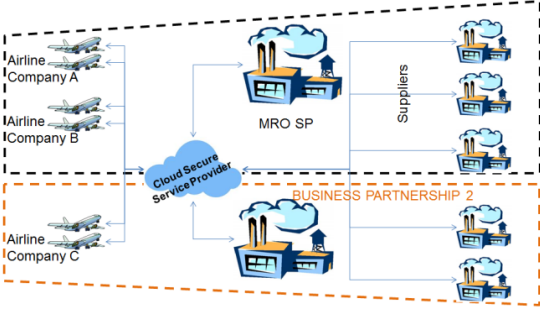
2.4 Scenario Animations

To provide an easy access to fundamental concepts of secure cloud computing scenarios, multiple scenarios in different areas were animated. A short video visualizes what the basic ideas behind the application scenarios are and how they operate in an abstract way. These animation videos enrich the scenario descriptions presented in this deliverable and are accessible for the consortium on the PRACTICE-website: <http://www.practice-project.eu/applicationscenarios>. In the next chapter, the application scenarios are presented and when available, a screen shot for the animated scenarios is given next to the scenario description.

Chapter 3

Application Scenarios

3.1 Joint Business Applications

<p>Scenario: Aeroengine Fleet Management</p>																										
<p>Summary: An online system (portal) enabling the optimization of the maintenance repair and overhaul (MRO) process for the engine sector of the aeronautic supply chain. Fleet owners provide their engine work load and status data, MRO service providers contribute their current work plan and inventory status, the suppliers provide their production plans and inventory data. Given all data in encrypted form, the system can compute an optimal service plan for the engines. This involves computing of supply plans as well as delivery orders for the involved suppliers. Moreover, spontaneous changes in the supply plans, e.g., production delays, are reported and update the plans accordingly.</p>																										
<p>Scenario Illustration:</p> 	<p>Participants:</p> <ul style="list-style-type: none"> • $P1$: Cloud Service Provider \mathcal{C} • $P2$: Airline Companies $\mathcal{I}^k \mathcal{R}^k$ • $P3$: MRO Service Provider $\mathcal{I}^m \mathcal{R}^m$ • $P4$: Suppliers $\mathcal{I}^n \mathcal{R}^n$ 																									
<p>Security Goals:</p> <ul style="list-style-type: none"> • The participants input data cannot be decrypted by the cloud service provider, neither by any other participants. • Computed supply plans, the resulting work and supply orders can only be decrypted by the designated suppliers and providers. 	<p>Attacker Model:</p> <table border="1"> <thead> <tr> <th>Party</th> <th>trusted</th> <th>semi-ho.</th> <th>covert</th> <th>malicious</th> </tr> </thead> <tbody> <tr> <td>$P1$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P2$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>$P3$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>$P4$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Party	trusted	semi-ho.	covert	malicious	$P1$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P2$	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	$P3$	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	$P4$	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Party	trusted	semi-ho.	covert	malicious																						
$P1$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																						
$P2$	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>																						
$P3$	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>																						
$P4$	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>																						
<p>Architectural Constraints:</p> <ul style="list-style-type: none"> • The platform should run on commodity cloud service providers. • The system should manage concurrent users when moving from the simulation to the supply planning service. • Execution time should be in minutes. • The system input should be updatable when critical events in the MRO service plan appear. 																										
<p>Workpackage References: WP 24.1, 24.2 and 24.3</p>	<p>Literature References: [KSZ⁺11]</p>																									

Scenario Animation

An animation of of scenario *Aeroengine Fleet Management* can be found on the PRACTICE website. A screen shot from the animation is given below.

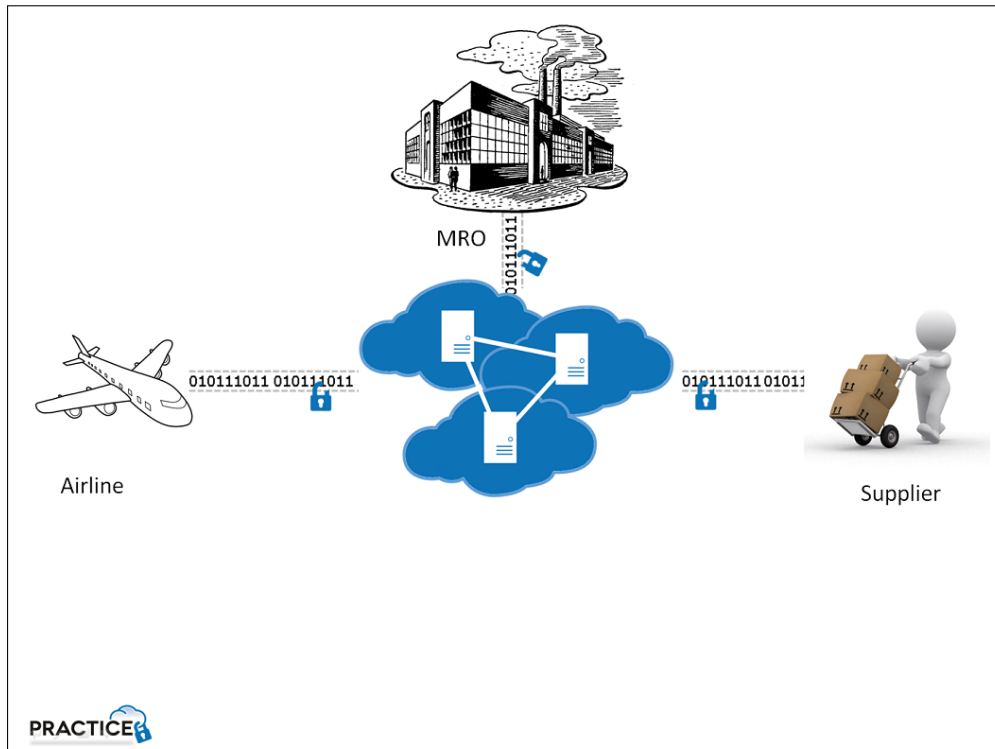
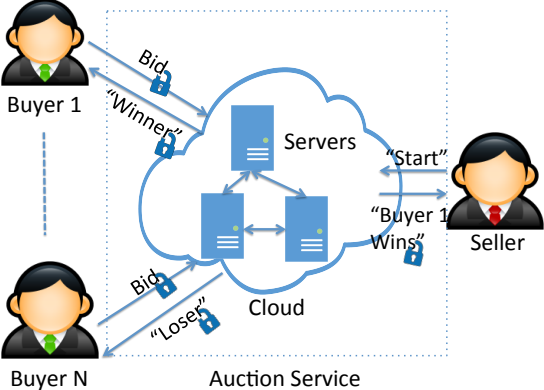


Figure 3.1: Aeroengine Fleet Management Illustration

Animation URL: http://www.practice-project.eu/animations/Aeroengine_Fleet_Management.mp4

<p>Scenario: Platform for Auctions</p>																																									
<p>Summary: Auctions is a mean to control the ways information is coordinated on a market and most auctions has elements of sealed bidding. Apart from the submitted bids, confidential information may also concern private information used to describe the commodities or services traded e.g. a consumption profile in procurement of electricity. As such, auctions may be interlinked with secure statistics. Secure multiparty computation is used commercially for handling confidential bids in some of the most common types of auctions, the double auction known from most exchanges for financial as well as physical commodities and the classical first price sealed bid auctions used in many procurement scenarios.</p>																																									
<p>Scenario Illustration:</p> 	<p>Participants:</p> <ul style="list-style-type: none"> • $P1$: Cloud service providers \mathcal{C}^k • $P2$: Auction service provider \mathcal{C} • $P3$: TTPs controlling the cloud entities \mathcal{C}^l • $P4$: Auction administrator \mathcal{C} • $P5$: Buyers one or more – $\mathcal{I}^n \mathcal{R}^m \mathcal{V}^n$ • $P6$: Sellers one or more – $\mathcal{I}^n \mathcal{R}^n \mathcal{V}^n$ • $P7$: Competition regulator – \mathcal{V} 																																								
<p>Security Goals:</p> <ul style="list-style-type: none"> • The private information cannot be recovered by any individual apart from the bidder that submitted the bid. • The auction result cannot be manipulated by any single participant (a part from the manipulation that may or may not result from the submitted bids) • A competition regulator may be included as designated verifier. 	<p>Attacker Model:</p> <table border="1"> <thead> <tr> <th>Party</th> <th>trusted</th> <th>semi-ho.</th> <th>covert</th> <th>malicious</th> </tr> </thead> <tbody> <tr> <td>$P1$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P2$</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P3$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P4$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P5$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P6$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P7$</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Party	trusted	semi-ho.	covert	malicious	$P1$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P2$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P3$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P4$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P5$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P6$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P7$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Party	trusted	semi-ho.	covert	malicious																																					
$P1$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																					
$P2$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																					
$P3$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																					
$P4$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																					
$P5$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																					
$P6$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																					
$P7$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																																					
<p>Architectural Constraints:</p> <ul style="list-style-type: none"> • The platform should run on commodity cloud service providers. • The TTPs, auction administrator, buyers and sellers interact through a intuitive web-interface provided by the cloud service provider. 																																									
<p>Workpackage References: W24 (to some extent)</p>	<p>Literature References: [BCD⁺09]</p>																																								

Scenario Animation

An animation of of scenario *Platform for Auctions* can be found on the PRACTICE website. A screen shot from the animation is given below.

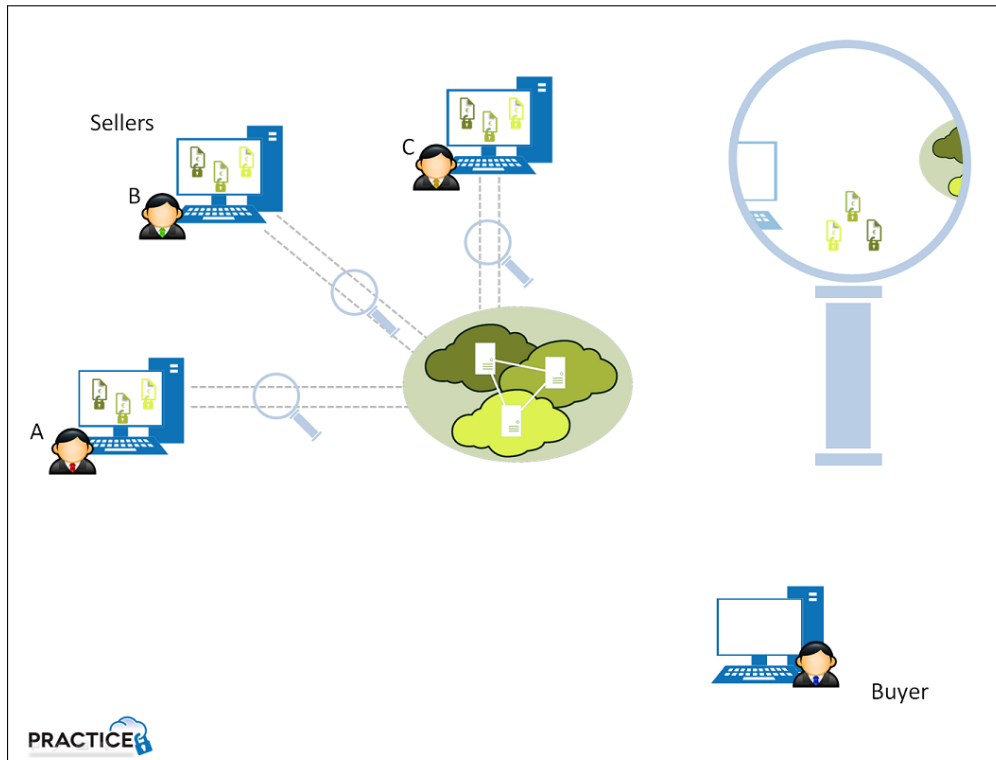
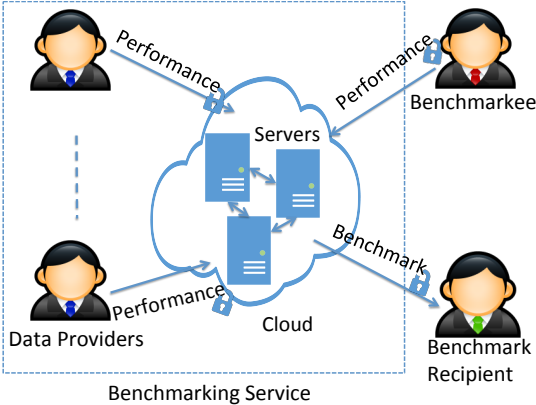
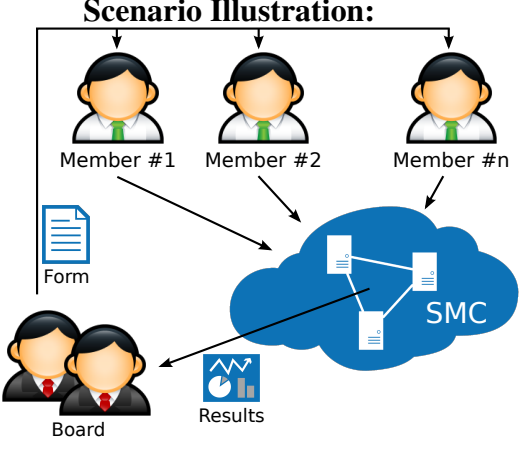
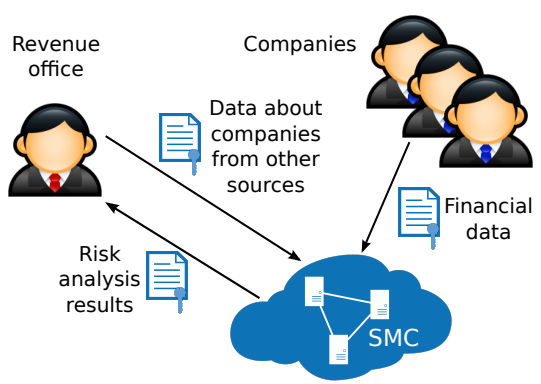


Figure 3.2: Platform for Auctions Illustration

Animation URL: http://www.practice-project.eu/animations/Platform_for_Auctions.mp4

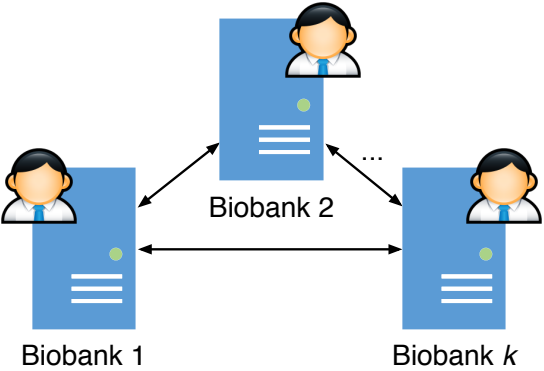
<p>Scenario: Platform for Benchmarking</p>																																				
<p>Summary: Benchmarking, understood as relative performance evaluation of "alternatives" (typically decision making units), is widely used to generate insight, planning as well as motivation. Keeping private information that describes the decision making units is typically critical. One exemplary deployment is the benchmarking of commercial bank customers. Here, benchmarking economic efficiency of the commercial customers can function as a complement to traditional credit rating. The value-added may e.g. come from a richer data foundation (which may also be used for credit rating) and/or the possibility to explore how exposed a given bank is. This solution requires a third party to confidentially handle information and no natural third party institution exists.</p>																																				
<p>Scenario Illustration:</p>  <p style="text-align: center;">Benchmarking Service</p>	<p>Participants:</p> <ul style="list-style-type: none"> • <i>P1</i>: Cloud service providers C^k • <i>P2</i>: Benchmarking service provider C • <i>P3</i>: SMC Server admins C^l • <i>P4</i>: Benchmarkee (entity to be benchmarked) \mathcal{I} • <i>P5</i>: Data providers (providing data to benchmark against) \mathcal{I}^n • <i>P6</i>: Benchmark recipient \mathcal{R} 																																			
<p>Security Goals:</p> <ul style="list-style-type: none"> • The private information (bids) cannot be recovered by any individual a part from the participant that submitted the information. • The benchmarking result cannot be manipulated by any single participant (a part from the manipulation that may or may not result from the submitted information). 	<p>Attacker Model:</p> <table border="1"> <thead> <tr> <th>Party</th> <th>trusted</th> <th>semi-ho.</th> <th>covert</th> <th>malicious</th> </tr> </thead> <tbody> <tr> <td><i>P1</i></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><i>P2</i></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td><i>P3</i></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><i>P4</i></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><i>P5</i></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><i>P6</i></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> </tbody> </table>	Party	trusted	semi-ho.	covert	malicious	<i>P1</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<i>P2</i>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<i>P3</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<i>P4</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<i>P5</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<i>P6</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Party	trusted	semi-ho.	covert	malicious																																
<i>P1</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																
<i>P2</i>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																																
<i>P3</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																
<i>P4</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																
<i>P5</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																
<i>P6</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																
<p>Architectural Constraints:</p> <ul style="list-style-type: none"> • The platform should run on commodity cloud service providers. • The SMC servers and other participants interact through a intuitive web-interface provided by the benchmark service provider. 																																				
<p>Workpackage References: WP23</p>	<p>Literature References: [Tof09]</p>																																			

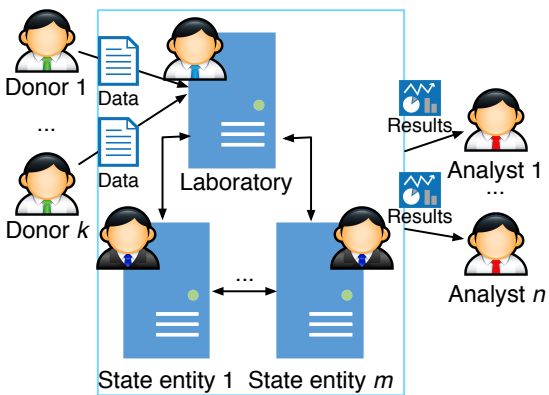
<p>Scenario: Consortium Gathering Information From its Members</p>																					
<p>Summary: Considering a scenario where a consortium would like gather information from its members, e.g. benchmark their joint economic results. However, consortium members might be competing companies and are, thus, reluctant to share that kind of information with the consortium board, which probably consists of some consortium members. Since, the consortium board should only be interested in aggregate results, a privacy breach can be alleviated by using SMC without losing functionality.</p>																					
<p>Scenario Illustration:</p>  <p>The diagram illustrates the scenario. At the top, three icons represent 'Member #1', 'Member #2', and 'Member #n'. Arrows from each member point to a central blue cloud labeled 'SMC'. To the left of the cloud is a document icon labeled 'Form'. Below the cloud, two icons represent the 'Board', with an arrow pointing from the 'SMC' cloud to them. A document icon labeled 'Results' is also shown near the Board.</p>	<p>Participants:</p> <ul style="list-style-type: none"> • $P1$: Consortium board – \mathcal{R}, \mathcal{V} • $P2$: Consortium members – $\mathcal{I}^n, \mathcal{V}^n$, where n is the total number of members • $P3$: Consortium members that execute the SMC for all members – $\mathcal{C}^k, k \leq n$ 																				
<p>Security Goals:</p> <ul style="list-style-type: none"> • Consortium board cannot see individual inputs. • Consortium members learn nothing about each other’s inputs. • If the consortium members have an interest in the results, or the correctness thereof, designated verifier or public verifiability can be used to prove correctness while limiting the number of interactive parties. • Due to the similarity of this scenario and electronic voting, the requirements of a voting application may also be imposed. 	<p>Attacker Model:</p> <table border="1"> <thead> <tr> <th>Party</th> <th>trusted</th> <th>semi-ho.</th> <th>covert</th> <th>malicious</th> </tr> </thead> <tbody> <tr> <td>$P1$</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>$P2$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P3$</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Party	trusted	semi-ho.	covert	malicious	$P1$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	$P2$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P3$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Party	trusted	semi-ho.	covert	malicious																	
$P1$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																	
$P2$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																	
$P3$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																	
<p>Architectural Constraints:</p> <ul style="list-style-type: none"> • Consortium members should not be forced to install any special software to submit their data. Web-based forms are preferable. 																					
<p>Workpackage References: WP22.1</p>	<p>Literature References: [Tal11, BTW12]</p>																				

<p>Scenario: Tax Fraud Detection</p>																										
<p>Summary: Detecting tax frauds is one of the cases where state entities, i.e., the revenue office, are interested in analyzing precise financial data of companies. However, such a risk analysis would require the creation of so-called super-databases, which might be prohibited by the law. With the help of SMC, a precise analysis of cash flows can be executed that follows the law without the necessity to reveal the companies' sensitive financial data to the revenue office. Moreover, the revenue office can input data from other sources to improve the risk analysis results.</p>																										
<p>Scenario Illustration:</p> 	<p>Participants:</p> <ul style="list-style-type: none"> • $P1$: Private companies – \mathcal{I}^n • $P2$: State cloud – \mathcal{C}^k • $P3$: Revenue office – \mathcal{ICR} • $P4$: Referee – \mathcal{V} 																									
<p>Security Goals:</p> <ul style="list-style-type: none"> • The revenue office can not see any financial data of any of the companies. • Only the revenue office can see the risk analysis results, which only lists suspicious companies. • Companies can not see any data about other companies. Not even which companies are being analyzed. • A referee or (independent) state entity may need to be involved as designated verifier for the risk analysis. 	<p>Attacker Model:</p> <table border="1"> <thead> <tr> <th>Party</th> <th>trusted</th> <th>semi-ho.</th> <th>covert</th> <th>malicious</th> </tr> </thead> <tbody> <tr> <td>$P1$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P2$</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>$P3$</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>$P4$</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Party	trusted	semi-ho.	covert	malicious	$P1$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P2$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	$P3$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	$P4$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Party	trusted	semi-ho.	covert	malicious																						
$P1$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																						
$P2$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																						
$P3$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																						
$P4$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																						
<p>Architectural Constraints:</p> <ul style="list-style-type: none"> • Data collection and analysis should run in a cloud provided by the revenue office. • Data collection should be done via web-interface provided by the revenue office. • Data submission should be fast even in case of large amount of data. • Data analysis parallel to the data submission should be possible to reduce the overall time consumption of the computation. 																										
<p>Workpackage References:</p>	<p>Literature References:</p>																									

3.2 Joint Studies Applications

<p>Scenario: Joint Statistical Analysis Between State Entities</p>																										
<p>Summary: Often, the public administration would like to have an overview of how one of its governance fields reflects on another, e.g. how does working during university studies influences the drop-out rate of university students. As the law forbids the compilation of a so-called <i>super-database</i> between the different state entities, the analysis can only be carried out by using pre-aggregated data or some other such method. This, however, can reduce the quality of analysis results as more subtle nuances can be overlooked. In this scenario, the state entities combine their databases in a privacy preserving manner and allow a data analyst to perform pre-agreed queries.</p>																										
<p>Scenario Illustration:</p> <p>The diagram illustrates the data flow in the scenario. On the left, there are two icons representing 'State entity 1' and 'State entity k'. Arrows labeled 'Data' point from these entities to a central area containing two icons representing 'Host 1' and 'Host m'. From the hosts, an arrow labeled 'Results' points to an icon of an 'Analyst'.</p>	<p>Participants:</p> <ul style="list-style-type: none"> • $P1$: Hosts – \mathcal{C}^m • $P2$: State entities – \mathcal{I}^k • $P3$: Data analyst(s) – \mathcal{R}, \mathcal{V} • $P4$: Referee – \mathcal{V} 																									
<p>Security Goals:</p> <ul style="list-style-type: none"> • The input data cannot be decrypted by any computing or result party. • <i>Output privacy</i> is guaranteed for the analysis result. • The analysis result can only be decrypted by the data analyst. • A referee or (independent) state entity may need to be involved as designated verifier to guarantee correctness of the results on behalf of the general public. 	<p>Attacker Model:</p> <table border="1"> <thead> <tr> <th>Party</th> <th>trusted</th> <th>semi-ho.</th> <th>covert</th> <th>malicious</th> </tr> </thead> <tbody> <tr> <td>$P1$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P2$</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>$P3$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P4$</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Party	trusted	semi-ho.	covert	malicious	$P1$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P2$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	$P3$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P4$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Party	trusted	semi-ho.	covert	malicious																						
$P1$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																						
$P2$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																						
$P3$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																						
$P4$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																						
<p>Architectural Constraints:</p> <ul style="list-style-type: none"> • If needed, state entities can host the servers themselves. The hosts can also be chosen among state entities that are not sharing their data. In this case, these parties can be considered semi-honest. • The analyst interacts with the system through an intuitive web-interface provided by the hosts or through a command line tool that allows only previously agreed queries. The command line tool must resemble existing statistical analysis tools, such as GNU R, to be intuitive for the analyst. 																										
<p>Workpackage References: WP 22.1</p>	<p>Literature References: [BKL⁺14]</p>																									

<p>Scenario: Privacy Preserving Genome-Wide Association Studies Between Biobanks</p>																
<p>Summary: Biobanks from different countries wish perform a joint genome-wide association study using each other’s data. The biobanks already have collected the data based on signed consent forms from their donors. To collaborate, and, hence, get more accurate and interesting results, they want to share the data among each other without breaching the donors’ privacy.</p>																
<p>Scenario Illustration:</p> 	<p>Participants:</p> <ul style="list-style-type: none"> • $P1$: Biobanks – ICR^k • $P2$: Referee or state entity – \mathcal{V} 															
<p>Security Goals:</p> <ul style="list-style-type: none"> • The donors’ input data cannot be decrypted other biobanks. • The parties are not able to make sure which records were input by which biobanks. • <i>Output privacy</i> is guaranteed for the analysis result to the highest possible degree. • A referee or state entity may need to be involved as designated verifier to guarantee correctness of the results on behalf of the general public. 	<p>Attacker Model:</p> <table border="1"> <thead> <tr> <th>Party</th> <th>trusted</th> <th>semi-ho.</th> <th>covert</th> <th>malicious</th> </tr> </thead> <tbody> <tr> <td>$P1$</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>$P2$</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Party	trusted	semi-ho.	covert	malicious	$P1$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	$P2$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Party	trusted	semi-ho.	covert	malicious												
$P1$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												
$P2$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												
<p>Architectural Constraints:</p> <ul style="list-style-type: none"> • The biobanks host the shared database themselves or the hosting can be outsourced to cloud service providers, but in the latter case, k biobanks should have the same service provider in case of k-out-of-n privacy. • Data analysts in biobanks interact with the service through an intuitive web-interface or through a command line tool that allows only previously agreed queries. The command line tool must resemble existing statistical analysis tools, such as GNU R, to be intuitive for the analysts. • The biobanks must have the possibility to delete data of a donors if asked to do so by the donor. 																
<p>Workpackage References: WP 22.1</p>	<p>Literature References: [KBLV13]</p>															

<p>Scenario: Privacy Preserving Personal Genome Analyses and Studies</p>																															
<p>Summary: Donors can submit their DNA to a laboratory to receive feedback on genetic associations with specific illnesses and disorders. This genome data can then be added to a databases for further genome research. With the help of SMC, donors can also enter their phenotype information so that no involved organization sees their individual data, while analysts can still perform genome-wide association studies. Thus, in contrast to the 23andMe project, which is the largest genetic testing service provider, the sensitive phenotype data is protected. This can be realized by splitting (secret sharing) the sensitive data between laboratories and multiple state entities.</p>																															
<p>Scenario Illustration:</p> 	<p>Participants:</p> <ul style="list-style-type: none"> • $P1$: Laboratory – \mathcal{C} • $P2$: Donor(s) – \mathcal{I}^k • $P3$: State entities – \mathcal{C}^m • $P4$: Data analyst(s) – $\mathcal{R}^n, \mathcal{V}^n$ • $P5$: Referee or state entity – \mathcal{V} 																														
<p>Security Goals:</p> <ul style="list-style-type: none"> • The donors’ phenotype data cannot be decrypted by other parties. • <i>Output privacy</i> is guaranteed for the analysis result to the highest possible degree. • The survey result can only be decrypted by the data analysts. • Donors learn <i>nothing</i> about other donors. • A referee or state entity may need to be involved as designated verifier to guarantee correctness of the results on behalf of the general public. 	<p>Attacker Model:</p> <table border="1"> <thead> <tr> <th>Party</th> <th>trusted</th> <th>semi-ho.</th> <th>covert</th> <th>malicious</th> </tr> </thead> <tbody> <tr> <td>$P1$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P2$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P3$</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>$P4$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P5$</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Party	trusted	semi-ho.	covert	malicious	$P1$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P2$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P3$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	$P4$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P5$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Party	trusted	semi-ho.	covert	malicious																											
$P1$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																											
$P2$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																											
$P3$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																											
$P4$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																											
$P5$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																											
<p>Architectural Constraints:</p> <ul style="list-style-type: none"> • The laboratory can host one of the servers, state entities can host others. • Data donors and analysts interact through an intuitive web-interface provided by the computing hosts. • Data donors must have the option and possibility to delete their data from the system. 																															
<p>Workpackage References: WP 22.1</p>	<p>Literature References: [23a, KBLV13]</p>																														

Scenario Animation

An animation of of scenario *Privacy Preserving Genome Analysis and Studies* can be found on the PRACTICE website. A screen shot from the animation is given below.

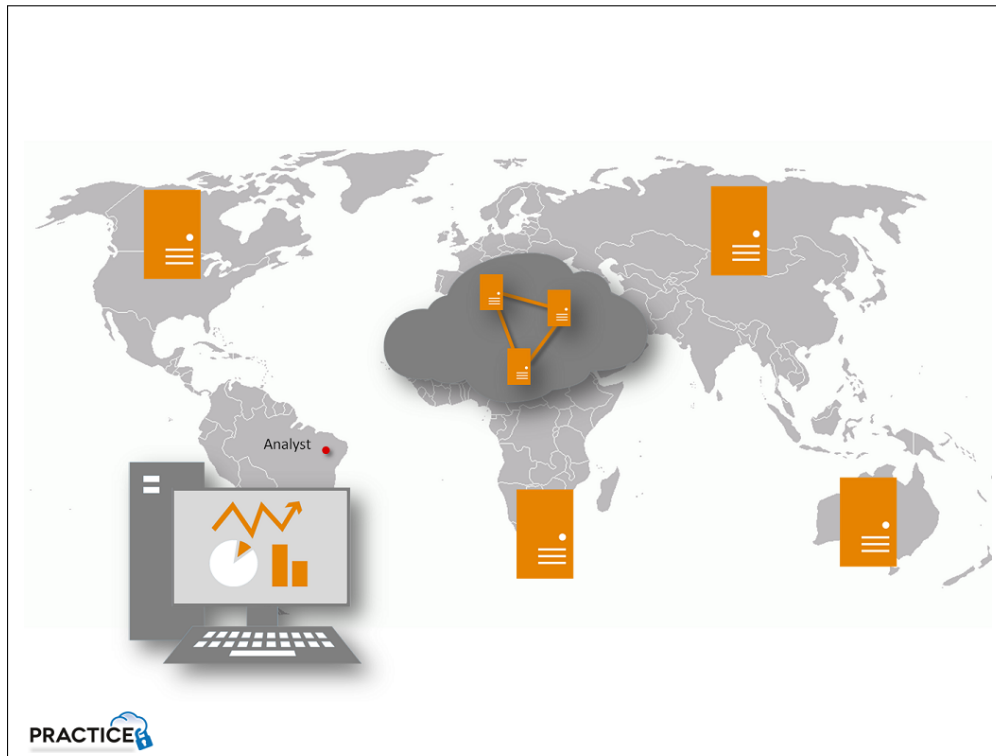
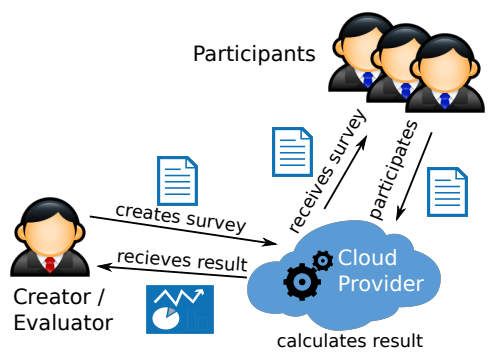
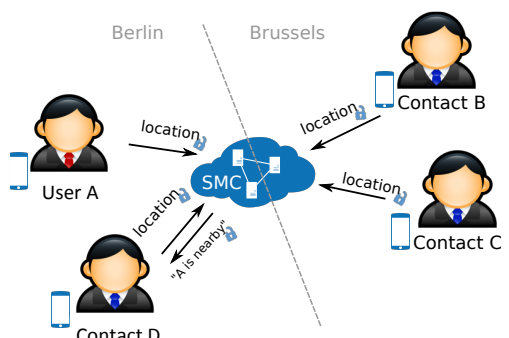


Figure 3.3: Privacy Preserving Genome Analysis and Studies Illustration

Animation URL: http://www.practice-project.eu/animations/Privacy_Preserving_Personal_Genome_Analysis_and_Studies.mp4

<p>Scenario: Platform for Surveys on Sensitive Data</p>																															
<p>Summary: An online platform that allows users to design and run surveys while preserving the participants privacy. Survey creators can create and upload their surveys to the platform that is also accessible to the participants. After participation a report generation system compiles a report based on the participants encrypted data for the evaluator. The portal is designed to reduce all kinds of leaks of private data.</p>																															
<p>Scenario Illustration:</p> 	<p>Participants:</p> <ul style="list-style-type: none"> • $P1$: Cloud service provider – \mathcal{C} • $P2a$: Survey creator – \mathcal{I} • $P2b$: Survey evaluator – \mathcal{R}, \mathcal{V} • $P3$: Survey participant(s) – \mathcal{I}^k • $P4$: General public – \mathcal{V} 																														
<p>Security Goals:</p> <ul style="list-style-type: none"> • The participants input data cannot be decrypted by the cloud provider, neither by the survey creator/evaluator. • The survey's result can only be decrypted by the survey evaluator. • <i>Output privacy</i> is guaranteed for the survey's result. • Participants learn <i>nothing</i> about other participants. • By making the evaluator ($P2b$) a designated verifier, they do not have to participate interactively in the protocol. • If there is a public interest in the survey results, the scenario is similar to electronic voting. In this case universal verifiability may be required, in addition to other requirements for voting. 	<p>Attacker Model:</p> <table border="1"> <thead> <tr> <th>Party</th> <th>trusted</th> <th>semi-ho.</th> <th>covert</th> <th>malicious</th> </tr> </thead> <tbody> <tr> <td>$P1$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P2a$</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P2b$</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P3$</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P4$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> </tbody> </table>	Party	trusted	semi-ho.	covert	malicious	$P1$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P2a$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P2b$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P3$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P4$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Party	trusted	semi-ho.	covert	malicious																											
$P1$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																											
$P2a$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																											
$P2b$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																											
$P3$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																											
$P4$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																											
<p>Architectural Constraints:</p> <ul style="list-style-type: none"> • The platform should run on commodity cloud service providers. • Survey creator, evaluator and participant interact through a web-interface provided by the cloud service provider. 																															
<p>Workpackage References: W23.1</p>	<p>Literature References:</p>																														

3.3 Location Sharing Applications

<p>Scenario: Location Sharing with Nearby Contacts</p>																
<p>Summary: A smart phone app that lets users announce their location to nearby contacts, while not leaking location information to far away contacts. This is useful when users want to meet up with their contacts for various activities (dating, networking, etc.). As a users location can communicate a lot of private information (sexuality, religion, occupation, etc.), the users prefer to reveal their location only to relevant contacts (i.e. those nearby). The system protects the user's privacy by computing proximity using SMC.</p>																
<p>Scenario Illustration:</p> 	<p>Participants:</p> <ul style="list-style-type: none"> • <i>P1</i>: User (revealing her location) – <i>IRC</i> • <i>P2</i>: Contacts (potentially learning <i>P1</i>'s location) – <i>IRC^k</i> 															
<p>Security Goals:</p> <ul style="list-style-type: none"> • The location of neither the user nor her contacts should be revealed unless so intended (e.g. locations can not be permanently broadcasted, or registered at some third party). • If the user decides to announce her location only nearby contacts should learn her location. • The user should not learn the location of her contacts. 	<p>Attacker Model:</p> <table border="1"> <thead> <tr> <th>Party</th> <th>trusted</th> <th>semi-ho.</th> <th>covert</th> <th>malicious</th> </tr> </thead> <tbody> <tr> <td><i>P1</i></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><i>P2</i></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> </tbody> </table>	Party	trusted	semi-ho.	covert	malicious	<i>P1</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<i>P2</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Party	trusted	semi-ho.	covert	malicious												
<i>P1</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>												
<i>P2</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>												
<p>Architectural Constraints:</p> <ul style="list-style-type: none"> • Communication and computation is done on smartphones, with potentially quite limited resources. • The computation should be quick for the app to appear responsive. 																
<p>Workpackage References:</p>	<p>Literature References: [NPS12]</p>															

Scenario Animation

An animation of of scenario *Location Sharing with Nearby Contacts* can be found on the PRACTICE website. A screen shot from the animation is given below.

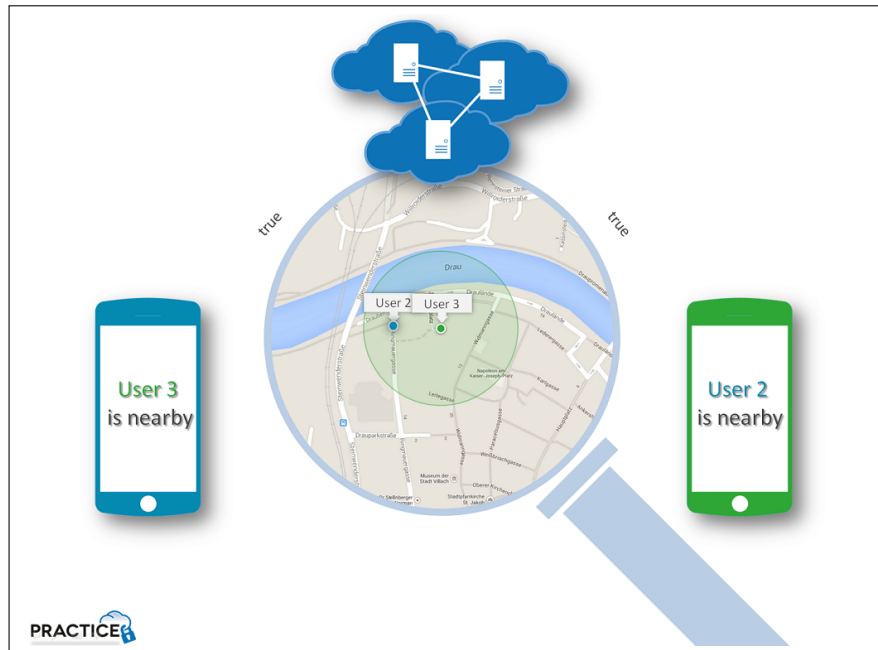
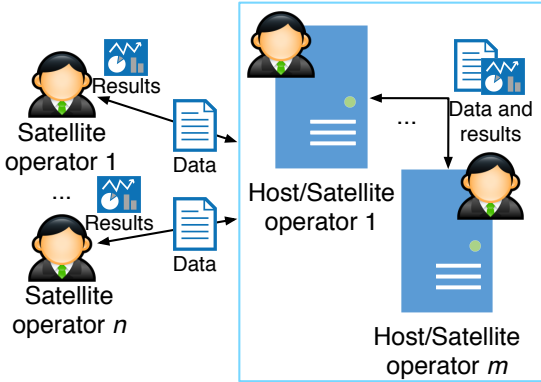
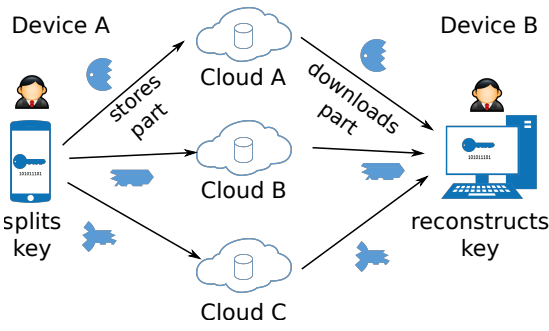


Figure 3.4: Location Sharing with Nearby Contacts Illustration

Animation URL: http://www.practice-project.eu/animations/Location_Sharing_with_Nearby_Contacts.mp4

<p>Scenario: Privacy Preserving Satellite Collision Detection</p>																					
<p>Summary: Different countries wish to detect collisions between their satellites without revealing the exact location and trajectory of their satellite.</p>																					
<p>Scenario Illustration:</p> 	<p>Participants:</p> <ul style="list-style-type: none"> • $P1$: Hosts chosen from among the satellite operators – ICR^m • $P2$: Satellite operators – IR^n, \mathcal{V}^n • $P3$: Authority – \mathcal{V} 																				
<p>Security Goals:</p> <ul style="list-style-type: none"> • Satellite operators and hosts learn nothing about satellite locations or trajectories. • Only the collision probability is revealed if it exceeds a threshold. • In case of a collision the operators involved may wish to prove correctness of protocol executions to a designated authority. This is possible by using verifiable computation. 	<p>Attacker Model:</p> <table border="1"> <thead> <tr> <th>Party</th> <th>trusted</th> <th>semi-ho.</th> <th>covert</th> <th>malicious</th> </tr> </thead> <tbody> <tr> <td>$P1$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P2$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P3$</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Party	trusted	semi-ho.	covert	malicious	$P1$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P2$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P3$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Party	trusted	semi-ho.	covert	malicious																	
$P1$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																	
$P2$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																	
$P3$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																	
<p>Architectural Constraints:</p> <ul style="list-style-type: none"> • Hosting parties are chosen among satellite operators. • Satellite operators interact through an intuitive web-interface provided by the computing hosts. 																					
<p>Workpackage References: WP 22.1</p>	<p>Literature References: [KW13]</p>																				

3.4 End User Applications

Scenario: Key Management																
Summary: The increasing use of multiple devices by the same person for business and other purposes has amplified the annoyance of making cryptographic keys available across different platforms and devices. Typing cryptographic keys into a smart phone interface is at best very impractical. Copying the key to a media (e.g. USB) is not possible for many devices. Emailing the key, using sharing services or a central key server is in most cases a security liability. A solution to enable an easy access to cryptographic keys is to use SMC by delegating the trust to multiple cloud providers. In this way the required security properties can be achieved.																
Scenario Illustration: 	Participants: <ul style="list-style-type: none"> • $P1$: User ICR • $P2$: Cloud service providers C^n 															
Security Goals: <ul style="list-style-type: none"> • Ensure that no individual cloud provider can obtain the keys. 	Attacker Model: <table border="1"> <thead> <tr> <th>Party</th> <th>trusted</th> <th>semi-ho.</th> <th>covert</th> <th>malicious</th> </tr> </thead> <tbody> <tr> <td>$P1$</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>$P2$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> </tbody> </table>	Party	trusted	semi-ho.	covert	malicious	$P1$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	$P2$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Party	trusted	semi-ho.	covert	malicious												
$P1$	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												
$P2$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>												
Architectural Constraints: <ul style="list-style-type: none"> • The platform should run on commodity cloud service providers. • The user can download and access keys from the cloud providers from a range of devices. 																
Workpackage References:	Literature References:															

Scenario Animation

An animation of of scenario *Key Management* can be found on the PRACTICE website. A screen shot from the animation is given below.

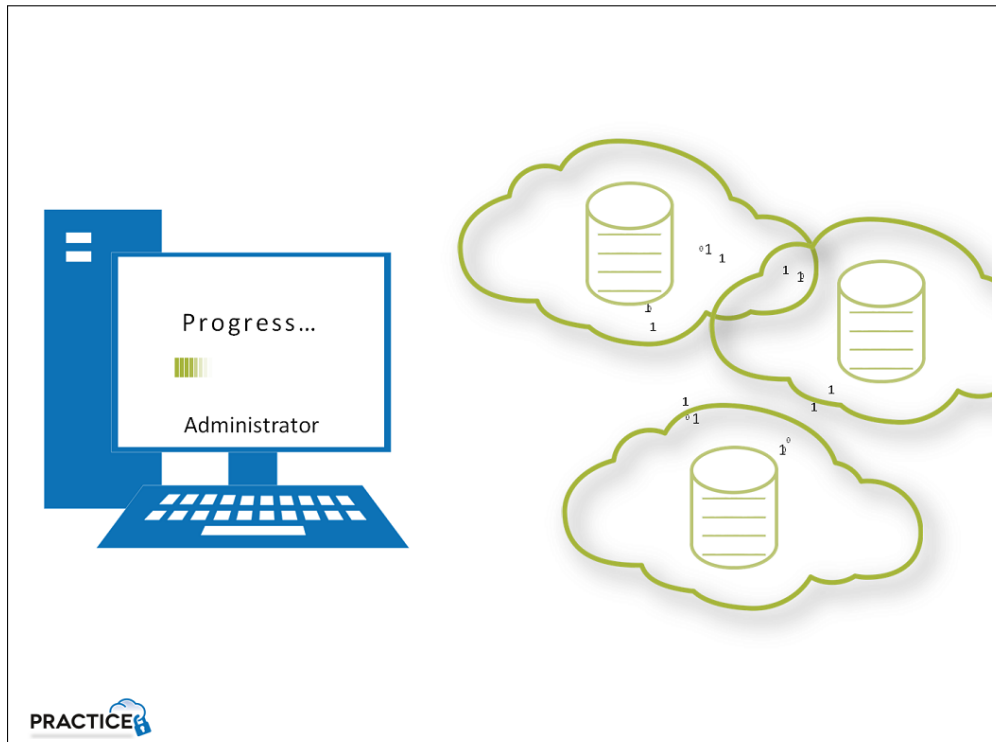
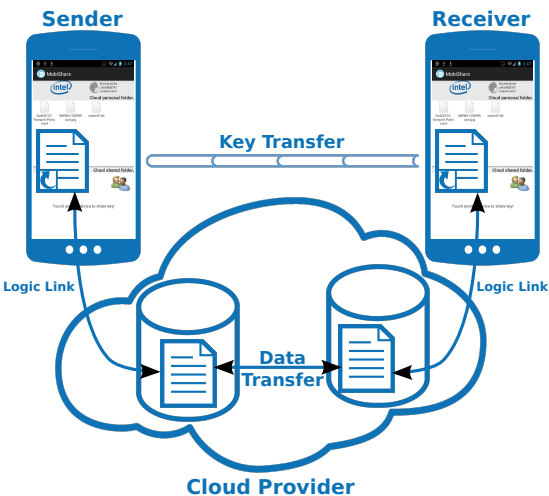


Figure 3.5: Key Management Illustration

Animation URL: http://www.practice-project.eu/animations/Key_Management.mp4

<p>Scenario: Mobile Data Sharing</p>																					
<p>Summary: Mobile Data Sharing enables users of cloud storage services to encrypt their data in the cloud while still being able to share the data with other (trusted) users. All files are always encrypted while being in the cloud; the files are encrypted when stored and also while they are transferred between users. For the receiver to be able to access the encrypted data she has to get access to the corresponding keys. These keys are transferred via a secure channel between the sender and the receiver, the secure channel is established based on a shared secret exchanged between the users smart phones, e.g. via NFC.</p>																					
<p>Scenario Illustration:</p> 	<p>Participants:</p> <ul style="list-style-type: none"> • $P1$: Cloud service provider C • $P2$: Sender IC • $P3$: Receiver RC 																				
<p>Security Goals:</p> <ul style="list-style-type: none"> • Provide confidentiality for data in the cloud. • Data is only shared with others when intended by the data owner (sender). 	<p>Attacker Model:</p> <table border="1"> <thead> <tr> <th>Party</th> <th>trusted</th> <th>semi-ho.</th> <th>covert</th> <th>malicious</th> </tr> </thead> <tbody> <tr> <td>$P1$</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>$P2$</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>$P3$</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Party	trusted	semi-ho.	covert	malicious	$P1$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	$P2$	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	$P3$	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Party	trusted	semi-ho.	covert	malicious																	
$P1$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																	
$P2$	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																	
$P3$	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																	
<p>Architectural Constraints:</p> <ul style="list-style-type: none"> • The system should run on commodity cloud service providers and smart phones. • The app should be responsive on limited capabilities of smart phones. 																					
<p>Workpackage References: WP22.1</p>	<p>Literature References:</p>																				

Scenario Animation

An animation of of scenario *Mobile Data Sharing* can be found on the PRACTICE website. A screen shot from the animation is given below.

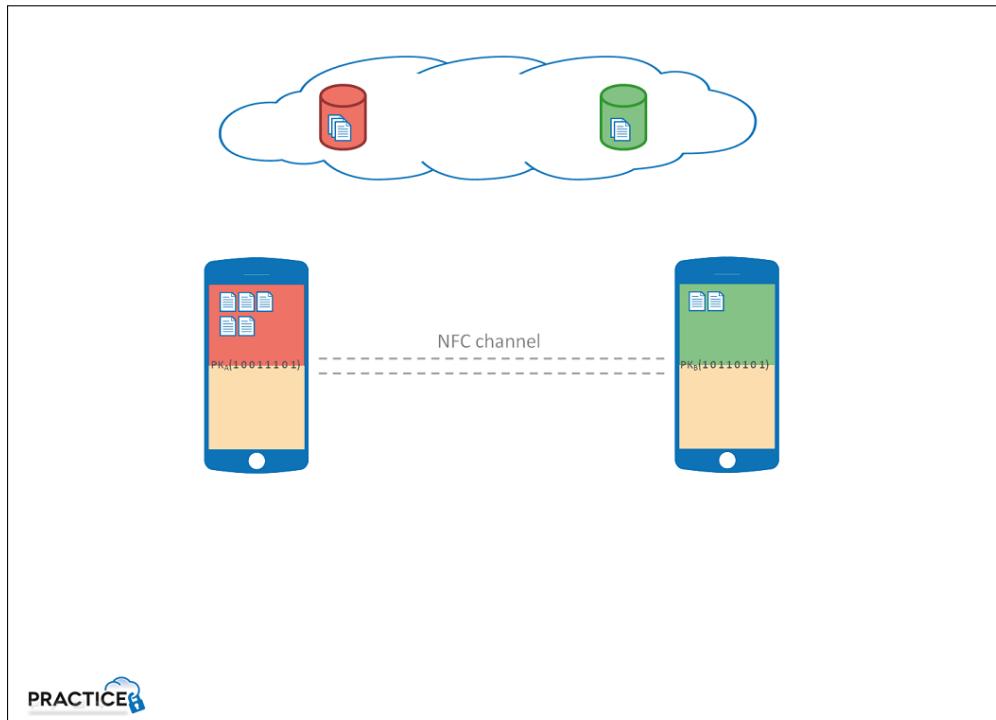


Figure 3.6: Mobile Data Sharing Illustration

Animation URL: http://www.practice-project.eu/animations/Mobile_Data_Sharing.mp4

Chapter 4

Conclusion

In this deliverable, different application scenarios that greatly benefit from SMC are presented. The connecting motivation for all scenarios is the requirement for privacy and confidentiality of the participants' data. In most scenarios, multiple parties are interested in computing a common result without fearing the risk of a privacy breach or issuing trust into other parties. Even so, in all scenarios the participants inputs have to be kept private, only in a few scenarios the output is not shared between multiple participants. The variety of scenarios itself shows that SMC is not only a promising enabler for joint business cases but could also be used to avoid legal hurdles and to reduce the required trust for end user applications that function on sensitive data.

Moreover, two distinct deployment models become visible when comparing the scenarios. The first model involves an additional external party, i.e., a cloud service provider, to outsource the computation. In the second model the computation is done between the already existing input and result parties. In the latter case, the SMC implementations have to cope the (limited) computational capabilities of the participating parties and their devices. Another architectural requirement that occurs multiple times in the scenarios is the need for an accessible interface, e.g. web site, to the application and hence, SMC. Thus, integrating secure cloud computing with ease-of-use into existing platforms is also challenge that should be tackled within the further work packages.

Furthermore, we observe that most scenarios have at least one participant that might behave malicious. Consequently, efficient SMC implementations that are secure against malicious adversaries should be of special interest in PRACTICE.

During the further course of WP12 a more detailed analysis of the here listed scenarios will be given. This involves a detailed evaluation of the trust, adversary, verification, communication and system models.

Chapter 5

List of Abbreviations

EC	European Commission
SMC	Secure Multiparty Computation
TTP	Trusted Third Party
WP	Work Package

Bibliography

- [23a] 23andMe Project. <https://www.23andme.com/>.
- [AL07] Yonatan Aumann and Yehuda Lindell. Security against covert adversaries: Efficient protocols for realistic adversaries. In *Theory of Cryptography*, pages 137–156. Springer, 2007.
- [BCD⁺09] Peter Bogetoft, Dan Lund Christensen, Ivan Damgård, Martin Geisler, Thomas P. Jakobsen, Mikkel Krøigaard, Janus Dam Nielsen, Jesper Buus Nielsen, Kurt Nielsen, Jakob Pagter, Michael I. Schwartzbach, and Tomas Toft. Secure multiparty computation goes live. In Dingledine and Golle [DG09], pages 325–343.
- [BKL⁺14] Dan Bogdanov, Liina Kamm, Sven Laur, Pille Pruulmann-Vengerfeldt, Riivo Talviste, and Jan Willemson. Privacy-preserving statistical data analysis on federated databases. In *Proceedings of the Annual Privacy Forum. APF'14*, LNCS. Springer, 2014.
- [BKLPV13] Dan Bogdanov, Liina Kamm, Sven Laur, and Pille Pruulmann-Vengerfeldt. Secure multi-party data analysis: end user validation and practical experiments. Cryptology ePrint Archive, Report 2013/826, 2013.
- [BTW12] Dan Bogdanov, Riivo Talviste, and Jan Willemson. Deploying secure multi-party computation for financial data analysis (short paper). In *Proceedings of the 16th International Conference on Financial Cryptography and Data Security. FC'12*, pages 57–64, 2012.
- [DG09] Roger Dingledine and Philippe Golle, editors. *Financial Cryptography and Data Security, 13th International Conference, FC 2009, Accra Beach, Barbados, February 23-26, 2009. Revised Selected Papers*, volume 5628 of *Lecture Notes in Computer Science*. Springer, 2009.
- [Gre11] Andy Greenberg. Darpa will spend \$20 million to search for crypto's holy grail. *Forbes*, 2011.
- [KBLV13] Liina Kamm, Dan Bogdanov, Sven Laur, and Jaak Vilo. A new way to protect privacy in large-scale genome-wide association studies. *Bioinformatics*, 29(7):886–893, 2013.
- [KSZ⁺11] Florian Kerschbaum, A Schröpfer, Antonio Zilli, Richard Pibernik, Octavian Catrina, Sebastiaan de Hoogh, Berry Schoenmakers, Stelvio Cimato, and Ernesto Damiani. Secure collaborative supply-chain management. *Computer*, 44(9):38–43, 2011.
- [KW13] Liina Kamm and Jan Willemson. Secure floating-point arithmetic and private satellite collision analysis. Cryptology ePrint Archive, Report 2013/850, 2013. <http://eprint.iacr.org/>.

- [NPS12] Janus Dam Nielsen, Jakob Illeborg Pagter, and Michael Bladt Stausholm. Location privacy via actively secure private proximity testing. In *PerCom Workshops*, pages 381–386. IEEE, 2012.
- [SPA] Security And Privacy Assurance Research (SPAR) Program Broad Agency Announcement (BAA). <https://www.fbo.gov/?s=opportunity&mode=form&id=c55e38dbde30cb668f687897d8f01e69>.
- [Tal11] Riivo Talviste. Deploying secure multiparty computation for joint data analysis—a case study. Master’s thesis, Institute of Computer Science, University of Tartu, 2011.
- [Tof09] Tomas Toft. Solving linear programs using multiparty computation. In Dingledine and Golle [DG09], pages 90–107.