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

D24.3

Industrial Settings

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

Deliverable type:	Report
Deliverable reference number:	ICT-609611 / D24.3/ DRAFT | 0.1
Activity and Work package contributing to the deliverable:	Activity 2 / WP 24
Due date:	October 2015 – M24
Actual submission date:	9th November 2015

Responsible organisation:	DTA/CCII-UNISA
Editor:	Antonio Zilli
Dissemination level:	PU
Revision:	1.0

Abstract:	Data leakage risks in collaborative SC are measured. The architecture and design strategy of the prototype cloud SCM system is introduced. An assessment framework to evaluate the pilot cases is prepared.
Keywords:	Data leakage risk measurement; prototype security assumptions; security and business pilot assessment framework.

Editor

Antonio Zilli (UNISA/CCII - third party of DTA)

Contributors (ordered according to beneficiary numbers)

Angelo Corallo, Giuseppe Grassi, Marianna Lezzi (UNISA/CCII - third party of DTA)

Fabian Taigel, Julian Kurz, Jan Meller, Richard Pibernik (UWUERZ)

Florian Hahn (SAP)

Kurt Nielsen (PAR)

Stelvio Cimato (UMIL)

Cem Kazan, Buket Serper, Elif Özdoğan (ARC)

Mario Münzer (TEC)

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 (PRACTICE).

Executive Summary

This report focuses on three themes: the validation of the collaborative supply chain management models through the measurement of data protection level, the preliminary design of the architecture of the cloud supply chain management prototype and the preparation of the prototype assessment framework. In particular, collaborative supply chain management models are: the collaborative forecasting and planning model for the maintenance, repair and overhaul (MRO) service in the aero-engine business segment, and the Vendor Managed Inventory model in the consumer goods industry.

The validation of the models was realized by measuring the risks associated with data involved in the collaborative computation. Risks were measured by interviewing industrial players on the impacts and the tolerable probability of data leakage events (indeed some risks are acceptable in exchange of certain business benefits). In the aeronautic case, a web survey was conducted. The survey was implemented by leveraging the platform for secure survey developed in WP23; Sharemind architecture, indeed, improves standard web survey systems providing high data security. IT, supply chain and management industrial staff mainly composed the sample. In the consumer good industry, risks were assessed through face-to-face meetings between the ARC staff involved in PRACTICE and ARC suppliers' and customers' staff. The interviews and surveys were preceded by a presentation of data protection performance of secure computation, of the PRACTICE project expected results and of the partial results achieved.

The results of the measurements are:

- the supply chain collaborative models represent valid solution to the challenges of the two industries,
- the acceptance of collaborative supply chain models are actually strongly limited by the high confidential data they involve,
- the use of cloud applications is related to higher concerns on the security issues, for example associated with data storage location in the aeronautic case,
- and, finally, the measured risk values, in the aeronautic case, belong to the highest 30% of the risk assessment scale. The qualitative analysis in consumer goods industry provides similar results.

The risks measurement completes the security requirements. They are taken in consideration in the definition of the architecture and in the selection of the Order Preserving Encryption Scheme in order to implement algorithms into the prototype cloud supply chain management systems.

A pilot assessment framework, spanning from the identification of the expected security improvements, brought by the cloud collaborative planning system, to the metrics measuring the business impacts, was developed to evaluate business benefits more precisely. Specifically, the business impact of collaborative planning is measured in four management areas: customer, process, inventory and financial; in this way it is possible to recognize in the most comprehensive way how collaboration among supply chain participants affects business management.

Based on these results, the following recommendations raise for next periods:

1. Assess the security performance of the prototype cloud supply chain management system, currently in development phase, in order to verify that data protection capabilities satisfy the high security requirements validated by industrial staff,

2. Measure business improvements that can be achieved (at individual and at supply chain level) applying collaborative planning algorithms; this measurement can be realized by applying the pilot assessment framework.

By knowing at the same time business benefits and risks it will be possible for organizational management to make decisions about cloud collaborative supply chain management systems.

While the methodology applied to achieve the presented results is general, the results themselves are strongly limited to the specific industries taken in consideration, for this reason any application of cloud collaborative supply chain management require a similar specification study in order to tailor both the security and the business functionalities.

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

List of Figures

List of Tables

Chapter 1 Introduction

In the first half of WP24 – Supply Chain Prototype of PRACTICE project, innovative collaborative supply chain processes for aeronautical and consumer goods industries were analysed in order to highlight business improvement opportunities enabled by supply chain collaborative planning, as well as risks related to the introduction of collaborative ICT systems, in particular a cloud collaborative supply chain management system.

In the following sections the contents of the report are briefly introduced: firstly the methodology applied in the quantitative analysis of two industrial scenarios and the achieved results; secondarily the design of the architecture and the implementation strategy of the cloud supply chain management system is presented; lastly the presentation of a pilot assessment framework enabling the evaluation of the business benefits that can be achieved through the collaborative forecasting and planning models implemented in the secure cloud system.

1.1 The aeronautic industry case

The fleet management business process was taken in consideration in the aeronautical scenario. This is the process through which a provider of maintenance, repair and overhaul (MRO) services maintains the security and safety conditions of air vehicles. In order to leverage the relationship of the authors with a firm involved in the after sale service business segment, the focus of the analysis was on the engine maintenance.

The analysis showed that the MRO service provider can benefit from more accurate information on the status of the engine, available to the engine owners. Benefits are related to the capability to optimize service planning, to reduce delays and then penalties related to the unsatisfied service levels agreement, to improve inventory management policy, as well as reduce safety stock levels. In this case, engine owners (airlines and air forces) also obtain benefits, in term of longer usage time achieved through the reduction of service turn-around-time (TAT).

Higher benefits can be achieved if information about engine status from different customers can be processed homogeneously, so that operation in the whole supply chain system can be optimized.

The process was analysed also from a mathematical point of view: an optimization protocol and a number of algorithms able to implement that protocol were developed and provided to the developer of the supply chain management system. The prototype implementation is on going under 24.4 task and will be delivered on M30.

As the fleet management process can be optimized if certain data of different supply chain participants are computed concurrently, a database was designed in order to collect and store all those data. The case is that a lot of considered data is confidential, hence data owners are very reluctant to share them. The confidentiality is justified by the fact that other supply chain participants can leverage data and modify their business strategy accordingly. For example, a competitor can launch focused offers, a customer (or the service provider) can negotiate more favourable agreements, and so on. The result is the worsening of the business position (that is lower gains) of the actor whose data have leaked.

1.1.1 Introduction to latest results

The analysis of risks associated to the confidentiality of data was carried out in two steps: in the first one qualitative risks run by a data owner leaked by other supply chain participants were identified (this step was discussed in the deliverable D24.2 – Business modelling); in the second one, risks associated to the data leakage involving other supply chain participants were measured. An online survey was conducted over a group composed of people operating in IT and supply chain departments of aeronautic firms. It was developed by using the platform for secure survey, the prototype system developed for WP23. The list of questions, as well as the analysis model, were designed and shared with the WP23 staff in order to verify if they were compliant. Actually some minor updates were required in order to create the survey and share it in the sample community. By using this system two benefits were achieved: updating and promoting the prototype developed in order to be applied in real cases; providing higher data security properties to involve people so that their actual answers were not accessed during the analysis. The second step is the object of this report, in particular of the Chapter 3.

The survey was built by referring to a risk measurement model (see Chapter 2). The model tries to measure risks related to the leakage of different data involving different supply chain nodes (competitors, customer, supplier), and takes into consideration if these leaked data were already known by some of the supply chain actors (for example due to previous business relationship).

Results of the survey (discussed in section 3.3.3) are used to create a list of planning parameters, ranked with respect to their risk value. This ranked list will be used in defining and implementing the right security conditions in the cloud system and in managing the specific confidential data. Indeed, it is possible (at least in principle) to implement cloud architectures providing different levels of security to the different components, in order to provide the right global security level at the lowest implementation cost.

The business and risks analysis of the fleet management process led to the preparation of the assessment framework prototype. This is composed of two main parts: the first one (section 6.1) reports the security assumptions, deduced by the whole process analysis, that the designed prototype will implement; the second one measures business performance improvements brought by the cloud supply chain management system implementing the optimization algorithms (section 6.2).

In order to measure business performance improvements, it was necessary to study the relationship among different parameters, such as financial performance and inventory policy. Using this new knowledge, a concept of innovative simulation application able to support managers in visualizing business improvement opportunities was designed (section 6.3). The application is based on the model of the relationship between forecast capabilities (for example short vs long term forecasts), inventory policy, process features, and others. This model can be implemented, so that global business performance can be simulated by setting different specific conditions. The objective is to provide to supply chain managers a tool able to measure the impact of collaborative processes. It is expected that such a tool leads to extended and more accurate forecasts, improves individual business capabilities and financial benefits in terms of money saved or gained.

1.2 The consumer goods industry case

The second industry under scrutiny of WP24 is that of consumer goods, and in particular the supply chain of Arcelik (ARC).

In the first part of the project, the bottlenecks of ARC supply chain were identified and analysed. The roots of the bottlenecks are in part in the supply chain structure, and in part in the procedures applied by ARC. Some of supply chain structural characteristics are: a huge number of suppliers of components that serve also ARC's competitors, a global distribution of manufacturing and assembly plants, and a widespread availability of customers composed of big as well as small subsidiaries, resellers and stores. These actors have very competing business goals (for example, regional resellers and subsidiaries compete on selling the same ARC products to the same community of potential end users) so that collaboration in this supply chain is a very hard challenge. Moreover, each participant has high interest in an unfair behaviour in order to protect its own business performance. On the procedural side, data (orders, costs, delivery deadlines, and so on) moves between customer and supplier on low security communication systems, such as email or phone call. This introduces high risks since confidential data can be available to staff members, who are not educated to properly handle confidential data.

At the same time, due to the high volatility of the market and the rapid obsolescence of products, production and delivery planning is a strategic process: business performance is strongly dependent on the capability to assign production orders to the right manufacturing and assembling plants in order to satisfy orders received from customers at the lowest costs. The plant, selected on a quite global basis, has to respect delivery deadline, has to present the opportune production capacity, has to procure parts (and a significant part of costs is related to their shipment) and to deliver products to customers (also in this case shipment is a significant cost). Moreover, shipment introduces high risks in the timely delivery of products. For this reason, the selection of the plant, to which production is assigned, is a strategic task for the whole supply chain.

The analysis of ARC supply chain leads to the identification of a new business model for future applications: the Vendor Managed Inventory. It is based on the direct management of customers' inventories by the producer. It requires that updated information on inventory levels and on selling trends to customers are available to the producer. Lastly, the benefits are strongly related to the number of customers involved in this business model in order to leverage regional figures of the product distribution. This means that data belonging to a wide community of competing actors should be processed in a unique system, so the challenge is how such data is communicated and processed in order to reduce business risks.

Having that in mind, an analysis of the risks was carried out in order to identify where they manifest and to measure their relevance to the involved actors. Risks taken in consideration are those related to the data leakage as they are the most critical for the industrial users of such an innovative system.

Cloud systems are very effective in integrating many partners on the same system providing the same security performance to each of them. Concerning the data processing a model and an algorithm to merge demands of the same products coming from different regional customers were developed; they were followed by a model and an algorithm to assign production orders to different manufacturing and assembling plants.

1.2.1 Introduction to latest results

Peculiarities of consumer goods industry were taken in consideration to develop and customize the mentioned model, whose innovativeness is enabled by the security properties of the cloud technologies. Indeed, the supply planning algorithms are based on secure multi-party computation, so that input data, encrypted during upload, are processed without being decrypted; in such a way they are not available to other participants. Also outputs of computation are encrypted and only the addressees have decryption keys. The prototype system will be developed by leveraging the novel architecture and systems developed in WP21 and 22. These concepts were well discussed in deliverable (D24.1 and D24.2).

In this report, the issues related to the management and processing of confidential data were explored in a quantitative way in order to identify the most risky data and to tailor the final implementation of the prototype system implementing the collaborative supply chain management process. In this report, the measure of risks associated to the data leakage is reported. As in the aeronautical case, the risk measurement model presented in the Chapter 2 was applied, even if a version customized for ARC supply chain. In particular, a number of ARC customers and suppliers were interviewed in two phases, with the aim to highlight the risk value characterizing the parameters involved in the production planning algorithm. In Chapter 4 results of the interviews are reported.

Also in this case, the value of the risk analysis is linked to the capability to develop a cloud architecture able to implement security levels suited to the data that will be managed.

1.3 The prototype architecture

In Chapter 5, a prototype architecture and the deployment strategy will be presented. They are built on the computation components and algorithms defined for both industrial cases. In particular, the architecture presents some common components but differentiates in order to respect the peculiarities of the two cases.

In that chapter it is shown how architectural components developed in other WPs, in particular WP21 and WP2, are leveraged in order to comply with the two industrial peculiarities.

The implementation of the prototypes is ongoing and is related to T24.4 – Prototype implementation task (deadline of which is in M30 of PRACTICE project).

1.4 The pilot assessment

Last chapter of the report is dedicated to the presentation of a pilot assessment framework. It will be applied to evaluate the benefits of the cloud collaborative supply chain management system. The assessment framework focuses on two main areas: the security capabilities of the cloud system, and the business benefits. The security capabilities of the system regards both industrial pilot cases; on the contrary the business benefits section is focused on the aeronautic case.

Benefits of collaborative service forecasting and planning span four business management areas: customer, process, inventory, finance. For each area a set of metrics is proposed. The pilot assessment approach for the consumer goods pilot case will be object of future research activities.

The study for the assessment framework highlighted also the opportunity to define the relationship between forecasting capabilities and the economic performance of the inventory management. By modelling the relationship between forecasting and financial aspects it will be possible to design and develop a simulation tool able to show clearly the benefits of collaborative supply chain management. It seems very useful as, with this tool, industrial managers and practitioners are enabled to see the economic impacts of innovative collaborative processes involving other supply chain partners and business risks. Indeed, the economic impacts are the strongest motivations for business process redesign also at supply chain level and for justifying new business risks.

Chapter 2 Risk measurement model

In this subchapter we adapt and apply a framework for the criticality assessment in supply chain collaboration scenarios that was developed in the Secure Supply Chain Management Project in D2.1 titled "4PP Scenario Requirements".

Based on the notion that there are fundamental obstacles preventing collaborative cloud-based supply chain planning, we can specify two major issues that have to be taken into account when implementing a cloud-based management approach:

1. Data owners are generally hesitant to reveal required planning data to avoid any potential disadvantage. Potential disadvantages may occur if partners in the supply chain (mis-)use the shared data to their own advantage and to the disadvantage of the data owner. The reluctance to share certain data depends on the potential negative consequences a data owner may experience.
2. Data owners may have incentives to report false data in order to gain advantages in terms of costs and volume allocation in a centralized master planning scheme, i.e. there exists a risk that data owners behave opportunistically when providing input data to a central planner.

Although both aspects have to be considered for a cloud-based planning system, the focus of this section lies on potential disadvantages a data owner may incur when sharing his personal data. We assume that potential for reporting false data is strongly limited due to technical solutions. If the data is acquired directly from the parties' internal Enterprise Resource Planning (ERP) systems, manipulations would be risky for each party for two main reasons: first, any manipulation would typically also distorts the company's own planning; secondly, manipulation could rather easily be detected and can therefore be tackled by some form of compliance monitoring.

In the following sections we systematically analyse the criticality of each identified relevant parameter. In doing so, we specifically address the following questions:

1. What potential disadvantage may a data owner potentially incur when sharing private data? We have to consider that the negative impacts may vary depending on the position of the data source within the supply chain and the potential incentives partners in the supply chain may have to (mis-)use the data to their own advantage. We differentiate between partners who are responsible for nodes on the same stage of the material flow network (competitors) and those who are responsible for nodes on previous or subsequent stages (supplier-buyer-relationships).
2. What is the probability that a partner in the supply chain (mis-)uses the shared data to the disadvantage of the data owner? For each of the aforementioned cases it is necessary to assess the likelihood of a disadvantage on the side of the data owner.
3. To what extent is the data prior knowledge? It is reasonable to assume that the criticality of certain data elements is lower if it is already accessible for the partners in the supply chain.

Based on questions one and two we assess the criticality of each relevant data element. We then use the extent to which the data has already been known to individual partners in the SC as a weight for determining an overall protection level (question 3). We apply the following scheme to derive the protection levels of the individual input and output data (Figure 1).

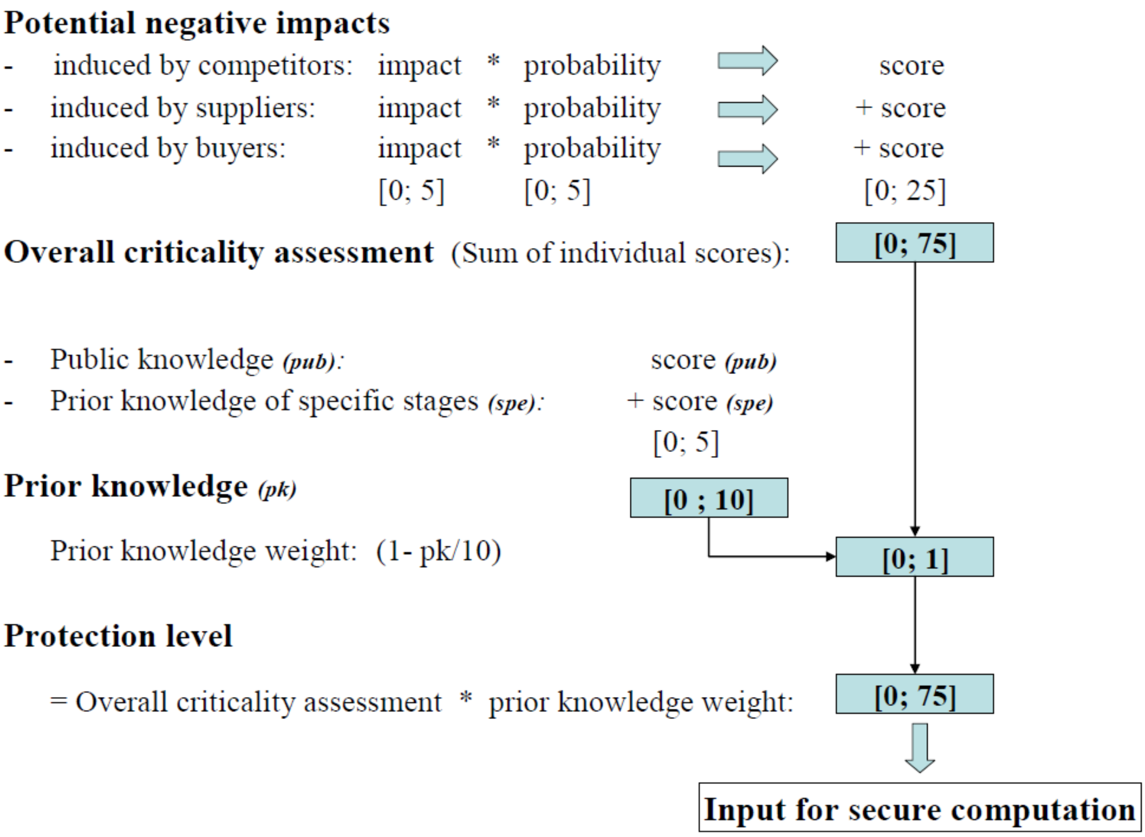

Potential negative impacts
- induced by competitors: impact * probability score
- induced by suppliers: impact * probability + score
- induced by buyers: impact * probability + score
[0; 5] [0; 5] [0; 25]
Overall criticality assessment (Sum of individual scores):
[0; 75]
- Public knowledge (pub): score (pub)
- Prior knowledge of specific stages (spe): + score (spe)
[0; 5]
Prior knowledge (pk)
[0 ; 10]
Prior knowledge weight: (1- pk/10)
[0; 1]
Protection level
= Overall criticality assessment * prior knowledge weight:
[0; 75]
Input for secure computation

Figure 1: Risk measurement model.

We use a scoring range between zero and five to assess the potential negative impact and the expected probability of data misuse. Through multiplication of both scores, we get a particular criticality measure for negative impacts induced by competitors, suppliers, or buyers. Their addition delivers the value of overall criticality. In this context we define “competitors” as supply chain partners that are responsible for nodes providing identical processes on the same stage of the SC, while “suppliers” and “buyers” represent nodes on previous and subsequent process stages respectively. Potential risks associated with opportunistic behaviour through these groups are captured through the extent of negative impacts and the probability that the negative impact will occur. The assessment of the probability depends on:

- whether partners in the SC are at all capable to use the information to their advantage;
- whether partners that misuse the data to their advantage have to be sanctioned;
- the relationship and trust between individual partners.

As mentioned before, the overall criticality for each data element is then weighted with a value that expresses the prior knowledge of data. A scoring range from zero to five is used to measure the degree of public knowledge in general as well as specific knowledge of individual SC partners. The sum of both scores measures the level of prior knowledge. A score of zero indicates that the data is pertinent to the data owner, while higher scores indicate that the data may anyways be known prior to centralized master planning. We determine an aggregate weight for the prior knowledge as $\left[1-\frac{score}{10}\right]$ in order to derive the protection level.

The criticality of the individual data elements depends strongly on the specific supply chain under consideration. We will now use the developed general framework to assess the criticality of relevant data in the ARC supply chain master planning scenario. Therefore we will use a questionnaire that can be utilized to assess the criticality levels in specific supply chain setting.

Chapter 3 Aero-engine fleet management pilot case preparation

3.1 Identification of the test case and data availability

In this period, the aeronautic firm, partner of DTA, that is following the project activities and results explored its MRO programs to select the case to offer for the pilot application of the prototype. Given that the confidentiality of data is involved in this research, it was decided to take into consideration a closed program. In this way no high business risks are directly taken from the firm, furthermore also the performance of the firm in that program is well known and can be compared with the performance enabled by the collaborative planning system.

The aeronautic firm has selected a program involving the engine family JT8, a Pratt & Whitney product. This program is already closed and data belongs to the aeronautic firm; only in this way their application into the pilot case doesn't need other industrial players to participate.

On the other hand, there are a couple of problems that will be definitively evaluated and faced as soon as data will be made available. The most relevant issue is that data related to that program doesn't match exactly with the data model developed; this case is due to the fact that the aeronautic organization didn't (and doesn't) store all that data. The second issue is related to the unavailability of any cost data since organizational privacy policy cost data must not be provided to any external actors. We assume that costs will be simulated and validated by the organizational staff.

At present PRACTICE partner and the aeronautic firm have prepared an NDA which was proposed to the legal department for final approval and ratification.

3.2 Planning parameters and confidentiality issues

The data model designed in D24.2 defined all data useful to forecast MRO service demand and, more generally, to better plan the entire fleet management process (see the database schema in the Figure 2). In particular, keeping track of all overhaul events performed on engines, as well as of their working statuses (in terms of flight cycles and hours since new or other sensor data), it is possible to forecast, with a certain accuracy, when engines will need to be overhauled again. Merging such data with those concerning available resources (number of resources available with specific competences for each overhaul activity) allows to provide an indication of:

- the date in which the engine has to be delivered in order to reduce delays;
- the service plan;
- the delivery date, that is the time necessary to complete overhaul operations (Turn Around Time).

The data model contains confidential data belonging to different supply chain participants (engine owner, MRO service provider or parts supplier) that should be provided in order to improve the overall supply chain performance, in terms of a more efficient use of resources, reduction of turn around time, and inventories optimization.

Table 1 summarizes information that each actor should provide to the Cloud Planning System, and the main services that will be received in return.

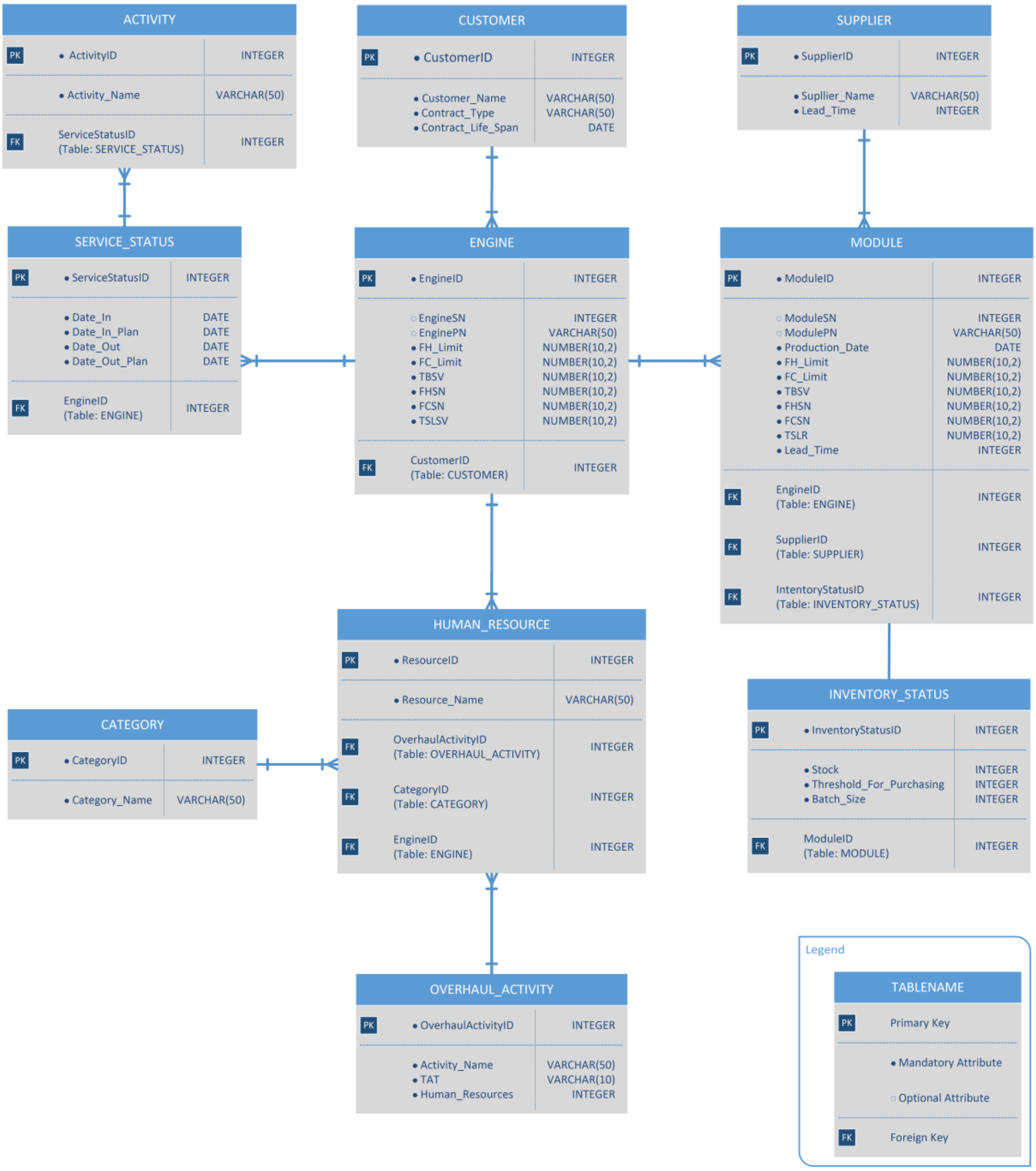


Figure 2: Relation data model

As a consequence of confidential data available in the same computing system, risks related to confidential data leakage at the hand of supply chain partners or IT service provider are a real issue. In particular, opportunistic risks can occur when an insider (i.e. a supply chain participant or the IT service provider) is allowed to access input data provided by other participants in order to deduce more information than those that can be inferred from computation results addressed to him.

	INFORMATION TO BE SHARED	SERVICES IN RETURN
Airline/ Air Force	• Engine working parameters	• Fleet status monitoring
MRO Service Provider	• Short term service plans, inventory status, and penalties conditions	• Forecast on engines maintenance needs • Management of resources, inventory status and penalties
Spare Parts' Supplier	• Current production plans, inventory status, and penalties conditions	• Forecast on spare parts demand • Management of resources, inventory status and penalties

Table 1: Information to be share and services received in return.

In the Table 2, for each actor of the aero fleet management supply chain, identified risks are summed up in relation to the attacker (the actor who can access private data) and to the victim (the actor whose data is leaked). Risks reported in cell are those experienced by the actor type in the row header if the confidential data are leaked by actors type reported in the column headers.

VS	Airline/Air force	MRO service provider	Supplier	External actor
Airline	✓ *Loss of information advantage*	✓ Weakening *of the bargaining power after disclosure of purchase volume*	✓ *Weakening of the bargaining power after disclosure of purchase volume* ✓ *Loss of information advantage*	✓ *Loss of information advantage*
MRO service provider	✓ *Weakening of the bargaining power after disclosure of supply volume*	✓ *Loss of information advantage* ✓ *Development of a competitive product/service*	✓ *Weakening of the bargaining power after disclosure of purchase volume* ✓ *Loss of information advantage*	✓ *Loss of information advantage*
Supplier	✓ *Loss of information advantage*	✓ *Weakening of the bargaining power after disclosure of supply volume*	✓ *Development of a competitive product/service*	✓ *Loss of information advantage*

Table 2: Risks for the actors of the aero engine overhaul supply chain. In cells risks experienced by actors in row header if data are leaked by actors in column header.

The risk analysis carried out in the collaborative planning process highlighted that individual business capabilities are threatened. Different competitors participate in the same supply chain (different engine owners and different spare part suppliers), so the victim risks losing the competitive advantage if its data is visible to competitors; for example if the working status of the fleet of an airline is known by another airline. Otherwise, if confidential data of partners involved in a business agreement (an example is the partnership between the service provider and its customer) are leaked, the bargaining power of the victim is seriously threatened. An extended discussion on the risks related to data leakage in the supply chain is available in deliverable D24.2 "Business modelling".

After having identified risks, it is necessary to see the real perception of industrial people on those risks. In particular, industrial people can state how significant are risks for their current business practice. In the next section a survey aimed at measuring the risks value, built on the methodology discussed in the previous chapter, is presented. Results follow.

3.3 Survey

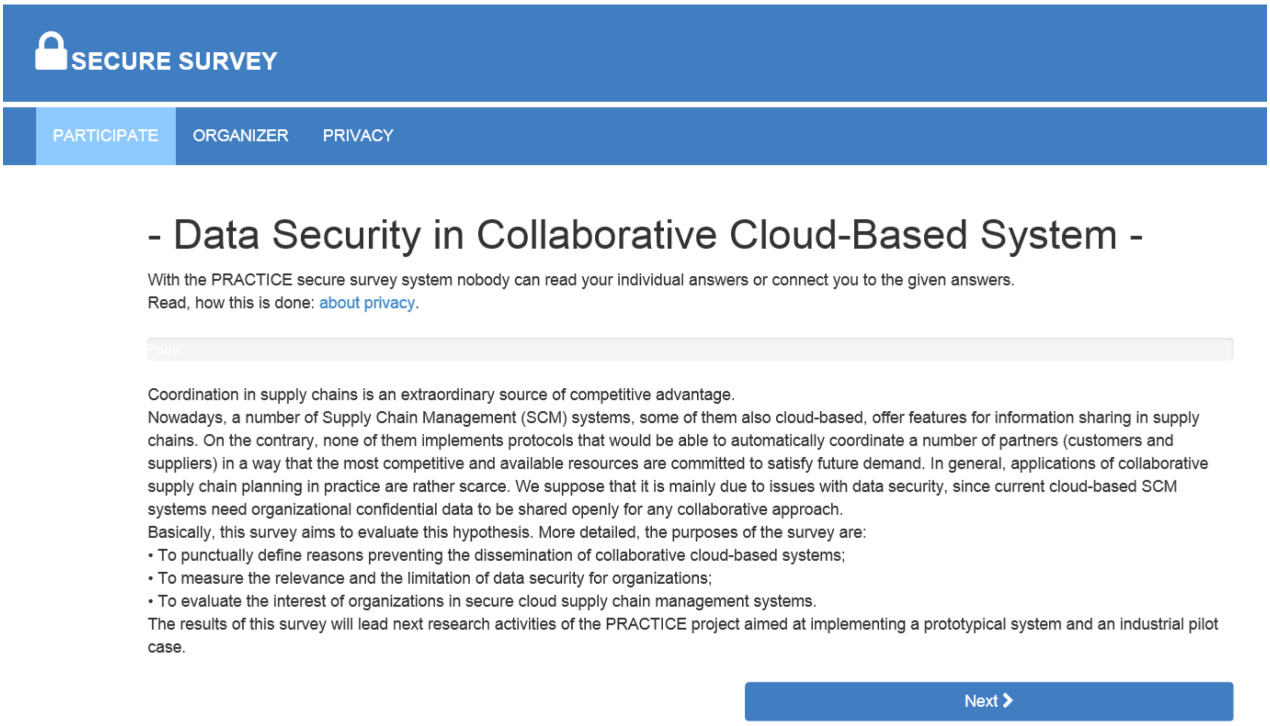
As the aeronautical industry is quite dispersive on a global basis, a web based survey was arranged in order to interview people belonging to different firms (Figure 3). The survey, titled 'Data Security in Collaborative Cloud-based Systems', had two main objectives: the first one is to measure risks summarized in section 3.2; the second one is to make respondents aware of the impact of security issue on their business management approach and on business processes.

Some questions of the survey involve private arguments, in example those about the use of cloud collaborative systems that ask for the motivations leading to or preventing such usage. In order to reduce privacy concerns of respondents, it was considered opportune to leverage available project results to alleviate this kind of potential obstacles to the survey participation. The Platform for Secure Survey, result of the WP23, appeared very effective in satisfying this privacy preserving requirement. The survey and the analysis were shared with the WP31 team in order to verify if were compliant with the prototype functionalities and which actions were necessary to implement the survey with system. The WP31 team took in consideration this opportunity for two main motivations: 1) it was a real case (new real requirements emerged) so that the functionalities of the prototype were extended and its alignment with the market standards improved, 2) it was an opportunity for the results dissemination opportunity as the secure survey platform, and its security approach, were promoted in a selected industrial community. In particular it was shown to that community that higher benefits in terms of data security can be provided presenting the end user the same data management tools. Indeed compiling a questionnaire implemented using a privacy preserving technology (Shareming platform[1]) is not different from compiling a standard questionnaire.

The prototype platform for secure survey was enriched with some functionalities to implement specific question's types and during the survey administration some trouble were recognized and solved.

The survey, targeted to the aeronautic industry, is mainly focused on the measurement of risks involved in a cloud supply chain management system. In the following section 3.3.1 the survey aims, structure and characteristics were introduced, while in the section 3.3.2 the Sharemind architecture of the secure survey platform as well as the implementation and the improvements developed for this survey are described. The complete questionnaire is discussed in this section and is available in the appendix A.

[1] https://sharemind.cyber.ee/



- Data Security in Collaborative Cloud-Based System -

With the PRACTICE secure survey system nobody can read your individual answers or connect you to the given answers.
Read, how this is done: about privacy.

Coordination in supply chains is an extraordinary source of competitive advantage.
Nowadays, a number of Supply Chain Management (SCM) systems, some of them also cloud-based, offer features for information sharing in supply chains. On the contrary, none of them implements protocols that would be able to automatically coordinate a number of partners (customers and suppliers) in a way that the most competitive and available resources are committed to satisfy future demand. In general, applications of collaborative supply chain planning in practice are rather scarce. We suppose that it is mainly due to issues with data security, since current cloud-based SCM systems need organizational confidential data to be shared openly for any collaborative approach.
Basically, this survey aims to evaluate this hypothesis. More detailed, the purposes of the survey are:
• To punctually define reasons preventing the dissemination of collaborative cloud-based systems;
• To measure the relevance and the limitation of data security for organizations;
• To evaluate the interest of organizations in secure cloud supply chain management systems.
The results of this survey will lead next research activities of the PRACTICE project aimed at implementing a prototypical system and an industrial pilot case.

Figure 3: Data Security in Collaborative Cloud-Based System[2]*.*

3.3.1 Description of the survey

In accordance with the research approach and goals, the survey faces the following main points:

- Enumerate reasons preventing the dissemination of collaborative cloud-based systems;
- Measure the relevance and the limitation brought by data security to organizations;
- Evaluate the interest of organizations in secure cloud supply chain management systems;
- Assess risks involved in a cloud collaborative supply chain management systems.

As it was said above, the survey described here has four sections.

In particular, the first preliminary section focuses on general information, such as the company name for which the respondent works, the specific industry of the company, as well as the respondent's functional area.

The second section analyses the adoption of cloud computing systems to collaborate with supply chain partner, in order to collect the main limiting factors. Respondents are required to specify if the company uses cloud computing technologies to share data and information with suppliers and/or customers, and the main issues related to the missed or limited use of cloud computing systems. These issues are gathered into three different categories:

1. Need of cloud specific requirements for data security;
2. Lack of trust in the security provided by the cloud service provider;
3. Lack of trust in the way customers and suppliers could use the system or data.

[2] https://smpsurvey.cyber.ee/application/assets/index.html#/participant/participate/84ff366a-3578-44f2-9a88-8e697de6a60d

Moreover, it is asked if the choice of a cloud service provider is bound to the presence of certifications related to data protection. In such a way, it is possible to better understand the importance of data security in collaborative contexts for each industry.

The third section explores the theme of protection of organizational data and information.

In particular, the commitment of the company in this direction is measured through the following three levels:

1. The management and the board of directors are strongly committed to data security and protection;
2. The management and the board of directors consider data security and protection as a minor issue;
3. Only the IT department is committed to data security and protection.

Furthermore, it is required to specify if the company applies any tools to prevent disclosure of digital data by insiders, or by customer and supplier once this data is shared with them. At last, it is useful to know if the company is certified for the management of information security.

To conclude, the fourth section represents an application of the risk measurement methodology described in Chapter 2. The focus is on risks related to the loss of confidential data and information in cloud collaborative supply chain management systems.

In particular, the industrial scenario analysed is the fleet management supply chain, in which the engine owners, the MRO service provider, and spare parts suppliers are the main actors. The confidential data taken into consideration are:

- Usage condition of the air fleet engines (such as flight hours, flight cycles, previous overhaul services, and so on) for the engine owners;
- Data describing the overhaul process (such as execution time of tasks, Turn Around Time, available resources, service plan, inventory status, and so on) for the MRO service provider;
- Data related to the production plan and the inventory status for the spare parts supplier.

Whereas the risk is measured as the product of the potential negative impact and the expected probability of data misuse, in the survey the risk is evaluated considering all combinations between the three categories of actors (airline vs another airline; airline vs MRO service provider; airline vs spare parts supplier; MRO service provider vs airline; MRO service provider vs another MRO service provider; and so on).

3.3.2 Survey implementation

The Survey has been conducted with an improved version of the Secure Survey system delivered in D23.1. Here we briefly present the survey system as well as a list of improvements made since D23.1.

The Secure Survey system uses secure multi-party computation (MPC) to keep answers to questionnaires confidential. The individual and confidential answers are encrypted (secret shared) on submission and split between different servers on independent cloud computing service providers and stay encrypted at all time.

The Secure Survey application is based on the general SPEAR & DAGGER approach laid out in work package WP21. The flexibility of the SPEAR & DAGGER approach consists of layers that e.g. allow the same web service to be run on independent MPC systems. The secure survey system is designed to run on Sharemind and Fresco/SPDZ.

The two secure multi-party computation engines differ in terms of number of servers used and security level. Sharemind runs on three servers and provides passive security and Fresco/SPDZ runs on two servers and provides active security. Passive security in survey system guarantees that semi-honest adversaries cannot decrypt any private data. With active security the survey system ensures that a malicious adversary cannot affect input data or submit answers nor alter the outcome of the survey result in any way.

This survey uses the Sharemind version and each of the three servers is controlled independently by one of the three partners in WP23: Cybernetica, the Alexandra Institute and Partisia as illustrated in Figure 4. Sharemind is using additive secret sharing scheme with three parties connected over secure asynchronous network channels to preserve the confidentiality of data, but also supports two party secret sharing schemes. The secret sharing of secret values is performed at the source (web browser) and each share is sent to a different server instance over a secure channel. This guarantees that no one but the data owner will know the original value. Next, Sharemind server instances engage secure MPC protocols to compute the results. When results are computed, the aggregated data will be available for the survey organizer who can see computation results after his web browser reconstructs the values from secret shares coming from different servers.

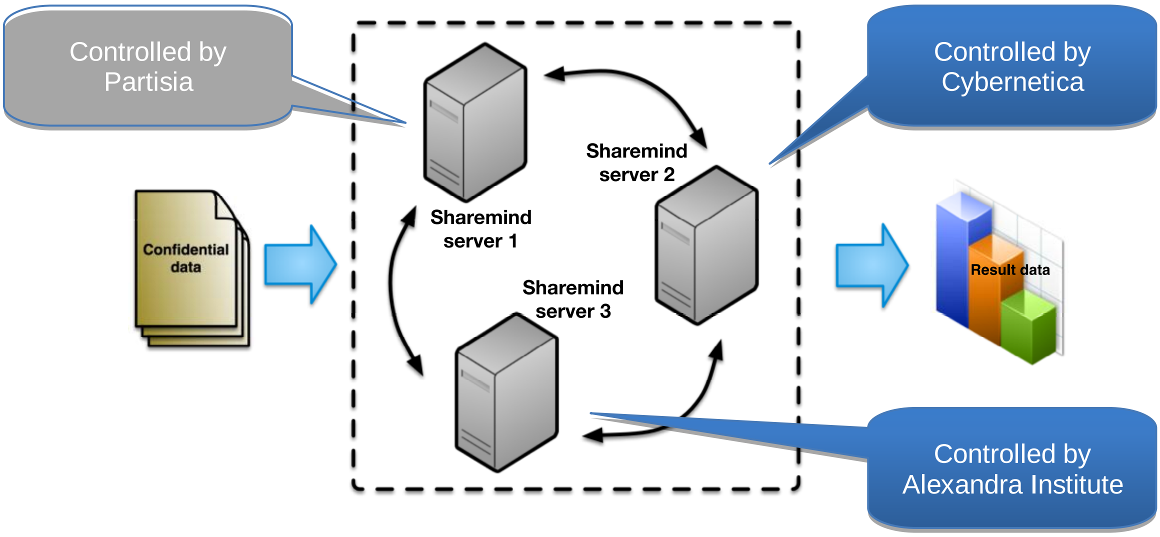


Figure 4: The deployment setup and trust model

The D23.1 was designed to conduct simple surveys and the analysis results part was in the form of tables and frequency diagrams. Below we report on a number of improvements to the Secure Survey system relative to the delivered version in D23.1. The improvements include new types of questions and analysis that allows for more advanced surveys as well as improvements of the basic system that makes the system suitable for real life deployment and usage.

Optional questions:

In the D23.1 version all questions were mandatory for the participants. This has been changed such that the organizer can choose whether answering a question should be optional or mandatory. By allowing the participants to simply skip questions, the survey system has become more widely applicable.

Multiple selections:

In the D23.1 version of Secure Survey system there were only single choice questions. Meaning that participant could only choose one option from the given list of choices. This has been changed so that the organizer of the survey can now choose the question to be multiple-choice question so the participant can choose more than options from the given list of choices. For example, a question like "What do you like?" with the choices: [x] ice-cream [x] candy [ ] chicken, should allow multiple selections.

Matrix selections:

In the D23.1 version each question was presented and analysed separately. This has been changed such that the organizer can choose to group multiple sub-questions that deal with the same topic. For example, with a question like: "At you place of work, where do you get the most information?" multiple sub-questions, with possibility to rate each option, could be:

- From internal web [ ] 1 [ ] 2 [x] 3 [ ] 4 [ ] 5 [ ] don't know
- From mailing lists [ ] 1 [ ] 2 [] 3 [ ] 4 [x] 5 [ ] don't know
- From your project manager [ ] 1 [ ] 2 [ ] 3 [ ] 4 [x] 5 [ ] don't know

Conditional analysis:

The D23.1 version included all questions and all answers in the analysis and analysed each question independently. This was changed such that the organizer can specify a filter that selects a subset of the respondents' answers, based on some other questions answer, to be analysed. For example if the survey questions are:

- sex: male/female
- age: below 20/20-30/30-40/40-50/50-60/above 60
- do you like ice-cream?: yes/no/don't know

The filter may then select males between 20 and 30 years old and produce statistics for this segment's preferences for ice-cream. The analysis is only allowed if the number of respondents in the chosen segment is 5 or more. The system allows the organizer to use one of more of such filters.

Proper database:

The D23.1 version did not have a database for saving the data; instead all of the data was saved to servers' memory. This has been replaced by a MySQL database for survey data and answers to questionnaries.

Automatic testing:

The D23.1 version did not have any automatic testing included. Now a number automatic tests has been added to ensure that continued development and bug fixing can be done with a lower risk of affecting the functionality of the system as a whole.

Validating survey answers:

The D23.1 version validated separately whether each answers has been answered within the valid range. This has been changed such that all questions from a respondent are validated altogether when answers are submitted. This has significantly improved the speed of saving answers and the participants' user experience.

3.3.3 Survey results: data security requirements

A general overview of the survey results is provided here.

3.3.3.1 **Population**

As the main objective of the survey was measuring the risks associated to the variables involved in the collaborative planning, it was decided to involve a limited group of people by selecting among those well informed about the process and the data managed. The group was composed of 10 people operating in aeronautical companies, and in particular belonging to IT, supply chain and management units.

The reason for that is their sensitivity to the research topics. Very precise answers were expected from their side as well as a multi-perspective view on the same organizational and supply chain issues. Analysing survey results, the majority of actual respondents (90%) works in AvioAero, which is one of the main industrial partner of DTA/CCII and moreover is involved in the aeronautic MRO business segment.

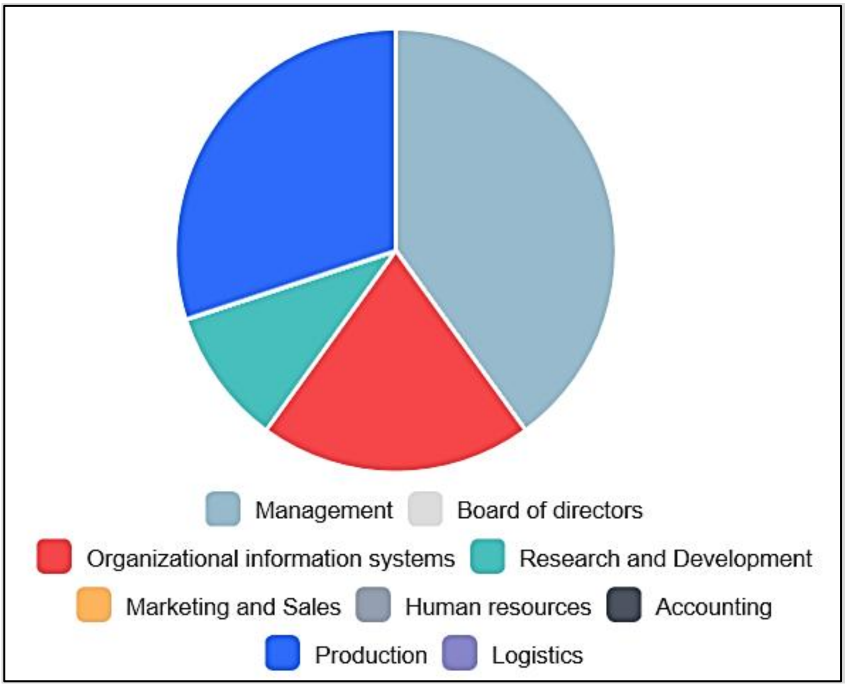


Figure 5. Functional area. The sample is composed by 10 persons.

Figure 5 shows the functional areas of the respondents: management, production, organizational information systems, and research and development, in descending order. These functional areas are characterized by completely different processes and dynamics, but all of them represent a good point of view for the purpose of our research. Furthermore, the possibility to have different perspectives of the same research topic is certainly a point in favour of the reliability of survey results.

3.3.3.2 Cloud technologies for data sharing

This section analyses the adoption of cloud computing systems in the supply chain, focusing on the main limiting factors.

Concerning the current use of cloud computing technologies, able to share data and information with suppliers and customers, the answers are discordant: just over half of respondents think their company doesn't use cloud computing technologies, while the remaining part thinks the opposite (see Figure 6). This shows a different awareness of the respondents as regards to the technological infrastructures used by the company and could be explained by the fact that the sample involve people from quite different parts of the organizational value chain.

On the contrary, everyone agrees that the use and the diffusion of cloud computing technologies in their organization is strongly limited by data security requirements (Figure 7). This confirms that data security is a critical theme for the aeronautic industry and the relevance of the security requirements developed through this as well as previous deliverables for the implementation of a cloud-based supply chain management system.

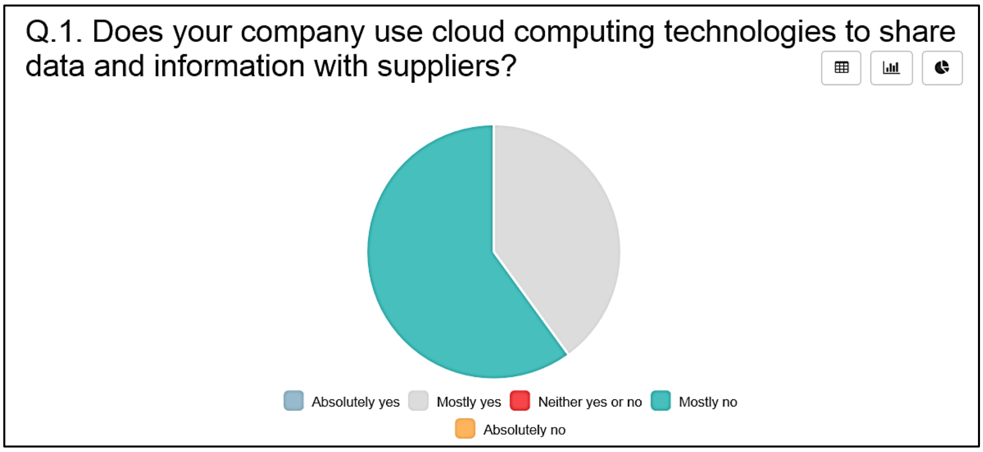

Q.1. Does your company use cloud computing technologies to share data and information with suppliers?

Figure 6. Use of cloud computing technologies with suppliers

(The same results occurs for the use of cloud computing technologies with customers)

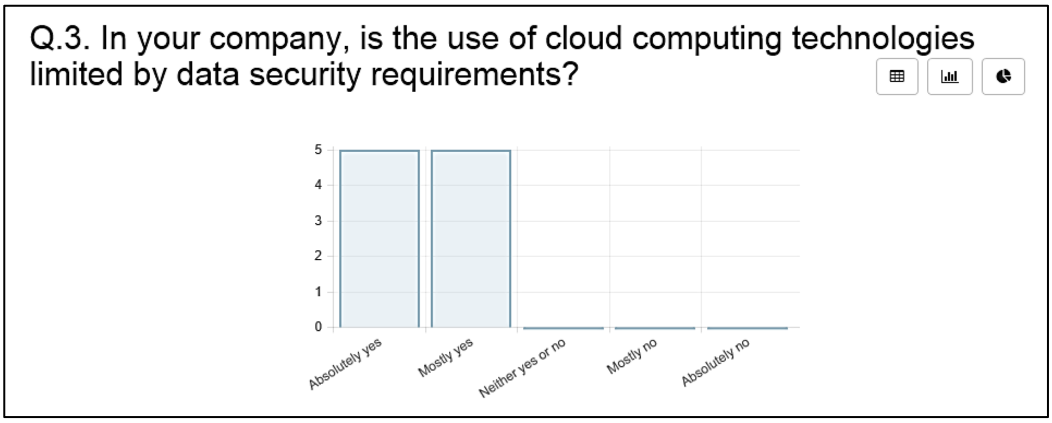
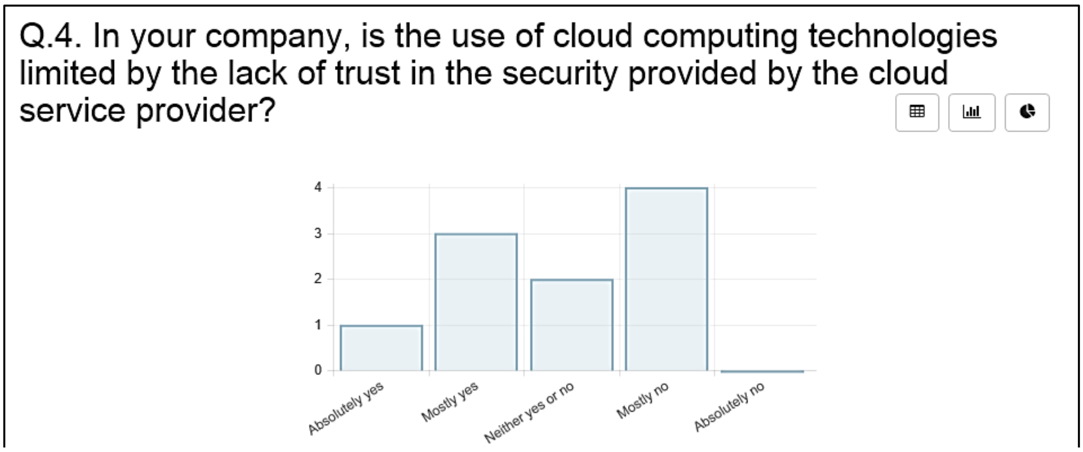

Q.3. In your company, is the use of cloud computing technologies limited by data security requirements?

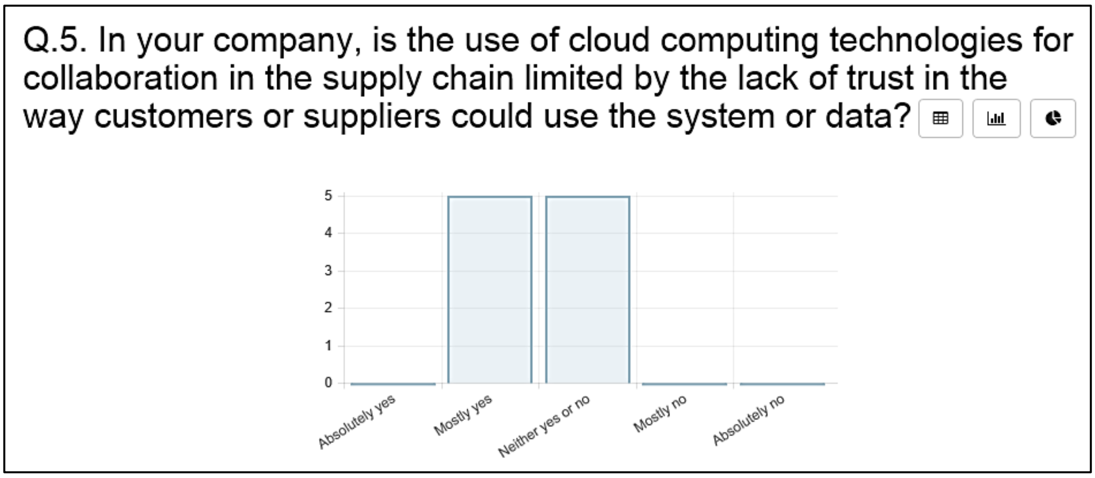
Figure 7. Data security requirements

In Figure 8 and Figure 9, the sources of risks are more deeply questioned: lack of trust in the security provided by the cloud service provider, and lack of trust in customers and suppliers behaviour. Here, the opinion is not so oriented as in the previous question: the trust on the cloud service provider is not always recognized as a real security issue as, instead, it should be, authors justify these responses by the fact that in the sample there are people not directly involved in the IT issues; trust on other supply chain participant is recognized as a cloud usage limiting factor even if not at the maximum level. The first block of responses can be justified by the fact that survey respondents are not directly involved in IT area; while the second block of responses can be explained by the fact that business relationships between customer and supplier in the aeronautic industry binds strongly players so that risks associated to unfair behaviours are higher than the potential economic benefits.



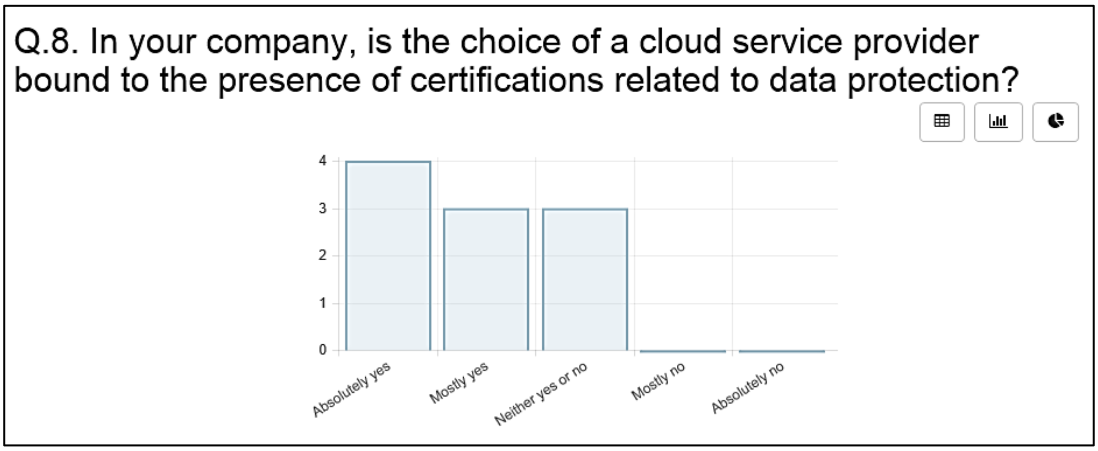
Q.4. In your company, is the use of cloud computing technologies limited by the lack of trust in the security provided by the cloud service provider?

Figure 8. Lack of trust in the security provided by the cloud service provider



Q.5. In your company, is the use of cloud computing technologies for collaboration in the supply chain limited by the lack of trust in the way customers or suppliers could use the system or data?

Figure 9. Lack of trust in customers and suppliers behaviour



Q.8. In your company, is the choice of a cloud service provider bound to the presence of certifications related to data protection?

Figure 10. Certifications on data security and protection

The question about factors limiting the use of cloud systems gives also the opportunity to respondents to add other factors beyond the two mentioned. Most respondents used this opportunity to claim the presence of the some international norms, ITAR and EAR, which limit the export of product and information. These regulations actually limit the use of cloud computing technologies in the industry as they require to certificate the location of residence of aeronautic data. This result reinforces even more our research, since in the aeronautical industry, and in particular in its military and ‘dual use’ business sectors, the adoption of a highly secure system of data computation could represent a very innovative change towards new collaborative scenarios. Moreover, also results developed in other work packages, in particular those related to the exploration of the private and confidential encrypted data in cloud environment, can impact on this issue specific to the aeronautic industry.

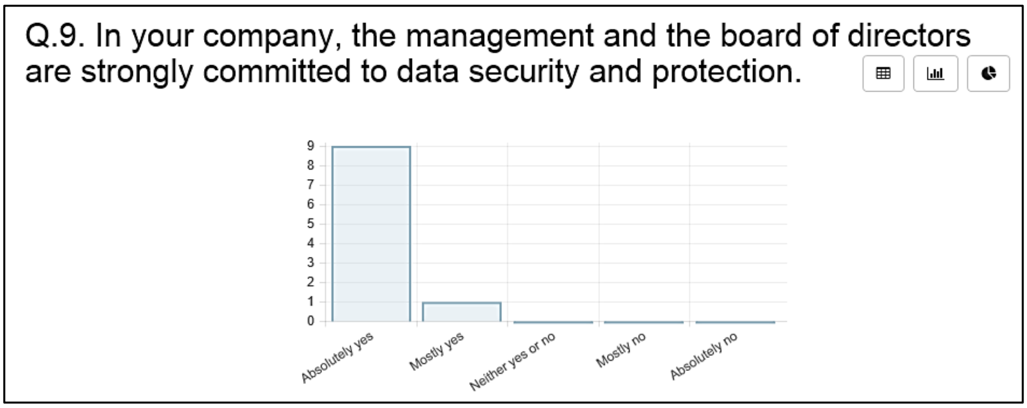
Finally, the majority of respondents state that the choice of a cloud service provider is bound to the presence of certifications on data security and protection (Figure 10). Once again, as in Q3 in the Figure 7, the theme of data security stands out, here in the form of required certifications.

To summarize, in the aeronautical industry, the use of cloud computing technologies for the collaboration with supply chain partners is today mainly obstructed by the low guarantees on data protection and security and by the difficulties to evaluate the privacy aspects of encrypted data.

3.3.3.3 **Data security**

In continuity with the previous section, the theme and the results about protection of organizational data and information is discussed next.

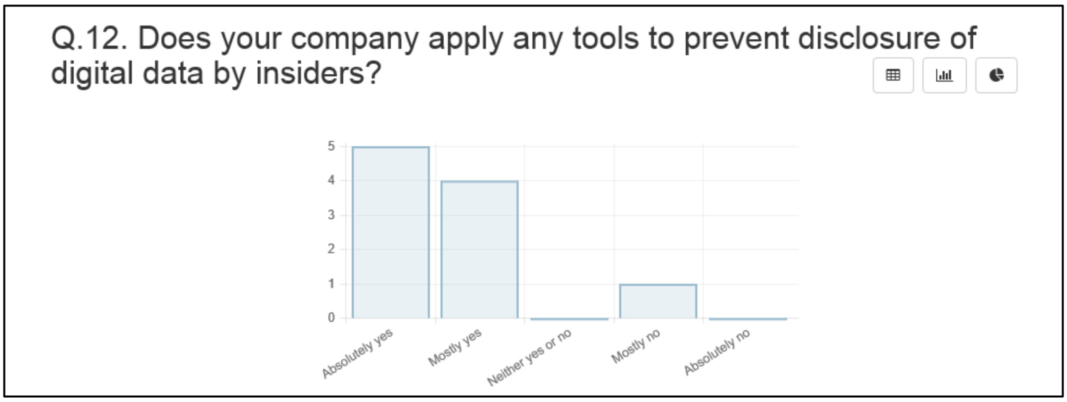
In particular, Figure 11 shows that, in the aeronautic industry, the management and the board of directors are strongly committed to data security and protection. The awareness of managers about the need to protect organizational data is increasingly widespread, and this issue is explored in many organizational innovation initiatives.



Q.9. In your company, the management and the board of directors are strongly committed to data security and protection.

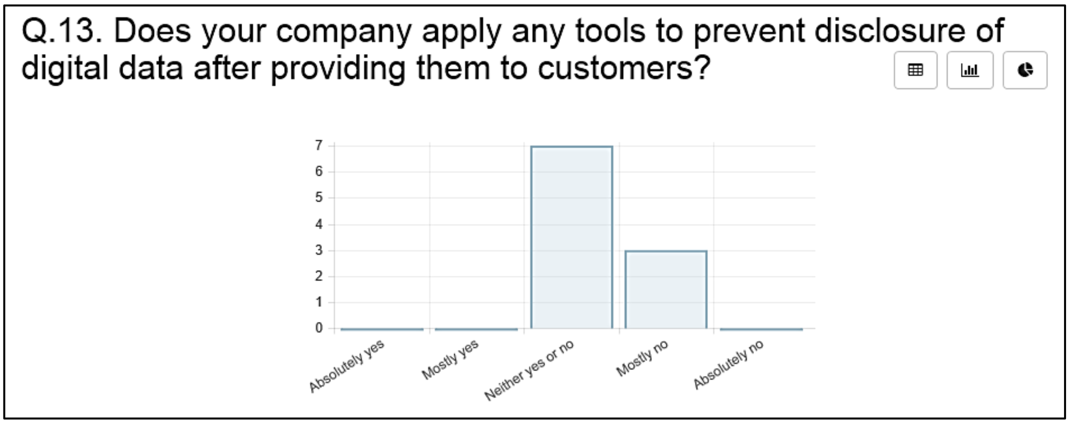
Figure 11. Management and board of directors

However, if almost all respondents declare that their company uses tools to prevent disclosure of digital data by insiders (see Figure 12), it seems that organizations don't face (currently) the disclosure of digital data provided to customers and suppliers (Figure 13). This suggests that PRACTICE deliverable is facing an issue currently not definitively solved by the aeronautic organizations involved in the survey. Currently custody of confidential data is given to customer or suppliers on the base of NDAs, assessment of technological systems and on trust. The PRACTICE approach, using architecture and tools, will extend the means to provide security in collaborative data management and processing.



Q.12. Does your company apply any tools to prevent disclosure of digital data by insiders?

Figure 12. Disclosure of digital data by insiders



Q.13. Does your company apply any tools to prevent disclosure of digital data after providing them to customers?

Figure 13. Disclosure of digital data by customers

(Very similar results occurs for the case of disclosure of digital data by suppliers)

3.3.3.4 Risk assessment

In this last section, risks related to the loss of confidential data and information, resulting from the use of collaborative supply chain management systems, are measured. In particular, the risk measurement model (defined in Chapter 2) is here applied, with the aim to derive the protection levels of individual input and output data.

We remember that the focus is on the aero fleet management supply chain, and confidential data taken into consideration are:

- Usage condition of the engines fleet;
- MRO process data;
- Production plans and the inventory status of spare parts suppliers.

The elementary variables involved in the planning algorithms are here aggregated in three groups for the following reasons: first of all because the number of variables are quite numerous so the survey would have become too large, the variables can change in the future as new sensor data will be available to the planning algorithms, the variables represent different aspects of the same business block. Authors are confident that grouping the variables did not change the results of the survey.

The survey asks respondent to estimate the 'potential negative impact' of a data leakage event involving a specific data group, a data owner and a data receiver.

The potential negative impact is computed as the product of the damage (impact) incurred by the data owner and the maximum probability for that event he can accept in change of the business improvements bought by the collaborative cloud system. The fleet management supply chain is composed by three roles: the customer (airline or air force), the MRO service provider, and spare parts suppliers. Following results of qualitative risks analysis provided in deliverable (D24.1 and D24.2), the potential negative impact induced by the leakage of a specific data group is calculated for each pair of roles. While the 'overall criticality assessment' of a specific data group is the sum of potential negative impacts computed for each couple of supply chain participants.

The survey requires to provide values on a Likert scale (from 0 to 5) for the two variables: 'impact' and 'probability', so we gathered 10 values (one for each respondent) for each variable. In order to compute the 'overall criticality assessment', authors considered for each variable the highest value, as they will lead to the highest data protection level. This decision is based on the fact that an IT system has to satisfy the specific requirements of all stakeholders involved in the process which the system is targeted to.

Confidential data	Actors combination	Impact variables	max value
Usage condition of the engines fleet	airline VS airline	impact	5
		probability	5
	airline VS MRO service provide	impact	4
		probability	4
	airline VS suppliers	impact	4
		probability	4
MRO process data	MRO Service Provider vs Airline	impact	4
		probability	5
	MRO Service Provider vs	impact	5

Confidential data	Actors combination	Impact variables	max value
	MRO Service Provider	probability	5
	MRO Service Provider vs Spare Parts Suppliers	impact	4
		probability	3
Production plans and the inventory status of spare parts suppliers	Spare Parts Suppliers vs Airline	impact	5
		probability	2
	Spare Parts Suppliers vs MRO Service Provider	impact	4
		probability	5
	Spare Parts Suppliers vs Spare Parts Suppliers	impact	5
		probability	5

Table 3. Overall criticality assessment

The risk measurement model, discussed in the Chapter 2, introduces also the concept of ‘prior knowledge’ of data. This parameter takes in consideration different cases that can happens: some data can be periodically published on specific reviews, or some data can be inferred by partners on the base of historical relationship.

Actually, specialized magazines periodically publish general information about fleet status, while there are web services able to provide information about which aircraft flied a specific flight. For this reason, we assume that an estimate of the data ‘Usage condition of the air fleet engines’ can be roughly and with very high effort inferred from public knowledge. Thus, the ‘prior knowledge’ factor for that data is esteemed to be 0,9.

On the contrary, the value of ‘prior knowledge’ parameter for the other two data groups is considered to be 0. The data regarding the MRO service provider can be only known once and as a global value (the complete TAT service), while individual data (the number of workstations, the workforce, the TAT for each service step, inventory levels, activity costs) is totally not known to anyone. The data representing the spare parts suppliers are always dependent on the base of the actual parts demand and of the business relationship between it and its customers, so prior knowledge has very little value in forecasting its capabilities.

The ultimate result of the survey, the protection level of each data group, is reported in the Table 4. Take in consideration that the value for the ‘usage condition’ variable was multiplied with the ‘prior knowledge’ parameter. The obtained values support and validate the risk model already developed for the fleet management process.

CONFIDENTIAL DATA	**PROTECTION LEVEL (scale: 0-75)**
Usage condition of the engines fleet	51,3
MRO process data	57
Production plans and the inventory status of spare parts suppliers	55

Table 4. Protection level

3.4 Process innovation requirements

While different aspects of the business process and the security requirements are well discussed in this report as well as in previous one of the WP24 – “Supply chain prototype”, in this section the technological issues are briefly presented.

The cloud planning system can deliver business benefits to supply chain partners if correct values are provided by participants. Authors are confident the security performance of the prototype implementation will push engagement of supply chain participants. However, it is necessary to recognize that a lot of data is required from each user: data describing engine condition, data describing overhauling process, data describing inventory management related processes. The effort required to provide frequently updated data could discourage users to use the system, thus reducing the overall effectiveness of the supply chain planning. This is a much more relevant aspect for customers (airlines and air force) as the quantity of data is quickly going to increase with the diffusion of the usage of engine sensors in the service planning.

To reduce this effect, it is strongly recommended that the cloud system provider enriches the system with software interfaces able to automate the flow of data from organizational databases to the cloud planning database. It will reduce the effort required by each user the supply chain to achieve business benefits. Moreover, automating the data flow between organizational and cloud systems will reduce the risk of unfair behaviour from participants. Indeed, if organizational data is automatically extracted from organizational system (i.e. Enterprise Resource Planning system, Product Lifecycle Management system, Inventory Management system, Fleet Management system), it will be quite hard to provide false data because this behaviour will require a strong commitment and high effort and because there will be much more opportunities for the cloud planning system to recognize such an event.

Moreover, integrating organizational data management systems and the cloud planning system permits to increase the frequency of the plan computation, for example once a week, thus improving the alignment between forecasts, plans and on going activities. This opportunity will also impact the quality of results provided and the benefits achieved by supply chain participants.

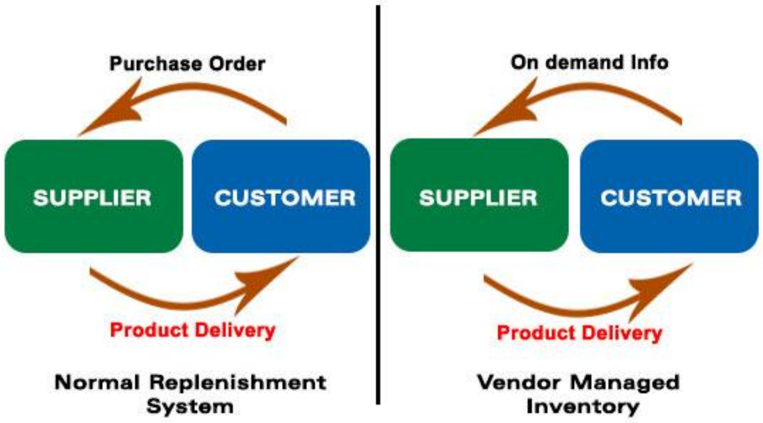
To conclude, it is not required that the supply chain system prototype is integrated with organizational systems, but authors recommend that such technological improvement should be considered in the future industrialization phase.

Chapter 4 Consumer goods supply chain: moving into the Cloud

4.1 Vendor managed inventory: parameters and risks measurement

Arçelik (ARC) as a vendor and the retailers of ARC consider only their own profitability instead of total supply chain profitability. Industry structure drives retailers to overestimate pre-orders by adding buffer quantities in their real order quantities. Thus, ARC wants to set up a cloud based system between the facility and customer levels of its supply chain for more efficient planning. In the current system, ARC's subsidiaries collect forecast data from local players and end customers. However, in order to achieve more realistic and efficient planning level, ARC should access sellers' periodical inventory levels to calculate regional and local demand forecasts.

In vendor managed inventory model (VMI) retailer and vendor levels of the supply chain are closely connected and collaborate within each other. In this approach, vendor decides to replenish the customers' inventory according to actual sales and contractual agreement between vendor and retailer. Vendor has to pay if it exceeds upper and/or lower bounds for inventory level.



ARC proposes to use cloud based VMI system to improve its supply chain efficiency. As a result of well integrated cloud based VMI, ARC aims to achieve:

- Automated system instead of current manual system (Excel files, e-mails etc.). Thus, human errors are immediately reduced, even removed, with the help of systematical applications.
- More protected data from irrelevant users.
- More accessibility. Users can access cloud based system whenever they have an Internet connection.
- More dynamic and realistic planning.

VMI model requires different parameters as an input from the users. Some of them are provided by vendor, some of them are provided from by retailers. Moreover, model presents some outputs which can be classified as outcome parameters. It is important for ARC to point out which of these parameters have to be protected and which not, to preclude users to obtain unfair advantages. In order to analyse the models and algorithms (VMI & Collaborative forecasting for mid-term production planning) for collaborative (secure) supply chain, we've created a survey assessment for the data owners whether there appeared any risks during the usage of the model. Therefore, eleven of these parameters' risk levels are investigated via conducted surveys.

4.1.1 Measurement methodology

Three vendor driven inputs, five retailer driven inputs and three outputs are selected for survey. They are:

- m: number of retailers (ARC's customers) that take part in the "VMI-system"
- A_V: production cost for one lot for vendor
- h_v: inventory holding cost for vendor
- h_j: inventory holding cost for retailer
- D_j: demand rate for retailer
- U_j: upper limit of inventory for retailer
- A_j: order cost for retailer
- π_j : overstock penalty cost of retailer
- q_j: quantity of a certain product dispatched to retailer
- n: number of shipments
- S: Set of retailer whose upper inventory limits that where denoted as U_j are exceeded

For vendor driven inputs, survey is conducted with central planning teams:

- International Order Management,
- Stock Control,
- Sales,
- Purchasing,
- Demand and Production Planning teams.

On the other hand, for retail driven parameters distinguished subsidiaries (6) and direct customers (4) of ARC are indicated. Selected customers' demands generate approximately half of the total monthly demands. BEKO PLC (BEKO ENGLAND), BEKO FRANCE, BEKO GERMANY, BEKO ITALY, GRUNDIC NORDIC and BEKO SPAIN are the chosen subsidiaries. Moreover, 4 direct customers from Middle East, Balkans, South America and OEM companies are selected for conducted survey.

Survey was performed in two steps via video conferences. In the first step of the survey, open ended "if parameter x is known by competitor/other retailers/vendor, then it causes…" questions were asked. Participants explained their foresights about the safety issues about each parameter. Before the second step, answers were evaluated, more common threats were matched with relevant parameters, and comprehensive safety problem descriptions were defined for each of the parameters. In the second part, participants gave grade to safety importance level of each parameter on the provided scale of the survey. Finally, answers were combined and all parameters' importance levels were calculated.

First section in survey assessment is the Vendor's sensitivity analysis. In this sensitivity analysis data owners are sales team, order management team, production planning team and purchasing team. Every data owner filled the survey separately. Number of retailers, vendor's production cost and vendor's holding cost are discussed in this part of the research. Second section is retailers' sensitivity analysis. In this part of the research, data owners are selected 6 subsidiaries and 4 direct customers. Retailers' holding cost, demand rate of customer, upper inventory level for customer, order cost for retailer and penalty cost for exceeding upper inventory limit are discussed in this part. Finally, in the third part, outcome parameters are discussed which are quantity of a certain product dispatched to retailer, number of shipments and set of retailers whose upper inventory limits are exceeded.

4.1.2 Risk values

In costumers goods industry scenario, data leakage for the planning team means losing competitive advantage with respect to competitors and bargaining power with respect to subsidiaries and direct customers. As a result of data leakage, capacity utilization is reduced, on-time-in-full levels are negatively affected, and moreover vendor cannot see the actual trends in market. Each of the eleven parameters is graded from this aspect.

Parameter 1: m – number of retailers

Depending on the number of selected customers, cycle time to satisfy their requirements becomes longer. Thus, fulfilling requirements of the customers take more time. If the competitors know all selected customers, he will adjust his strategy accordingly. Thus, they increase their market share by fast response times for some specific customers. However, this data cannot satisfy clear advantage to any retailer inside the system. The number of retailers is most likely known by the members of the chain. Thus, it does not need to be hidden data; it needs low level of protection.

Parameter 2: A_v – vendor's production cost

If competitor can produce the same lot with lower cost, then they would reduce their selling price below the ARC's production cost. Thus, customers buy cheaper products' of ARC's competitors; ARC loses its market share. Moreover, if ARC reduces its prices below its competitors' price then they make loss. On the other hand, retailers bargain with ARC for lower selling price, which reduces profitability of ARC, if they know the production costs of ARC. Thus, production cost is private data for ARC and needs to be hidden. Otherwise, the profitability is threatened by customers and market shares are given away to competitors.

Parameter 3: h_v – vendor's holding cost

When holding cost increases, the vendor's lot size Q decreases in order to reduce holding cost. If competitor knows holding cost, he will work for sudden high increment of demands in the market with promotions, discounts etc. As a result of sudden high sales, ARC cannot satisfy demands of the market with its low inventory levels.

Inside the chain, if the retailers know that holding cost is lower at ARC's warehouses, he will reduce amount of dispatched quantity by reducing overstock level. As a result, smaller warehouse with lower cost becomes enough for customer. ARC pays more for transportation. Furthermore, it becomes difficult to respond to any changes in the market, because retailers have very limited number of products on hand and if they need any shipment, they have to wait at least lead time amount of time. Thus, this parameter needs high security requirements; holding cost is private data of the vendor and needs to be hidden.

Parameter 4: h_j – retailers' holding cost

With the vendor's holding cost, retailers holding cost determines inventory policy. Inventory policy on the other hand determines responsiveness level of the retailer. As a result, if competitor knows the holding cost of retailer, then he arranges his own policy accordingly.

On the other hand, knowing other retailers' holding cost by one retailer indirectly takes advantage for it. One retailer can use other retailers' inventory policy for taking advantage. Moreover, if vendor knows the holding cost they force the retailer to follow his offered policy, which increases vendor's profitability.

Therefore, this parameter needs high security requirements; holding cost is private data of the retailers and needs to be hidden from vendor and other retailers.

Parameter 5: D_j – demand rate of retailer

Demand rate of certain products demonstrate trends, requirements and wealth of the market. If competitors know which products sell more which less, they adjust their inventory and advertisements based on these data. As a result, focusing only on demanded products of the market gives a big competitive advantage to competitors.

If other retailers know the rate, like as competitors they change their policy. On the other hand, vendor should know the rates for more optimistic management of the inventory of the retailer.

As a result, it needs medium security requirements; rate of selling a product should be known by the vendor to manage process more optimistically. However, this data should not be shared with other retailers or competitors.

Parameter 6: U_j – upper inventory level of retailer

Upper limit of the inventory level determines maximum lead time for replenishment. Also, responsiveness is dependent on this upper limit. If competitor knows the upper limits, he will force to exceed this limit to be more responsive to customers.

Upper limit can be used among the chain, but vendor should know the upper limit to manage inventory. It needs medium security requirements; upper inventory limit may be openly shared with the vendor, but needs to be hidden from other retailers and competitors.

Parameter 7: A_j – order cost for retailer

As the vendor ordering cost increases, the vendor's lot size is expected to increase. Thus, inventory levels increase; effectiveness and flexibility of the retailer decreases. In such a situation, competitor declares new technologies to the market and makes retailer's inventory outmoded. Outmoded products can only be sold with high discounts which decreases profitability.

If other retailers know the ordering cost, they compare it with their own cost and investigate optimistic holding policy. This increases their profitability, when it decreases complete supply chains surplus. On the other hand, vendor should know the cost for determining the best replenishment policy. As a result, it needs medium security requirements; order cost may be openly shared with the vendor (as the vendor has to pay it anyway) but needs to be hidden from other retailers and competitors to protect relative inventory policy.

Parameter 8: π_j – penalty cost for exceeding upper limit

When the penalty cost is very high, the upper limit acts as a capacity constraint. This draws bounds of the inventory policies. If competitors know it, he takes action to gain advantage. Retailers inside the chain have same motivation with competitors. On the other hand, vendor should know the data to determine whether using upper inventory limit as a capacity constraint is optimistic or not. Thus, it requires medium security level; overstock penalty cost may be openly shared with the vendor (as the vendor has to pay it anyway), but needs to be hidden from other retailers.

Parameter 9: q_i – quantity of a certain product dispatched to retailer

If competitor knows the quantity of product on hand of retailer, he may design his inventory and respective marketing policy accordingly to take advantage in the competition. Retailer may know quantity of a certain product held by his vendor. Thus, relevant marketing policy applied. On the other hand, other retailers may not know quantity. Hence, it needs medium security requirements; quantity dispatched to retailer may be openly shared between the vendor and the respective retailer to apply best inventory and marketing policy. On the other hand, it needs to be hidden from other retailers and competitors.

Parameter 10: n_i – number of shipment

No risk is realized that it need not be hidden.

Parameter 11: S – set of retailers whose upper inventory limits are exceeded.

By knowing retailers whose upper limit is exceeded, competitor can estimate upper inventory limits and holding costs of other retailers. As a result of this knowledge, he arranges his inventory policy and relevant marketing policy to increase his market share. Among the retailers, data may be used for the same motivation. Thus, it needs high security requirements; set of retailers whose upper limit is exceeded is sensitive information, which could lead to conclusions about upper inventory limits and/or holding costs of other retailers and hence needs to be hidden.

Chapter 5 Supply Chain Management Prototype preparation and design

5.1 Architecture of the prototype for secure collaborative maintenance demand forecasting

As worked out in the previous Deliverable D24.2, the concept of decision trees can be used for collaborative maintenance demand forecasting. This concept consists of two steps, namely:

1. The learning phase where the decision tree is built using a given set of training data.
2. The classification phase where the established tree is used to classify new (sensitive) data.

For the learning phase we have assumed that the MRO has one central database that stores all historic condition and usage data. All the data is known by the MRO, so there is no need to encrypt this data in the decision tree building phase.

In the classification phase privacy requirements are higher because datasets of different (competing) customers need to be classified. For example, in the aerospace use case these datasets contain current flight plans and real-time condition data. This is sensitive data, especially for national air forces. In this scenario we propose to store the customers' data in encrypted databases using an order preserving encryption scheme (OPES) as introduced by Agrawal (Agrawal et al., 2004). In more detail, we implement a scheme presented by Boldyreva et al in (Boldyreva et al., 2009). The present Deliverable focuses rather on the conceptual architecture than on the technical details of a possible implementation which is described in the previously mentioned paper by Boldyreva et al.

Combining OPES with decision tree classification has big advantages regarding functionality and performance: for classification the functional requirements are rather low: we only need comparison operations (<; >; =) to classify an instance. OPES allows to perform exactly these required comparison operations on encrypted data.

Main features of an encrypted database utilizing order preserving encryption scheme (OPES) are:

- Ordering and comparison operations can be directly applied to encrypted data, including equality and range queries, MAX, MIN and COUNT queries.
- Updates on the encrypted database (e.g. adding values or modifying an already existent value) can be executed without changing the encryption of other values.
- All underlying database techniques (e.g. data compression using dictionaries, performance optimizations using additional indexes) on order preserving encrypted data can be used without modifications. This allows deployment in real systems.

In our proposed scheme, the MRO does not need to know the actual sensor data, but only its classification. As a result, sensitive data does not need to be decrypted by the MRO. Customers are in full control over their encryption and decryption keys. The customers update the encrypted database which can be accessed by the MRO via SQL queries. These queries are then rewritten by the customers (using their encryption key to encrypt plaintext query values) resulting in encrypted queries. (The example query for Figure 14 presents a concrete example of a rewrite operation.)

To classify an instance by comparing its attributes' values with all splits of a given decision tree, comparison operations are sufficient. Exactly this needed functionality is given by order preserving encrypted databases. To obtain the number of instances in each class the before mentioned COUNT query capability is sufficient.

For clarification, a fictional example is evaluated using the presented architecture:

In an initial step, the MRO creates a binary classification tree using historical data (for a detailed description of the used algorithm see Deliverable D24.2, Algorithm 2 on p. 64). Let's assume this analysis of historical data results in the decision tree depicted in Figure 14.

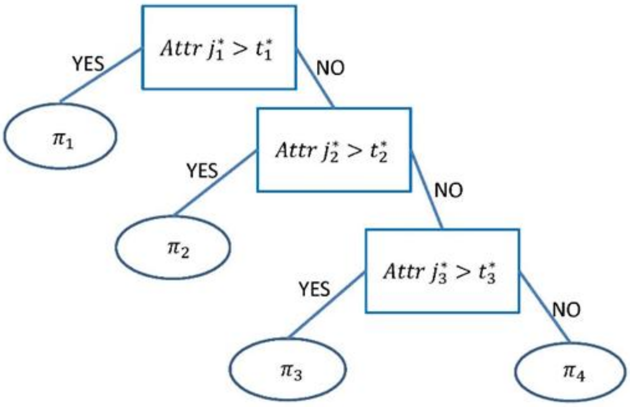


Figure 14: Example of a binary decision tree of depth 3.

The MRO can calculate the necessary forecasts by running the classification of the developed tree via SQL queries. For each leaf of the binary decision tree, there is one query which counts how many instances fall into this leaf. For example, the second leaf of the tree depicted in Figure 14 can be represented by two comparisons, namely $j_1^* \leq t_1^*$ and $j_2^* > t_2^*$.

Assuming the real-time sensor data is stored in a table RT-DATA the resulting plain SQL query looks as follows:

SELECT COUNT(*) FROM RT-DATA WHERE $Attr_{j_1^*} \leq t_1^*$ AND $Attr_{j_2^*} > t_2^*$.

This plaintext SQL query is sent to one customer (e.g. an airline) holding his encryption key K. Using this encryption key, the query values given in plaintext can be replaced with their encrypted values, denoted as $Enc_K(\cdot)$. We emphasize, that this transformation happens in a transparent way using the SEEED JDBC driver (for more details see Deliverable D22.1 and D22.2).

SELECT COUNT(*) FROM RT-DATA WHERE $Attr_{j_1^*} \leq Enc_K(t_1^*)$ AND $Attr_{j_2^*} > Enc_K(t_2^*)$.

Now, this encrypted query can be evaluated on the encrypted database, using state-of-the-art database technology. One example for an encrypted database is given in Table 5; this table contains encrypted real-time data that has to be classified by the corresponding decision tree.

This (encrypted) query returns the number of engines which are assigned to the leaf with $(\pi_2;1-\pi_2)$ as the probabilistic distribution over the two classes (replace; repair). By similar queries all leaves can be evaluated. This yields the expected result of instances that have to be replaced resp. that can be repaired without replacement (for a more detailed discussion see Deliverable D24.2).

$Attr_1$	$Attr_2$	$\dots$	$Attr_k$
$Enc_K(x_{11})$	$Enc_K(x_{12})$	$\dots$	$Enc_K(x_{1k})$
$\vdots$			$\vdots$
$Enc_K(x_{n1})$	$\dots$		$Enc_K(x_{nk})$

Table 5: Example for encrypted database

The only operation that is left for the cloud-based platform is aggregating the expected results for all customers. Finally, this aggregated result is sent back and presented to the MRO.

5.2 Architecture of the prototype for secure Vendor Managed Inventory

As explained in the previous Deliverable D24.2, collaborative forecasting for mid-term production planning can be boiled down to aggregation of individual sensitive data. More particular, the basic idea for the use case of ARC is as follows: ARC does not need the individual data of each customer but only the aggregated numbers. These can be computed without revealing individual input data by using (additive) homomorphic encryption.

For example, consider a product x_1 and three customers called Alice, Bob and Charlie reselling this product. Their individual, sensitive forecast for product x_1 is denoted as x_{A1}, x_{B1} and x_{C1}. For a solid capacity planning, ARC is not needed to know the individual forecasts, but only the overall expected demand for product x_1. Formally, ARC is interested in the sum over all individual forecasts, namely $S_{x1} \coloneqq x_{A1} + x_{B1} + x_{C1}$.

For this kind of secure aggregation, we use an additive homomorphic encryption scheme, e.g. (Paillier, 1999) with encryption algorithm $Enc_{PK}^{HOM}(.)$ using public key PK and decryption algorithm $Dec_{SK}^{HOM}(.)$ using secret key SK. This scheme has the following property: multiplication of ciphertexts maps to addition of the plaintext, i.e.

$$Dec_{SK}^{HOM}\left(Enc_{PK}^{HOM}(x) \cdot Enc_{PK}^{HOM}(y)\right) = x + y.$$

ARC publishes their public key PK and keeps the corresponding secret key SK private. Now Alice, Bob and Charlie encrypt their private inputs to $Enc_{PK}^{HOM}(x_P), P \in \{A, B, C\}$ and send these ciphertexts to one party without access to the secret key (e.g. one centralized cloud-based platform). This party aggregates all ciphertexts to

$$Enc_{PK}^{HOM}(x_{A1}) \cdot Enc_{PK}^{HOM}(x_{B1}) \cdot Enc_{PK}^{HOM}(x_{C1})$$

Finally, this aggregation is sent to ARC who can decrypt it:

$$Dec_{SK}^{HOM}\left(Enc_{PK}^{HOM}(x_{A1}) \cdot Enc_{PK}^{HOM}(x_{B1}) \cdot Enc_{PK}^{HOM}(x_{C1})\right) = x_{A1} + x_{B1} + x_{C1}$$

resulting in S_{x1} as required.

None of the parties can learn the input data of another individual party, neither can the computing party since the secret key for decryption stays private at ARC. Furthermore, ARC does get the aggregation and only the aggregation and is not able to reconstruct values of individual parties.

Assuming all individual forecast data is stored in a table IND-FORECASTS hosted at any party (that has no access to the secret key SK) as outlined in Table 6 the resulting plain SQL query looks as follows:

SELECT SUM($Prod_1$) FROM IND-FORECASTS.

ARC sends this query to the party holding the IND-FORECASTS table; this query is evaluated on encrypted data and the aggregated (still encrypted) result is sent back to ARC. ARC holding the secret key SK is the only party capable of decrypting the result.

$Prod_1$	$Prod_2$	$\cdots$	$Prod_k$
$Enc_{PK}^{HOM}(x_{A1})$	$Enc_{PK}^{HOM}(x_{A2})$	$\cdots$	$Enc_{PK}^{HOM}(x_{Ak})$
$\vdots$			$\vdots$
$Enc_{PK}^{HOM}(x_{C1})$	$\cdots$		$enc_K(x_{Ck})$

Table 6: Example for encrypted forecast

5.3 System and customizations

The functional requirements of both use-cases can be transformed to privacy-preserving SQL queries. Here sensitive data is stored at a cloud based platform in an encrypted SQL database. This encrypted data can then be filtered and aggregated as described in the previous sections.

The planned prototype will be the second prototype in PRACTICE and is heavily based on input from other work packages. In more detail, Figure 17 illustrates all (preliminary planned to be) used components of the prototype embedded in the versatile landscape of secure multi-party computation techniques. The components work together as follows: The end user sends a plain SQL statement P to the Java Interface via a Web interface or Java client application. The SEEED JDBC driver rewrites P to an encrypted SQL statement E. HANA's SQL query engine interprets E so it can be executed on the encrypted data store. The encrypted result of the execution of E is send back to the SEEED JDBC driver, which decrypts the result so it can be presented to the end user. (For a more detailed description we refer to Deliverable D21.2.) The integration into the SPEAR & DAGGER system that has been developed in work package WP 21 is one primary insight for our prototype development. This allows an easy development and deployment of the prototype for secure supply chain management.

A combination of this analysis and the knowledge gained from work package WP 22, namely the principles for developing a database containing private data is applied to our prototype. Especially the possibility to filter and sort encrypted data is the main functionality we have concentrated on to realize secure supply chain management in the Aerospace use case 7scenario. Our proposed database will operate on encrypted data and the key necessary to decrypt the customer’s sensitive real-time data will never leave the customer’s trusted zone.

In theory, it is possible to switch the underlying technique – SEEED in our case – with any other encrypted database that allows SQL queries on encrypted data. We have decided to make use of SEEED because of its easy integration into SAP landscapes. A more detailed deployment model is described in the following section.

For future work, the flexible design of the SPEAR & DAGGER framework allows cross-integration of other techniques for secure multi-party computation. Outsourcing the learning algorithm for binary decision trees into the cloud is one use-case that could be realized with moderate overhead using the SDK that is in development process in work package WP 22.

5.4 Deployment strategy and solution

In the following section presenting the deployment strategy we focus on the more complicated use-case, that is secure collaborative maintenance demand forecasting described in section 5.1. For the use-case of Vendor Inventory Management one has to replace the MRO party with ARC (compare Figure 15). Furthermore, all customers can contribute their encrypted demand forecasts to one central database hosted at the cloud-based platform.

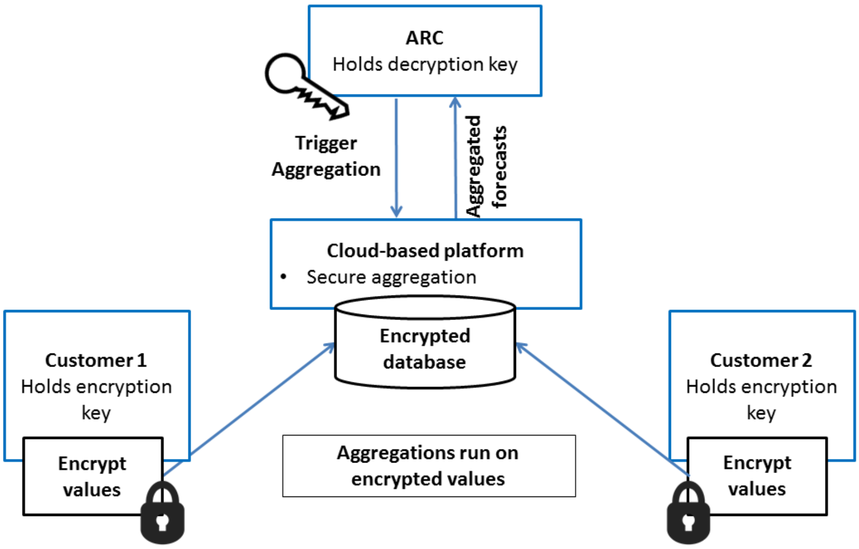


Figure 15: Concept for secure vendor managed inventory

As depicted in Figure 16, our solution for the aerospace use-case consists of three different components:

1) The MRO software that has to create the decision tree using historical data,
2) the cloud-based platform that forwards the plain SQL query to n customers, collects the result sets, aggregates them and sends them back to the MRO, and
3) the customer software, that stores real-time data in an encrypted database, holds the encryption key, and transforms the plaintext SQL query to an encrypted version (using the stored encryption key).

The MRO software consists of a database to store and access historical data which is used to learn a decision tree. Since results of the decision tree evaluation should be accessible by end users, this software is planned to be a web application for general browsers, consisting of usual HTML, CSS and JavaScript. This solution does not need to install any custom software on the end user’s system and can be accessed from every machine that has access to the internet and a common browser. Furthermore, data confidentiality and data integrity between the cloud-based platform and the MRO end user can be accomplished using state-of-the-art techniques like TLS / SSL.

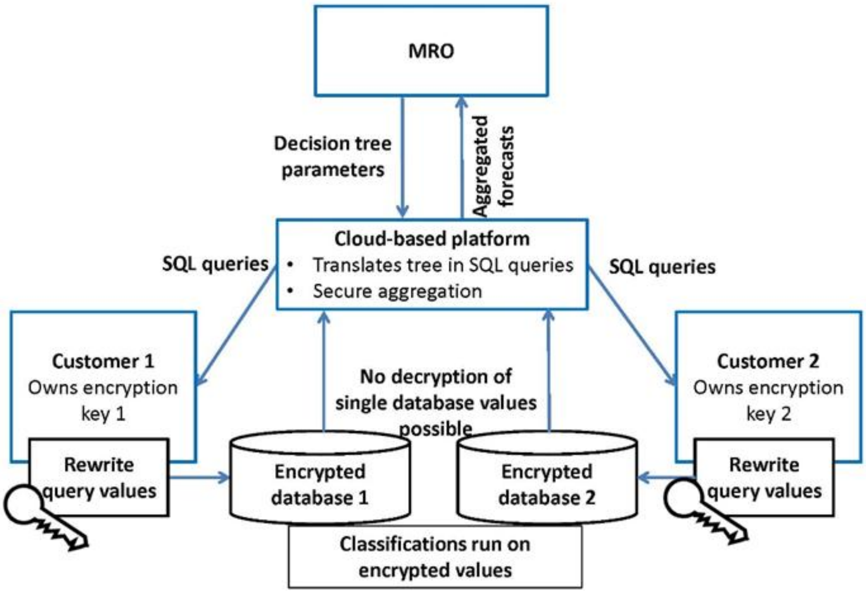


Figure 16: Concept for secure decision tree evaluation utilizing OPES

The cloud-based platform is planned to be written in Java to be portable to different systems and operating systems using the properties of the JVM. Furthermore, Apache Tomcat is chosen to create and deliver HTML files that contain the result of the secure aggregation from the cloud-based platform to the MRO end-user.

The customer software (like the MRO software) consists of a database to store and access real-time sensor data. This database is realized as a (slightly modified) SAP Hana system to be easy to adopt into the existing business landscape powered by SAP. With slight modifications of SEEED, it would be possible to choose any other SQL database as well. In our case, no human interaction is needed, since all data is read from real-time sensors in an automatic fashion. Combining this fact with the current implementation of SEEED (it is a modified JDBC driver, see Deliverable D22.2 for more details), it is straightforward to implement the MRO software as a Java application that initializes the SEEED driver before usage.

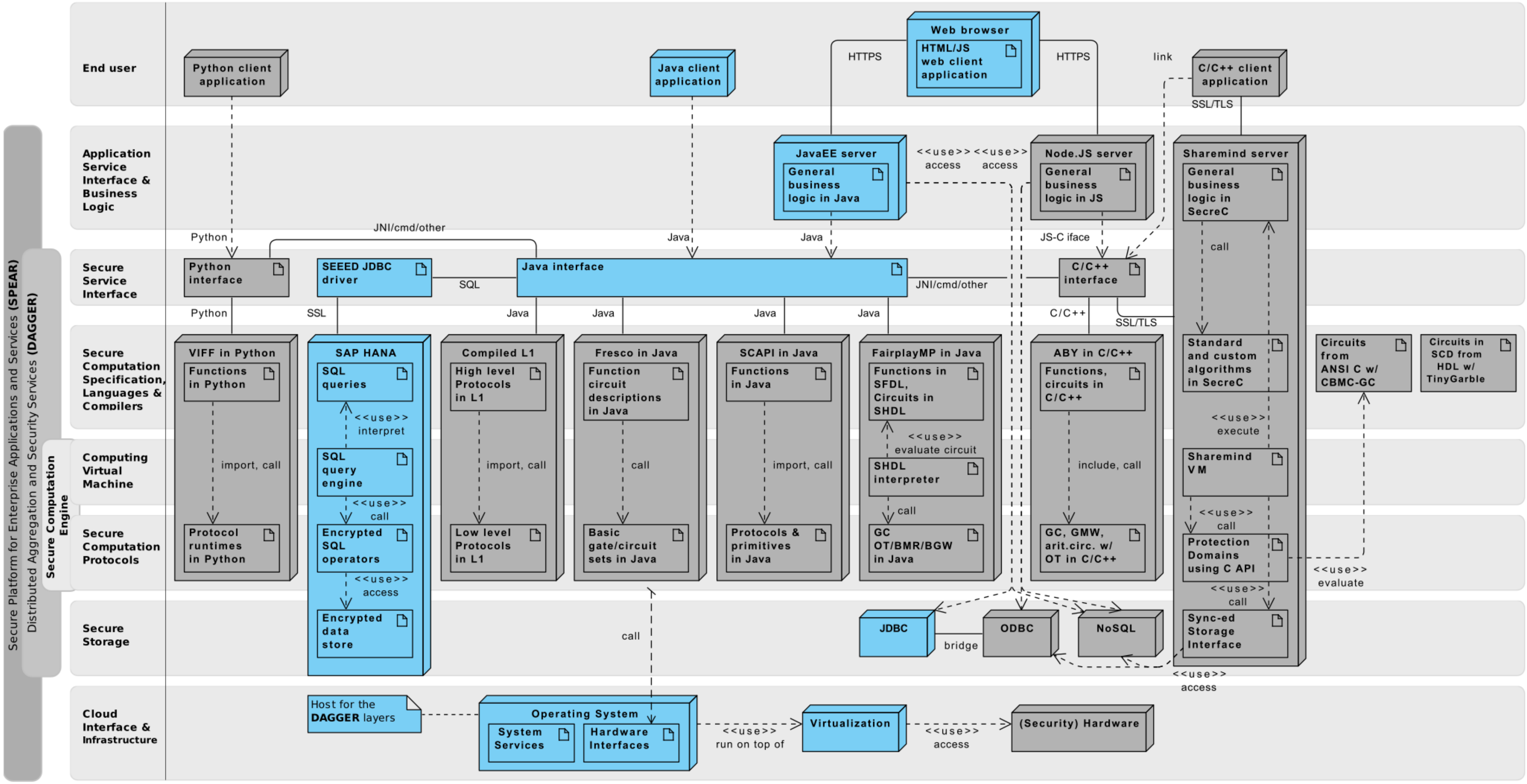

Secure Platform for Enterprise Applications and Services (SPEAR)
Distributed Aggregation and Security Services (DAGGER)
Secure Computation Engine
End user
Application Service Interface & Business Logic
Secure Service Interface
Secure Computation Specification, Languages & Compilers
Computing Virtual Machine
Secure Computation Protocols
Secure Storage
Cloud Interface & Infrastructure
Python client application
Java client application
Web browser
HTML/JS web client application
C/C++ client application
HTTPS
HTTPS
link
SSL/TLS
JavaEE server
General business logic in Java
<<use>> access
<<use>> access
Node.JS server
General business logic in JS
Sharemind server
General business logic in SecreC
call
JNI/cmd/other
Python
Java
Java
JS-C iface
Python interface
SEEED JDBC driver
SQL
Java interface
JNI/cmd/other
C/C++ interface
Python
SSL
Java
Java
Java
Java
C/C++
SSL/TLS
VIFF in Python
Functions in Python
import, call
Protocol runtimes in Python
SAP HANA
SQL queries
<<use>> interpret
SQL query engine
<<use>> call
Encrypted SQL operators
<<use>> access
Encrypted data store
Compiled L1
High level Protocols in L1
import, call
Low level Protocols in L1
Fresco in Java
Function circuit descriptions in Java
call
Basic gate/circuit sets in Java
SCAPI in Java
Functions in Java
import, call
Protocols & primitives in Java
FairplayMP in Java
Functions in SFDL, Circuits in SHDL
<<use>> evaluate circuit
SHDL interpreter
call
GC OT/BMR/BGW in Java
ABY in C/C++
Functions, circuits in C/C++
include, call
GC, GMW, arit.circ. w/ OT in C/C++
Standard and custom algorithms in SecreC
<<use>> execute
Sharemind VM
<<use>> call
Protection Domains using C API
<<use>> call
Sync-ed Storage Interface
Circuits from ANSI C w/ CBMC-GC
Circuits in SCD from HDL w/ TinyGarble
<<use>> evaluate
JDBC
bridge
ODBC
NoSQL
<<use>> access
call
Host for the DAGGER layers
Operating System
System Services
Hardware Interfaces
<<use>> run on top of
Virtualization
<<use>> access
(Security) Hardware

Figure 17: PRACTICE architecture big picture with used components highlighted

Chapter 6 Pilot assessment framework

In the first part of this report the target industrial scenarios are resumed and the data protection levels are proposed, in the second part instead preliminary results on the prototype development are exposed. The prototype will be delivered in the next period, at M30, and during the last semester it will be tested on industrial cases. The tests are aimed at verifying how the system work in terms of security and in terms of business benefits bought to supply chain.

In this chapter the security aspects of the cloud system that will be validated during the tests (section 6.1) and the metrics applied to measure the business impacts of the collaborative supply chain management systems are presented. In particular, metrics will be measured on the test cases in two conditions: with and without the collaborative planning system. By comparing the results obtained in the two conditions the improvements of the collaborative supply chain management will be measured.

The presented metrics are targeted to the aero-engine fleet management case. It is characterized by 4 management areas that are impacted by the collaborative system (customer, process, inventory, finances), for each of them a set of metrics is developed.

The comprehension that inventory management policy and financial figures are both related to the forecast capabilities has led to the conceptualization of an innovative tool able to simulate the impacts of forecast capabilities on the organizational economy. Indeed, if forecasts regards a longer period, more effective inventory management policies are enabled and more economic purchases of goods are possible. In the last section of this chapter, the benefits of such a system and the general requirements are introduced.

6.1 Security assessment

Our prototype approach provides a significant difference to the current approach of securing outsourced data. Just encrypting tables is not sufficient as any application would require decryption before processing. If this happens in the cloud, we are vulnerable to any attacks from the cloud provider and if the decryption and query execution happen on the on-premise client any Database as a Service offering is pointless.

Our approach scales as it also allows to leave non-critical columns in plaintext without any change to a query required.

General trust assumptions that are the basis of our prototypes are depicted in Figure 18; for the vendor managed inventory use case exactly one database is outsourced (i.e. $n = 1$). Note, that key material cannot be accessed by the cloud-based platform, hence it is not able to decrypt outsourced data. The final result set of decision tree evaluations is an aggregation of all customers' classified data and sent back to the MRO. The same argument holds for vendor managed inventory, where the final result set is an aggregation of all customer's sensitive data and sent back to ARC.

In our aerospace use case a database filter-query (e.g. COUNT) triggered by the MRO is sent (over an untrusted network) to the customers containing all decision tree parameters. Decision tree parameters are learnt using historical data and we assume them to be not confidential.

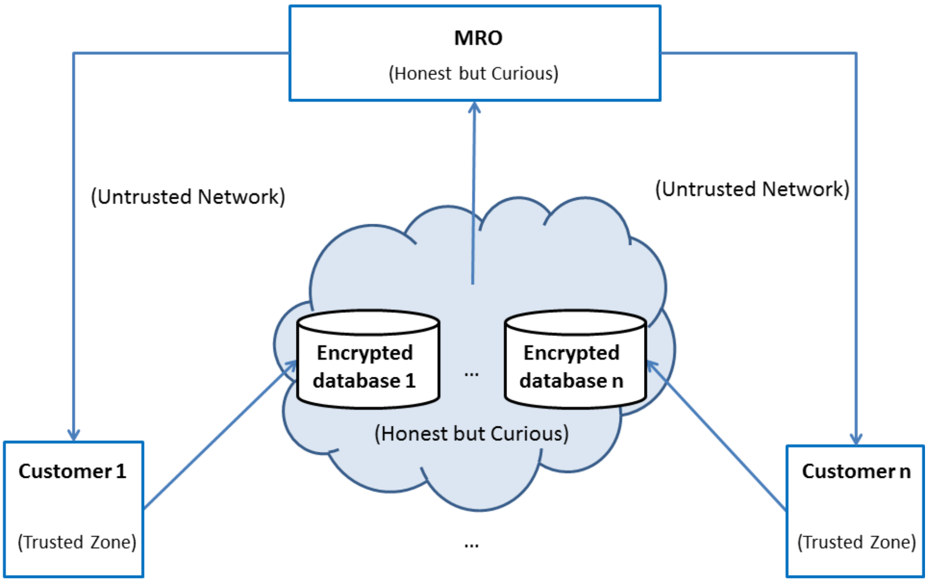


Figure 18: Simplified Architecture with Trust Assumptions

At the customer, the SEEED database driver (e.g. JDBC) driver will encrypt the query elements. Either query elements are database updates consisting of sensitive real-time data from the engine sensors; here confidentiality is guaranteed by using order-preserving encryption. Otherwise these elements are decision tree parameters that have been sent by the MRO; here order-preserving encryption is used to enable comparison with real-time data. If the query was a database filtering query, the results of all customers are aggregated and sent back to the web application at the MRO. We emphasize, that only the aggregated result is sent back the MRO while primary encryption keys never leave the customers' zone.

In the vendor managed inventory use case, ARC sends the public key to all their customers over the untrusted network. At the customer, this public key is registered at and managed by SEEED for future update queries. Updates of the database contain sensitive inventory forecast data; confidentiality is guaranteed by using (additive) homomorphic encryption. Furthermore, aggregation of this sensitive data is triggered by ARC and the result is sent back to ARC who can decrypt the result. Again, we emphasize that only the aggregated result is sent back to ARC, hence individual data is protected.

6.1.1 Aspects of the process that will measured

The aero fleet management process was described in detail in D24.2; here, the Figure 19 shows an effective representation of it.

In this context, it is expected that the adoption of a planning optimization system at supply chain level (Figure 20) and the proper use of the associated methods and information summarized (enablers) improves the overall performance in terms of:

- **Reduction of Turn Around Time**
  In the fleet management process, TAT is the time spent by the engine into the service provider plant in order to be overhauled. More accurate service planning methods and, in general, a collaborative supply chain planning, should lead to a reduction of TAT.
- **Reduction of penalties**

Penalties are paid due to delivery delays with respect to contract obligations. Thanks to a continuous process monitoring and controlling, penalties should be reduced. It will lead to higher service levels, as well as costs containment.

- **Reduction of total costs**
  The Cloud Planning System promises a more efficient use of resources (human resources and equipment) and an optimized spare parts management (lower inventory levels). It means a reduction of total costs, since productivity of resources should increase and safety stocks should be reduced[3].

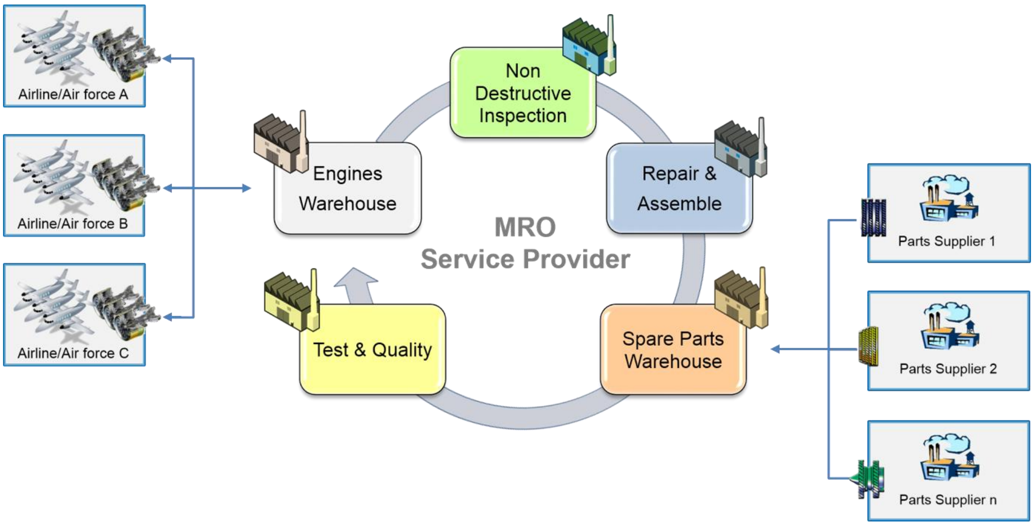


Figure 19: Aero fleet management process: Material Flow.

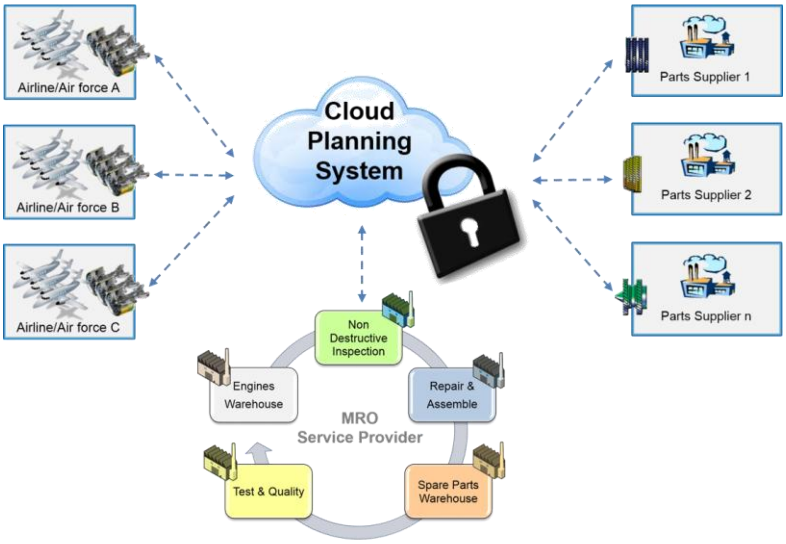


Figure 20: Cloud Planning System model.

The Table 7 sums up objectives and enablers resulting from the adoption of the Cloud Planning System within the aero fleet management process.

[3] We remind the reader that aeronautic industry is capital intensive and the inventory is a big cost.

OBJECTIVES	ENABLERS[4]
Reducing Turn Around Time	➢ More accurate planning methods ➢ Supply chain planning
Reducing penalties	➢ Process monitoring and controlling
Reducing total costs	➢ More efficient use of resources ➢ Lower inventory levels

Table 7: Objectives and Enablers.

6.1.2 Business assessment framework

The aim of the present analysis is to define a set of Key Performance Indicators (KPIs) in order to evaluate the effectiveness of the Cloud Planning System into the aero fleet management process.

The Figure 21 shows an overview of the business assessment framework proposed.

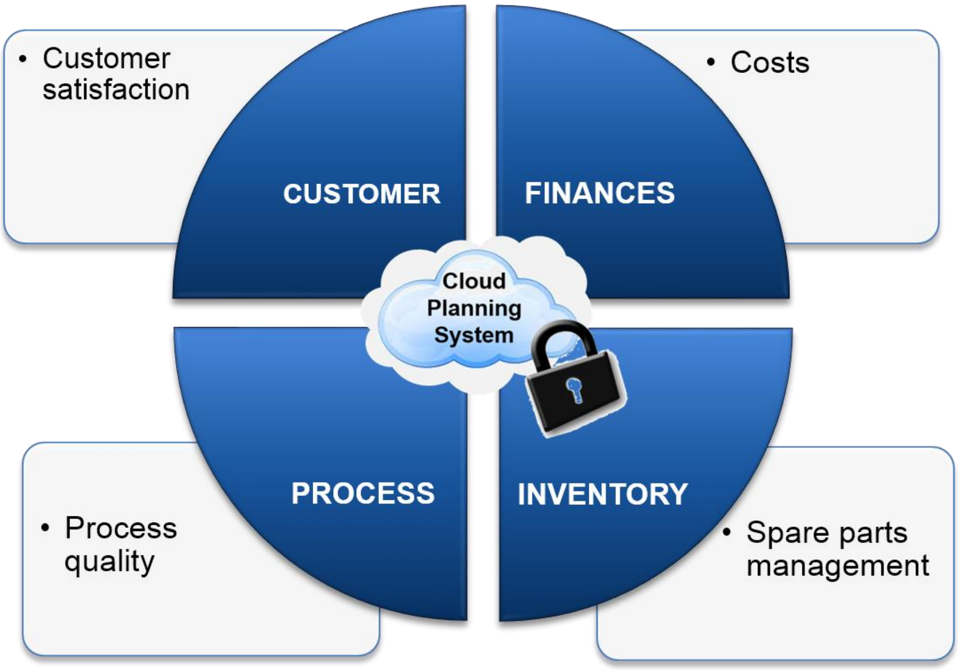


Figure 21: Business assessment framework.

KPIs are divided in four different impact areas in relation to the performance of the fleet management process that we are interested in evaluating.

[4] Methods and information that lead to the achievement of the objectives.

All KPIs will be characterized by a set of properties: the name of the indicator; a general description; the calculation formula; the unit of measure; and a target value in order to compare the current KPI value with this target and to identify shortcomings or improvement potentials.

6.1.2.1 CUSTOMER impact area

According to Balance Scorecard Institute[5], recent management philosophy has shown an increasing realization of the importance of customer focus and customer satisfaction in any business. Moreover, Gebauer et al. (2011) state that customer satisfaction represents a fundamental indicator to evaluate the attractiveness of business and to preserve companies' competitive advantage.

In line with this philosophy of thought, KPIs in Customer impact area have the aim to measure the satisfaction of engine owners in terms of service level. In general, customers expect the agreed service level in any demand condition. In Table 8 the identified KPIS measure the capability of the MRO service provider to respect the service level agreed and which part of the demand is satisfied in a certain period of time. These metrics inform about the capability of the supply chain network to integrate other engine owners (the MRO can attack the market) or the need to increase service and production resources not to lose some of new potential customers due to the low real service level.

CUSTOMER IMPACT AREA	
KPI name	**KPI attributes**
C.1 Delivery performance to customer	**Description** This KPI monitors the number of engines which are delivered back to the owner (airline/air force) according to contract times. It is calculated as the percentage of engines that are delivered back to the owner on or before the relevant reference-date, respect the total number of deliveries. It has to consider a range of time.
	Calculation formula $\frac{\#\ of\ deliveries\ in\ due\ time}{Total\ \#\ of\ deliveries}$
	Unit of measure %
	Target value 100%
C.2 Responsiveness	**Description** This KPI measures the capability of the supply chain to satisfy the demand in the current market (composed of all engines owners).

[5] http://balancedscorecard.org/Customer-Perspective

CUSTOMER IMPACT AREA	
KPI name	**KPI attributes**
	It is calculated as the percentage of engine maintenances carried out in a given time frame, respect the total number of engine maintenances requested. It has to consider a range of time.
	Calculation formula $\frac{\#\ of\ maintenances\ carried\ out}{Total\ \#\ of\ maintenances\ requested}$
	Unit of measure %
	Target value 100%

Table 8: KPIs of CUSTOMER impact area.

6.1.2.2 PROCESS impact area

Metrics based on the process perspective allow managers to know how well their business is running, and whether its products and services conform to customer requirements (Swierk and Mulawa, 2014).

Here, KPIs in Process impact area want to measure the ability of the service provider to execute the MRO process in an effective and efficient way. In particular, the process should be executed smoothly (without delays or stops in between two steps), within the expected TAT even in case of unplanned events, and with an efficient use of resources.

KPIs belonging to this impact area are described in the following Table 9.

PROCESS IMPACT AREA	
KPI name	**KPI attributes**
P.1 Mean Turn Around Time	**Description** This KPI evaluates time necessary to carry out planned maintenance events. It is calculated as the average time taken from the engines receipt in the MRO plant till maintained engines are given back to airlines. It has to consider a range of time.
	Calculation formula $\frac{\sum_{e=1}^{n} TAT_e}{n}$ e: engine n: total number of planned engines maintained in the unit of time

PROCESS IMPACT AREA	
KPI name	**KPI attributes**
	Unit of measure [Days]
	Target value As short as possible
P.2 Mean TAT for unplanned maintenance	**Description** This KPI evaluates time necessary to carry out unplanned maintenance events. It is calculated as the average time taken from the unplanned engines receipt in the MRO plant till maintained engines are given back to airlines. It has to consider a range of time.
	Calculation formula $\frac{\sum_{e'=1}^{n'} TAT_{e'}}{n'}$ e': unplanned engine n': total number of unplanned engines maintained in the unit of time
	Unit of measure [Days]
	Target value As short as possible
P.3 Maintenance rate	**Description** This KPI wants to check the service capacity. It is calculated as the number of engines maintained in the unit of time (e.g. in a year).
	Calculation formula $\frac{\#\ of maintained\ engines}{Defined\ range\ of\ time}$
	Unit of measure [Number of engines/Year]
	Target value As high as possible
P.4 Uncertainty rate	**Description** This KPI aims to understand the entity of the error between the expected

PROCESS IMPACT AREA	
KPI name	**KPI attributes**
	demand and the real one. It is calculated as the percentage of unplanned engines maintenances, respect the total number of maintained engines. It has to consider a range of time.
	Calculation formula $\frac{Unplanned\ engines\ maintenances}{Total\ \#\ of\ maintained\ engines}$
	Unit of measure %
	Target value As low as possible
P.5 Number of engines in WIP	**Description** This KPI wants to check the service capacity. It is calculated as the total number of engines with a Work In Progress status at a specific time.
	Calculation formula *# of engines in WIP*
	Unit of measure [Number of engines]
	Target value As high as possible
P. 6 Resources efficiency	**Description** This KPI tests the real use of available resources. It is calculated as the time of actual use of the resource, in function of its total amount of work time. It has to consider a range of time.
	Calculation formula $\frac{Resource\ uptime}{Total\ hours}$
	Unit of measure %
	Target value

PROCESS IMPACT AREA	
KPI name	**KPI attributes**
	100%
P.7 Waiting time	**Description** This KPI monitors the entity of downtimes in the engine maintenance process. It is calculated as the difference between TAT to maintain the engine and the sum of times to execute all maintenance activities on it.
	Calculation formula $TAT - \sum_{i=1}^{n} ta_i$ ta: time to execute the single activity n: number of activities
	Unit of measure [Days]
	Target value As short as possible

Table 9: KPIs of PROCESS impact area.

6.1.2.3 INVENTORY impact area

In the aero fleet management process, an effective and efficient spare parts management is indispensable to achieve better performance in terms of minimum engine downtimes (Tracht et al., 2013).

In particular, inventory impact area is focused on the MRO service provider - parts' supplier relationship, where KPIs have the objective to show how effective is the inventory management policy in terms of capability to not introduce delay in the service execution due to lacking of a spare parts. KPIs are shown in the Table 10.

INVENTORY IMPACT AREA	
KPI name	**KPI attributes**
I.1 Spare parts availability	**Description** This KPI evaluates the spare parts availability when they are required by the maintenance process. It is calculated as the percentage of spare parts available in the warehouse respect the total number of spare parts required. It has to consider a range of time.

INVENTORY IMPACT AREA	
KPI name	**KPI attributes**
	Calculation formula $\frac{\#\ of\ available\ spare\ parts}{Total\ \#\ of\ spare\ parts\ required}$
	Unit of measure %
	Target value 100%
I.2 Lead time	**Description** This KPI wants to measure the amount of time necessary to receive the spare part from the supplier. It is calculated as the difference between the date in which the spare part arrives to the MRO plant and the date in which the same was requested.
	Calculation formula $LT = ADSP - RDSP$ SPA: Arrival Date of Spare Part SPR: Request Date of Spare Part
	Unit of measure [Days]
	Target value As short as possible

Table 10: KPIs of INVENTORY inventory impact area.

6.1.2.4 FINANCES impact area

According to Kotane and Kuzmina-Merlino (2012), financial indicators are one the main criteria to take into consideration in order to evaluate business performance.

In this analysis, KPIs in the Finance impact area aims to measure extra costs introduced by the inefficiencies of the supply chain. Inefficiencies can be related to low inventories that give raise to stock out events, leading to inefficient resources application and to potential delays; while an effective servicing process management can lead to direct delays (in both case delays imply the payment of a penalty).

Herewith, KPIs taken into consideration are reported in Table 11.

FINANCE IMPACT AREA	
KPI name	**KPI attributes**
F.1 Stock out costs	**Description** This KPI evaluates economic consequences of not being able to meet the spare part demand from the current inventory. It is calculated as the sum between the product of the number of days in which the spare part is out of stock and the cost per day for the downtime, and the possible penalty cost for the engine delivery delay.

	Calculation formula
	$CS = (NDOS * DCPD) + PC$
	CS = Cost of a Stock out
	NDOS = Number of Days Out of Stock
	DCPD = Downtime Cost Per Day
	PC = Penalty Cost

	Unit of measure [Euro]
	Target value As low as possible
F.2 Average penalties cost on customer base	**Description** This KPI measures the average cost for penalties paid by the MRO service provider due to failed contract fulfilment. This cost is calculated for each airline/air forces, in a range of time.
	Calculation formula $\frac{\sum_{A=1}^{m} COST_A}{m}$ A: engine of a certain Airline/Air force for which the penalty has paid m: total number of engines of the Airline/Air force for which the penalty has been paid
	Unit of measure [Euro]
	Target value As low as possible
F.3 Average penalties cost on engine model base	**Description** This KPI measures the average cost for penalties paid by the MRO service provider due to failed contract fulfilment. This cost is calculated for each engine model, in a range of time.

FINANCE IMPACT AREA	
KPI name	**KPI attributes**
	Calculation formula $\frac{\sum_{E=1}^{m\prime} COST_E}{m'}$ E: engine model for which the penalty has paid m’: total number of engine models for which the penalty has been paid
	Unit of measure [Euro]
	Target value As low as possible

Table 11: KPIs of FINANCE impact area.

6.2 Performance simulation tool

As stated in the work package description of WP24, task 2.4.3, “the industrial practices required to apply the new cloud system will be evaluated, specific industry-dependent requirements will be outlined.” One certainly industry-dependent requirement is the degree of improvement in forecast accuracy that our cloud based system can offer. In some industrial settings already a small improvement in accuracy yields high savings in inventory costs. In other settings the same added value requires a much higher improvement.

We therefore develop a performance simulation tool that allows us to quantify the benefit of improved forecast accuracy in different supply chain settings. With this tool we will be able to evaluate cases for possible implementation of our cloud based system. We can estimate potential benefits and therefore offer incentives to companies, which are interested in an application.

Furthermore, we see this simulation tool as a preliminary step for the performance assessment, which will be the main content of work package 24. There we will evaluate “[t]he economic performances, the effective improvements brought to the users (the firms) as autonomous individual and as part of a network; this aspect will be analysed by analysing some real (or quasi-real, if confidentiality reasons apply) cases;

This assessment is expected to highlight the effective value of the system for the industries and to provide some more industry-focused requirements for the future industrialization phases of the cloud.” (Work package description WP24, task 2.4.5)

The remaining subchapter is structured as follows. First, we describe what exactly we want to assess with special focus on the aero-fleet case. Then we argue why this is best done with a simulation approach. Finally, we specify the requirements for our simulation tool. The results from the simulations will be part of deliverable D24.5.

6.2.1 Assessing the benefits of improved forecast accuracy in the aero-fleet case

The models developed for the aero-fleet setting in deliverable 2.4.2 can roughly be divided in two parts: first, we provided methods to improve the quality of the demand forecasts in the supply chain mainly from the MRO's perspective. The improvement of the forecasts can only be achieved by using the customers' data that is only made available if its privacy can be assured. In the second part, we described different approaches how these (improved) forecasts can be used in subsequent planning activities.

A specific setting, that will serve as an assessment case for the prototype is the spare parts inventory problem of the MRO. We choose this case for several reasons: First, excessive spare parts inventories are considered an urgent (and expensive) issue for our industrial partners. Second, we expect that secure collaborative forecasting could significantly improve the quality of the forecasts on spare parts demand. Third, the spare parts problem is not limited to the aero-space industry but is relevant for any industry where heavy machinery has to be kept in service.

Our goal is to estimate the monetary benefit of an implementation of the prototype given the specific parameters for the inventory planning.

The secure collaborative forecasting that is part of the prototype models provides as an output a forecast (expected demand) and a measure for the attached forecast uncertainty (e.g. the expected deviation from this forecast). The latter drives the required safety stock that has to be kept in order to deal with the deviations from the forecast.

The forecast and the forecast uncertainty are input parameters for the inventory planning model. There the actual decision about how much to order is made based on the forecast information, the current inventory position and the relevant parameters of the inventory system such as lead times and holding costs. The dynamic inventory model we proposed in deliverable 2.4.2 then yields reorder point and an order quantity (for each specified component). In order to assess the economic performance we need to monitor the inventory level over a longer period. There are two main cost drivers that are of relevance in this context: First, the costs for keeping a part on stock (inventory costs). Second, the costs if a part that is needed for overhaul operations is not kept on stock and can't be replenished on time, which will typically induce some form penalty costs.

The actual results of the benefit assessment will be part of deliverable 2.4.5, but in order to prepare the prototype's implementation it makes sense to clarify how it will be assessed. Especially the simulation tool described in the following subsections will also be used during implementation to continuously test and refine the theoretical models that were developed in deliverable 2.4.2.

6.2.2 Opportunities from simulation approach

Since we don't just want to measure single KPIs but rather look at the interdependencies and the performance of our complex model, a simulation approach is appropriate here. Besides, it has the advantage that we can start assessing the performance of implemented inventory policies, without depending on real data.

The opportunities from a simulation approach for benefit assessment of inventory policies can be summarized as follows:

- *Trade-off analysis:* Analyze the relationship between Finance and Inventory;
- *Economic benefit analysis*: how much money can be saved depending on certain improvements in forecasting performance;

- *Sensitivity analysis*: what consequences would changes in certain parameters (e.g. lead-times, holding costs,…) have on MRO service costs;
- *Model testing:* Test the performance of inventory policy in various settings.

6.2.3 Requirements specification for a benefit assessment simulation tool

We now describe the basic features of our simulation tool to show how the opportunities from the preceding subchapter are to be realized. The tool should be able to simulate potential benefits in different supply chain constellations. Therefore, the following parameters are considered to enable adjustment to different settings:

- Number of customers

For each customer:

- Number of components of each type in use
- Agreed on turnaround times

For each component:

- Lead time
- Ordering costs
- Holding costs (central inventory at the MRO's site
- Penalty costs (if assumed to be similar for all customers)

Given a setting described by the parameters above the variables are:

- the demand forecasts and
- the attached forecast uncertainties

In a supply chain, subject to stochastic demand and discrete time, the objective is then in each period to decide how much spare parts of each type need to be ordered to minimize the overall cost over the planning horizon. These costs are mainly driven by holding costs and penalty costs. Fixed order costs will probably be negligible given the expected low order volumes. Then we can assess the benefit of improved forecasts under simulated realisations of demand.

Chapter 7 Conclusion

By leveraging the industrial role of ARC and of DTA and the aeronautic partners of UNISA-CCII, the models of collaborative supply chain management developed in previous project phases were validated. The validation process was focused on the actual measurement of the risks associated to the management of confidential and private data in a collaborative supply chain management system.

The risk measurement model applied is based on the qualitative assessment of the outcomes of a data leakage event for specific supply chain participant. Indeed, a data leakage event produces business damages (the 'impact') to the data owner; on the other hand, it is assumed that a certain risk can be run in exchange of business benefits. In our case, the benefits are the improved performance of the supply chain, in terms of higher service levels at lower costs, from which each participant deduces its own economic benefit. For this reason, the data owner can accept a certain likelihood for a data leakage event: the maximum tolerable event 'probability'. The risk measurement model takes in consideration also the case of 'prior knowledge' of the confidential and private data, this parameter reduces the risk associated to the specific data whose value can be inferred through experience, (old) publication, previous business relationships. The risk value of each parameter is a function of these three inputs: the impact, the probability and prior knowledge.

The risk measurement was carried out through a survey. The persons that participated were accurately informed about the data protection and the security performance of the secure computation technology, about the innovation objectives and the results expected and achieved by the PRACTICE project, and on the business benefits of collaborative planning.

In the aeronautic network, a web survey was administered, while in the consumer goods industry a number of face to face interview were carried out on a two steps approach. The results of the surveys in both the industries are that the risks associated to the variables involved in the collaborative supply chain management models (the collaborative service planning for the fleet management and the inventory managed model for the consumer goods industry) are very high, even if there are minor differences among the different parameters.

Basing on the results survey it is possible to state that the security requirements are aligned to the industrial expectations.

In the second part of the deliverable, the assessment framework for the pilot case is presented. It is composed of three main parts. The first one presents the main security expected improvements in order to target the evaluation of the security performance of the prototype application. The second part focused on the business improvements bought by the collaborative planning, 4 management areas are expected to be impacted: customers, process, inventory, financial; for each management area a set of metrics are proposed to measure the impact of the collaborative planning models.

During the development of the assessment framework, it was recognized the usefulness of a system to verify economic potentiality of collaborative planning. By leveraging the analytical relationship between the financial performance, the inventory management policy and forecasting capabilities, a simulation tool is sketched. It will enable supply chain practitioners to verify how longer forecasts, enabling more effective inventory policy, impact on costs of the organization.

The developed assessment framework will lead the evaluation of the application of the prototype supply chain management system to the industrial pilot cases.

Chapter 8 List of Abbreviation

MRO	Maintenance, Repair and Overhaul
ICT	Information Communication Technology
TAT	Turn Around Time
IT	Information and Technology
ERP	Enterprise Resource Planning
SC	Supply Chain
NDA	Non-Disclosure Agreement
MPC	Multi-Party Computation
ITAR	Traffic in Arms Regulations
EAR	Export Administration Regulations
VMI	Vendor Management Inventory
OPES	Order Preserving Encryption Scheme
SPA	Arrival Date of Spare Part
SPR	Request Date of Spare Part
CS	Cost of a Stock out
NDOS	Number of Days Out of Stock
DCPD	Downtime Cost Per Day
PC	Penalty Cost
WIP	Work In Progress

Chapter 9 Bibliography

Agrawal, R., Kiernan, J., Srikant, R., & Xu, Y. (2004). “Order preserving encryption for numeric data”. In *Proceedings of the 2004 ACM SIGMOD international conference on Management of data* (pp. 563-574)

Boldyreva, A., Chenette, N., Lee, Y., & O’Neill, A. (2009). “Order-preserving symmetric encryption”. *In Advances in Cryptology – EUROCRYPT’09*, (pp. 224-241)

D21.2: Roman Jagomagis, Florian Hahn, Kasper Lyneborg Damgard, Peter Sebastian Nordholt, Reimo Rebane, PRACTICE Deliverable D21.2, Unified architecture for programmable secure computations, 2015

D22.1: Isabelle Hang, Ferdinand Brasser, Niklas Buescher, Stefan Katzenbeisser, Ahmad Sadeghi, Kai Samelin, Thomas Schneider, Jakob Pagter, Janus Dam Nielson, Peter Sebastian Nordholt, Kurt Nielsen, Johannes Ulfkjaer Jensen, Dan Bogdanov, Roman Jagom¨ agis, Liina Kamm, Jaak Randmets, Jaak Ristioja, Reimo Rebane, Jaak Ristioja, Sander Siim, Riivo Talviste, Manuel Barbosa, Bernardo Portela, Rui Oliveira, Stelvio Cimato, Ernesto Damiani, PRACTICE Deliverable D22.1, State-of-the-Art Analysis, 2015

D22.2: Tobias Mueller, Niklas Buscher, Hiva Mahmoodi, Janus Dam Nielsen, Peter S. Nordholt, Dan Bogdanov, Manuel Barbosa, Johannes U Jensen, Kurt Nielsen, PRACTICE Deliverable D22.2, Tools design document, 2014

D23.1: Johannes Ulfkjaer Jensen, Kurt Nielsen, Peter S. Nordholt, Roman Jagomagis, Marko Joemets, Reimo Rebane, Meril Vaht, PRACTICE Deliverable D23.1, Secure Survey Prototype - a supplementary report, 2015

D24.1: Angelo Corallo, Mario Münzer, Georg Hafner, Florian Hahn, Cem Kazan, Huseyin Serif Beyaztas, Onur Gures, Hakan Tufek, Julian Kurz, Richard Pibernick, Antonio Zilli, Giuseppe Grassi, Stelvio Cimato, PRACTICE Deliverable D24.1, Business and Security Requirements, 2014

D24.2: Antonio Zilli, Mario Münzer, Florian Hahn, Cem Kazan, Elif Ozdogan, Buket Serper, Richard Pibernik, Julian Kurz, Fabian Taigel, Jan Meller, Fabian Diehm, Antonio Zilli, Marianna Lezzi, Stelvio Cimato, Ernesto Damiani, Kurt Nielsen, PRACTICE Deliverable D24.2, Business Modelling, 2015

Gebauer H., Gustafsson A., Witell L., (2011), “Competitive advantage through service differentiation by manufacturing companies”, Journal of Business Research

Kotane I., Kuzmina-Merlino I., (2012), “Assessment of financial indicators for evolution of business performance”, European Integration Studies, n°6

Paillier, P. (1999). “Public-key cryptosystems based on composite degree residuosity classes”. In *Advances in Cryptology—EUROCRYPT’99* (pp. 223-238)

Swierk J and Mulawa M., (2014), “IT balanced scorecard as a significant component of competitive and modern company”, Management, Knowledge and Learning International Conference 2014

Tracht K., Niestegge A., Schuh P., (2013), “Demand planning based on performance measurement systems in closed loop supply chains”, Eighth CIRP Conference on Intelligent Computation in Manufacturing Engineering

Chapter 10 Appendix A

DATA SECURITY IN COLLABORATIVE CLOUD-BASED SYSTEMS

Coordination in supply chains is an extraordinary source of competitive advantage.

Nowadays, a number of Supply Chain Management (SCM) systems, some of them also cloud-based, offer features for information sharing in supply chains. However, none of them implement protocols that would be able to automatically coordinate a number of partners (customers and suppliers) in a way that the most competitive and available resources are committed to satisfy future demand. In general, applications of collaborative supply chain planning in practice are rather scarce. We suppose that it is mainly due to issues with data security, since current cloud-based SCM systems need organizational confidential data to be shared openly for any collaborative approach.

Basically, this survey aims to evaluate this hypothesis. In more detail, the purposes of the survey are:

- Punctually define reasons preventing the dissemination of collaborative cloud-based systems;
- Measure the relevance and the limitation of data security for organizations;
- Evaluate the interest of organizations in secure cloud supply chain management systems.

The results of this survey will lead next research activities of the PRACTICE project aimed at implementing a prototypical system and an industrial pilot case.

SECTION 1/4 – General information

Please indicate the company you work for, its industry, as well as your functional area in the company.

Company (optional): …………………………………………………………………….

Industry:

□ Security Electronics
□ Aeronautics
□ Space and Defence Systems
□ Transport
□ Marine
□ Energy and Oil & Gas
□ Software System
□ Hardware

- □ Education
- □ Automotive
- □ Heath Care
- □ Other

Functional area (optional):

- □ Management
- □ Board of directors
- □ Organizational information systems
- □ Research and Development
- □ Marketing and Sales
- □ Human resources
- □ Accounting
- □ Production
- □ Logistics

SECTION 2/4 – Cloud technologies for data sharing

Nowadays, collaboration between suppliers and customers is accomplished by the use of a certain number of technologies; the most innovative and fastest adopted ones are those based on cloud computing.

This section of the questionnaire intends to analyse the spread of cloud computing systems within collaborative supply chains.

Q.1. Does your company use cloud computing technologies to share data and information with suppliers?

- □ **Absolutely yes**
- □ **Mostly yes**
- □ **Neither yes or no**
- □ **Mostly no**
- □ **Absolutely no**

Q.2. Does your company use cloud computing technologies to share data and information with customers?

- □ **Absolutely yes**
- □ **Mostly yes**
- □ **Neither yes or no**
- □ **Mostly no**
- □ **Absolutely no**

Q.3. In your company, is the use of cloud computing technologies limited by data security requirements?

- □ **Absolutely yes**
- □ **Mostly yes**
- □ **Neither yes or no**
- □ **Mostly no**
- □ **Absolutely no**

Q.4. In your company, is the use of cloud computing technologies limited by the lack of trust in the security provided by the cloud service provider?

- □ **Absolutely yes**
- □ **Mostly yes**
- □ **Neither yes or no**
- □ **Mostly no**
- □ **Absolutely no**

Q.5. In your company, is the use of cloud computing technologies for collaboration in the supply chain limited by the lack of trust in the way customers or suppliers could use the system or data?

- □ **Absolutely yes**
- □ **Mostly yes**
- □ **Neither yes or no**
- □ **Mostly no**
- □ **Absolutely no**

Q.6. In your company, is the use of cloud computing technologies limited by other reasons?

- □ **Absolutely yes**
- □ **Mostly yes**
- □ **Neither yes or no**
- □ **Mostly no**
- □ **Absolutely no**

Q.7. Which are the other reasons limiting the use of cloud computing technologies in your company? (optional)

……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
………………………

Q.8. In your company, is the choice of a cloud service provider bound to the presence of certifications related to data protection?

- □ **Absolutely yes**
- □ **Mostly yes**
- □ **Neither yes or no**
- □ **Mostly no**
- □ **Absolutely no**

SECTION 3/4 – Data security

Data sharing with suppliers and customers puts emphasis on data security issues.

This section of the questionnaire explores the theme of protection of organizational data and information.

Q.9. In your company, the management and the board of directors are strongly committed to data security and protection.

□ **Absolutely yes**
□ **Mostly yes**
□ **Neither yes or no**
□ **Mostly no**
□ **Absolutely no**

Q.10. In your company, the management and the board of directors consider data security and protection as a marginal issue.

□ **Absolutely yes**
□ **Mostly yes**
□ **Neither yes or no**
□ **Mostly no**
□ **Absolutely no**

Q.11. In your company, only the IT department is committed to data security and protection.

□ **Absolutely yes**
□ **Mostly yes**
□ **Neither yes or no**
□ **Mostly no**
□ **Absolutely no**

Q.12. Does your company apply any tools to prevent disclosure of digital data by insiders?

□ **Absolutely yes**
□ **Mostly yes**
□ **Neither yes or no**
□ **Mostly no**
□ **Absolutely no**

Q.13. Does your company apply any tools to prevent disclosure of digital data after providing them to customers?

□ **Absolutely yes**
□ **Mostly yes**
□ **Neither yes or no**
□ **Mostly no**
□ **Absolutely no**

Q.14. Does your company apply some tools to prevent disclosure of digital data after providing them to suppliers?

□ **Absolutely yes**
□ **Mostly yes**
□ **Neither yes or no**
□ **Mostly no**
□ **Absolutely no**

Q.15. Is your company certified for the management of information security?
(One of the most common international standard is ISO/IEC 27001.2013)

□ **Absolutely yes**
□ **Mostly yes**
□ **Neither yes or no**
□ **Mostly no**

□ **Absolutely no**

SECTION 4/4 – Risk assessment

Risk is defined as the product of the probability a specific event happens and the impact it produces: *Risk = Probability * Impact.*

Supply chain models and practices show that more effective coordination and higher business performance can be achieved by calculating collaboratively demand forecasts and production plans.

In PRACTICE project, mathematical models of collaborative forecasting and planning are developed and will be implemented in a prototype that uses the privacy-preserving cloud infrastructure.

This last section is related to the aero-engine Maintenance, Repair and Overhaul (MRO) supply chain, composed of the airlines/air forces, the MRO service provider, and spare parts suppliers.

Data required by the PRACTICE collaborative model describe:

A. Usage and condition information of the engines fleet;
B. Overhaul process and inventory status of MRO service provider;
C. Production and delivery plans of spare parts suppliers.

The goal of this section is to assess the risk level associated with using these data in a cloud-based collaborative supply chain management system.

A.1. How harmful is for an airline the disclosure of data related to the usage and condition information of its engines fleet (for example flight hours, flight cycles, previous overhaul services, …) to another airline? *(Select the value on a scale from 0 to 5, where 0 is "not harmful at all" and 5 is "extremely harmful"; choose "don't know" if you don't have an opinion on this)*

□ **0**
□ **1**
□ **2**
□ **3**
□ **4**
□ **5**
□ **Don't know**

A.2. In exchange for better supply chain performance (lower overall costs, shorter off-wing time, higher service level, …), what is the probability of a data leakage event involving other airlines, tolerable by an airline? *(Select the value on a scale from 0 to 5, where 0 is "high data leakage probability can be tolerated' and 5 is 'no data leakage probability can be tolerated'; choose "don't know" if you don't have an opinion on this)*

□ **0**
□ **1**
□ **2**
□ **3**
□ **4**

- □ **5**
- □ **Don’t know**

A.3. How harmful is for an airline the disclosure of data related to the usage and condition information of its engines fleet (for example, flight hours, flight cycles, previous overhaul services, …) to the MRO service provider? *(Select the value on a scale from 0 to 5, where 0 is “not harmful at all” and 5 is “extremely harmful”; choose “don’t know” if you don’t have an opinion on this)*

- □ **0**
- □ **1**
- □ **2**
- □ **3**
- □ **4**
- □ **5**
- □ **Don’t know**

A.4. In exchange for better supply chain performance (lower overall costs, shorter off-wing time, higher service level, …), what is the probability of a data leakage event involving MRO service provider, tolerable by an airline? *(Select the value on a scale from 0 to 5, where 0 is “high data leakage probability can be tolerated’ and 5 is ‘no data leakage probability can be tolerated’; choose “don’t know” if you don’t have an opinion on this)*

- □ **0**
- □ **1**
- □ **2**
- □ **3**
- □ **4**
- □ **5**
- □ **Don’t know**

A.5. How harmful is for an airline the disclosure of data related to the usage and condition information of its engines fleet (for example, flight hours, flight cycles, previous overhaul services, …) to the spare parts supplier? *(Select the value on a scale from 0 to 5, where 0 is “not harmful at all” and 5 is “extremely harmful”; choose “don’t know” if you don’t have an opinion on this)*

- □ **0**
- □ **1**
- □ **2**
- □ **3**
- □ **4**
- □ **5**
- □ **Don’t know**

A.6. In exchange for better supply chain performance (lower overall costs, shorter off-wing time, higher service level, …), what is the probability of a data leakage event involving spare parts suppliers, tolerable by an airline? *(Select the value on a scale from 0 to 5, where 0 is “high data leakage probability can be tolerated’ and 5 is ‘no data leakage probability can be tolerated’; choose “don’t know” if you don’t have an opinion on this)*

- □ **0**
- □ **1**
- □ **2**

□ **3**
□ **4**
□ **5**
□ **Don't know**

B.1. How harmful is for a MRO service provider the disclosure of data related to internal activities (for example, execution time of tasks, Turn Around Time; resources available; service plan; inventory status, …) to an airline? *(Select the value on a scale from 0 to 5, where 0 is "not harmful at all" and 5 is "extremely harmful"; choose "don't know" if you don't have an opinion on this)*

□ **0**
□ **1**
□ **2**
□ **3**
□ **4**
□ **5**
□ **Don't know**

B.2. In exchange for better supply chain performance (lower overall costs, shorter off-wing time, higher service level, …), what is the probability of a data leakage event involving an airline, tolerable by a MRO service provider? *(Select the value on a scale from 0 to 5, where 0 is "high data leakage probability can be tolerated' and 5 is 'no data leakage probability can be tolerated'; choose "don't know" if you don't have an opinion on this)*

□ **0**
□ **1**
□ **2**
□ **3**
□ **4**
□ **5**
□ **Don't know**

B.3. How harmful is for a MRO service provider the disclosure of data related to internal activities (for example, execution time of tasks, Turn Around Time; resources available; service plan; inventory status, …) to another MRO service provider? *(Select the value on a scale from 0 to 5, where 0 is "not harmful at all" and 5 is "extremely harmful"; choose "don't know" if you don't have an opinion on this)*

□ **0**
□ **1**
□ **2**
□ **3**
□ **4**
□ **5**
□ **Don't know**

B.4. In exchange for better supply chain performance (lower overall costs, shorter off-wing time, higher service level, …), what is the probability of a data leakage event involving another MRO service provider, tolerable by a MRO service provider? *(Select the value on a scale from 0 to 5, where 0 is "high data leakage probability can be tolerated' and 5 is 'no data leakage probability can be tolerated'; choose "don't know" if you don't have an opinion on this)*

- □ **0**
- □ **1**
- □ **2**
- □ **3**
- □ **4**
- □ **5**
- □ **Don’t know**

B.5. How harmful is for a MRO service provider the disclosure of data related to internal activities (for example, execution time of tasks, Turn Around Time; resources available; service plan; inventory status, …) to spare part suppliers? *(Select the value on a scale from 0 to 5, where 0 is “not harmful at all” and 5 is “extremely harmful”; choose “don’t know” if you don’t have an opinion on this)*

- □ **0**
- □ **1**
- □ **2**
- □ **3**
- □ **4**
- □ **5**
- □ **Don’t know**

B.6. In exchange for better supply chain performance (lower overall costs, shorter off-wing time, higher service level, …), what is the probability of a data leakage event involving spare part suppliers, tolerable by a MRO service provider? *(Select the value on a scale from 0 to 5, where 0 is “high data leakage probability can be tolerated’ and 5 is ‘no data leakage probability can be tolerated’; choose “don’t know” if you don’t have an opinion on this)*

- □ **0**
- □ **1**
- □ **2**
- □ **3**
- □ **4**
- □ **5**
- □ **Don’t know**

C.1. How harmful is for a spare parts supplier the disclosure of data related to the production plan and the inventory status to an airline? *(Select the value on a scale from 0 to 5, where 0 is “not harmful at all” and 5 is “extremely harmful”; choose “don’t know” if you don’t have an opinion on this)*

- □ **0**
- □ **1**
- □ **2**
- □ **3**
- □ **4**
- □ **5**
- □ **Don’t know**

C.2. In exchange for better supply chain performance (lower overall costs, shorter off-wing time, higher service level, …), what is the probability of a data leakage event involving an airline, tolerable by a spare part supplier? *(Select the value on a scale from 0 to 5, where 0 is “high* *data leakage probability can be tolerated' and 5 is 'no data leakage probability can be tolerated'; choose "don't know" if you don't have an opinion on this)*

□ **0**
□ **1**
□ **2**
□ **3**
□ **4**
□ **5**
□ **Don't know**

C.3. How harmful is for a spare parts supplier the disclosure of data related to the production plan and the inventory status to a MRO service provider? *(Select the value on a scale from 0 to 5, where 0 is "not harmful at all" and 5 is "extremely harmful"; choose "don't know" if you don't have an opinion on this)*

□ **0**
□ **1**
□ **2**
□ **3**
□ **4**
□ **5**
□ **Don't know**

C.4. In exchange for better supply chain performance (lower overall costs, shorter off-wing time, higher service level, …), what is the probability of a data leakage event involving a MRO service provider, tolerable by a spare part supplier? *(Select the value on a scale from 0 to 5, where 0 is "high data leakage probability can be tolerated' and 5 is 'no data leakage probability can be tolerated'; choose "don't know" if you don't have an opinion on this)*

□ **0**
□ **1**
□ **2**
□ **3**
□ **4**
□ **5**
□ **Don't know**

C.5. How harmful is for a spare parts supplier the disclosure of data related to the production plan and the inventory status to another spare parts supplier? *(Select the value on a scale from 0 to 5, where 0 is "not harmful at all" and 5 is "extremely harmful"; choose "don't know" if you don't have an opinion on this)*

□ **0**
□ **1**
□ **2**
□ **3**
□ **4**
□ **5**
□ **Don't know**

C.6. In exchange for better supply chain performance (lower overall costs, shorter off-wing time, higher service level, …), what is the probability of a data leakage event involving another spare parts supplier, tolerable by a spare part supplier? *(Select the value on a scale from 0 to*

5, where 0 is “high data leakage probability can be tolerated’ and 5 is ‘no data leakage probability can be tolerated’; choose “don’t know” if you don’t have an opinion on this)

- □ **0**
- □ **1**
- □ **2**
- □ **3**
- □ **4**
- □ **5**
- □ **Don’t know**

You completed the questionnaire, Distretto Tecnologico Aerospaziale and University of Salento staff thank you for your cooperation.