Grant Agreement Number: 825225

Safe-DEED

www.safe-deed.eu

D2.6 User experiment report v2

Deliverable number	D2.6
Dissemination level	Public
Delivery date	25.11.2020
Status	Final
Author(s)	Masud Petronia, Wirawan Agahari, Mark de Reuver

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 825225.

Changes Summary

Date	Author	Summary	Version
25.09.2020	Masud Petronia	First draft	0.1
05.11.2020	Wirawan Agahari, Mark de Reuver	Second draft	0.2
06.11.2020	Leonie Disch	Internal review WP2	0.3
12.11.2020	Tobias Leander Welling, Alessandro Bruni, Dieter Decraene	Internal review	0.4
17.11.2020	Wirawan Agahari	Final version (incorporated reviews)	1.0

Executive summary

The Safe-DEED project strives to improve security technologies by enabling large-scale implementation of privacy-preserving technologies to overcome data sharing barriers and ultimately accelerate the European data economy. The objective of task T2.3 is to measure the impact of Safe-DEED technologies on trust and willingness to share data as a key to unlock the data economy potential.

One of the technologies developed in Safe-DEED is Multi-Party Computation (MPC). It is a cryptography technology that involves sharing information while not disclosing submitted data between the involved parties. Despite its potential to tackle barriers in data sharing, MPC implementation remains limited, and we lack knowledge about the willingness to use MPC-enabled applications in organizational settings. Hence, in this deliverable, we investigate MPC's effect on organizational willingness to contribute protected data for collective purposes. We focus on MPC deployments in supply chains (SCs). Nevertheless, the study results would provide useful information beyond this domain.

We construct a conceptual model that explains organizational willingness to contribute protected data through MPC. This model consists of three dimensions: trustworthiness, relative advantage, and security. To measure the extent to which MPC affects willingness to contribute protected data, we make a comparison between MPC and Trusted Third Party (TTP). To do this, we develop two identical applications that reflect a TTP and an MPC-based application. The comparison of perception between the two applications can be interpreted as the effect of MPC. An experiment was designed to examine willingness to contribute, both quantitatively and qualitatively. This experimental setup consisted of two groups and four observations. The pretest measured respondents' expectations, whereas the post-test rated their perceptions of the application.

MPC enhances organizational perceptions of data contribution and, therefore, significantly increases perceived trustworthiness and perceived security. Both of these aspects are found to be important and of approximately equal importance when considering the contribution of protected data. Both are considered the locus of willingness to contribute protected data through a web-based application. The qualitative assessment suggests that MPC's positive contribution is because it allows data contribution independently from conventional data processors, which typically have access to raw data. The extent to which MPC increases perceptions depends on how an organization can assert the application's trustworthiness and the security measure used by the application. MPC also affects the perceived relative advantage. A weak correlation is reported between perceived relative advantage and willingness to contribute protected data, suggesting that relative importance is not perceived to be important as perceived trustworthiness and perceived security concerning willingness to contribute protected data. Nevertheless, MPC also seems to enhance the perceived relative advantage. Finally, although MPC's relative advantage was not perceived as necessary, several findings are reported to improve further the utility provided by an MPC application.

Table of Contents

List of Figures

List of Tables

Abbreviations

ANOVA	Analysis of Variance
CMV	Common-Method Variance
CPMT	Communication Privacy Management Theory
CoED	Computation on Encrypted Data
CP	Computing Parties
CI	Confidence Interval
DC	Distribution Centers
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
IP	Input Parties
IOS	Inter-Organizational Systems
MPC	Multi-Party Computation
PCA	Principal Component Analysis
RP	Result Parties
Safe-DEED	Safe Data Enabled Economic Development
SCN	Supply Chain Network
SSCC	Secure Supply Chain Collaboration
SC	Supply Chain
SCI	Supply Chain Integration
SCM	Supply Chain Management
TTP	Trusted Third Party
VIF	Variance Inflation Factor

1. Introduction

The Safe-DEED project strives to improve security technologies by enabling large-scale implementation of privacy-preserving technologies to overcome data sharing barriers and ultimately accelerate the European data economy. To achieve this objective, WP2 aims to promote the diffusion of technology developed in the Safe-DEED project by understanding its economic and business value. One of the tasks is T2.3, which focuses on the economic modeling, adoption, and value creation of Safe-DEED technologies.

In this deliverable, which is part of T2.3, we focus on evaluating Multi-Party Computation (MPC) as one of the technologies developed in Safe-DEED. First addressed by Yao (1986), MPC is a cryptography technology that involves sharing information while not disclosing submitted data between any of the involved parties. Put differently, MPC deals with the problem of jointly computing a function amongst a set of possibly mutually distrusting parties (Archer et al., 2018). With MPC, parties engage in a protocol to obtain the desired output. These parties only gain knowledge based on the protocol's output and their own private input.

Within the context of data sharing, MPC can be used as a tool to overcome trust concerns (Zare Garizy et al., 2018), create new business opportunities (Arnaut, Pont, Scaria, Berghmans, & Leconte, 2018; Koutroumpis, Leiponen, & Thomas, 2020), and foster the European data economy to be in line with the European data strategy (European Commission, 2020; Zafrir, 2020). However, from a managerial perspective, its potential impact within the business domain in terms of sharing capabilities and value creation remains unclear (Damgård, Damgård, Nielsen, Nordholt, & Toft, 2017; Kerschbaum et al., 2011). Moreover, MPC is non-transparent in nature because it runs in the back-end (i.e., cryptography protocols), with some degree of "newness" in organizational settings. As a result, the lack of awareness and uncertainty may limit an organization's willingness to use MPC-enabled applications. In turn, this lack of awareness hinders acceptance, perhaps waving aside a potential technology that might solve the issue of business-wide aggregate data analysis.

This deliverable's primary research objective is to understand how organizations perceived MPC for "data-sharing practices" that would be averted by these same firms. By assessing the extent, we understand the sustainability of MPC as a solution in business contexts. The objective presents a cause-and-effect relationship between MPC and willingness to contribute data through an application. The unit of analysis comprises organizations, and the unit of observation includes individuals (i.e., decision-makers).

Given that MPC is useful for specific functions, a context must be defined in which MPC is studied. For this deliverable, MPC is discussed in the context of Supply Chains (SCs) because SCs are highly competitive environments with numerous data-sharing opportunities blocked by many barriers (e.g., Khurana, Mishra, & Singh, 2011), thus making them appropriate domains for MPC applications. Nevertheless, the study results are relevant beyond SCs, and the logistics sector as SCs are only used to discuss MPC's application to real-world problems.

To fulfill our research objective, we opt for the pre and post-test experimental design. In this approach, treatment is required to compare the MPC to a conventional non-MPC-based solution. This comparison indicates the extent to which MPC affects organizational willingness to contribute data. For this deliverable, we built upon findings from D2.4 (i.e., the first cycle of user evaluation) to develop an improved version of a mock-up that illustrates how MPC works. Then, this mock-up is used to conduct the second cycle of user evaluation described in this deliverable. This methodology allows for both quantitative and qualitative assessments, thereby providing a prime indication of MPC's contribution to the process of contributing protected data. To increase the richness of our findings, the quantitative results are supported by a qualitative assessment.

We strive to understand how Safe-DEED technologies, particularly MPC, create economic impact within a specific use-case through this deliverable. The use case scenario developed mock-ups, and empirical findings provide a valuable reference for the prototype and business models development of Safe-DEED technologies.

This deliverable is structured as follows. In section 2, we provide a background on MPC and supply chain domain. We also develop our conceptual model as a basis to measure MPC's impact on firms' willingness to contribute protected data in this section. Subsequently, we present the demonstration platform in section 3. After that, we elaborate on our experimental design and outline our findings in section 4 and section 5, respectively. Finally, we discuss our results and conclude the deliverable in section 6.

2. Background

In this section, we seek to understand the aspects that must be understood to examine organizational willingness to contribute protected data through MPC. In section 2.1, MPC is decomposed to understand its intricacies and to determine a suitable approach for the given problem. Next, section 2.2 provides an overview of the supply chain domain and the relevance of MPC. After that, section 2.3 describes a theoretical basis on trustworthiness, security, and relative advantage as factors that are likely to determine an organization's willingness to contribute protected data through MPC. Finally, in section 2.4, we propose our conceptual model and hypotheses that will be tested in the experiment.

2.1 Secure MPC

MPC is a powerful instrument because it provides a possible solution to Computation on Encrypted Data (CoED) (Archer et al., 2018). In the mainstream of MPC research, MPC comprises two or n number of IPs $P_i(i = 1, ..., n)$, each with a concealed dataset xi, whereby they jointly and interactively compute an objective functionality $f(x_1, ..., x_n) = (y_1, ...y_n)$ (application-oriented task such as electronic voting) based on their inputs (Zhao et al., 2019) (see Figure 1).

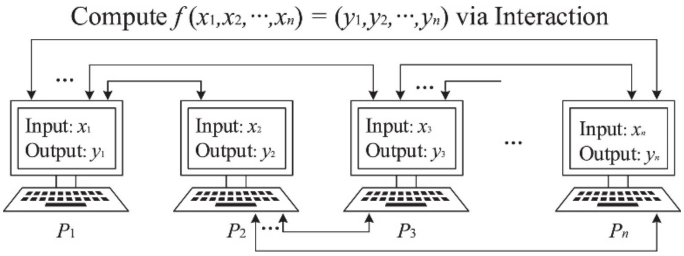


Figure 1 Diagram of Secure Multi-Party Computation, adapted from Zhao et al. (2019)

These challenges concern requirements that MPC protocols must satisfy to cover possible adversarial attacks related to privacy, correctness, independence of input, the guarantee of output, and fairness (Zhao et al., 2019). Thereby several security models for MPC are defined. Based on the behavior of the adversary, there are four security models:

1. **Semi-honest or passive adversary model:** users execute protocol as provided but may attempt to glean information from the output
2. **Malicious adversary model:** corrupted participants may arbitrarily deviate from the protocol's specifications based on the adversary's instructions (Bestavros, Lapets, & Varia, 2017; Catrina & Kerschbaum, 2008)
3. **Covert adversary model:** users who cheat if only they are unlikely to be caught or cheat as long as the expected payout is larger than the expected penalty if caught (Zhao et al., 2019)
4. **Rational adversary model:** users will only cheat the protocol to maximize their utility function (Miltersen, Nielsen, & Triandopoulos, 2009).

In broad terms, the more sophisticated a security model, the more suited it is in environments where participants may behave dishonestly; however the more computationally expensive it becomes– and therefore impractical. Nevertheless, "A protocol is considered secure only if it can resist any adversarial attacks under the corresponding security model" (Zhao et al., 2019). However, MPC is still in its infancy (Choi & Butler, 2019). To date, not all technical challenges have been practically solved (Zhao et al., 2019). Besides performance limitations, several implementation challenges are identified and addressed (e.g., Toldsepp, Pruulmann-Vengerfeldt, & Laud, 2012). Some scholars have worked around this challenge. As a result, it is becoming more accepted to accept 'weak' models. For instance, Bestavros, Lapets, and Varia (2017) argue that weak adversary models, which are technically more efficient, can still be satisfactory when considering the collaboration incentives. Other forms to cope with these challenges are applications that are complemented with risk profiles (Kerschbaum et al., 2011), reputation-based systems (Bestavros, Lapets, & Varia, 2017), or ironically using MPC on top of the MPC applications (secret sharing of secret keys).

Trust is also an essential factor. In D2.4, we examine MPC's role in perceived security and trust regarding willingness to use. It is demonstrated that the presentation of MPC affects the way security and trust are perceived. However, enhanced perceptions do not necessarily lead to an increase in MPC's adoption. That is, a feeling of improved security does not necessarily imply consent. Meanwhile, when considering MPC's usage, information sharing benefits depend on one's ability to use the algorithm's output. Hence, this requires a function backed by win-win scenarios.

MPC can be deployed in many ways. In essence, MPC is deployed in a distributed computing environment. Figure 2 illustrates an example of architecture. In general, MPC comprises three actors: (1) input parties (IP) who deliver concealed data (i.e., sensitive, confidential, private) to the confidential computation; (2) the result parties (RP) who receive results (or partial results) from the confidential computation; and (3) the independent computing parties (CP) who jointly computing the confidential computation (Archer et al., 2018).

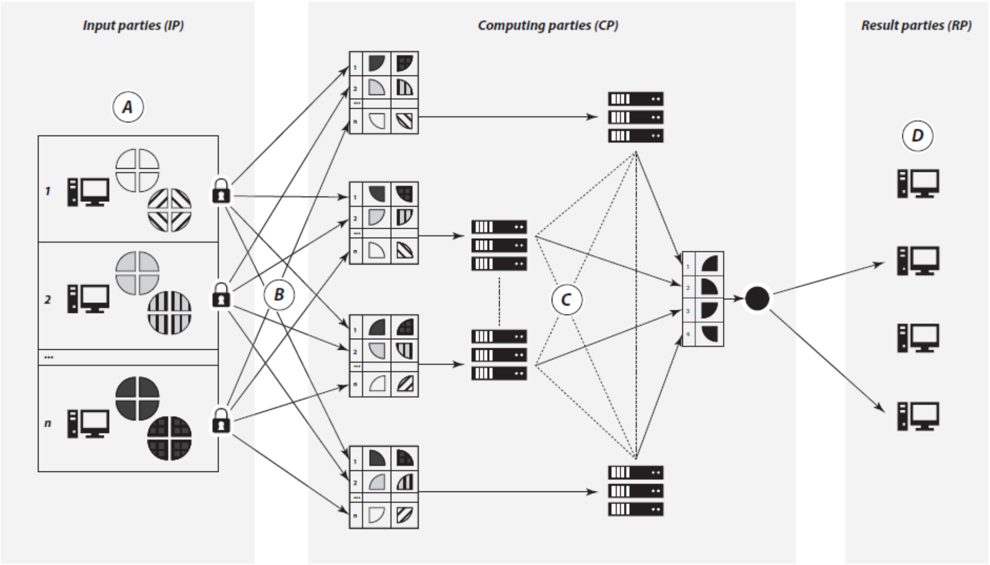


Figure 2 Example MPC application architecture with data flow (adapted from Bestavros et al., 2017; Bogetoft et al., 2009; and Bogdanov et al., 2012)

The data exchange process comprises two phases. The first phase includes submitting and distributing the input (indicators A and B in Figure 2). Data can be, for instance, collected through interfaces such as web-based forms, applets, or other plug-ins. From a practical view, each input interface has different requirements. Nevertheless, IP input data have to be secret-shared at the source. For instance, in Bogetoft et al. (2009), each share is encrypted with a different public key and sent to a storage server. In the case of Bogdanov et al. (2012) (web-based), each share is sent directly to a different proxy server over a secure HTTPS channel. Each interface has other perceived benefits; for example, a web-based form allows application-users to authenticate themselves to the application and benefit from the public internet.

The second phase (indicators C and D in Figure 2) comprises the multi-computation part and the distribution results. Typically, MPC participants perform identical instructions dictated by an MPC protocol on the shares they possess. Finally, the output is distributed to the RPs, which does not need to be the same as IPs. The CP environment's architecture needs to protect against the reconstruction of shares to the original input value at the proxy server (e.g., through private and public keys). A requirement is that both IPs and CPs must be independent and incentivized not to collude.

MPC can be deployed in different frames of reference. Applications can be deployed between companies within the same domain (e.g., assessing common customers between organizations for marketing purposes), across other units within the same company (e.g., cross-selling), and across supply chain tiers (e.g., streamlining manufacturer-supplier SC). Information sharing within these contexts can lead to enhanced information integration. However, the challenge is that in a decentralized system, each party (can) act based on its separate objective functions. As a result, once information is shared within a network, the companies' incentive could dissolve due to information asymmetry. This issue may result in the so-called "one-shot game", a situation where a party or parties have an incentive to behave opportunistically or in self-interest, which results in a single transaction with no repercussions. As a result, Atallah et al. (2004) and Kerschbaum et al. (2011) established generic supply chain protocols under the name Secure Supply Chain Collaboration (SSCC) in the context of such opportunistic behavior.

Due to the specificity in previous literature, we recognize the need to clarify the characteristics of the context in which MPC is deemed fruitful. These characteristics are also necessary to understand the (supply chain) domains in which it is of interest. We characterize MPC context by an environment where:

- A trusted third party (TTP) may be needed as a trusted middleman;
- A data protection regime inhibits data-sharing, or;
- data usage goes beyond legitimate purpose;
- Collusion is impractical or futile (not relevant for all adversary models);
- Exposure from traditional non-MPC data sharing practices can lead to a one-shot game;
- Parties can agree on a computation function, while;
- all parties can gain from the output, and;
- are able to distill and provide corresponding input data at the required level of quality.

2.2 MPC and data sharing in supply chains

Scholars defined a supply chain as an organized system that represents a series of interrelated entities, members, or partners, with different functions directly involved in flows of products, services, information, and finances from and to end-customers (Atallah et al., 2004; Curkovic, Scannell, & Wagner, 2015; Min & Zhou, 2002). A simplified SC network example is depicted in Figure 3.

Goods typically move from top to bottom in stages (e.g., Producer 1, Supplier 2); this is referred to as "forward" integration—closer to the end-customer—while information tends to flow in both forward and backward directions between the different stages. Moreover, vertical integration encompasses cooperation between companies at various stages. In contrast, horizontal integration occurs between companies at the same stage (e.g., Supplier 1, Supplier 2). Finally, diagonal integration–or cross-linkage–involves both vertical and horizontal integration.

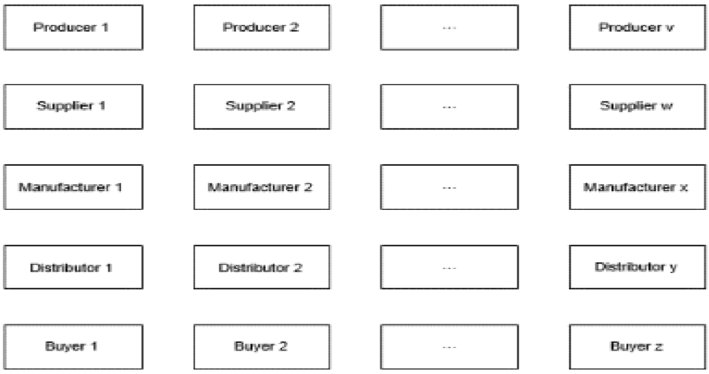


Figure 3 Simplified supply chain network

Within SC networks, Cooper, Lambert, and Pagh (1997) define Supply Chain Management (SCM) as “the integration of key business processes from end-users through original suppliers that provide products, services, and information and add value for customers and other stakeholders.” Per this definition, SCM encompasses activities at many levels: strategic, operational, and tactical. SCM has become increasingly important due to competitiveness introduced by market globalization, which resulted in a growing interest in dealing with inefficiencies and the uncertainties faced by supply chains’ dynamic complexity (Milch & Laumann, 2016). The increasing body of research on supply chain models also confirms this (Min & Zhou, 2002). Supply chain model research aims to advance the frontiers of knowledge to integrate the entire supply chain process successfully. Herein, information serves as a means for Supply Chain Integration (SCI) in decentralized supply chains. More concisely, Lotfi et al. (2013) provide a synthesis of data-sharing benefits in supply chains.

Different theoretical incentives for data-sharing exist. For instance, successful integration can reduce supply chain inefficiencies, such as the well-known ‘bullwhip’ effect. The bullwhip effect is a phantom market demand, which is amplified due to a lack of information synchronization between supply chain members, which leads to higher operating costs (Li, Shaw, Sikora, Tan, & Yang, 2001). Such issues entail information such as “prices, customer profiles, sales forecasts, and order history” (Min & Zhou, 2002), accounting for strategic, operational, and tactical information.

Evidence for the net outcome in supply chains remains limited with regards to data-sharing efforts within business-enhancing activities. The reason is that the data-sharing landscape faces many barriers. For instance, there is shareable and non-shareable data and firms can be unwilling or unable to share certain types of data (e.g., Ojha, Sahin, Shockley, and Sridharan, 2019). Concerns may initially arise regarding the purpose of sharing data, and fear of sensitive information leakage may also exist. With such uncertainty, firms may choose to refrain from data sharing. This uncertainty can reflect security concerns, liability concerns, accountability concerns, legislative concerns, and strategic concerns (Khurana et al., 2011). Also, when there is a legitimate purpose for sharing data, there can be a fear of information leakage. When there is uncertainty over outcomes, or wrong incentives, and non-aligned goals, firms may also refrain from sharing data (e.g., when both firms have profit-maximizing goals). Finally, because of the complexity of SC/SCN, incentives to share data may be overwhelmed by the unknown risks. Altogether, we can group these into a liability, accountability, legislative, and strategic concerns.

These are concerns that MPC could overcome technical and managerial barriers in particular. The degree to which MPC is perceived as a solution to these barriers depends on the organizations. However, from the use cases, we cannot draw any conclusions on the reasons that explain the organizations’ willingness to contribute data. For example, for the use case of Bogetoft et al. (2009), we cannot make inferences on the aspects that led to MPC’s positive perception amongst farmers to solve the problem. While the authors show the level of satisfaction perceived confidentiality provided by MPC, it is not clear whether this is also affected by the pressing need and urgency for a solution to the problem of reallocation of contracts.

Looking back at the use-case characteristics described in the previous section, we can identify several general supply chain scenarios suitable for MPC implementation. For instance, MPC can facilitate **freight bidding** between carriers and shippers. In this scenario, both parties can match the bid, ask prices, and release information only when there is a match without the need for a trusted third party (cf. Bogetoft et al., 2009). Another scenario involves **performance benchmarking** between organizations that require them to share sensitive data. While the typical scenario includes building trusted networks or using a trusted third party, MPC is also relevant in this case (e.g., Damgård et al., 2017). With MPC in place, benchmarking metrics can be calculated without each party seeing the underlying data. Furthermore, another use case is **risk analysis of SCNs,** which is even more relevant given the increasing complexity of SCNs due to globalization and new business models (e.g., Zare Garizy et al., 2018). MPC can serve as a means to calculate risks in the network without giving away protected data (e.g., Adhikari, Bisi, and Avittathur, 2020).

2.3 Factors relevant to the willingness to contribute data

This section draws upon literature on Inter-Organizational Systems (IOS) and MPC to understand the factors addressed by companies when considering willingness to contribute protected data through MPC. The attributes are conceptualized in MPC's context and comprise three constructs: perceived trustworthiness, perceived security, and perceived relative advantage. Each concept is discussed below and serves as a basis to develop a conceptual model in section 2.4.

2.3.1 Trustworthiness

Trustworthiness is a characteristic of a person that is the object of someone's trust. If one is perceived to be trustworthy, we trust his or her ability to execute our decision. The same can be said about an application. If the application is believed to be trustworthy, it meets a prerequisite for 'acceptance' (Pavlidis, 2011). In terms of MPC, trustworthiness refers to the extent to which the MPC is perceived as suitable for providing its stated functionalities according to agreed-upon norms. Trustworthiness is an essential concept within the context of MPC because its presence is not apparent to the Input Party (IP), thus requiring the IP to rely on its perceptions of the system as a whole. Therefore, trustworthiness should be a verifiable property of the system (Feller, 2014).

For instance, active security with abort is an MPC property that could result in unexpected opportunistic behavior (Archer et al., 2018). While this behavior can be dealt with through the MPC environment's protocol or infrastructure, this condition is not (clearly) visible to IPs, which act based on their beliefs of the information provided at the front-end. These aspects relate to the application's perceived trustworthiness. It requires one first to understand the meaning of active security with abort and then understand how this is dealt with by the application and finally deciding if this satisfies their requirements.

Trustworthiness is associated with risk (Hart & Saunders, 1997). In the MPC context, we consider the risks perceived by potential adopters with trying "something new", which is associated with uncertainties due to the application's complexity, divisibility, and observability. As a result, it is assumed that when one agrees to use MPC, it is likely the result of a positive view of these factors.

For this deliverable, we argued that the system's trustworthiness is imperative for understanding the willingness to use the MPC application. We base this argument on the extreme case of using an MPC in an environment with unknown participants, requiring input parties to rely on their perceptions of the system itself. Besides, the system's trustworthiness is expected to increase the level of trust one lays in other (unknown) contributors' behavior. For instance, system integrity prevents inconsistencies, positively affecting others' predictability (Raj et al., 2014).

2.3.2 Security

Security refers to the degree to which the technology's protective measures are perceived to ensure the confidentiality of the information being processed, stored, or transmitted despite risks posed by outside threats (CNSS, 2015). At a fundamental level, usually, security concerns protecting assets of value to an organization. In the context of MPC, security is defined from the view of possible attacks (adversarial attacks discussed in Section 2.1). The purpose of adversarial attacks may be to discover others' sensitive information or disrupt computation tasks (based on protocols). Researchers have proposed several definitions of security to prove that a protocol is secure. These definitions mainly attempt to guarantee several security requirements, including but not limited to privacy, correctness, independence of input, a guarantee of output, and fairness. The standard definition of security in the MPC literature is based on these requirements.

However, unlike real or technical security, perceived security is a psychological concept. From a physiological perspective, perceived security plays a vital role in users' behaviors related to technology.

“Perceived security protection mechanism refers to one’s perception of the existence and effectiveness of hardware, software, and physical security protection” (Zhang, Reithel, & Li, 2009). In the context of MPC, perceived security relates to the degree to which contributors believe that their submitted data is kept confidential in the knowledge sharing process. To examine perceived security in the context of MPC, we assume that we can apply the general (cognitive) determinants of perceived security in information systems.

Huang et al. (2011) examined the role of perceived knowledge, perceived control, and perceived awareness on perceived security. They found perceived control as an effective measure. Perceived control is the extent to which one feels in control of a situation. It is the difference between ‘real’ security and believes about security. Although perceived control falsely indicates one’s actual control, perceptual control influences behavior significantly (Chang, 2010; Wu, Wang, & Huang, 2010). Besides, with MPC, it is assumed that (non-technical) users do not fully understand security control’s technical mechanisms.

Thus, perceived control is determined by the interface’s information or functions (or information control (Skinner, 1996). These include: “explicit information, choice, warning signals, regulated administration, help, feedback, and instructions and, depending on how they are provided, may or may not achieve the intended effect of changing the actual amount of control present (objective control conditions) or the individual’s perceptions of control” (Skinner, 1996, p. 558). In D2.4, we found that the way information is displayed affects the way the application is perceived. Therefore, perceived control has a positive effect on the perceived security of MPC-enabled applications.

Another phenomenon that affects perceived security is perceived risk. Risk (not perceived risk) is a phenomenon that is difficult to measure. Therefore, the risk is becoming more perceptually based (Stewart, 2004). As introduced by Mitchell (1992), perceived risk is viewed from a buyer consumer perspective, making it unsuitable for the study. Chang (2010) adapted this theory to understand managerial behavior in terms of adopting information security technology. “Perceived risk increases with uncertainty and/or the magnitude of the associated negative consequences.” (ibid.). Thereby, “managerial perceptions regarding potential risks to organization information systems impact their expectations of security risk management programs” (ibid). From this, we can agree that perceived risk plays a role in protecting organizational assets (i.e., the protected data) from loss or disclosure.

2.3.3 Relative advantage

Rogers (2003) refers to relative advantage as “the degree to which an innovation is perceived as being better than the idea it supersedes”. However, it is such a general notion that Tornatzky and Klein (1982) consider it not to be of much use if not properly defined, making it difficult to measure. We agree with their argumentation due to the dynamics of MPC. Therefore, in this deliverable, the relative advantage is viewed from the perspective of data sharing advantage, consistent with Kanger and Pruulmann-Vengerfeldt (2015). Consequently, relative advantage refers to the extent to which MPC can be used as a solution to data-sharing cases relative to non-MPC solutions.

We explain the relation between relative advantage on willingness to contribute data in the following paragraph. The required security is relative to the type (or class) of data being shared. However, when assuming a secure platform for data exchange, strictly speaking, this platform is not used since the advantage it provides with respect to alternatives is not defined (not known to users). This argument is in line with Kanger and Pruulmann-Vengerfeldt (2015), which points out that organizations might perceive other solutions as better alternatives. As an implication, while the application might be trustworthy and secure, willingness to contribute is also affected by the relative advantage provided by MPC. Therefore, willingness to contribute refers to the state of a person being willing to contribute data through MPC depending on the perceived advantage (relative advantage) of MPC, with respect to and relative to perceived security and perceived trustworthiness of the MPC application. In other words, when MPC is perceived to provide a low level of advantage (e.g., low security and/or no viable solution to the matter at hand) in comparison to other alternatives, it may not be considered as a solution for the given activity.

2.4 Conceptual model and hypotheses development

We develop a theoretical model on the antecedents of data sharing through MPC. In this deliverable, MPC is discussed as an enabler for contributing protected data. Given MPC's primary purpose and several successful deployments of MPC, it is expected that MPC will increase one's willingness to contribute data–when properly presented. Thus, we propose the following hypothesis:

> **H1: Willingness to contribute protected data through MPC is more significant than the willingness to contribute protected data over Trusted Third Party (TTP).**

To understand MPC's effect on perceived trustworthiness, MPC is compared to a conventional data sharing application that relies on a trusted third party. In a sense, if the application is perceived as trustworthy, input parties have fewer worries about the trusted third party's data handling capabilities. As a result, the service provider becomes less relevant. We can even perceive the application as a trustless consensus (one trusts the application regardless of the parties involved).

These two aspects laid on a spectrum. At one end is an "untrustworthy application" (the input party has no trust in the application) and at the other end of the spectrum is a trustless consensus. This view suggests that a 'name' (name of organization) the application is needed. However, any organization's name that is put and used within an experiment can confound research results. Therefore, we need to assume that the application resides within and is controlled by a nameless entity, which shapes its perception of trustworthiness based on the overall perceived trustworthiness. With this in mind, we can argue that MPC enhances trustworthiness perceptions of data contribution applications. Therefore, we propose the following hypothesis:

> **H2: Perceived trustworthiness of an MPC-enabled application is greater than the perceived trustworthiness of a TTP-based application.**

In the Information Systems (IS) literature, trust is usually a strong predictor of behavior. However, we would like to understand how this relates to the case of MPC. It is self-explanatory that no party is expected to contribute data through an MPC application, which is perceived as untrustworthy and already clear from the data perspective (loss of data). We can also explain through the lens of social exchange theory (Cook & Rice, 2006). While trust in the social exchange theory is intuitively an interpersonal phenomenon, it is extended by many scholars to an organizational level (Young-Ybarra & Wiersema, 1999). However, trust is still limited to a dyadic relationship, even though this is fundamentally the aspect being addressed.

Although we have argued that trust between the different contributors becomes less relevant, the application owner (or "the MPC application service provider") is still essential. A form of partnership is established where the trustor (contributor) becomes dependent on the trustee (the application owner). In the context of partnership, Zaheer and Venkatraman (1995) characterize trust-based dependability, predictability, and faith. Even though this construct of trust is based on strategic partnerships, it can be conceptualized in terms of an MPC application: dependability refers to one's beliefs that the application is designed to function in the best interest of the contributors; predictability refers to the belief that the application functions according to claims made, and; faith refers to the belief that the trustee does not behave opportunistically. Thus, a positive perception of trustworthiness as a construct comprised of these three components is required for contributing data over an MPC application. However, we should note that faith relates to the service provider (not part of the scope as previously described). Our key takeaway from the above is that an application's perceived trustworthiness is an important item of consideration.

H2a : Perceived trustworthiness of a data contribution application is considered an important aspect.

From D2.4, we found that the effect that MPC has on perceived security–to a great extent–is determined by the way the technology is presented. We can explain this relationship through the lens of the Communication Privacy Management Theory (CPMT), which is rule-based and posits costs (e.g., risk) and benefits (e.g., usefulness) that individuals develop to aid in decisions about whether to disclose private information. Although CPMT is limited to the individual level (e.g., see Petronio (1991)), the concept of boundary rule formation (boundary management) (Petronio, 2013) is borrowed. Conceptualized in terms of MPC, MPC can provide a means for boundary management and lower perceived risk and increase perceived control.

It should be noted that although not studied in this deliverable, MPC is perceived by the author as a technology that is much dependent on network-effect. The higher the number of responsible MPC applications, the more popular it becomes, fostering further diffusion of the technology and more acceptance–in case of high success factors. Simultaneously, from the same line of reasoning, negative associations can occur when the reverse is the case (i.e., irresponsible applications and low success factors). Therefore, the level of familiarity with MPC also affects perceived security. As explained, this can have both a positive and negative effect–although the latter is not expected due to assumed lack of familiarity with MPC amongst respondents. Altogether, we hypothesize that:

H3 : Perceived security of an MPC-enabled application is greater than the perceived security of a TTP-based application.

MPC is, in broad terms, a security technology. However, there is no international or widely accepted security criteria or standard at this point. Therefore, when managers are faced with this emerging technology, it is expected that they are more likely to base their judgment on their perception. Given that MPC's value in terms of security is not apparent to the contributor, emphasis on perception is further enhanced. As a result, whether one will contribute protected data via MPC is, to a great extent, determined by MPC's perceived security. In fact, security is perceived as the main goal of MPC. Therefore, the direct primary utility provided by MPC is its ability to enable confidential data sharing. Thereby, it is unlikely that an organization contributes protected data in case of negative perceptions of security. As a result, the conjecture is that perceived security, to a great extent, determines the willingness to contribute data via MPC. Hence, we hypothesize that:

H3a : Perceived security of a data contribution application is considered an important aspect.

A person may be willing to contribute data through MPC, depending on the type of data shared. Whether this person views MPC as a solution depends on whether he/she perceived advantage provided by MPC concerning alternatives (i.e., the relative advantage of MPC). However, if one is not familiar with conventional data transactions or interoperability issues, they may not perceive an advantage from MPC's use. The reason is that they are not aware of the implications of conventional data sharing solutions. In such a case, the perceived relative advantage is opaque and might not significantly affect the willingness to contribute through MPC. Since there is no clear direction on the effect of MPC on relative advantage, the following hypothesis is proposed:

H4 : Perceived relative advantage of an MPC-enabled application is equal to the perceived relative advantage of a TTP-based application.

Similarly, the importance of relative advantage on willingness to contribute data via MPC depends on the degree of familiarity with conventional data transactions or interoperability issues. What can also affect the willingness to contribute data via MPC is the degree to which a party needs to share but is faced with technological barriers. As Kanger and Pruulmann-Vengerfeldt (2015) point out, if MPC's perceived advantage does not seem pressing to the organization, they might not consider MPC for the given task. To some extent, this is similar to "perceived benefits" in the boundary rule formation, as discussed in Petronio (2013). In the context of Petronio (2013), perceived benefits effects willingness to disclose personal information. Therefore the following hypothesis is formulated:

> **H4a : Perceived relative advantage of a data contribution application is considered an important aspect.**

Based on the elaboration of the three variables under study and the proposed hypotheses above, we composed the following conceptual model (see Figure 4). It is worth noting that this model only illustrates the relation between antecedents of data contribution (i.e., H2a, H3a, H4a) and not the comparison between MPC and non-MPC solution (i.e., H1, H2, H3, H4). Nevertheless, we will test all hypotheses in the experiment through the developed mock-up.

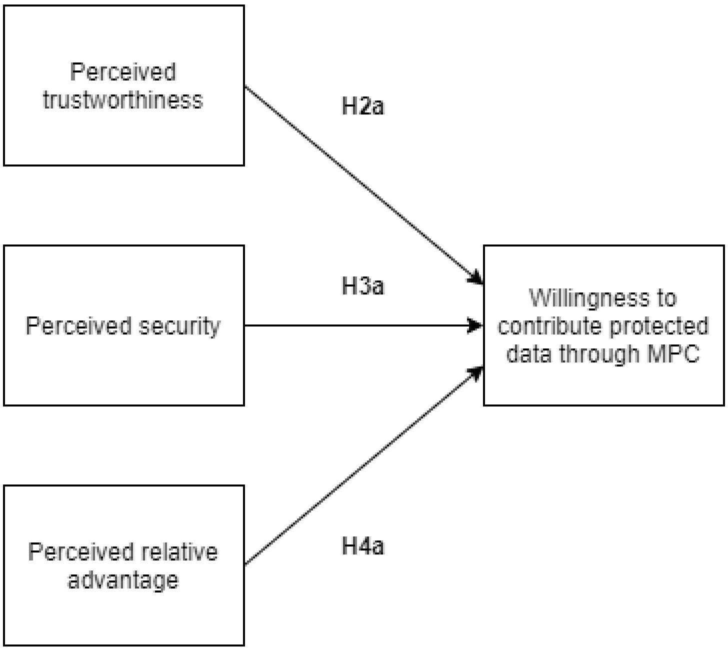

Perceived trustworthiness
H2a
Perceived security
H3a
Willingness to contribute protected data through MPC
Perceived relative advantage
H4a

Figure 4 Conceptual model

3. Demonstration platform

In this section, the structure and development process of the demonstration platform is described. This demonstration platform is used for the treatment of the experiment. It comprises two main parts: the platform and content. The platform is a web application that allows input parties to (remotely) access the content for treatments. In section 3.1, the demonstration platform's overall goal is described. Through a persona, respondents see the workings of the application in practice. Hence, in section 3.2, the content is framed in line with the use-case. The application (based on the use-case) is a working mock-up[1] that will be described in section 3.3.

3.1 Goal

The purpose of this study is to understand how MPC affects the willingness to contribute protected data. However, there is a lack of case studies on the perceptions of MPC. Given the phase of MPC development, there is also a lack of awareness of MPC in general amongst industry professionals. Thus there is a need to educate. The fundamental goal of the demonstration platform is to educate potential adopters. This approach is based on an "educate niche strategy" (Ortt, Langley, and Pals, 2013).

3.2 Use-case

A use-case is a deployment of an MPC application (such as those described in Section 2.2). Since MPC is assumed to be unknown to respondents, the use-case must be easy to enact while making clear that it concerns protected data. The use-case of "performance benchmarking" in distribution centers (DC) (presented in Section 2.2) is suited for this purpose.

At the moment, an objective overview that showcases DC performance concerning the different compositions of machines, equipment, and technology amongst warehouses is lacking. While it may seem not to be the case, information concerning the comparison of operational efficiency amongst warehouses is scarce. We based this argument on quality and insights and not the number of comparison reports available on the market. For instance, a comparison of ratio-based indicators, while often used by some companies, are considered highly misleading (Hackman, Frazelle, Griffin, Griffin, & Vlasta, 2001). Warehouses are wishing to improve usually approach solution providers with their wishes and demand. HoweverHoweverHowever, each solution provider 'sells' their solution, resulting in the bias of the proposals. Nevertheless, what is lacking is an objective overview of how different solutions (actually) perform.

With this in mind, the proposed output of the application is a report that provides concrete performance indicators covering multiple dimensions to provide a meaningful overview of industry performance. An example of a partial output of the MPC application used for the use-case is shown (see Figure 5). This graph is meant to give a concrete example of the output.

[1] For replicability and reproducibility, the mock-up and demonstration platform are publicly available at https://github.com/sitWolf/mpc-mock-up and the Safe-DEED github (https://github.com/Safe-DEED/mpc-mock-up)

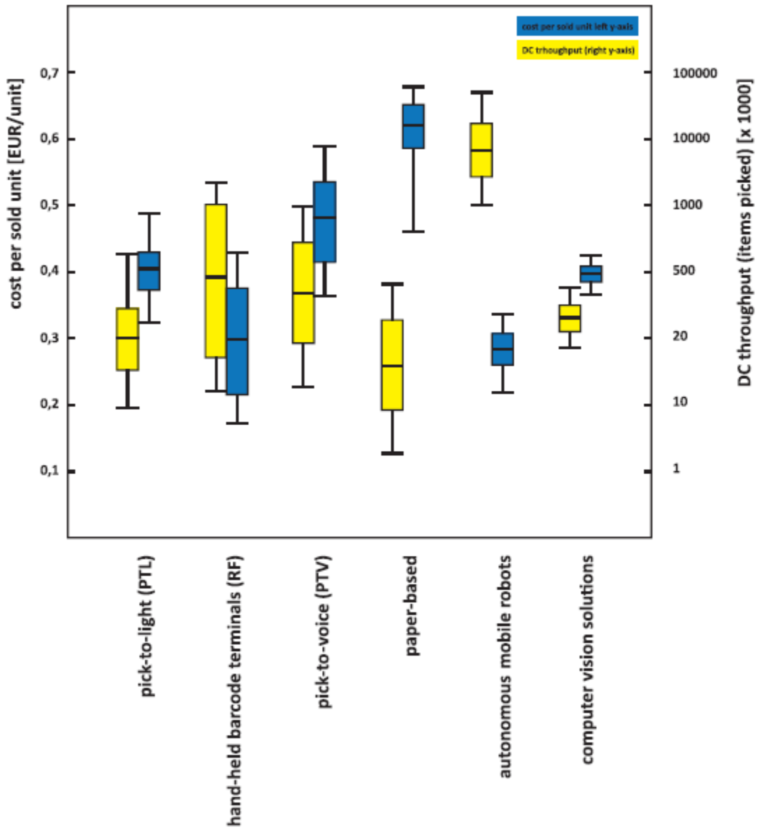


Figure 5 For illustrative purpose only: an exemplary plot of output generated by the MPC application.

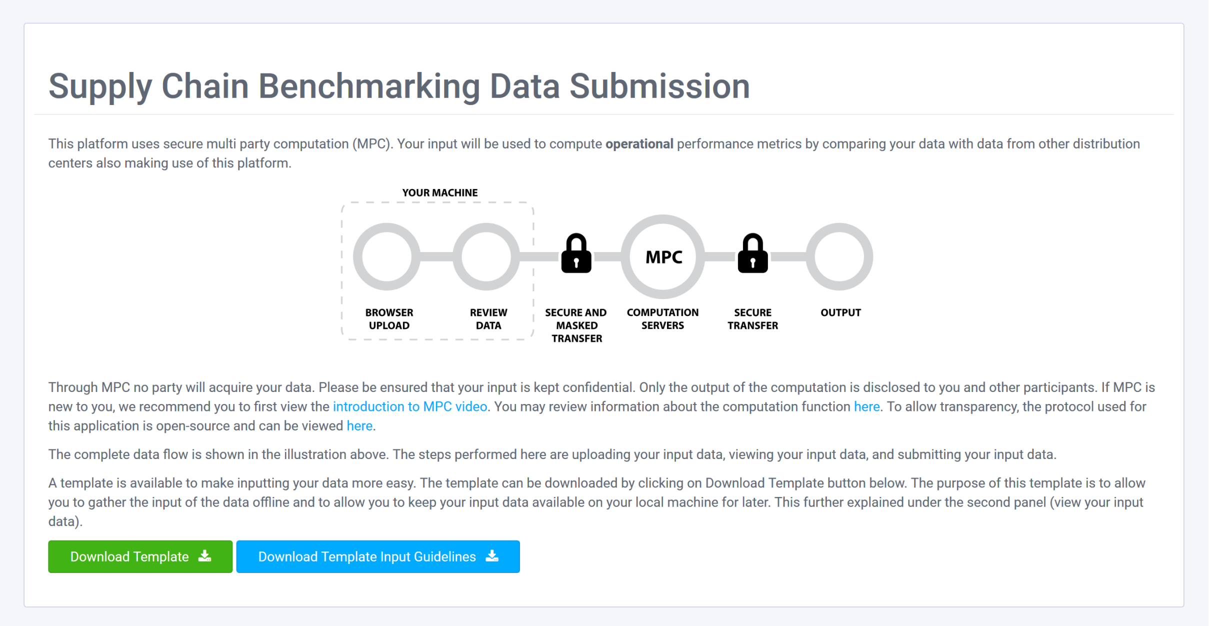
Using conventional solutions, the type of data required to provide meaningful insights is likely to raise confidentiality concerns that result in companies refraining from sharing data. This statement is based on the following reasoning. The input data needed (e.g., labor and capital costs, total revenue, warehouse throughput, incoming goods, items dispatched, warehouse utilization) to make the required computations to plot the information is internal information that can give away company strategies and show vulnerabilities. The input data, when disclosed, can be used by competitors to exploit (internal) vulnerabilities. A trusted party could solve this issue, however, with implications, as discussed in previous chapters. Needless to say, MPC provides a solution to this issue. The application-specific issues raised following the use of MPC are discussed in the next section.

The goal of the application is to enable corporate decision-makers to (1) become more proficient in assessing the value of efficiency-enhancing technologies; (2) be better capable in identifying performance gaps; (3) be better capable of re-engineering warehousing operations, and; (4) be better qualified in assessing actual industry performance.

3.3 Mock-up design

As previously mentioned, a real working application is not developed. The use-case is presented through a mock-up (i.e., non-working MPC application). The mock-up represents an MPC application that provides decision-makers with the distribution center (DC) performance indicators – as previously described.

Following an experimental design employed in this research, we require two applications that are used as a treatment. The experimental setup comprises two groups. One group is the MPC group; the second group is the TTP group. Hence one application is MPC based (MPC-enabled), and the other application is TTP based. The applications (i.e., the experimental treatments) for the two groups follow a common tread – with minimal changes between the two to rule out research bias. In this section, we describe how the two treatments are designed. First, we describe the overall structure of the applications, followed by a description of the content.



Supply Chain Benchmarking Data Submission

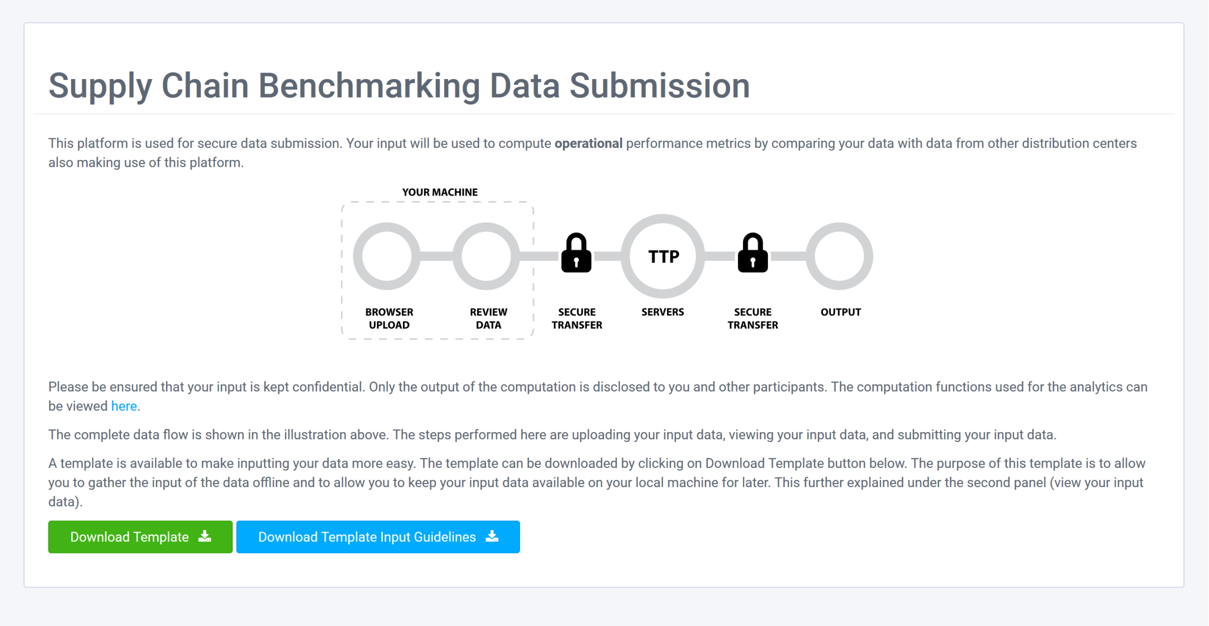
This platform uses secure multi party computation (MPC). Your input will be used to compute **operational** performance metrics by comparing your data with data from other distribution centers also making use of this platform.

Through MPC no party will acquire your data. Please be ensured that your input is kept confidential. Only the output of the computation is disclosed to you and other participants. If MPC is new to you, we recommend you to first view the introduction to MPC video. You may review information about the computation function here. To allow transparency, the protocol used for this application is open-source and can be viewed here.

The complete data flow is shown in the illustration above. The steps performed here are uploading your input data, viewing your input data, and submitting your input data.

A template is available to make inputting your data more easy. The template can be downloaded by clicking on Download Template button below. The purpose of this template is to allow you to gather the input of the data offline and to allow you to keep your input data available on your local machine for later. This further explained under the second panel (view your input data).

Figure 6 Start panel screenshot for MPC application



Supply Chain Benchmarking Data Submission

This platform is used for secure data submission. Your input will be used to compute **operational** performance metrics by comparing your data with data from other distribution centers also making use of this platform.

Please be ensured that your input is kept confidential. Only the output of the computation is disclosed to you and other participants. The computation functions used for the analytics can be viewed here.

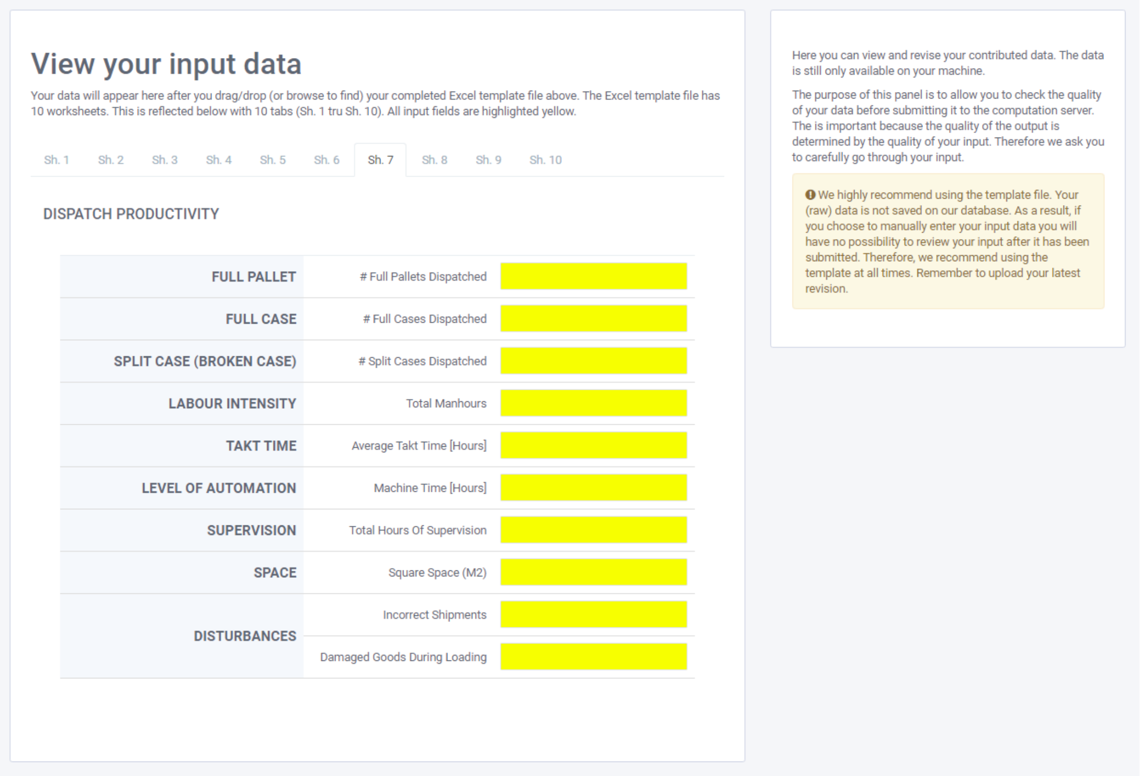
The complete data flow is shown in the illustration above. The steps performed here are uploading your input data, viewing your input data, and submitting your input data.

A template is available to make inputting your data more easy. The template can be downloaded by clicking on Download Template button below. The purpose of this template is to allow you to gather the input of the data offline and to allow you to keep your input data available on your local machine for later. This further explained under the second panel (view your input data).

Figure 7 Start panel screenshot for TTP application

The structure for the two treatments is identical. Both treatments have four panels. The first panel describes the application, including an overview of the sources. The second panel comprises the input panel. This panel has a side panel with additional information. The third panel is the review data panel. The fourth panel is the “review and submit data” panel. These panels’ content differs slightly since one treatment represents an MPC-application, whereas the other is a TTP application. The content and differences are described in the following paragraph.

Regarding the content, in the first panel, a description is provided of the sources behind the application and the data flow. See Figure 6 and Figure 7 for a comparison between the panels. As can be noted, we have attempted to mirror both cases. We do this by asking, “What is the intent of the sentence or figure, and is this intent equally reflected in both applications?”. Take, for instance, the first line. For the MPC group, this is: *“This platform uses multi-party computation for secure data contribution. Your input will be used …use of this platform”*. For the TTP group, this is: *“This platform uses a trusted third party for secure data contribution. Your input will be used…use of this platform”*. The intent is to induce a feeling of trust based on the measure used, which is reflected in both descriptions.



View your input data

Your data will appear here after you drag/drop (or browse to find) your completed Excel template file above. The Excel template file has 10 worksheets. This is reflected below with 10 tabs (Sh. 1 tru Sh. 10). All input fields are highlighted yellow.

DISPATCH PRODUCTIVITY

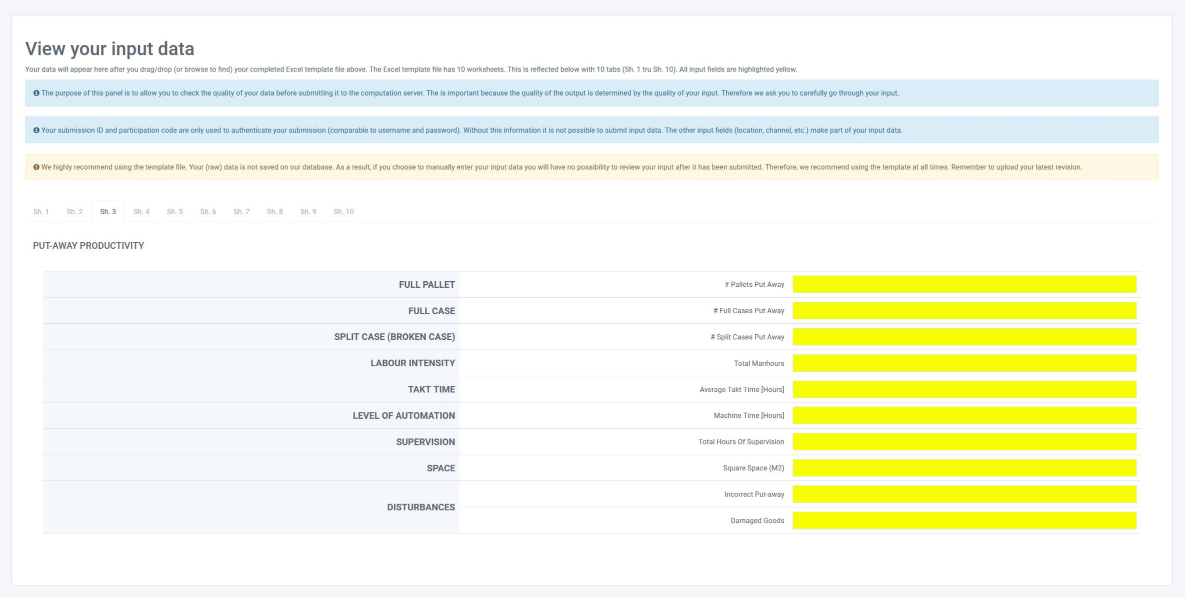
FULL PALLET	# Full Pallets Dispatched
FULL CASE	# Full Cases Dispatched
SPLIT CASE (BROKEN CASE)	# Split Cases Dispatched
LABOUR INTENSITY	Total Manhours
TAKT TIME	Average Takt Time [Hours]
LEVEL OF AUTOMATION	Machine Time [Hours]
SUPERVISION	Total Hours Of Supervision
SPACE	Square Space (M2)
DISTURBANCES	Incorrect Shipments
	Damaged Goods During Loading

Here you can view and revise your contributed data. The data is still only available on your machine.

The purpose of this panel is to allow you to check the quality of your data before submitting it to the computation server. The is important because the quality of the output is determined by the quality of your input. Therefore we ask you to carefully go through your input.

❗ We highly recommend using the template file. Your (raw) data is not saved on our database. As a result, if you choose to manually enter your input data you will have no possibility to review your input after it has been submitted. Therefore, we recommend using the template at all times. Remember to upload your latest revision.

Figure 8 Panel to review input data



View your input data

Your data will appear here after you drag/drop (or browse to find) your completed Excel template file above. The Excel template file has 10 worksheets. This is reflected below with 10 tabs (Sh. 1 tru Sh. 10). All input fields are highlighted yellow.

ℹ The purpose of this panel is to allow you to check the quality of your data before submitting it to the computation server. The is important because the quality of the output is determined by the quality of your input. Therefore we ask you to carefully go through your input.

ℹ Your submission ID and participation code are only used to authenticate your submission (comparable to username and password). Without this information it is not possible to submit input data. The other input fields (location, channel, etc.) make part of your input data.

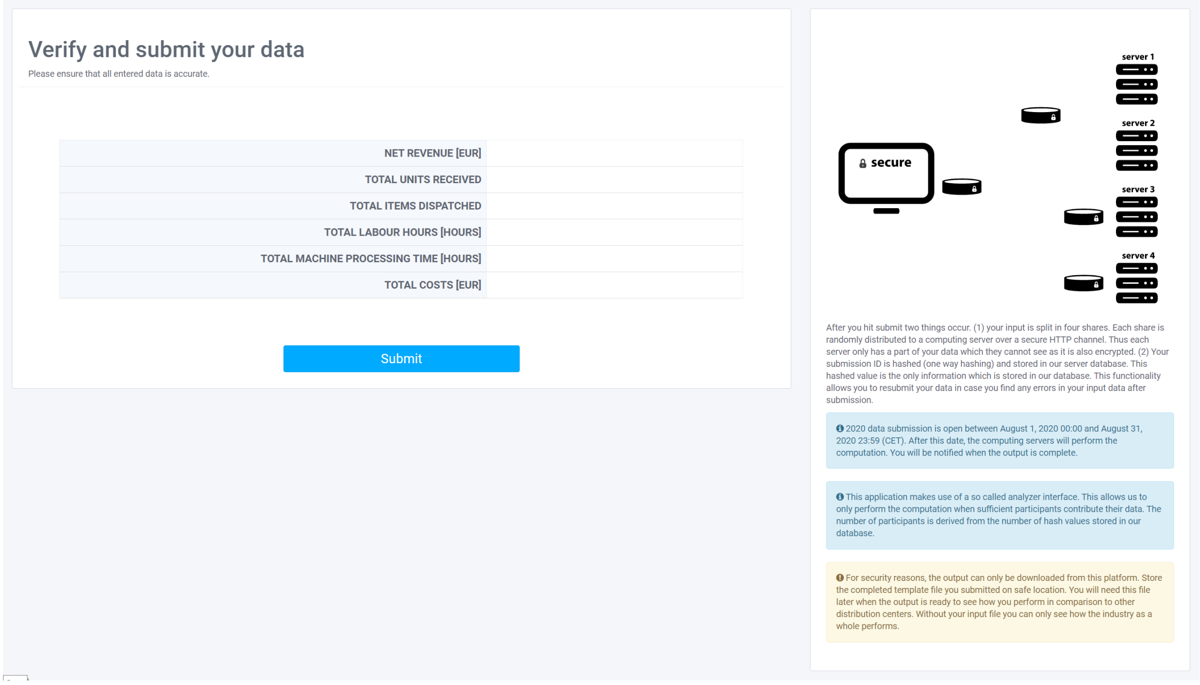
❗ We highly recommend using the template file. Your (raw) data is not saved on our database. As a result, if you choose to manually enter your input data you will have no possibility to review your input after it has been submitted. Therefore, we recommend using the template at all times. Remember to upload your latest revision.

PUT-AWAY PRODUCTIVITY

FULL PALLET	# Pallets Put Away
FULL CASE	# Full Cases Put Away
SPLIT CASE (BROKEN CASE)	# Split Cases Put Away
LABOUR INTENSITY	Total Manhours
TAKT TIME	Average Takt Time [Hours]
LEVEL OF AUTOMATION	Machine Time [Hours]
SUPERVISION	Total Hours Of Supervision
SPACE	Square Space (M2)
DISTURBANCES	Incorrect Put-away
	Damaged Goods

Figure 9 View input data panel for MPC and TTP application

The main difference between the two panels is that the MPC group provides a generic high-level introductory video to MPC[2]. Generic refers to a video that can be used for any MPC application. This video is necessary since MPC is expected to be unknown to most contributors. Other than that, MPC code is open source, and for the TTP application, only the functions used for the aggregate analysis are accessible. We do this because the MPC application functions independently from the application owner (or service provider), while for the TTP, the input data is held by the TTP. The second (see Figure 8) and third panel (see Figure 9) is the same for both groups. The data panels are the same for the two groups since the features used to provide functionality for both MPC and non-MPC based applications.



Verify and submit your data

Please ensure that all entered data is accurate.

NET REVENUE [EUR]	
TOTAL UNITS RECEIVED	
TOTAL ITEMS DISPATCHED	
TOTAL LABOUR HOURS [HOURS]	
TOTAL MACHINE PROCESSING TIME [HOURS]	
TOTAL COSTS [EUR]	

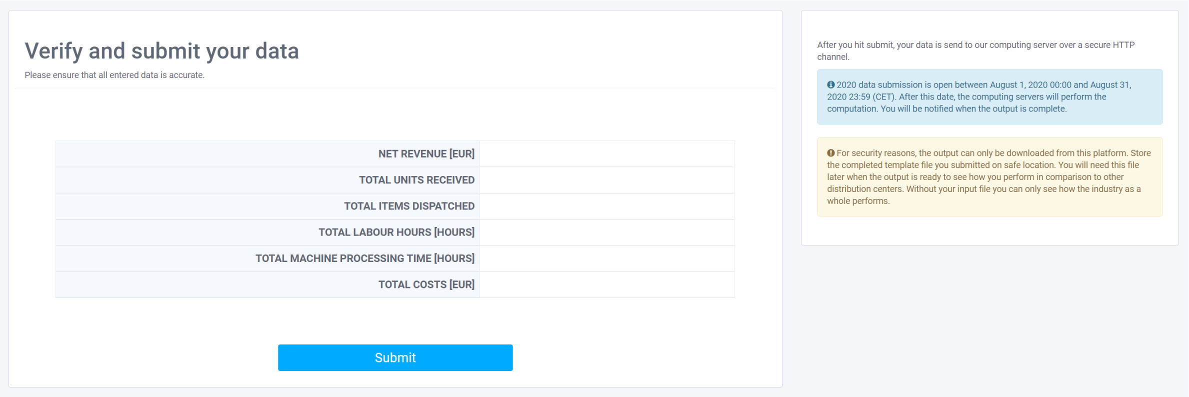
After you hit submit two things occur. (1) your input is split in four shares. Each share is randomly distributed to a computing server over a secure HTTP channel. Thus each server only has a part of your data which they cannot see as it is also encrypted. (2) Your submission ID is hashed (one way hashing) and stored in our server database. This hashed value is the only information which is stored in our database. This functionality allows you to resubmit your data in case you find any errors in your input data after submission.

ℹ 2020 data submission is open between August 1, 2020 00:00 and August 31, 2020 23:59 (CET). After this date, the computing servers will perform the computation. You will be notified when the output is complete.

ℹ This application makes use of a so called analyzer interface. This allows us to only perform the computation when sufficient participants contribute their data. The number of participants is derived from the number of hash values stored in our database.

❗ For security reasons, the output can only be downloaded from this platform. Store the completed template file you submitted on safe location. You will need this file later when the output is ready to see how you perform in comparison to other distribution centers. Without your input file you can only see how the industry as a whole performs.

Figure 10 Verify and submit input data panel screenshot for MPC application



Verify and submit your data

Please ensure that all entered data is accurate.

NET REVENUE [EUR]	
TOTAL UNITS RECEIVED	
TOTAL ITEMS DISPATCHED	
TOTAL LABOUR HOURS [HOURS]	
TOTAL MACHINE PROCESSING TIME [HOURS]	
TOTAL COSTS [EUR]	

After you hit submit, your data is send to our computing server over a secure HTTP channel.

ℹ 2020 data submission is open between August 1, 2020 00:00 and August 31, 2020 23:59 (CET). After this date, the computing servers will perform the computation. You will be notified when the output is complete.

❗ For security reasons, the output can only be downloaded from this platform. Store the completed template file you submitted on safe location. You will need this file later when the output is ready to see how you perform in comparison to other distribution centers. Without your input file you can only see how the industry as a whole performs.

Figure 11 Verify and submit input data panel screenshot for TTP application

In the fourth panel (verify and submit your data), the animated MPC illustration is removed for the TTP application (see Figure 10 and Figure 11). Although it makes sense in the MPC application that the service provider does not keep a copy of the raw data on its servers, we see no reason why such a feature would not make sense for the TTP-based application.

[2] The introductory video to MPC is available at the Safe-DEED YouTube channel: https://youtu.be/90jcXCHsBF0

Even though one might argue that it does not make sense not to temporarily store the data – since it is the raw data that is sent to the servers in the case of non-MPC – we can think of several reasons why this such feature could still be used. Thus, this information is the same. On the other hand, the information about the analyzer interface is removed. This feature does not make any sense since the service provider has the raw data upon submission.

4. Experiment

This deliverable aims to explore the effect MPC has on data sharing. Hence, a "cause-and-effect" methodology is needed. In this regard, we require a high internal validity to lay confidence in our findings. At the same time, we conducted this study in both a natural setting and a lab setting. Allowing participants to conduct the experiment in a natural setting ensures that the study also has external validity. We have described in section 1 that the unit of observation is the decision-maker or a person that affects decision making processes within organizations. Therefore, in section 4.1, we start with participant selection criteria for target respondents. Then, in section 4.2, the pool from which the respondents are acquired is described, followed by the description of the experimental design and setup in section 4.3. We conclude by describing the experimental procedure in section 4.4.

4.1 Measurement

Based on our conceptual model (see section 2.4), we derive 25 perceptually-based survey items for the experiment. Several questions (marked by an asterisk) can only be asked during the post-test. The word METHOD (in uppercase) must be replaced with MPC or TTP for each respective solution. We list our survey items in Table 1. In each survey item, respondents will rate their score using a 5-point Likert scale. A 5-point Likert scale is used because during testing of the experiment, a 7-point Likert scale–which was initially used–some respondents felt that it required more mental effort, potentially leading to cognitive overload in later phases of the experiment.

Construct	Dimension	Item wording
Trustworthiness	Observability of the data transaction process	The intent of the application is clear to me.
		The application clearly describes how my data is processed from data submission to output.
		The application provides a complete and detailed description of how METHOD is used to protect my data
	Perceived complexity of the application	Interaction with the application is clear and understandable.
		The descriptions of METHOD are complex.
		Understanding how the data is processed does not require a lot of my mental effort.
	Perceived trustworthiness of the application	Claims made by the application are clear and accurate.
		The application is open and transparent in how it protects my data.
		*I am satisfied with the trustworthiness of the METHOD application.
Security	Perceived risk	It feels safe contributing sensitive company data over the application.
		The use of METHOD gives me a feeling of security assurance.
	Perceived control over input data	Only I am able to view my contributed data.
		The service provider cannot examine my data beyond my control.
		I feel capable of using the application.
		My data cannot be accessed by other contributors.

	Perceived security of the application	I am satisfied with the security the METHOD provides.
Relative advantage	Perceived simplification of the data sharing process	The application provides a simple way to securely contribute data.
		The application does not require expertise from multiple organizational departments.
		The application provides an advantage over conventional data sharing practices.
		When contributing data, no other party knows about my participation.
		I feel less hesitant with contributing sensitive company data when using this METHOD application.
	Perceived relative advantage	*METHOD provides a simple solution to secure data contribution.
Willingness	Willingness to use the application	*I would be willing to use METHOD based on the solution it provides to secure data contribution.
		*I would be willing to use this application based on its trustworthiness.
		*I would be willing to use this application based on the security provided by METHOD.
		*Overall, if the output (the analytics) of the application provides sufficient value to my organization, then I would be willing to contribute sensitive company data over a METHOD application.

Table 1 Variables measured

4.2 Participants

In selecting our participants, some important factors are considered, such as the occupation and level of involvement in the evaluation, adoption, or implementation of these individuals. In the best case, the selection of respondents (seeking the "dominant coalition") requires multiple respondents (e.g., from several echelons of the organization) within each of the organizations under study (Tornatzky & Klein, 1982, p. 30). We will refer to the groups of respondents from several echelons of the organizations as batches. These batches comprise decision-makers with roles such as technology managers, business strategists, improvement managers, IT advisors, program managers, project managers, and project engineers.

We consider the best case batches discussed above as the "holy grail". To recruit such specific batches to conduct this experiment results in an expensive experimental setup. The fundamental problem is that the desired respondents (i.e., decision-makers) are 'expensive' because these are gold collar workers. It is expected that acquiring sufficient respondents in batches will require more time due to this study's experimental setup (discussed in the next section).

On the other hand, crowd-sourcing platforms make data acquisition more attainable in terms of costs. However, none provide effective ways to select 'groups' of respondents within the same organization. Nonetheless, there is the possibility to specify education level and occupation level– which can be used to specify a viable proxy. Therefore, data collection is broken up into two clusters: the proxy group and the "holy grail".

The first collection will be performed using Prolific[3], a crowd-sourcing platform used to reach a sufficient number of participants for the sample. Prolific does provide filters on educational level and occupation level. This feature is called *custom prescreening*. The education level filter, *Highest education level completed*, is set to Undergraduate degree (BA/BSc/other) AND Graduate degree (MA/MSc/MPhil/other) AND Doctorate degree (Ph.D./other). The occupation level, *Industry Role* is set to Upper Management AND Trained Professional AND Middle Management AND Junior Management.

The second collection will be performed in person in a lab setting. Here we make use of strong and weak ties. To increase the participation rate (response rate), we opt to perform the experiment at the respondent's location. Further information is not provided to protect the confidentiality of the respondents. Nonetheless, these respondents do represent the target group. However, the number of participants is expected to be lower.

4.3 Setup

We opt for the pre-test and post-test experimental and control group design. This approach allows comparison of participant groups and the measurement of the degree of change stemming from the treatment.

Participants will be randomly assigned (R) to one of two experimental groups. There will be two observations (O) for each group. These observations are captured by a questionnaire before (i.e., pre-test) the treatment (X) and after the treatment (i.e., post-test). The treatment (X) for the experimental group will be a supply chain performance benchmarking application. An overview of the experimental research design is presented in Table 2.

Groups	Pre-test	Treatment	Post-test
Group 1 ($R1$)	$O1$	$X1$	$O3$
Group 2 ($R2$)	$O2$	$X2$	$O4$

Table 2 Pre-test and post-test experimental and control group design

Treatment ($X1$) will represent an MPC application with all features discussed in the previous chapter. Treatment ($X2$) represents a "conventional" data sharing application. By conventional, we refer to a data transfer through a trusted third party (TTP). The difference between the two is that ($X1$) contains MPC-only related features and information, whereas ($X2$) contains TTP related information–making it a data-sharing platform. Still, both treatments follow a common thread and are identical in terms of information displayed and look and feel.

The experiment comprises a comparison of means. Based on estimates for TTP mean of 3 (neutral), an MPC mean of 4, σ of 1, α of .05, and β of .8, a minimal sample size of 22 is suggested (one-sided test) and 28 (two-sided test). Nevertheless, the rule of thumb indicates that the sample size should be at least 30 (Field, 2017, ch. 2). The minimal sample size is increased to 100 to increase power.

At the highest level of abstraction, the experiment comprises four parts. The first part is the pre-test, which is exactly the same for the two groups. In the pre-test, perceptions are measured based on expectations for a data contribution platform, indicating the respondent's initial anchor point and a reference that allows measurement of the interaction effect due to the application.

The second part is the treatment. The treatment for the two groups has minor differences. As previously discussed, the difference between the two groups is that one group has MPC related information, whereas the other has not. We approached this difference so that all features that would be possible even

[3] https://www.prolific.co/

with non-MPC applications are left untouched. The differences between the applications are discussed in the previous section. The differences in the questionnaire are discussed in the next sections.

The third part comprises the post-test. The post-test is similar for the two groups. The main difference is that for the questions, group 1 questions refer to “MPC application,” whereas group 2 refers to “TTP application”. Group 1 post-test includes an additional question to measure familiarity of MPC prior to conducting the study.

The fourth part contains the demographic questions, which are the same for the two groups. Questions related to demographics are presented at the end of the experiment to decrease cognitive overload and reduce non-response. We found that during the testing, the experiment required much concentration. Giving the demographic questions at the beginning made the questionnaire feel lengthy. Since the demographic questions are generic, not directly related to the experiment, and do not require mental effort, placing these at the end induced a more positive feeling– of nearing the questionnaire’s end.

4.4 Procedure

The complete experiment process flow is shown in Figure 12. First, participants are provided with an introduction to the study and provided with terms for conducting the experiment. Then, all respondents are presented with the pre-test. The pre-test is perfectly identical for both groups. Next, the respondent is presented with the experimental treatment. Herein, the respondent is randomly assigned to one of each group, followed by the corresponding post-test. The treatment and corresponding post-test are grouped into blocks. Thus, there are two blocks, one for each group. After the respondent has finished the block, he/she will continue with the demographic questions. We followed the same flow for the lab experiment and added an extra block at the end to ask questions on observations from the results and findings.

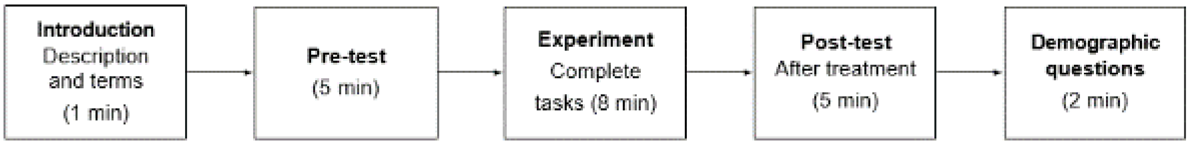


Figure 12 The (online) experiment process flow

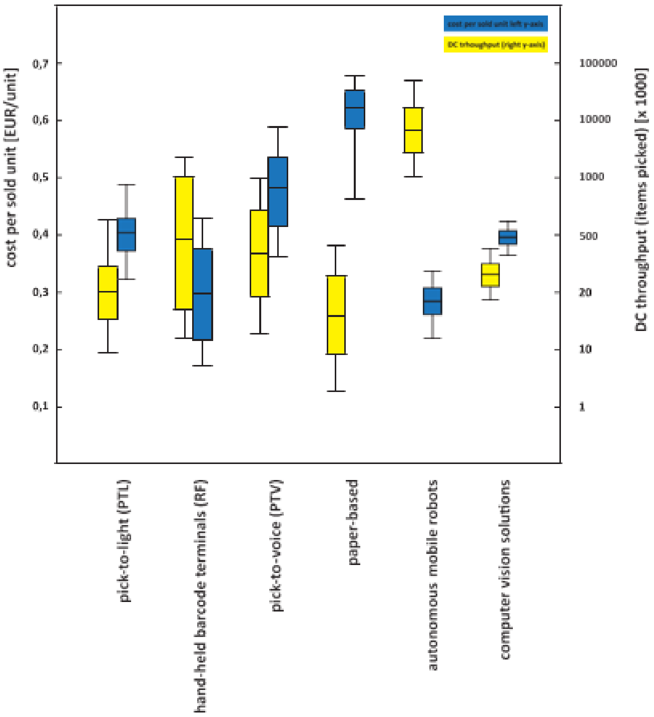
The treatment comprises a use-case that makes use of a persona, which is provided to the respondents. A persona is used to shape the context in which the application is used. A persona is used since MPC applications are likely to be built and designed for specific groups. Thus, the persona represents the users of the application. Through a persona, respondents can better understand user needs, which are not necessarily the same as theirs. Moreover, a persona allows the incorporation of assumptions in the design (Adlin & Pruitt, 2010). Hence, a persona is suited to incorporate previously made assumptions.

The persona description includes the role of an adopter and the problem this person faces, which is the same for both experimental groups. The persona is framed as follows:

> *You are a regional improvement manager responsible for the operational efficiency of the distribution center of your company. Your company is a well-known e-commerce player in the Netherlands and Belgium. You are constantly faced with industry challenges. Recently the question is raised, whether the distribution center can achieve full-scale same-day delivery.*
>
> *This question followed after consultancy firms addressed the need by consumers for faster delivery times. Your distributions center makes only use of labor (no machines) for the order fulfillment process. You know of the existence of many solutions offered on the market but have difficulty in understanding the operational and strategical benefits these solutions provide.*
>
> *You want to understand how the whole industry performs with respect to the different solutions available. You looked into how you could do this without harming your organization.*

Two scenarios are used–in coherence with the approach followed (MPC and TTP). The purpose of the scenario is to shape the context and guide users through the process. The use-case scenario description for the two experimental groups differ. Differences are highlighted yellow for group 1 (MPC) and red for group 2. Herein, texts with the same numbering replace each other for the respective group, whereas non-highlighted text is used for both groups. We attempted to provide the same level of objectiveness for both groups. Below is the description:

> *You found a [1]multi party computation [1]a trusted third party (TTP) application called PEBE (PErformance BEnchmarking) available for distribution centers. [2]You know that multi-party computation applications allow participants to share knowledge without sharing the underlying data. As a result, multi-party computation users contribute data and do not share their data - they only share knowledge, and their data is confidential by design. [2]You know that TTPs work under contracts or agreements to ensure confidentiality.*
>
> *This application requires the contribution of sensitive internal company data (protected data). This is data that may not be leaked. The company offering the benchmarking services provided a booklet with some examples of the analytics output generated. This is exactly the kind of information you need.*
>
> *This is your first time using the application. You want to submit your data but will carefully go through information provided by the application.*
>
> *(below graph is for illustrative purposes only. You do not need to understand the information presented for this study).*



For the experiment block in Figure 12, respondents are given several steps and tasks that need to be performed. These steps allow sufficient interaction with the application. To ensure that respondents have indeed completed the steps, they are provided a “code” after completion. Participants input this code in the questionnaire to indicate that the respondent has performed the steps.

5. Results

This chapter presents the results of the experiment[4]. First, the data collection process is described, along with the steps taken to ensure reliable data (section 5.1). Three channels were used to collect data. It is therefore needed to attest whether these datasets can be merged (section 5.2). Then, several checks are performed to evaluate the extent to which the respondents meet the decision-makers' profile (section 5.3). Subsequently, we report the correlation analysis results to test the importance-related hypotheses (section 5.4), followed by the testing of TTP-MPC-related hypotheses (section 5.5). Next, the treatment effects on each item are examined (section 5.6) to provide a better understanding of the impact of MPC on the different aspects. Then, a qualitative assessment is performed as a complement for quantitative analysis (section 5.7). Finally, a conclusion is drawn (section 5.8).

5.1 Data collection and data reliability

In total, 117 responses are collected, which comprises three datasets (see Table 3).

Source	N	Total %	Motive	Collection dates
Prolific	98	83.8	Incentive	July 7, 2020 - July 8, 2020
LinkedIn/Twitter	9	7.7	Voluntarily	July 8, 2020 - August 4, 2020
Lab setting	10	8.5	Voluntarily	July 16, 2020 and August 3, 2020

Table 3 Collected datasets (N = 117)

For the data collected via Prolific, we observed (real-time) how the progress proceeded after we published the questionnaire. During this process, we evaluated the responses using the following protocol for quality and reliability assurance:

- P1: Did the participant enter valid experiment codes?
- P2: Is the time taken to complete reasonable (> 14 min for Group 1 and > 10 min for group 2)?
- P3: Does the respondent meet the demographic requirements (educational and occupation requirements)?
- P4: Did the respondent provide consistent answers?

Data collection through Prolific took approximately 11 hours. In total, 12 responses were destroyed during the time: four responses were rejected and destroyed based on *P*1, two due to *P*2, four due to *P*3, and two due to *P*4. Upon rejection, this opened up new positions for other participants.

We missed identifying two responses that failed to meet criteria *P*3. These were later identified during the examination of the demographics. These are two responses that were removed after Prolific data collection, hence 98 responses. For what it is worth, these respondents confirmed our reasoning behind criteria *P*3: the participants have lower than undergraduate education, are skilled laborers (not skilled professionals), and difficulty understanding the application.

We also distribute the questionnaire within our network, resulting in 11 responses. Two responses were destroyed due to failing protocol item *P*1, leaving nine valid responses. Before data collection (one month) and during data collection, no events took place–of which we are aware of–that might have influenced the research results.

[4] For replicability and reproducibility, the dataset is publicly available at https://doi.org/10.4121/13102430.v1

5.2 Establishing the dataset

We performed a one-way analysis of variance (ANOVA) to compare the means of the three datasets for the variables. We do this to check whether the three datasets can be merged into a single dataset. We concluded that the three datasets could not be combined. The three datasets are considered significantly different on eight variables. Upon further examination of the means, it is found that the third dataset is the cause. Herein, trustworthiness related variables (for the MPC group) have been rated higher by the respondents in the third group. Therefore, we remove this dataset. The same test (comparable with an independent t-test) is then repeated for datasets 1 and 2. The output of this test shows a far from a significant difference in means. Therefore, it can be assumed that dataset 1 (Prolific) and 2 (LinkedIn/Twitter) comprise participants from the same population. This dataset is further used for this study.

5.3 Participant demographics

The final sample consists of 107 respondents, ranging from 21 to 54 years old, with an average age of 33 years and a standard deviation of 7.08. The majority of participants are skilled professionals (73.8%), while more than 90 percent possess an undergraduate degree or higher. As for the familiarity with MPC, almost 30% of the participant is not familiar with it.

Variable	Demographic	n	%
Age	21-29	46	43.0%
	30-39	43	40.2%
	40-49	14	13.1%
	> 49	3	2.8%
	Not available (missing value)	1	0.9%
Role at work	Middle management	7	6.5%
	Non-skilled	1	0.9%
	Skilled laborer	4	3.7%
	Skilled professional	79	73.8%
	Upper management	16	15.0%
Education level	No formal qualifications	0	0.0%
	Secondary education	2	1.9%
	High school diploma	4	3.7%
	Technical/Community college	3	2.8%
	Undergraduate (BA, BSc, other)	33	30.8%
	Graduate degree (MA, MSc, other)	52	48.6%
	Doctorate degree (PhD, other)	12	11.2%
	Not applicable/I do not know	1	0.9%
Familiarity with MPC	Not at all familiar	32	29.9%
	Slightly familiar	9	8.4%
	Somewhat familiar	9	8.4%
	Moderately familiar	3	2.8%
	Not available (missing value)	54	50.5%

Table 4 Demographic characteristics (N=117)

Next, we combine the respondents' role at work with industry function. This output shows a homogeneous distribution of industry domains and levels of seniority. Although the size of respondents in the technical domain comprises a large portion of the respondents' background, this favors the research results. These users are expected to have more affinity with data and more critical in assessing new technologies, and more likely to evaluate and assess new technologies. Thus, they contribute to the sample's representativeness.

Finally, we grouped organizational size with education level and the involvement in innovation with the role at work. These two outputs show that there is a sufficient degree of homogeneity. Also, no respondent is self-employed. In sum, after removing two responses, we can reasonably conclude that participants fit the selection proxy criteria related to being a decision-maker or having input on decision-making processes.

5.4 Correlation analysis

To recall, in this exploratory study, we seek to understand the effect MPC has on willingness to contribute protected data. To further enhance our understanding of this method, we examine the importance of the constructs (trustworthiness, security, and relative advantage) on willingness to contribute protected data. Moreover, we aim to understand how the different aspects (e.g., observability) are related to the constructs. We have employed a correlation analysis to address both of these questions.

In essence, the constructs, perceived trustworthiness, perceived security, and perceived relative advantage, are overarching higher-order constructs. In this study, it is not our aim to perform structural equation modeling. Instead, we view the main and sub-constructs as two separate models, which is possible because users were asked to rate their perceptions of the different aspects of the questionnaire and rate their willingness to contribute protected data based on the respective constructs. Concerning the latter, these questions are marked by an asterisk in Table 1.

Polychoric correlation (Olsson, 1979) is used for the correlation analysis due to PCA's limitations, which makes it not suited for Likert scales (Rigdon & Ferguson, 1991). Likert scale makes it challenging, if not impossible, to meet the assumption of homoscedasticity. Residuals may be randomly dispersed throughout the plot yet remain clustered. For the polychoric correlation, Baglin (2014) is used to guide the tests. The test is run using the program FACTOR[5]. Despite the above discussion, we have run the test using PCA. It can be observed that, in general, the polychoric correlations provide more conservative results.

Before conducting the analysis, several items for the trustworthiness construct are refactored. The components established are defined as perceived transparency (C1) and perceived coherence (C2), in lieu of, respectively, perceived observability and perceived complexity. Perceived transparency refers to the extent to which the application is precise in protecting the contributor's data. Perceived coherence refers to the application being clear in its intent and consistent with the presentation of information. This is reflected in the items (see Table 5 and Table 6).

Item	Rotation 1		Rotation 2		Bca	
	Component		Component			
	C1	C2	C1	C2	Lwr.	Uppr.
1 The intent of the application is clear to me	0.337	0.630		0.644	0.357	0.828
2 The application clearly describes how my data is processed from data submission to output	0.751		0.737		0.490	0.867
3 The application provides a complete and detailed description of how METHOD is used to protect my data	0.953		0.927		0.822	0.981

[5] http://psico.fcep.urv.es/utilitats/factor/index.html

4 Interaction with the application is clear and understandable		0.783		0.777	0.391	0.907
5 The descriptions of METHOD are complex		0.845		0.816	0.551	0.972
6 Understanding how the data is processed does not require a lot of my mental effort		0.727		0.725	0.414	0.873
7 Claims made by the application are clear and accurate**	0.407	0.564				
8 The application is open and transparent in how it protects my data	0.941		0.941		0.818	0.979

**Item was removed; a small difference in factor loading between components.

Table 5 Perceived trustworthiness: factor loadings

Component	Variance	Proportion of Variance	Reliability	Factor Determinancy Index
Perceived transparency (C1)	2.539	0.363	0.926	0.962
Perceived coherence (C2)	2.317	0.331	0.859	0.927

Table 6 Perceived trustworthiness: explained variance and reliability of rotated components

A noteworthy mention is that the item "The application does not require expertise from multiple organizational departments" is removed because it seems not a good indicator for the construct. We based this decision on the results of the qualitative assessment. We also found that the item "I feel capable of using the application" is also an inaccurate measure of perceived control. This item was found less important in willingness to contribute; however, it seems more important in the context of willingness to use (implementation), which puts focus on the end-users.

Next, we check the convergent and discriminant validity. The model's VIF values are all well below 10, and the tolerance all well above 0.2. Moreover, from the correlation table, it is also clear that there is no extremely high correlation (r>0.9) (Hair, Black, Babin, & Anderson, 2014, p. 196). Finally, concerning discriminant validity, it is observed that the inter-factors correlation shows that the predictors do not show high correlations. Hence, we can conclude that convergent and discriminant validity is provided. It is also shown that the data is robust to CMV. Our prediction model provides a good fit, while it seems that the perceived relative advantage is not a strong predictor.

As for the result, the correlation analysis showed that there is a correlation between perceived trustworthiness and perceived willingness to contribute (r=0,694, p<0.001) as well as between perceived security and perceived willingness to contribute (r=0,671, p<0.001). These are considered large effects (r>0.5) (Field, 2017, ch.2), which reflect important aspects (our cut-off point). However, a weak to a medium correlation (r=0,318, p<0.001) is reported between perceived relative advantage and perceived willingness to contribute. Moreover, a medium correlation of (r=0,405, p<0.001) is reported between perceived relative advantage and perception solution MPC provides. This result further indicates that the perceived relative advantage is not the primary concern, which also becomes clearer when comparing these values with the trustworthiness and security pairs.

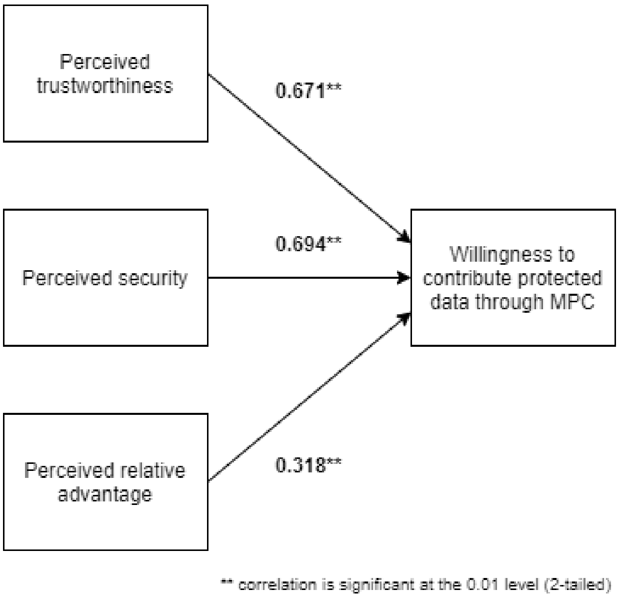

Perceived trustworthiness
0.671**
Perceived security
0.694**
Willingness to contribute protected data through MPC
Perceived relative advantage
0.318**
** correlation is significant at the 0.01 level (2-tailed)

Figure 13 Research model: polychoric correlations for complete sample (N=106)

An overview of the polychoric correlations is provided in Figure 13. From the values reported, we find evidence to **support hypotheses H2a and H3a**. However, we are unable to accept hypotheses H4a due to insufficient correlation.

5.5 Hypotheses testing

In this section, we test the hypothesis to fulfill our primary research objective. First, we analyze the extent to which MPC changes perception concerning willingness to contribute data. Then, we analyze the extent to which MPC affects the perception of trustworthiness, relative advantage, and security. Upon running the independent t-test, in some cases, Levene's test indicates that the two groups' variances are not equal. Put differently, the significance suggests that the assumption of homogeneity of variance is violated. Given that the data is acquired from the same population and that the sample sizes are the same size, there is a good reason to ignore Levene's test results (Stevens, 2016, ch. 6). Therefore the t-tests are ran using bootstrap (robust test) (Field, 2017, ch. 10).

In testing H1 (*willingness to contribute*), we should note that the question that measures willingness to contribute has only been measured in the post-test for both experimental groups. These groups can be compared, indicating the effect of the MPC. For testing the effect sizes for the two independent means (two experimental groups), we first performed a Bayesian comparison of means. On average, participants given an MPC application (N=53) are more willing to contribute data (M=3.924, SE=.080) than those given a TTP application (N=53) (M=3.604, SE=.108). The prior distributions for the group means were set to a mean of 3 and a standard deviation of 0.35 for the TTP group, and a mean of 4 and a standard deviation of 0.35 for the MPC group. The Bayes factor was estimated using Gönen's method with a prior difference between means of 1 with a variance of 0.25. The Bayesian estimate of the true difference between means was 0.3134, 95% confidence interval [0.075, 0.594]. The associated Bayes factor, BF01=3.144, suggested that the data were moderately more probable under the alternative hypothesis than the null.

Then, we performed an independent t-test using bootstrap. The result suggests that the homogeneity of variance assumption was not met (p=.001). On average, participants given an MPC application (N=53) are more willing to contribute data (M=3.924, SE=.080) than those given a TTP application (N=53) (M=3.604, SE=.108). This difference, .321, bias-corrected and accelerated (BCa) 95% confidence interval (CI) [0.052, 0.589], was significant t(95.5)=2.372, p=0.020 (two-tailed), and a Cohen's d effect of d=0.460 represents a 'medium' effect size. Thereby we find evidence to **support hypothesis H1**.

Like the willingness to contribute, the overall perception of trustworthiness, relative advantage, and security are measured post-test. Thus, measuring the effect of MPC over TTP is done similarly to the above. The Bayesian comparison of means is not performed here since we have no prior estimates.

An independent t-test is used to test H2 (*trustworthiness*). The robust test result indicates that the homogeneity of variance assumption was not met (p=.059). On average, participants given an MPC application (N=53) perceive a higher level of trustworthiness (M=3.849, SE=.102) than those given a TTP application (N=53) (M=3.585, SE=.112). This difference, (.264, 95% confidence interval (CI) [-.037, .565]), was not significant t(104)=1.738, p=.085 (two-tailed). Based on the two-tailed results, we cannot accept the alternate hypothesis.

However, to avoid making a type two error and increase power, a one-tailed approach is used. The critical values are t(104)[one-tailed]=1.660, and t(104)[two-tailed]=1.983. In SPSS, an independent t-test is used with a 90% confidence interval (one end of the distribution). The results of the one-tailed test indicate that, on average, participants given an MPC application (N=53) perceive a higher level of trustworthiness (M=3.849, SE=.102) than those given a TTP application (N=53) (M=3.585, SE=.112). This difference (.264, 90% confidence interval (CI) [.019, .516]) was significant t(104)=1.738, p=.043a (one-tailed). Thereby we find evidence to **support hypothesis H2**. A Cohen's d effect of d=0.408 represents a 'medium' effect size.

We also use an independent t-test to test H3 (*security*). The homogeneity of variance assumption was met (p=.550). On average, participants given an MPC application perceive a higher relative advantage (M=4.151, SE=.106) than those given a TTP application (M=3.340, SE=.093). This difference (.882, bias-corrected and accelerated (BCa) 95% confidence interval (CI) [.532, 1.090]) was significant t(104)=5.76, p<.001. Thereby we find evidence to **support hypothesis H3** with a 'very large' effect size (a Cohen's d effect of d=1.197).

As for H4 (*relative advantage*), the homogeneity of variance assumption was not met (p=.009). On average, participants given an MPC application (N=53) perceive a higher level of relative advantage (M=3.943, SE=.073) than those given a TTP application (N=53) (M=3.924, SE=.104). This difference (.018, bias-corrected and accelerated (BCa) 95% confidence interval (CI) [-.233, .271]) was not significant t(93.6)=.148, p=.882 (two-tailed). Thereby we find evidence to **support hypothesis H4**. It represented a Cohen's d effect of d=.03 (negligible effect size).

Initially, our data indicate that MPC does not affect perceived relative advantage (negligible Cohen's d). However, this is not exactly true. While it was not possible to measure trustworthiness and security in the pre-test, it was possible to do this with relative advantage. In the pre-test, respondents were asked to rate, "The application *should provide* a simple way to securely contribute data." Whereas in the post-test, they were asked to rate, "The application *provides* a simple way to securely contribute data." We report a significant difference by using a t-test. However, this question concerns the application as a whole. In contrast, the question used for testing the hypothesis is specific to MPC. We then evaluate whether we can use the pre-test scores of the application-related question for the MPC-related question. The values are compared before drawing any conclusions. We can see that substituting the post-scores will lead to an even higher F-score. Therefore, after manipulating the data, we can assume that MPC does affect willingness to contribute compared to TTP.

5.6 Interaction effect

The interaction effect can be measured by $[(O3 - O1) - (O2 - O4)]$. This comprises a two by two matrix: one between-subject independent factor (experimental groups) with two levels (MPC and TTP) and two within-subject independent variables (pre-test score and post-test score). Hence, we use a mixed-design analysis of variance model (Field, 2017, ch. 16), which is also called split-plot or two-way repeated-measures ANOVA. Overall, we can observe that respondents have high apparent needs. Ratings are found near the maximum (five-point Likert scale). Hence, it is expected that post-test ratings are lower than pre-test scores. Still, a comparison between TTP and MPC shows the extent to which the solutions affect perceptions on the different factors (see Figure 14-Figure 20).

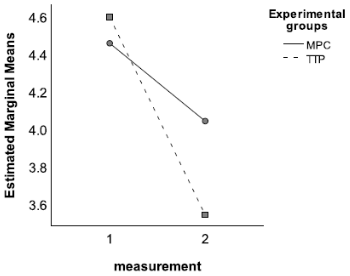


Figure 14 The application clearly describes how my data is processed from data submission to output. F(1,105)=8.017, p=.006

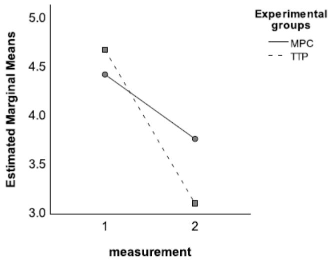


Figure 15 The application provides a complete and detailed description of how METHOD is used to protect my data. F(1,105)=15.315, p<.001

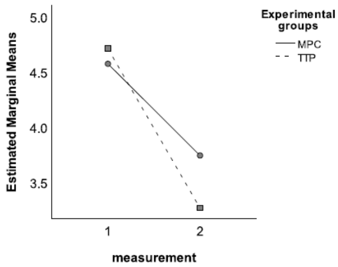


Figure 16 The application is open and transparent in how it protects my data. F(1,105)=8.629, p=.004

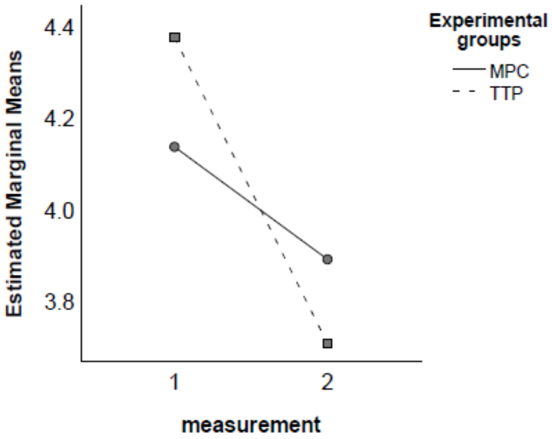


Figure 17 The application must provide a simple way to securely contribute data. F(1,105)=4.541, p=.035

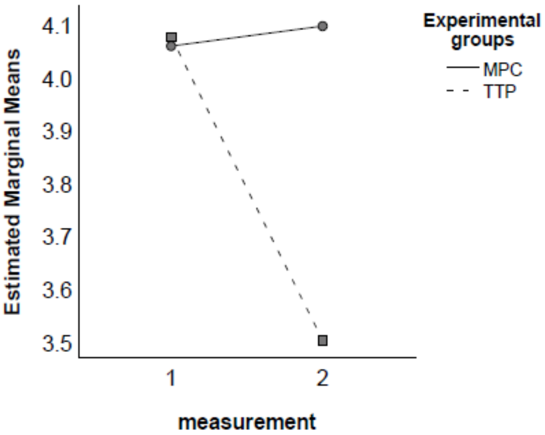


Figure 18 The application must provide an advantage over conventional data sharing practices. F(1,105)=9.813, p=.002

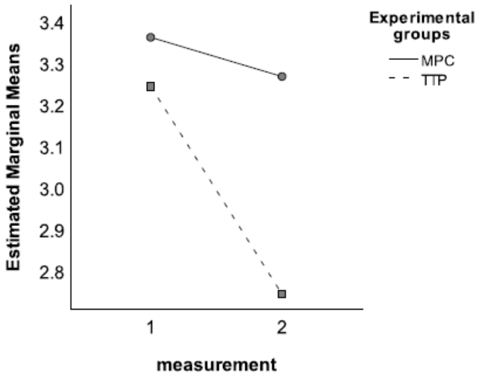


Figure 19 The descriptions of the METHOD are complex. F(1,105)=2.009, p=.159

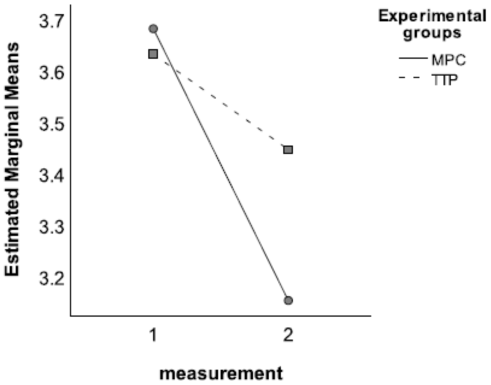


Figure 20 Understanding how the data is processed does not require a lot of my mental effort. F(1,105)=2.000, p=.160

Next, we will discuss the outputs of trustworthiness and security-related variables. First, for trustworthiness, three variables indicated a significant interaction effect. MPC significantly interacted with the degree to which respondents:

- perceived the complete data contribution process, F(1,105)=8.017, p=.006;
- perceived the completeness of the information regarding the protection of submitted data, F(1,105)=15.315, p<.001; and
- perceived the transparency in protecting data, F(1,105)=5.046, p=.004.

Second, for relative advantage, MPC significantly interacts with:

- the perceived advantage over conventional data sharing application, F(1,105)=9.813, p=.002; and
- perceived simplicity of the application provides for secure data-contribution, F(1,105)=4.541, p=.035.

Third and final, for security, the difference between MPC and TTP for all of the separate items are not statistically significant.

Finally, we compare outputs of MPC's interaction effect with the question *"the descriptions of the METHOD are complex"* and *"understanding how the data is processed does not require a lot of my mental effort"*. While there is no statistically significant interaction effect, these two outputs indicate that MPC introduces more complexity to the data contribution process. The tests indicate, respectively, a main effect of MPC F(1,105)=4.313, p=0.040 and F(1,105)=8.646, p=0.004.

5.7 Qualitative assessment

We conducted a qualitative study through follow-up interviews and observations to explore the potential reduction fallacy. The reason is that data is collected at an individual level (unit of observation), while we draw conclusions at an organizational level (unit of analysis). We do this in a lab setting, during our visit to companies participated in our study.

We observe that participants weigh the perceived gains and burden and draw a group perception, even though their rating differs individually. They do this through group dialogue. For instance, one of the managers was risk-averse when faced with protected data due to a lack of control over company policy. Hence, his rating of the MPC application itself was low compared to his colleagues. At the same time, he recognized potential value in the output. As a result, his input in the dialogue was mostly about value.

Meanwhile, his more-technical colleague criticized the trustworthiness and security of the application. Besides, the highest manager identified the flaws and missing elements in the conversation and stressed to his colleagues that the discussion was about problems that could be solved. He also argued that they make regular use of trusted third parties that is backed by a business case approved by his superiors due to associated costs and company policy. Thus, an important point to consider is the balance between total costs (resource and monetary) and "newness"–in terms of this study, relative advantage. In his case, TTP provides a viable solution to the problem of confidentiality; however, discussed only for high-impact business cases. While MPC was perceived as secure, it was based on the scope of the study. Nevertheless, several changes to the application were suggested. The following sections discuss the aspects that affected perceptions the most.

5.7.1 Trustworthiness

The first important finding was related to *the company behind the application*. For instance, one user–which was administered the MPC application–stated, *"I don't trust third parties with confidential data"*. For the lab participants, their main concern was related to knowing the organization behind the application. This is important, mainly due to liability concerns and the ability to evaluate the organization's credibility. They also needed to know where the computation servers are located (even though encrypted) due to proprietary concerns. One of the companies had a strict company policy–company data may not leave company boundaries without explicit formal approval. Thereby, trustworthiness perception is based on thorough evaluation.

To deal with this issue, one solution mentioned is by backing the application by an organization with a *"respected (responsible) reputation"*. The example given for the case was a university and cross-link to a forum on the university website. This forum should describe the activities concerning the MPC applications that are in use. However, if a commercial company backs the MPC application, this company (i.e., our lab participants) felt they need to participate in application development as an internal audit. Upon extending this question with divisibility, it was argued that an evaluation of the company is still required since "anyone can claim anything". Thereby divisibility, although it makes things clear, must be augmented with the possibility to trace whether, for instance, if it is the actual code.

5.7.2 Relative advantage

One finding from the responses (lab participants) was a 'contradiction' in relative advantage between the participants. The perception is that concerned with the level of involvement. The reason *workload spanning different departments* was not considered an advantage over TTP is that many departments still needed to be involved. In fact, it was mentioned that initially, the required resources for participation might be even more than would be the case in comparison to a straight-forward, trusted third party. However, participants discussed that such an application is perceived to provide a relative advantage over non-MPC based solution if the company (1) had "levers" to trace claims made by the application; and (2) able to evaluate the credibility of the application and the trustworthiness of the organization.

In sum, the extent to which MPC provides an advantage over TTP was still unclear at the moment. Participants did agree that, to some extent, the organization behind the application determines the way the advantage is perceived. One of the companies explained that MPC could, in such cases, serve as a form of reassurance. Given the discussion, we find that perceived relative advantage is also a function of trustworthiness since credibility is also a factor of trustworthiness. Both credibility and a link between trustworthiness and relative advantage (moderating effect of trustworthiness on relative advantage) are not included in the conceptual framework.

5.7.3 Security

The respondents who did not fully perceive the security of MPC felt that either the information or details were missing. Some of the comments are related to MPC vulnerabilities. For instance, *"I am not convinced that our data is not decoded throughout the process."* At the same time, some respondents felt that more detail had to be provided because "The description does not actually tell me how the data is being split. And after being split, how the data will be computed is not described". One respondent stated, "As much as it seems safe from many perspectives, there is always a risk for the leak of private business information".

The majority that entered a low value for willingness to contribute data were security-related. According to one participant: *"Information protection is the first priority no matter if the results are positive."* Similarly, another participant stated that *"Again, in order to contribute my company's data, I would need to be 100% sure that the application is safe. If it is safe, then I would."* In line with this, one participant is *"Not convinced that servers do not keep confidential data."* At the same time, some respondents were deterministic or risk-averse in terms of data contribution: *"There's always ways to leak information. Nothing is bulletproof regarding sensitive information nowadays"*. Another respondent expressed that *"I don't want to send any kind of secure company data to anybody at all."*

At the organizational level, in discussing MPC, the question was raised whether the protocol can withstand "brute-force type attack". Given the shares, this discussion directed itself to the possibility of collusion. Hence, it was stated that the protocol is as important as the infrastructure on which it is deployed. However, such information was missing in the application.

5.8 Summary

The quantitative and qualitative analyses show that MPC contributes to perceptions of willingness to contribute protected data. The results are reported in Table 7. We hypothesized that MPC contributes to perceived trustworthiness, perceived relative advantage, and perceived security. However, the quantitative results show that while respondents are more willing to contribute data over an MPC application than a TTP application, the difference lies primarily in perceived trustworthiness and perceived security due to MPC. These aspects seem to be perceived as important aspects in terms of willingness to contribute protected data, as evidenced in a significant correlation between these aspects and willingness to contribute.

Concerning the dimension of trustworthiness, the effect size of MPC in comparison to TTP is medium. We also found indications that MPC makes matters more complicated even though it does not negatively affect perceived trustworthiness. Concerning the dimension of relative advantage, the effect size is initially found negligible. The t-test reveals that MPC does contribute in terms of perceived relative advantage upon further examination. A weaker correlation between relative advantage and willingness to contribute is reported in comparison to trustworthiness and security.

#	Hypotheses	Results
H1	Willingness to contribute protected data through MPC is greater than the willingness to contribute protected data over TTP	Supported
H2	Perceived trustworthiness of an MPC-enabled application is greater than the perceived trustworthiness of a TTP based application	Supported
H2a	Perceived trustworthiness of a data contribution application is considered an important aspect	Supported
H3	Perceived security of an MPC-enabled application is greater than perceived security of a TTP based application	Supported
H3a	Perceived security of a data contribution application is considered an important aspect	Supported
H4	Perceived relative advantage of an MPC-enabled application is equal to the perceived relative advantage of a TTP based application	Supported
H4a	Perceived relative advantage of a data contribution application is considered an important aspect	Not Supported

Table 7 Hypotheses and results

The qualitative assessment indicates that more information and features are needed for MPC to enhance the perceived relative advantage further. The observed participants also advised several changes that should be considered concerning trustworthiness.

6. Discussion and conclusions

This section concludes our study. We first discuss our main findings in section 6.1. Then, we outlined the limitations of our study in section 6.2. We wrap up in section 6.3 by elaborating implications for the Safe-DEED project and the next step.

6.1 Main findings

We found that organizational willingness to contribute protected data through an MPC-based application is mainly affected by perceived trustworthiness and perceived security. When either trustworthiness or security is perceived as lacking, organizations are less willing to contribute protected (sensitive and confidential) data. Strong evidence was found to support our hypotheses. It thus seems reasonable to argue that perceived trustworthiness and perceived security should be carefully assessed when developing MPC-enabled applications.

We also found that MPC positively enhances perceived relative advantage, albeit to a lesser extent. Aligning our results with Harborth, Pape, and Rannenberg (2020), we argue that the weight of relative advantage could increase later in the pre-adoption phases since organizations stated that TTP does provide a viable solution in protecting confidentiality. However, TTP's use as a solution is backed by business cases and thorough assessments, suggesting that security is a secondary concern. The primary concern remains the purpose of data sharing. Despite this fuzzy view of priority, when viewing MPC as a solution to foster data contribution beyond data sharing initiated due to cooperation and collaboration endeavours, MPC was found to carry potential in this regard. However, the lab participants clearly stated that the application must provide contributors with levers that allow them to understand the data contribution process fully.

In essence, contributors must be able to perform a complete assessment of the application. Persuading organizations to contribute protected data through a web application requires full transparency. Therefore, it must be clear how MPC, and the application as a whole, protects the input parties' contributed data. Specifically, an MPC application is not likely to be used if (1) the application is not perceived as trustworthy; (2) the organization behind the application is credible and traceable; and (3) the data contributor can ensure that the protocols that are claimed to be used are in fact the protocols being used. The latter is perceived as a requirement when an organization has not been involved in developing the application or cannot perform an internal audit.

Regarding the credibility of an organization, we made assumptions to address potential bias to the results when including information about the service provider. While those assumptions have allowed us to diminish potential bias concerned with the organization behind the application and not the application itself, we found that the organization's credibility behind the application plays a vital role. Therefore, we emphasize that researchers attempting to understand MPC's effect on organizational behavior should follow a similar approach. Nevertheless, credibility could further enhance the variance explained in the willingness to contribute. Intuitively, this is because the contributor becomes dependent on the service provider. We consider this similar to the credence given to the service provider (Golbeck, Parsia, & Hendler, 2003, p. 238-249).

In sum, we found that MPC enhances organizational perceptions of data contribution. Thus, MPC is found to increase perceived trustworthiness and perceived security significantly. Both of these aspects are found to be important and of approximately equal importance when considering the contribution of protected data. Both are considered the locus of willingness to contribute protected data through a web-based application. From qualitative assessment, we found that MPC positively contributes since it allows data contribution independently of conventional data processors, which typically have access to raw data. Furthermore, the extent to which MPC increases perceptions depends on how an organization can assert the application'sapplication'sapplication's trustworthiness and the security measure used by the application. We also found that MPC affects perceived relative advantage, as shown by a weak to a medium correlation between perceived relative advantage and willingness to contribute protected data. This finding suggests that relative advantage is not perceived as important as perceived trustworthiness and perceived security concerning willingness to contribute protected data.

6.2 Limitations

There are two main limitations of this study. The first limitation concerns the data collection phase. As described, the majority of responses were collected through Prolific. The majority of responses were collected at an individual level, and these individuals met the proxy requirement for organizational decision-makers and shared their perception in the context of their organization. Yet, as discussed in this study, the “holy grail” of respondents encompasses decision-makers from several echelons within organizations; we referred to these as batches. During the lab experiment evaluation, we observed that decisions might occur in groups, such as project teams. That is, groups of individuals together shape a unified perception. In fact, we believe that the author's presence during the experiment might have even affected (i.e., biased) perceived trustworthiness. To recall, the trustworthiness scores for the lab participants were significantly higher than the Prolific dataset (which is the main reason this data set was removed).

Even though acquiring a pool of sufficient batches poses many challenges, our study suggests that overall, when individuals are asked to rate their perception, a significant positive effect of MPC is reported in terms of willingness to contribute. It is thus safe to assume that the aggregate results are also positive. However, we stress that questions should be properly framed in the interest of the organization they represent. Nonetheless, we suggest researchers perform case studies to enrich our general understanding of MPC adoption in organizational settings.

The second limitation is regarding the designed instrument. The mock-up was developed following scholars’ recommendations and suggestions. It was also based on the successful deployment of an MPC web application. However, in the article regarding the application, it is apparent that the application's development involved a lengthy discussion with many parties. As a result, these parties are more likely to be aware of the back-end before giving consent to their participation. We included more information than the reference application to address this issue—however, potentially at the cost of increased cognitive load. On the other hand, this provides a more complete way of demonstrating the application, assuming that participants are not familiar with it. When there is a higher degree of familiarity with MPC and when prospects are educated on the items and aspects that warrant attention, such an application can be “cleaned”-—while adhering to transparency requirements.

6.3 Implications for Safe-DEED

This study’s main contribution is to set the basis for understanding MPC’s impact on the willingness to contribute protected data within the supply chain context. We found that firms would be more willing to engage in data sharing activities via MPC instead of using Trusted Third Party (TTP). However, firms should perceive the MPC application as trustworthy and secure before they want to use it.

This deliverable also provides a valuable reference for the development of Safe-DEED technologies in the form of use case scenario, mock-up, video demonstrator, and empirical findings. Specifically, we confirm and extend our results in D2.4 that proper information communication method about MPC can increase trustworthiness and security perception. Ultimately, this will influence the willingness to share data, which is essential as a key condition to unlock the European data economy. Thus, we lay a foundation to understand aspects that should be considered in developing new applications and business models for Safe-DEED technologies.

As the next step within T.2.3, we will replicate and expand this study to evaluate the Safe-DEED prototype's final version. Also, we will likely evaluate the prototype through a large-scale survey on a wide range of use-cases. In this way, we will be able to look into (1) how the impact of MPC changes over time; and (2) how different settings perceive the value of MPC.

7. References

Adhikari, A., Bisi, A., & Avittathur, B. (2020). Coordination mechanism, risk sharing, and risk aversion in a five-level textile supply chain under demand and supply uncertainty. *European Journal of Operational Research, 282*(1), 93-107. doi: https://doi.org/10.1016/j.ejor.2019.08.051.

Adlin, T., & Pruitt, J. (2010). Chapter 1 - what are personas? In T. Adlin & J. Pruitt (Eds.), *The essential persona lifecycle: Your guide to building and using personas* (p. 1 - 5). Boston: Morgan Kaufmann. doi: https://doi.org/10.1016/B978-0-12-381418-0.00001-2.

Archer, D., Bogdanov, D., Lindell, Y., Kamm, L., Nielsen, K., Pagter, J., … Wright, R. (2018, 12). From keys to databases—real-world applications of secure multi-party computation. *Computer Journal, 61*, 1749-1771. doi: 10.1093/comjnl/bxy090.

Arnaut, C., Pont, M., Scaria, E., Berghmans, A., & Leconte, S. (2018). Study on data sharing between companies in Europe. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en.

Atallah, M., Deshpande, V., & Schwarz, L. (2004, 01). Secure supply-chain collaboration: A new technology for supply-chain management. *Unpublished*.

Baglin, J. (2014, 01). Improving your exploratory factor analysis for ordinal data: A demonstration using factor. *Practical Assessment, Research, and Evaluation, 19*, 1-14.

Bestavros, A., Lapets, A., Jansen, F., Varia, M., Volgushev, N., & Schwarzkopf, M. (2017). Design and Deployment of Usable, Scalable MPC. In *Theory and Practice of Multi-Party Computation Workshop*.

Bestavros, A., Lapets, A., & Varia, M. (2017). User-centric distributed solutions for privacy-preserving analytics. *Communications of the ACM*, *60*(2), 37-39.

Bogdanov, D., Talviste, R., & Willemson, J. (2012). Deploying secure multi-party computation for financial data analysis. In A. D. Keromytis (Ed.), *Financial cryptography and data security* (pp. 57–64). Berlin, Heidelberg: Springer Berlin Heidelberg.

Bogetoft, P., Christensen, D. L., Damgård, I., Geisler, M., Jakobsen, T., Krøigaard, M., … Toft, T. (2009). Secure multiparty computation goes live. In R. Dingledine & P. Golle (Eds.), *Financial cryptography and data security* (pp. 325–343). Berlin, Heidelberg: Springer Berlin Heidelberg.

Catrina, O., & Kerschbaum, F. (2008). Fostering the uptake of secure multiparty computation in e-commerce. In *2008 third international conference on availability, reliability, and security* (p. 693-700). doi: 10.1109/ARES.2008.49.

Chang, A. J. (2010). Roles of perceived risk and usefulness in information system security adoption. In *the 2010 IEEE international conference on management of innovation technology* (p. 1264-1269). doi: 10.1109/ICMIT.2010.5492818.

Choi, J. I., & Butler, K. R. (2019). Secure multiparty computation and trusted hardware: Examining adoption challenges and opportunities. *Security and Communication Networks*, *2019*.

CNSS. (2015). *CNSSI 4009 Committee on National Security Systems (CNSS) glossary* (Tech. Rep.). Committee on National Security Systems. Retrieved 25-06-20, from https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/Resources-Tools-and-Publications/Resources-and-Tools-Files/CNSSI-4009-Committee-on-National-Security-Systems-CNSS-Glossary.

Cook, K. S., & Rice, E. (2006). Social exchange theory. In J. Delamater (Ed.), *Handbook of social psychology* (pp. 53–76). Boston, MA: Springer US. doi: 10.1007/0-387-36921-X_3.

Cooper, M. C., Lambert, D. M., & Pagh, J. D. (1997). Supply chain management: more than a new name for logistics. *The international journal of logistics management*, *8*(1), 1-14.

Curkovic, S., Scannell, T., & Wagner, B. (2015). *Managing supply chain risk: integrating with risk management*. CRC Press.

Damgård, I., Damgård, K., Nielsen, K., Nordholt, P. S., & Toft, T. (2017). Confidential benchmarking based on multiparty computation. In J. Grossklags & B. Preneel (Eds.), *Financial cryptography and data security* (pp. 169–187). Berlin, Heidelberg: Springer Berlin Heidelberg.

European Commission. (2020). *A European strategy for data*. Retrieved from https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.

Feller, T. (2014). Requirements for trustworthiness. In *Trustworthy reconfigurable systems: Enhancing the security capabilities of reconfigurable hardware architectures* (pp. 35–60). Wiesbaden: Springer Fachmedien Wiesbaden. doi: 10.1007/978-3-658-07005-2_3.

Field, A. (2017). *Discovering statistics using IBM SPSS statistics* (5th ed.). Sage Publications Ltd.

Golbeck, J., Parsia, B., & Hendler, J. (2003). Trust networks on the semantic web. In M. Klusch, A. Omicini, S. Ossowski, & H. Laamanen (Eds.), *Cooperative information agents VII* (pp. 238–249). Berlin, Heidelberg: Springer Berlin Heidelberg.

Hackman, S. T., Frazelle, E. H., Griffin, P. M., Griffin, S. O., & Vlasta, D. A. (2001). Benchmarking warehousing and distribution operations: an input-output approach. *Journal of Productivity Analysis*, *16*(1), 79-100.

Hair, J. F., Black, J. W. C., Babin, B. J., & Anderson, R. E. (2014). *Multivariate data analysis*. Pearson Education Limited.

Harborth, D., Pape, S., & Rannenberg, K. (2020). Explaining the Technology Use Behavior of Privacy-Enhancing Technologies: The Case of Tor and JonDonym. *Proceedings on Privacy Enhancing Technologies*, *2020*(2), 111-128.

Hart, P., & Saunders, C. (1997). Power and trust: Critical factors in the adoption and use of electronic data interchange. *Organization science*, *8*(1), 23-42.

Huang, D. L., Rau, P. L. P., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies*, *69*(12), 870-883.

Kanger, L., & Pruulmann-Vengerfeldt, P. (2015). Social need for secure multiparty computation. *Cryptology and Information Security Series, 13*, 43-57. doi: 10.3233/978-1-61499-532-6-43

Kerschbaum, F., Schröpfer, A., Zilli, A., Pibernik, R., Catrina, O., de Hoogh, S., ... & Damiani, E. (2011). Secure collaborative supply-chain management. *Computer*, *44*(9), 38-43.

Khurana, M., Mishra, P., & Singh, A. (2011). Barriers to information sharing in supply chain of manufacturing industries. *International Journal of Manufacturing Systems*, *1*(1), 9-29.

Koutroumpis, P., Leiponen, A., & Thomas, L. D. (2020). Markets for data. *Industrial and Corporate Change*, *29*(3), 645-660.

Li, J., Shaw, M. J., Sikora, R. T., Tan, G. W., & Yang, R. (2001). *The effects of information sharing strategies on supply chain performance.* Retrieved from *http://citebm.cba.uiuc.edu/B2Bresearch/ieee_em.pdf*.

Lotfi, Z., Mukhtar, M., Sahran, S., & Taei Zadeh, A. (2013). Information sharing in supply chain management. In *The 4th International Conference on Electrical Engineering and Informatics*.

Milch, V., & Laumann, K. (2016). Interorganizational complexity and organizational accident risk: A literature review. *Safety science*, *82*, 9-17.

Miltersen, P. B., Nielsen, J. B., & Triandopoulos, N. (2009, August). Privacy-enhancing auctions using rational cryptography. In *Annual International Cryptology Conference* (pp. 541-558). Springer, Berlin, Heidelberg.

Min, H., & Zhou, G. (2002). Supply chain modeling: past, present and future. *Computers & industrial engineering*, *43*(1-2), 231-249.

Mitchell, V. W. (1992). Understanding consumers' behaviour: Can perceived risk theory help. *Management Decision*, *30*(3), 26-31.

Ojha, D., Sahin, F., Shockley, J., & Sridharan, S. V. (2019). Is there a performance tradeoff in managing order fulfillment and the bullwhip effect in supply chains? The role of information sharing and information type. *International Journal of Production Economics*, *208*, 529-543.

Olsson, U. (1979). Maximum likelihood estimation of the polychoric correlation coefficient. *Psychometrika*, *44*(4), 443-460.

Ortt, J. R., Langley, D. J., & Pals, N. (2013, June). Ten niche strategies to commercialize new high-tech products. In *2013 International Conference on Engineering, Technology and Innovation (ICE) & IEEE International Technology Management Conference* (pp. 1-12). IEEE.

Pavlidis, M. (2011). Designing for Trust. In *CAiSE (Doctoral Consortium)* (pp. 3-14).

Petronio, S. (1991). Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication theory*, *1*(4), 311-335.

Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication*, *13*(1), 6-14.

Raj, G., Sarfaraz, M., & Singh, D. (2014). Survey on trust establishment in cloud computing. In *2014 5th international conference - confluence the next generation information technology summit (confluence)* (p. 215-220). doi: 10.1109/CONFLUENCE.2014.6949375

Rigdon, E. E., & Ferguson Jr, C. E. (1991). The performance of the polychoric correlation coefficient and selected fitting functions in confirmatory factor analysis with ordinal data. *Journal of marketing research*, *28*(4), 491-497.

Rogers, E. M. (2003). *Diffusion of innovations*. Simon and Schuster.

Skinner, E. A. (1996). A guide to constructs of control. *Journal of personality and social psychology*, *71*(3), 549.

Stevens, J. P. (2016). *Applied multivariate statistics for the social sciences, 6th ed*. New York, NY, US: Routledge/Taylor & Francis Group.

Stewart, A. (2004). On risk: perception and direction. *Computers & Security*, *23*(5), 362-370.

Toldsepp, K., Pruulmann-Vengerfeldt, P., & Laud, P. (2012, July). *Usable and Efficient Secure Multiparty Computation* (ETLA Working Papers). Specific Targeted Research Project supported by the 7th Framework Programme of the EC. Retrieved from https://cordis.europa.eu/docs/projects/cnect/1/284731/080/deliverables/001-D12.pdf

Tornatzky, L. G., & Klein, K. J. (1982). Innovation characteristics and innovation adoption-implementation: A meta-analysis of findings. *IEEE Transactions on engineering management*, (1), 28-45.

Wu, J., Wang, Z., & Huang, L. (2010, August). The relationship among propensity to trust, institution-based trust, perceived control, and trust in platform. In *2010 IEEE 2nd Symposium on Web Society* (pp. 424-428). IEEE.

Yao, A. C. (1986, Oct). How to generate and exchange secrets. In *27th annual symposium on foundations of computer science (sfcs 1986)* (p. 162-167). doi: 10.1109/SFCS.1986.25.

Young-Ybarra, C., & Wiersema, M. (1999). Strategic flexibility in information technology alliances: The influence of transaction cost economics and social exchange theory. *Organization science*, *10*(4), 439-459.

Zafrir, N. (2020). *Beyond trust: Why we need a paradigm shift in data-sharing [White paper]* (Tech. Rep.). World Economic Forum. Retrieved 16-03-20, from https://www.weforum.org/agenda/2020/01/new-paradigm.

Zaheer, A., & Venkatraman, N. (1995). Relational governance as an interorganizational strategy: An empirical test of the role of trust in economic exchange. *Strategic management journal*, *16*(5), 373-392.

Zare Garizy, T., Fridgen, G., & Wederhake, L. (2018, 07). A privacy preserving approach to collaborative systemic risk identification: The use-case of supply chain networks. *Security and Communication Networks*, *2018*, 1-18. doi: 10.1155/2018/3858592.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security, 17*, 330-340.

Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C.-Z., Li, H., & an Tan, Y. (2019). Secure multi-party computation: Theory, practice and applications. *Information Sciences, 476*, 357 - 372. doi: https://doi.org/10.1016/j.ins.2018.10.024