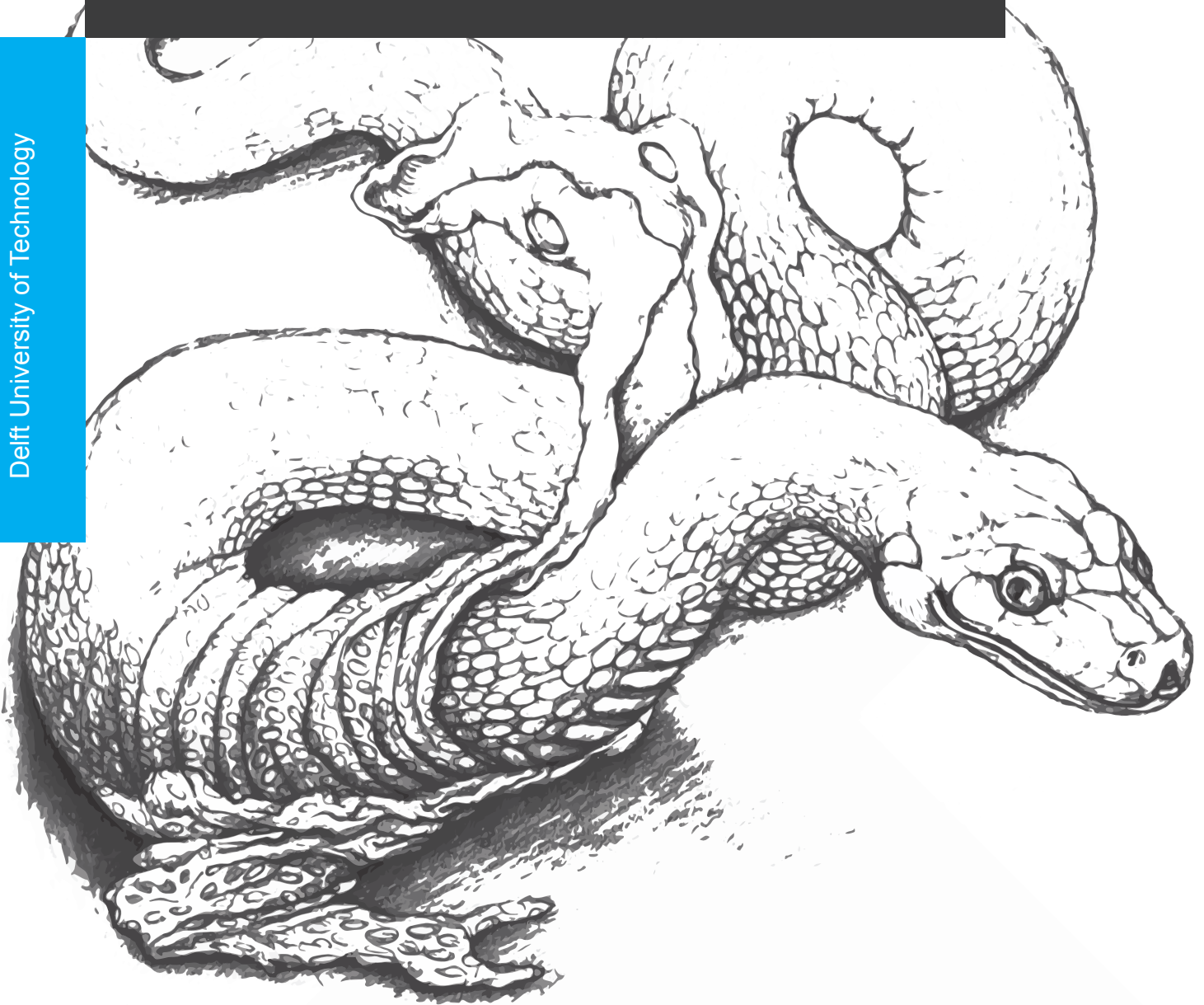


Multiparty Computation

*The effect of multiparty computation
on firms' willingness to contribute pro-
tected data*

Masud Petronia

Delft University of Technology



Multiparty Computation

The effect of multiparty computation on firms'
willingness to contribute protected data

by

Masud Petronia

to obtain the degree of Master of Science
at the Delft University of Technology,
faculty of Technology, Policy and Management,
to be defended publicly on Wednesday September 30, 2020 at 10:00 AM LT.

Student number: 4265297
Project duration: March 16, 2020 – August 31, 2020
Thesis committee: Dr. ir. M. de Reuver, TU Delft, first supervisor
MSc. Ph.D. student W. Agahari, TU Delft, daily supervisor
Dr. ir. H. Asghari, TU Delft, second supervisor

An electronic version of this thesis is available at <http://repository.tudelft.nl/>.

Preface

The work in this thesis is for anyone interested in multi-party computation or is interested in developing a research approach suitable for the acceptance of emerging technologies in organizations. In this thesis, I have worked on a cryptography technology whose value is challenging to communicate. My main aim is to impart a methodology to study the lack of awareness amongst organizations in regards to adopting cryptography technology, in an effort to research responsible and effective technology development approaches. It is also my attempt to share my journey from stripping a technology, which I was unfamiliar with, to academic contribution. Besides, I have laid out a map of Multiparty Computation (MPC) research domains, which may be of interest to the reader.

This thesis is divided into four parts. Part I, introduces the background of the problem, provides the thesis definition, and the research methodology used for this study. In Part II we seek to understand the aspects that must be understood in order to examine organizational willingness to contribute protected data. In Part III, the experiment and statistical analysis is described. Part IV, discusses the findings and recommendations for future research.

If you liked this study, and wish to replicate or reproduce it, contribute or improve findings, then appendix [A.2](#) might interest you. This appendix lists all resources developed for this study. I have made every part of the research open to the public. If you have any comments, questions, or suggestions. I would love to hear them as well.

I hope you enjoy reading this thesis as much as I enjoyed writing it.

*Masud Petronia
Rotterdam, September 2020*

Acknowledgements

When I resigned from my full-time job to pursue my master's degree, I had a plan, but in no way was I able to predict the way it turned out: working part-time, becoming a father, and raising him/her while having a loving relationship. At the same time, I knew I had to work with my girlfriend's unpredictable schedule (stewardess). All seemed manageable and "perfectly doable." Despite all of the hurdles, I still managed to thrive—so you can hear it coming, I have some people to thank for it.

Thanks goes to my mom and dad for their encouragement and in believing I could pull off this life-changing endeavor. Thank you for your moral support throughout the master's program and this last part of this journey. Without you, I would not have been able to reach this point.

Thanks goes to Laura (girlfriend) without whose patience I would also have never made it and would have resulted in a lonely endeavor. I apologize for the time spent with nose buried in the computer. The same goes for you, Elon (son).

Thanks go to Monique, Hans (parents in law), and Moedjinem (childminder or third grandmother as we like to call her) for your flexibility. Without you, I am confident Elon had to attend some lectures as well.

Thanks go to Mark de Reuver, Wirawan Agahari, and Hadi Asghari (see title page) for your invaluable feedback. You have shaken my view of perception in many grateful ways, which I will forever cherish.

A final thank you to Lateef and Sizwe (brothers) and Deniece (neighbor) for allowing me to share and discuss my findings with them.

Finally, I would like to spend some closing words about the front cover design. I have always liked the quirkiness of the O'Reilly animal illustration on the front covers. Most carry a "story" or meaning behind them; this intrigued me to find an animal that fits this thesis's context. In writing this thesis, I have related MPC as a means for businesses to create new value. I found snakes to fit this context. Historically, snakes represent a creative life force. They are symbols of transformation, as they shed their skin through sloughing. With kind permission, all credits to John Dockus for the snake drawing¹.

*Masud Petronia
Rotterdam, September 2020*

¹<https://johndockus.wordpress.com/>

The cynical rhyme of the present data governance regime goes:

*Data, data, every where,
And all of it was stored away;
Data, data, every where,
Nor a byte to profit there.*

Executive Summary

Data is all around us. Sharing data between organizations can help resolve issues that become increasingly important and may create new business ventures. Altogether, this unlocks possibilities for economic growth and new markets. However, the data-sharing landscape faces many barriers. There is shareable and non-shareable data, and firms can be unwilling or unable to share certain types of data. Concerns may initially arise regarding the purpose of sharing data, and a fear of sensitive information leakage may also exist. With such uncertainty, firms may choose to refrain from data sharing, and this uncertainty can reflect in security concerns, liability concerns, accountability concerns, legislative concerns, and strategic concerns.

The problem Organizations share data for collective purposes: new opportunities are created to allow business enhancement. While new businesses contribute to economic development, valid reasons exist to inhibit data sharing (e.g. citizen privacy and sensitive information). Multi Party computation (MPC) provides a solution to these risks. However, MPC implementation remains limited, and we lack knowledge about the willingness to use MPC-enabled applications in organizational settings.

The research objective The objective of this study is to investigate the effect of MPC on organizational willingness to contribute protected data for collective purposes

The research question To what extent does MPC affect organizational perception of the [contribution](#) of protected data?

MPC implements cryptography technology and could allow for the aforementioned concerns to be resolved. However, the following are lacking: an understanding of how MPC is perceived from an organizational perspective and familiarity with MPC in various business settings. Therefore, this thesis starts with breaking down MPC to establish a common language in the discussion of organizational *willingness to contribute* protected data through MPC. Since MPC is usually effective for specific functions, the context in which it is studied must be defined. In this study, the focus is on MPC deployments in supply chains (SCs). The results of the study provide useful information beyond the scope of merely SCs.

Mapping out MPC

MPC allows for the sharing of knowledge without sharing the data provided by the independent input parties. This is achieved via a common function, which is computed through an MPC protocol. MPC deals with this problem of computing a function amongst a set of possibly mutually distrusting parties. These parties only learn from the output of the function.

To discuss MPC implementation with organizations, the setup and workings of the MPC protocol are illustrated because this overview is missing in literature. This illustration depicts the building blocks of MPC and shows a typical architecture of an MPC platform and the data flow thereof. Then,

to communicate the business value of MPC, the key elements of MPC are synthesized into eight characteristics, which clarify the situations in which MPC provides utility. Using this set of characteristics, seven potential use cases are identified from literature and informal interviews. These include collaborative distribution, freight bidding, demand and production coordination, group purchasing, inventory sharing, performance benchmarking, and SC network risk analysis. These use cases demonstrate business enhancement and new opportunities in SCs by means of MPC.

From the literature review, it is also clear that MPC research is scattered, thereby making it difficult to understand how research contributes to the whole picture. A diagram is thus created to clarify the MPC research domains. This diagram indicates that the distinction between input and output information is required because security is likely not the primary, but the secondary goal of users since they pursue value from the output (aggregated) information. For this study, the experimental scope is limited to the input stage, and the focus is on the organizational perceptions of MPC applications with respect to features that cover requirements and functionalities. As a result, the primary goal of users herein is confidentiality, not the value of the output.

Measuring perceptions

A conceptual framework was developed that uses an interorganizational system (IOS) as its departure. IOS literature allowed us to understand problems arising from software used for the movement of information across organizational boundaries. Then, innovation characteristics research is used to derive MPC-specific attributes that are likely to be considered by organizations when assessing this technology. In this process, generic characteristics were sought, particularly from IS literature, and contextualized and framed in terms of MPC. Moreover, to examine only the aspects related to the given innovation phase of MPC, the method willingness to contribute was viewed from an innovation development process perspective. Here, willingness to contribute was found to be the first concern addressed by organizations when presented with MPC as an emerging technology. Other methods such as willingness to use emerge later in the process. This approach allows proper scoping of the study. After scoping, the attributes were integrated into a conceptual framework comprising three dimensions: trustworthiness, relative advantage, and security. These are second-order constructs.

First, the trustworthiness dimension comprises the observability, complexity, integrity, and divisibility of the application. Integrity and divisibility are removed from the scope due their inherent complexity. Despite this decision, some valuable pointers were provided by organizations concerning divisibility. Second, relative advantage comprises simplification of the knowledge-sharing process and cost advantage. Cost advantage was removed because it does not fit well with the research methodology since it requires some direct comparison with conventional data contribution solutions. Third, security comprises perceived control and perceived risk.

Measuring organizational willingness to contribute data

The extent to which MPC affects willingness to contribute protected data is measured by the degree to which organizations are willing to contribute protected data through an MPC application rather than through a conventional solution such as a trusted third party (TTP). A comparison between two applications is thus needed. For the study, two identical applications were designed and built. These reflect a TTP and an MPC-based application. The comparison of perception between the

two applications can be interpreted as the effect of MPC. The application design is based on the previous contribution of scholars: a successfully deployed and currently in use MPC application. The researchers behind this application suggest features that should be embedded in an MPC application to elicit a trustworthy and usable MPC application.

Further considerations are taken into account regarding how visuals should be used to enhance perceptions of MPC-enabled applications. 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. This methodology allowed us to examine the difference between the pretest and post-test ratings and to compare the two groups, thereby providing an understanding of the effect of MPC versus conventional (e.g. TTP) solutions (t-test). Moreover, it allowed us to assess the importance of the attributes with respect to willingness to contribute (correlation).

Effect of MPC on willingness to contribute data

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 contribution of protected data. That is, both are considered as the locus of willingness to contribute protected data through a web-based application. From the qualitative assessment, it is assumed that the positive contribution of MPC herein 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 the extent to which an organization is able to assert the trustworthiness of the application and the security measure used by the application. MPC also affects 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 with respect to willingness to contribute protected data. Nevertheless, MPC also seems to enhance perceived relative advantage. Finally, although the relative advantage of MPC was not perceived as necessary, several findings are reported to further enhance the utility provided by an MPC application.

Contents

List of Figures	xvii
List of SPSS Outputs	xix
List of Tables	xxi
I Thesis Definition	3
1 Introduction	5
1.1 Data sharing towards data contribution	5
1.2 MPC as a problem-solving instrument. Is it?	6
1.3 Data sharing in supply chains and MPC	7
1.4 Knowledge gap and problem statement	9
1.5 Research objective and research questions	10
1.6 Societal relevance	12
1.7 Research approach and research methodology	12
1.8 Thesis structure and outline	14
II Literature research	17
2 MPC domain	19
2.1 Introduction to MPC	19
2.2 MPC architecture fundamentals	21
2.3 MPC landscape	23
2.4 Potential MPC application supply chain use case scenarios	24
2.5 Assumption, scope, and terminology	27
2.6 Conclusion	28
3 Willingness to contribute data	31
3.1 Interorganizational systems (IOS)	31
3.1.1 Introduction to IOS	31
3.1.2 Interoperability problems raised by IOS	32
3.1.3 Implications of IOS for the study of MPC	33
3.2 Innovation Characteristics	34
3.2.1 Innovation characteristics research	34
3.2.2 MPC as innovation: MPC attributes	35
3.3 An overview of MPC related attributes and determinants	40
3.4 Trust and trustworthiness	43
3.4.1 Trust	43
3.4.2 Trustworthiness	44

3.5	Security	45
3.6	Relative advantage	46
3.7	Hypotheses development	47
3.7.1	Trustworthiness	48
3.8	Conceptual framework	50
3.9	Perceptions of MPC	50
3.9.1	Elements of observability of the data contribution process (OBSE)	51
III	Experiment	55
4	Demonstration platform	57
4.1	Goal	57
4.2	Use-case	57
4.3	Mock-up design	60
4.3.1	Design considerations	60
4.3.2	Features	61
4.3.3	Information to be displayed	62
4.4	Final design.	65
4.5	Demonstration platform development	68
4.5.1	Platform	68
4.5.2	Mock-up	68
4.5.3	Deployment	69
5	Experiment design	71
5.1	Participants	71
5.2	Data collection	72
5.3	Experimental design.	72
5.3.1	Quantitative study.	72
5.3.2	Experiment setup	73
5.4	Procedure.	74
5.4.1	Persona	74
5.4.2	Use-case scenario	76
6	Results	79
6.1	Data collection and data reliability.	79
6.2	Establishing the dataset	81
6.3	Data preparation in SPSS	90
6.4	Participant demographics	90
6.5	Correlation Analysis.	93
6.5.1	PCA analysis, re-evaluation of constructs.	93
6.5.2	Validity	94
6.5.3	Results	94
6.6	Hypotheses testing	104
6.6.1	Willingness to contribute	104
6.6.2	Trustworthiness, relative advantage and security	105

6.7	Interaction effect	107
6.8	Qualitative assessment	112
6.8.1	Trustworthiness	112
6.8.2	Trustworthiness	113
6.8.3	Relative advantage	113
6.8.4	Security	114
6.9	Conclusions	114
IV	Upshot	117
7	Discussions & Conclusion	119
7.1	Theoretical implications	122
7.2	Practical implications	123
7.3	Limitations	125
7.3.1	Methodology	125
7.3.2	Protocol	125
7.3.3	Prolific	126
7.3.4	Framework	126
7.3.5	Designed instrument	127
7.4	Further recommendations for future research	127
7.5	Conclusions	128
7.6	Relevance with MoT programme	129
	References	131
A	Appendices	141
A.1	Technology acceptance models considered	142
A.2	Resource listing for replicating/reproducing this study	144
A.3	Interorganizational adoption and implementation factors	145
A.4	Operationalization of constructs	146
A.4.1	Background	146
A.4.2	Adaptability	146
A.4.3	Complexity	147
A.4.4	Data sharing in general	147
A.4.5	Divisibility	148
A.4.6	Set up effort	149
A.4.7	Effort in general	149
A.4.8	Integrity	150
A.4.9	Observability	151
A.4.10	Organization - Absorptive capacity	152
A.4.11	Simplification	152
A.5	SPSS syntax	154
A.5.1	Compare means of three data sets	154
A.5.2	Add experimental group column	154
A.5.3	Change variable scale	154
A.5.4	Create new column with ages	154

A.5.5	Merge variables	154
A.5.6	Sort by group, and invert reverse questions	155
A.5.7	Reliability:trustworthiness	155
A.5.8	Reliability:security	155
A.5.9	Reliability:relative advantage	155
A.5.10	Demographics: age	156
A.5.11	Industry role frequency table	157
A.5.12	Organizational size combined with level of involvement in development of new product, services and improvements	157
A.5.13	Organizational size combined with education level	157
A.5.14	Industry function and role of work	157
A.5.15	Level of familiarity with MPC	158
A.5.16	Participant final criteria check	158
A.5.17	Bayesian comparison of means	158
A.5.18	Independent t-test willingness to contribute	159
A.5.19	Independent t-test trustworthiness	159
A.5.20	Independent t-test trustworthiness 90% CI	159
A.5.21	Independent t-test relative advantage	159
A.5.22	Independent t-test security	159
A.6	Demographics SPSS output, pivot tables	161
A.7	Correlation tables for initial constructs	164
A.8	Tolerance, VIF, CR, C-alpha	167
A.9	Inter-Item correlation matrices and item-total statistics	170
A.10	Repeated SPSS syntax solution using Python	175
A.11	Questionnaire deployed via Qualtrics ^{XM}	177

List of Figures

1.1	Simplified supply chain network.	7
1.2	Thesis structure	15
2.1	Diagram of Secure Multi-Party Computation. Adapted from Zhao et al. (2019)	19
2.2	Example MPC application architecture with data flow. This diagram is based on building blocks drawn from the architectures of Bogetoft et al. (2009) and Bogdanov, Talviste, and Willemson (2012), and MPC working principles of Bestavros, Lapets, Jansen, et al. (2017).	22
2.3	MPC aspects identified	27
3.1	Overview of MPC attributes and determinants	41
3.2	Increasing data class requires higher levels of security. The higher the sensitivity of a input data, the greater the consequences, the higher the risks, the greater the degree of restrictions, thus requiring higher levels of security (Jr, Snyder, & Carr, 1991). Perceived sensitivity of the input data depends on external factors (e.g. institutional regimes).	47
3.3	In absolute terms, MPC with trustworthiness and security level X , may be used for activity Y , but not for activity Z . The plot illustrates an arbitrary set of combinations of trustworthiness and security (indifferent) levels on the X-axis relative to relative advantage. Since perceptually based, each type of input data has its own plot.	47
3.4	Simple conceptual framework	51
3.5	Measurement Model	51
4.1	For illustrative purpose only: an exemplary plot of output generated by the MPC application.	59
4.2	Screenshots of animated illustration used to depict the process behind “what happens after you submit your data”	60
4.3	The input panel makes use of input fields with search functionality. A drag-and-drop box allows easy uploading of the data file. The side-panel describes that data entered is not yet submitted at this stage.	62
4.4	Panel to review input data. The input fields reflect the excel template file. This example shows the seventh sheet.	63
4.5	Information displayed concerning Computation parties	64
4.6	Start panel screenshot for MPC application	65
4.7	Start panel screenshot for TTP application	65
4.8	View input data panel for MPC and TTP application	66
4.9	Verify and submit input data panel screenshot for MPC application	67
4.10	Verify and submit input data panel screenshot for TTP application	67
4.11	Demonstration platform architecture	68

5.1	The (online) experiment process flow. Time for completion is approximately 20 min.	74
5.2	Survey flow: randomization applied using Qualtrics ^{XM} survey flow feature.	75
5.3	The lab experiment procedure	75

List of SPSS Outputs

6.1	The intent of the application is clear to me	86
6.2	The application clearly describes how my data is processed from data submission to output	86
6.3	The application provides a complete and detailed description of how METHOD is used to protect my data	86
6.4	Interaction with the application is clear and understandable	86
6.5	The descriptions of METHOD are complex	86
6.6	Understanding how the data is processed does not require a lot of my mental effort	86
6.7	It feels safe contributing sensitive company data over the application	87
6.8	The use of METHOD gives me a feeling of security assurance.	87
6.9	Only I am able to view my contributed data	87
6.10	The service provider cannot examine my data beyond my control	87
6.11	I feel capable of using the application	87
6.12	My data cannot be accessed by other contributors	87
6.13	Claims made by the application are clear and accurate	88
6.14	The application is open and transparent in how it protects my data	88
6.15	The application provides a simple way to securely contribute data	88
6.16	The application does not require expertise from multiple organizational departments	88
6.17	The application provides an advantage over conventional data sharing practices	88
6.18	When contributing data, no other party knows about my participation	88
6.19	I feel less hesitant with contributing sensitive company data when using this mpc application	89
6.20	METHOD provides a simple solution to secure data contribution	89
6.21	I would be willing to use METHOD based on the solution it provides to secure data contribution	89
6.22	I am satisfied with the trustworthiness of the METHOD application	89
6.23	I would be willing to use this application based on its trustworthiness	89
6.24	I am satisfied with the security the METHOD provides	89
6.25	I would be willing to use this application based on the security provided by METHOD.	90
6.26	Overall, if the output (the analytic) of the application provides sufficient value to my organization, then I would be willing to contribute sensitive company data over a METHOD application.	90
6.27	Boxplot age distribution.	92
6.28	Participant age distribution.	92
6.29	Role at work	92
6.30	Education level	92
6.31	Level of familiarity with MPC	92
6.32	Research model: polychoric correlations for complete sample. N=106.	95
6.33	Split plot of MPC and TTP participants with and without an IT background.	107

6.34	The intent of the application is clear to me. $F(1,105)=.007, p=.934$	109
6.35	The application clearly describes how my data is processed from data submission to output. $F(1,105)=8.017, p=.006$	109
6.36	The application provides a complete and detailed description of how <i>METHOD</i> is used to protect my data. $F(1,105)=15.315, p<.001$	109
6.37	Interaction with the application is clear and understandable. $F(1,105)=.531, p=.468$	109
6.38	The descriptions of the <i>METHOD</i> are complex. $F(1,105)=2.009, p=.159$	109
6.39	Understanding how the data is processed does not require a lot of my mental effort. $F(1,105)=2.000, p=.160$	109
6.40	Claims made in the application must be clear and accurate. $F(1,105)=0.018, p=.893$	110
6.41	The application is open and transparent in how it protects my data. $F(1,105)=8.629, p=.004$	110
6.42	The application must provide a simple way to securely contribute data. $F(1,105)=4.541, p=.035$	110
6.43	The application must not require expertise from multiple organizational departments. $F(1,105)=.126, p=.723$	110
6.44	The application must provide an advantage over conventional data sharing practices. $F(1,105)=9.813, p=.002$	110
6.45	When contributing data, no other party should know about my organization's participation. $F(1,105)=.134, p=.715$	110
6.46	Through the method I feel less hesitant to contribute sensitive company data through a web application. $F(1,105)=.X, p=.X$	111
6.47	It feels safe contributing sensitive company data over the application. $F(1,105)=.253, p=.616$	111
6.48	The use of <i>METHOD</i> gives me a feeling of security assurance. $F(1,105)=.789, p=.376$	111
6.49	Only I am able to view my contributed data. $F(1,105)=.530, p=.468$	111
6.50	The service provider cannot examine my data beyond my control. $F(1,105)=1.167, p=.283$	111
6.51	I feel capable of using the application. $F(1,105)=.072, p=.789$	111
6.52	My data cannot be accessed by other contributors. $F(1,105)=2.233, p=.138$	112
A.1	Industry with role at work	161
A.2	Degree of level of involvement in development of new products, services, and with role at work	162
A.3	Organizational size with education level	162
A.4	Inter-Item Correlation Matrix: trustworthiness	170

List of Tables

1.1	Theoretical lenses applied vs unit of analysis. Adapted from Kembro, Selviaridis, and Naslund (2014)	9
1.2	Methodology per research question	13
3.1	MPC dimensions	36
3.2	Relative advantage determinants	37
3.3	Trustworthiness determinants	39
3.4	Compatability properties	40
3.5	Security determinants	40
3.6	Variables measured	54
5.1	Pre-test and post-test experimental and control group design	73
6.1	Collected datasets. Total N is 117.	79
6.2	Quality control protocol	80
6.3	Trustworthiness descriptive statistics	82
6.4	Relative advantage descriptive statistics	83
6.5	Security descriptive statistics	84
6.6	Willingness descriptive statistics	85
6.7	Overview of descriptive statistics and correlations	93
6.8	Correlation: trustworthiness and willingness to contribute	96
6.9	Adequacy of the polychoric correlation matrix	97
6.10	Perceived trustworthiness: Factor loadings. Test is run using FACTOR.	97
6.11	Perceived trustworthiness: Explained variance and reliability of rotated components.	97
6.12	Perceived trustworthiness: Explained variance of eigenvalues.	97
6.13	Perceived trustworthiness: inter-factors correlation.	97
6.14	Perceived trustworthiness: distribution of residuals.	98
6.15	Correlation: Security and willingness to contribute	99
6.16	Adequacy of the polychoric correlation matrix	99
6.17	Perceived security: factor loadings. Test is run using FACTOR.	100
6.18	Perceived security: explained variance and reliability of rotated components.	100
6.19	Perceived security: explained variance of eigenvalues.	100
6.20	Perceived security: inter-factors correlation.	100
6.21	Perceived security: distribution of residuals.	100
6.22	Correlation: Relative advantage and willingness to contribute	101
6.23	Adequacy of the polychoric correlation matrix	101
6.24	Perceived relative advantage: factor loadings. Test is run using FACTOR.	102
6.25	Perceived relative advantage: Explained variance and reliability.	102
6.26	Perceived relative advantage: Explained variance of eigenvalues.	102
6.27	Perceived relative advantage: distribution of residuals.	102

6.28 Correlation: Perceptions and overall willingness to contribute	103
6.29 Adequacy of the polychoric correlation matrix	103
6.30 Summary of accepted hypotheses.	116
7.1 Items for considerations for MPC application developers and organizations	130
A.1 References to sources for the purpose of replicability, reproducibility and research contribution.	144
A.2 Interorganizational system attributes	145
A.4 Measuring adaptability	146
A.10 Measuring integrity	151
A.14 Pearson correlation: trustworthiness and willingness to contribute	164
A.15 Pearson correlation: Security and willingness to contribute	165
A.16 Pearson correlation: Relative advantage and willingness to contribute	166
A.17 Descriptive statistics, FA, PCA, and reliability results for combined sample (MPC and TTP)	167
A.18 Descriptive statistics, FA, PCA, and reliability results for combined sample (MPC and TTP)	168
A.19 Item-Total Statistics: trustworthiness	171
A.20 Inter-Item Correlation Matrix: security	172
A.21 Item-Total Statistics: security	173
A.22 Inter-Item Correlation Matrix: relative advantage	174
A.23 Item-Total Statistics: relative advantage	200



Thesis Definition

Introduction

If organizations are liberated from barriers observed in conventional data-sharing practices, this could unearth untapped business opportunities. Multiparty computation (MPC) can provide a solution; however, shifting from conventional solutions to this emerging technology poses many challenges. Therefore, data sharing and MPC are introduced briefly (1.1). The challenges include, among other factors, a lack of understanding of how MPC is perceived from an organizational perspective (1.2). In this thesis, 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, thus making them appropriate domains for MPC applications (1.3). Per the preliminary research, research gaps are identified, and a problem statement (PS) is articulated (1.4). Thereafter, a research objective is devised, and research questions (RQs) are formulated (1.5), followed by a description of the societal relevance provided that the research objective is attained (1.6). Then, the research approach and research methodology for the objective and RQs are discussed (1.7). Finally, a clear overview of the research structure and thesis is provided (1.8).

1.1. Data sharing towards data contribution

Sharing data between companies brings a number of benefits: data can be shared and monetized (Thomas & Leiponen, 2016), or it can be shared with other parties to enhance business operations (Y. Huang, Hung, & Ho, 2017; Lotfi, Mukhtar, Sahran, & Zadeh, 2013; Sendhil Kumar & Pugazhendhi, 2012). When data from different entities and domains is put into context, new information and knowledge is created and discovered—see, for example Guan, Zhang, Zhou, and Dan (2020)—and this unlocks possibilities for economic growth (Zafir, 2006). Data sharing is also accompanied by barriers on different levels, for instance managerial, organizational, technological, individual and sociocultural barriers (Khurana, Mishra, & Singh, 2011). Such barriers result in a problem where companies refrain from sharing data beyond dyads (Du, Lai, Cheung, & Cui, 2012), resulting in data “silos”.

MPC, first addressed by Yao (1986), is a cryptography technology that can provide a solution to technological and managerial barriers in particular. MPC involves sharing information whilst not disclosing submitted data between any of the involved parties. As a result, it can be argued that MPC is not about sharing data, but about contributing data (Bestavros, Lapets, & Varia, 2017). Literature based on conventional or non-MPC-based data-sharing solutions use the term *share*.

However, *share* is avoided in this study because it suggests distribution to a trustee, for example, a third party. MPC users do not share their data; they contribute data, whilst not disclosing it¹. Furthermore, 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 a desired output—the output value of a function. These parties only gain knowledge based on the output of the protocol and their own private input (ibid.). At the same time, several practical intricacies are involved. Although the protocols themselves may be secure, the design of MPC applications must facilitate secure implementation (Herbohn, Frikken, & Schwarz, 2004) to decrease perceived barriers.

1.2. MPC as a problem-solving instrument. Is it?

MPC utilizes cryptography protocols to preserve the privacy and confidentiality of contributed data. Yao (1986) introduced MPC in 1986, and it has since been an active research area, mostly theoretical. Research has mainly focused on the technical aspects of MPC, such as finding cryptography methods for building SMC protocols; see, for example, Shukla and Sadashivappa (2014). This focus concerns performance improvements, namely algorithmic and security improvements; see, for example, Hirt and Maurer (2001); Maurer (2006). Scholars aim to make theoretical protocols more practical; however, despite advances in hardware, the underlying challenge is that practical implementation of MPC may be limited due to poor performance and scalability issues (Choi, Butler, & Genge, 2019).

Other streams of research focus on support for domain-specific applications; see, for example, Atallah, Deshpande, and Schwarz (2004). The body of literature showcases the many different applications for MPC; see, for example, Jagadeesh, Wu, Birgmeier, Boneh, and Bejerano (2017) and Zare Garizy, Fridgen, and Wederhake (2018) for two different applications. Moreover, there are various real-world deployments of MPC—Archer et al. (2018) highlighted some use cases and their technicalities. For example, in the context of SCs, Zare Garizy et al. (2018) presented an application to measure risk in SC networks. This use case is a clear example of a data-sharing case that would be averted by the users, or raise concern, in the absence of MPC.

However, MPC exists as an underlying protocol, meaning that the value proposition is not initially visible to the user. The utility of the output challenges the capabilities of the technology, given that the information from the output will lead to unlocking new values. In some cases, this would require users to provide more information to other parties. The use case of Zare Garizy et al. (2018) illustrates this challenge accurately. Furthermore, Kerschbaum et al. (2011) acknowledge that user acceptance is a critical issue since users must trust electronic systems, because “MPC raises the risk of selfish behavior, and all parties must feel confident that no one can game the system.”

It seems that there is a lack of understanding of how MPC is perceived from an organizational perspective and the true value it provides in the business environment. In its current form, MPC is deployed as an enabler for sharing protected data (i.e. sensitive, confidential, and private data). Nevertheless, literature that attempts to bridge the gap between a firm’s value creation, acceptance, and the potential of MPC is absent.

¹Data contribution is used throughout this thesis

MPC is effective for specific functions, suggesting that a context must be defined in which MPC is studied. MPC can be deployed in many areas, such as healthcare, aviation, and banking. For this study, SCs are the main focus, as previously introduced. Although the context may consequently seem to be limited to SCs, the results of the study are relevant beyond the scope of SCs and the logistics sector. This is because SCs are only used to discuss the application of MPC to real-world problems. In the next chapter, SCs and data sharing therein are further discussed, along with clearer descriptions of the reason that data sharing in SCs provides a suitable exhibition for MPC.

1.3. Data sharing in supply chains and MPC

An SC is referred to 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—a combined definition based on themes derived from SC definitions by [Atallah et al. \(2004\)](#); [Curkovic, Scannell, and Wagner \(2015\)](#); [Min and Zhou \(2002\)](#)). A simplified SC network example is depicted in Figure 1.1.

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 different stages, whereas 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

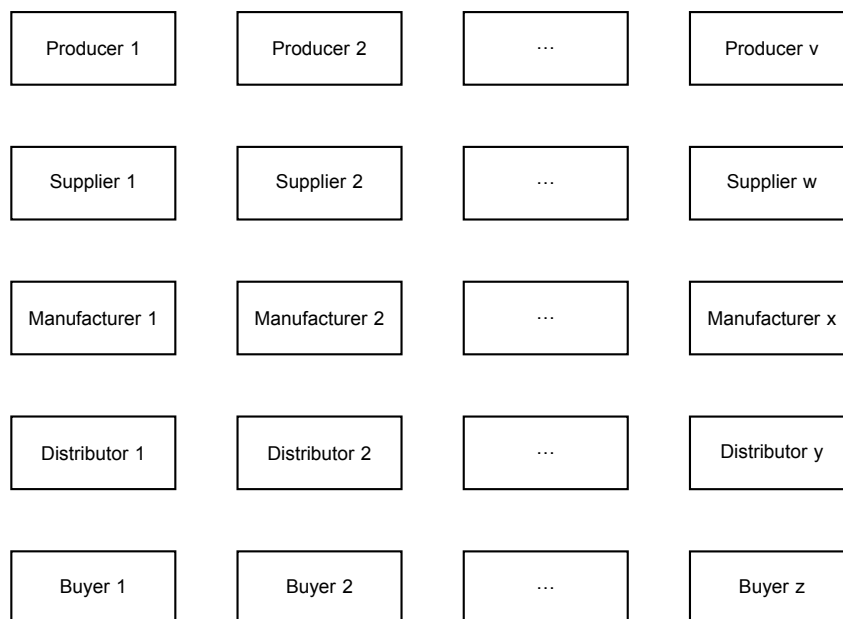


Figure 1.1: Simplified supply chain network.

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.” In addition, [Gopalakrishnan \(2001\)](#) defines SCM as a set of techniques utilized to efficiently integrate different entities to ensure that merchandise is produced and distributed in the right quan-

tities, to the right locations, and at the right time, to minimize system-wide costs while satisfying the service-level requirements.

Per these definitions, SCM encompasses activities at many levels: strategic, operational, and tactical. SCM has become increasingly important due to competitiveness introduced by market globalization. This has resulted in a growing interest in dealing with inefficiencies and the uncertainties faced by the dynamic complexity of supply chains (Milch & Laumann, 2016). The growing body of research on supply chain models also confirms this (Min & Zhou, 2002). Supply chain models 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, Loffi et al. (2013) provides 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 footnoteThe 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. (J. Li & Shaw, 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 in regards to data-sharing efforts within business-enhancing activities. This is because the data-sharing landscape faces many barriers. There is shareable and non-shareable data, and firms can be unwilling or unable to share certain types of data; see, for example, Ojha, Sahin, Shockley, and Sridharan (2019)). Concerns may initially arise regarding the purpose of sharing data, and a fear of sensitive information leakage may also exist. With such uncertainty, firms may choose to refrain from data sharing, and this uncertainty can reflect in security concerns, liability concerns, accountability concerns, legislative concerns, and strategic concerns (Khurana et al., 2011). In addition, 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, non-aligned goals, firms may also refrain from sharing data, for example, 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 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 are unable to draw any conclusions on the reasons that explain the rationale behind the organizations' contribution of protected data. For example, for the use case of Bogetoft et al. (2009), we are unable to make inferences on the aspects that led to the positive perception of MPC amongst farmers as a solution to 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.

Thus, while many potential opportunities are awaiting for MPC, an understanding is needed on

the elements that should reside in an MPC deployment for organizations to be willing to contribute data through it; regardless of the perceived value of the output, i.e., the aggregate analysis. Such insights allow us to increase the success rate of MPC deployments. Moreover, this enables us to separate MPC's actual value as a security mechanism from the value provided by the business case's output—although the two are interrelated when considering adoption. In other words, it provides a means which allows one to discriminate between the success or failure of the application of MPC and the underlying business case of the application.

1.4. Knowledge gap and problem statement

Most research on information and data sharing explain antecedents from a dyadic information sharing perspective. Table 1.1 provides an overview of different information sharing theories. In addition, several technology models were also considered. The reasoning why these were not suitable for this study is explained in Appendix A.1.

Theoretical lens	Diadic	Triadic	Extended	Total
Transaction cost economics	17	0	0	17
Relational governance theories (including relational view, social exchange theory, relational exchange theory, social contract theory and social capital theory)	17	0	0	17
Contingency theory (including information processing theory and configuration theory)	6	2	0	8
Resource dependency theory	7	0	8	7
Resource based view	3	1	0	4
Knowledge based view	2	0	0	2
Adaptive structuration theory	0	1	0	1
Capability-based perspective	1	0	0	1
Complex adaptive systems	1	1	0	1
Goal congruence theory	1	0	0	1
Industrial dynamics	1	0	0	1
Interdependence theory	1	0	0	1
Institutional theory	1	0	0	1
Organizational learning	1	0	0	1
Social network analysis	0	0	1	1
Socio-technical systems	1	0	0	1
Stakeholder theory	1	0	0	1
Total number of theories applied	60	5	1	66
Total number of papers reviewed	66	13	3	82

Table 1.1: Theoretical lenses applied vs unit of analysis. Adapted from [Kembro et al. \(2014\)](#)

Research on information and data-sharing typically explain antecedents for data-sharing from the dyadic information sharing perspective. Table 1.1 provides an overview of different information sharing theories. Besides, the models available in the literature are not suited for this study. This is explained in appendix refapp:Innovationadoptionimplementation.

These theoretical lenses focus heavily on the level of dyadic relationships ([Kembro et al., 2014](#)). They draw on relationship and trust models and the use of *traditional* channels of communication and traditional forms of information technologies; with setups that require organizational alignment, cultural, architectural, structural, and organizational shifts to mitigate risks, for example, see [Karafili et al. \(2017\)](#)). However, MPC is about sharing knowledge while not disclosing contributed data. As a result, many of the factors, as mentioned above, could be less relevant for MPC. This because MPC requires a different view of trust.

Our lack of understanding between this trust perception and willingness to contribute data indicates a research gap. The gap becomes clearer when taking into account the newness² of MPC in a business context. A knowledge gap is revealed when acknowledging that MPC's presence is not apparent within an MPC application. This gap is present in the space between literature concerned with application trustworthiness and requirements from the organizational side that should be met before they agree to submit their data through an MPC application. This gap hinders our understanding of the research areas that explain why MPC is, or is not, accepted as a solution to a problem. Thus, bridging the gap provides an understanding of an identifiable phenomenon which helps explain the acceptance of MPC for the security it provides.

A gap is also found in the space between MPC's technical theory and its use as a solution in the business context. As previously mentioned, the majority of research is concerned with the technical aspects of MPC protocols. However, while there are numerous MPC applications, there is a lack of literature that explains how MPC is perceived as a solution to the problem it solves. Bridging this gap allows the research community to develop new MPC solutions and effectively apply them to unresolved problems and provide the research community with insights on business requirements related to protected data through a privacy-preserving technology. The above is summarized into two main knowledge gaps:

KG₁ We lack an understanding of how MPC is perceived by organizations as a solution to secure data contribution even though it provides a solution to secure data contribution—this hinders us in our ability to discriminate between the value provided by MPC and other application-related aspects such as the value provided by the output of the application itself.

KG₂ We lack an understanding of how organizations perceive actual MPC deployments in terms of its adequacy in the data contribution process.

From the perspective of MPC adoption, this paper contributes the first—to our knowledge—on firms' willingness to contribute protected data through MPC applications. The following problem statement (PS) is formulated:

PS MPC could reduce organizational reluctance to contribute protected data. If organizations are convinced by it, they are more willing to contribute data, thereby allowing new business opportunities to evolve. This process is a positive contribution to economic development. However, we lack knowledge about organizations' willingness to contribute data through MPC-enabled applications, and we are unable to effectively draw inferences on their willingness to contribute data through an MPC-enabled application.

1.5. Research objective and research questions

There are several research areas concerning MPC (Zhao et al., 2019). The interest of this study lies in the practical side of MPC. Therefore, this study focuses on the area of *application-oriented MPC* (as coined by Zhao et al.). The conjecture is that MPC-enabled application users³ are more willing to partake in data-sharing-like activities in SCs compared to non-MPC-enabled users (i.e. those following contemporary practices). If this holds, then companies should ultimately be less

²The newness is assumed due to the lack of literature herein (e.g., case studies).

³for the purposes of this study *user* refers to the firm, including potential stakeholders, promoters, or actors that form part of data-sharing processes, e.g., data controllers, strategic managers, CIO, and data processors.

reluctant, or more inclined, to contribute data when MPC is adopted.

The objective of this study is to investigate the effect of MPC on organizational willingness to contribute protected data for collective purposes. The objective of this study is to investigate the effect of MPC on organizations' willingness to contribute protected data for collective purposes. We aim for the results to advance the frontiers of responsible MPC application development. The study should also provide clear directions for future developments. This is important because although MPC has potential, not all technologies are socially desired in the evolution of technical change. Per this objective, the following RQ is formulated:

RQ To what extent does MPC affect organizational perception of the [contribution](#) of protected data?

The purpose of this study is to understand how MPC is perceived by organizations for "data-sharing practices" that would be averted by these same firms. By assessing the extent, we gain a better understanding of the sustainability of MPC as a solution in business contexts. The RQ 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 is comprised of individuals (i.e. decision-makers).

Next, sub questions (SQs) are formulated to answer *RQ*. To examine the willingness to contribute data through an MPC application, a baseline is needed. A baseline defines a common language, helps to set the scope, and clarifies the direction of the research. Based on the literature review, MPC research is scattered, making it difficult to address the aforementioned problem. As a result, to define a baseline, the following question is proposed:

SQ₁ What is MPC, and what are the key aspects concerning the contribution of protected data through MPC?

The introduction explained that MPC is relatively new in organizational settings. Given that the literature regarding organizational willingness to contribute in the context of PPTs, or MPC in our case, is scarce, there is no framework that we can use. Nonetheless, we can establish a conceptual framework. Since there is no definitive theory, a conceptual model allows for combined theoretical constructs from different concepts within the literature ([Adom, Hussein, & Adu-Agyem, 2018](#)). This study therefore consolidates data-sharing implications that are raised separately in literature. In line with the problem statement, we ask the following question:

SQ₂ Along what dimensions would organizations evaluate an MPC application for the contribution of protected data, regardless of the value provided by the output of the application?

Using the findings of the qualitative study, a basis can be formed for the quantitative study. This allows us to quantitatively examine the contribution of MPC to a firm's willingness to contribute protected data, leading to the third SQ:

SQ₃ How is MPC perceived by organizations in terms of the previously defined dimensions?

Finally, the theoretical implications and the implications for practice must be described. The fourth SQ addresses this aspect:

SQ₄ What are the implications of the above findings in terms of the development of MPC?

1.6. Societal relevance

The MPC technology can be used as a tool to overcome trust concerns (Zare Garizy et al., 2018), create new business opportunities (European Union, 2018; Koutroumpis, Leiponen, & Thomas, 2017), and foster the European data economy in line with the European data strategy (European Commission, 2020; Zafir, 2006). 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, both lack of awareness and uncertainty may limit an organization’s willingness to use MPC-enabled applications, which in turn hinders acceptance, perhaps waving aside a potential technology that might solve the issue of business-wide aggregate data analysis. This is important because MPC seems highly dependent on network effects because sufficient participants are needed to conduct aggregate analysis.

This study contributes to the Safe-DEED⁴ (Safe Data-Enabled Economic Development) project. More specifically, this study contributes in terms of the area of perception of the technology (WP6, MPC demonstration). The Safe-DEED project brings together partners “from cryptography, data science, business innovation, and legal domain to focus on improving security technologies, improving trust as well as on the diffusion of privacy enhancing technologies to keep up pace with global macro-trends and the data economy, to enable the fastest possible growth.” The aim of the project is to provide “a set of tools to facilitate the assessment of data value, thus incentivising data owners to make use of the scalable cryptographic protocols developed in Safe-DEED to create value for their companies and their clients”⁵.

These endeavors are taken by TU Delft and six other participants, and they are funded by the European Union’s Horizon 2020 research. While, the Safe-DEED project considers MPC in data marketplaces, the study presented in this thesis positions itself in an SC context. Nonetheless, the result contributes to our understanding of the organizational perception of MPC.

1.7. Research approach and research methodology

The research seeks to understand the extent to which MPC affects willingness to contribute protected data. A hypothetico-deductive method is adopted as it provides a systemic approach to generate and test proposed explanations (Sekaran & Bougie, 2010). Next, a description is provided of the research method chosen to answer the previously discussed questions (summarized in Table 1.2).

The first SQ; “What is MPC, and what are the key aspects concerning the contribution of protected data through MPC?”, is answered through a literature review supported by informal interviews. The aim is to grasp the theoretical and practical bounds of MPC. This methodology helps to clarify the MPC research areas and current state of research. The informal interviews are performed to gain a better understanding of the problem and the reluctance phenomenon in practice. This is needed to properly scope our research.

⁴<https://safe-deed.eu/>

⁵<https://cordis.europa.eu/project/id/825225>

Research question	Methodology
What is MPC, and what are the key aspects concerning the contribution of protected data through MPC?	Literature review supported by informal interviews
Along what dimensions would organizations evaluate an MPC application for the contribution of protected data, regardless of the value provided by the output of the application?	Literature review, framework development
How is MPC perceived by organizations in terms of the previously defined dimensions?	Pre- and post-test experimental design
What are the implications of the above findings in terms of the development of MPC?	Desk research: reflection on findings

Table 1.2: Methodology per research question

The second SQ; “Along what dimensions would organizations evaluate an MPC application for the contribution of protected data, regardless of the value provided by the output of the application?”, is also answered by a literature review. As previously described in Section 1.4, a theoretical lens that fits the objective of the study (i.e. information sharing in the MPC context) is absent. Therefore, the concept of an IOS is used as a starting point; “Inter-organizational systems are information and communication technology-based systems that transcend legal enterprise boundaries” (Kumar & van Dissel, 1996).

IOS literature provides a useful starting point for the study by highlighting the problems arising with the adoption of IOSs, which pose many barriers, for instance the type of information that is shared, with whom information should be shared, and the challenges arising in the process of information sharing (Sendhil Kumar & Pugazhendhi, 2012).

Exploring the issues with the adoption of an IOS enables an understanding of the data-sharing issues that must be considered. Upon further investigation of these barriers, one can identify the parts of the technology that warrant attention and compare them with our understanding of MPC acquired from the previous sub question. This is done using innovation characteristics research. Then, a conceptual framework is established, and hypotheses are formulated. In essence, this study is theory-informed, not theory-driven (Waters, 2007).

The third SQ; “How is MPC perceived by organizations in terms of the previously defined dimensions?”, is answered by means of a pre and post-test experimental design. From the previous question, it is clear that an exploratory experiment is adopted, since “the concepts or categories in terms of which results should be understood are not obvious, the experimental methods and instruments for answering the questions are uncertain, or it is necessary first to establish relevant factual correlations in order to characterize the phenomena of a domain and the regularities that require (perhaps causal) explanation” (Burian, 2013).

Within the pre and post-test experimental design, a 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 protected data. This methodology allows for both quantitative and qualitative evaluations, thereby providing a prime indication of the contribution of MPC in the process of contributing protected data. To increase the richness of our findings, the quantitative results are supported by a qualitative assessment.

The fourth SQ; “What are the implications of the above findings in terms of the development of MPC?”, is answered through a reflection on the research results by means of desk research. Herein, the questions are answered, and the findings are discussed. The theoretical and practical implications as well as the contributions are presented, along with the limitations of the study and recommendations for future research.

1.8. Thesis structure and outline

The structure of the methodologies and the subsequent results, based on the problem statement, research objective, and RQ and SQs, is depicted in Figure 1.2. This diagram depicts the flow of the thesis. The aim of this diagram is to provide a clear understanding of the integration of the different parts towards a structured body of knowledge. This reflects the flow behind the conclusions drawn and suggestions proposed. The thesis is organized in four parts:

The thesis is organized in four parts:

Part I comprises the thesis definition and the research methodology used for this study.

Part II seeks to understand the aspects that must be understood to examine organizational willingness to contribute protected data through MPC. First, MPC is decomposed to understand its intricacies and to determine a suitable approach for the given problem. Next, a literature research is performed to understand the factors that must be examined with respect to an organization’s willingness to contribute protected data through MPC. Without being exhaustive, we set out to present a comprehensive understanding of the aspects that are likely to determine that willingness.

Part III shifts the focus towards the experiment and analysis. A treatment is used for the experiment. First, the design of this treatment is discussed—from concept to deployment—including the literature on which it is based. All information, features, and functionalities that should be included in the treatment are elaborated upon. In the subsequent chapter, the experimental design and data collection are discussed, and the quantitative and qualitative results of the experiment are presented.

Part IV concludes with a thorough discussion of perceptions of MPC in the business context. We elaborate on the contribution of this study to the academia and draw our final conclusion.

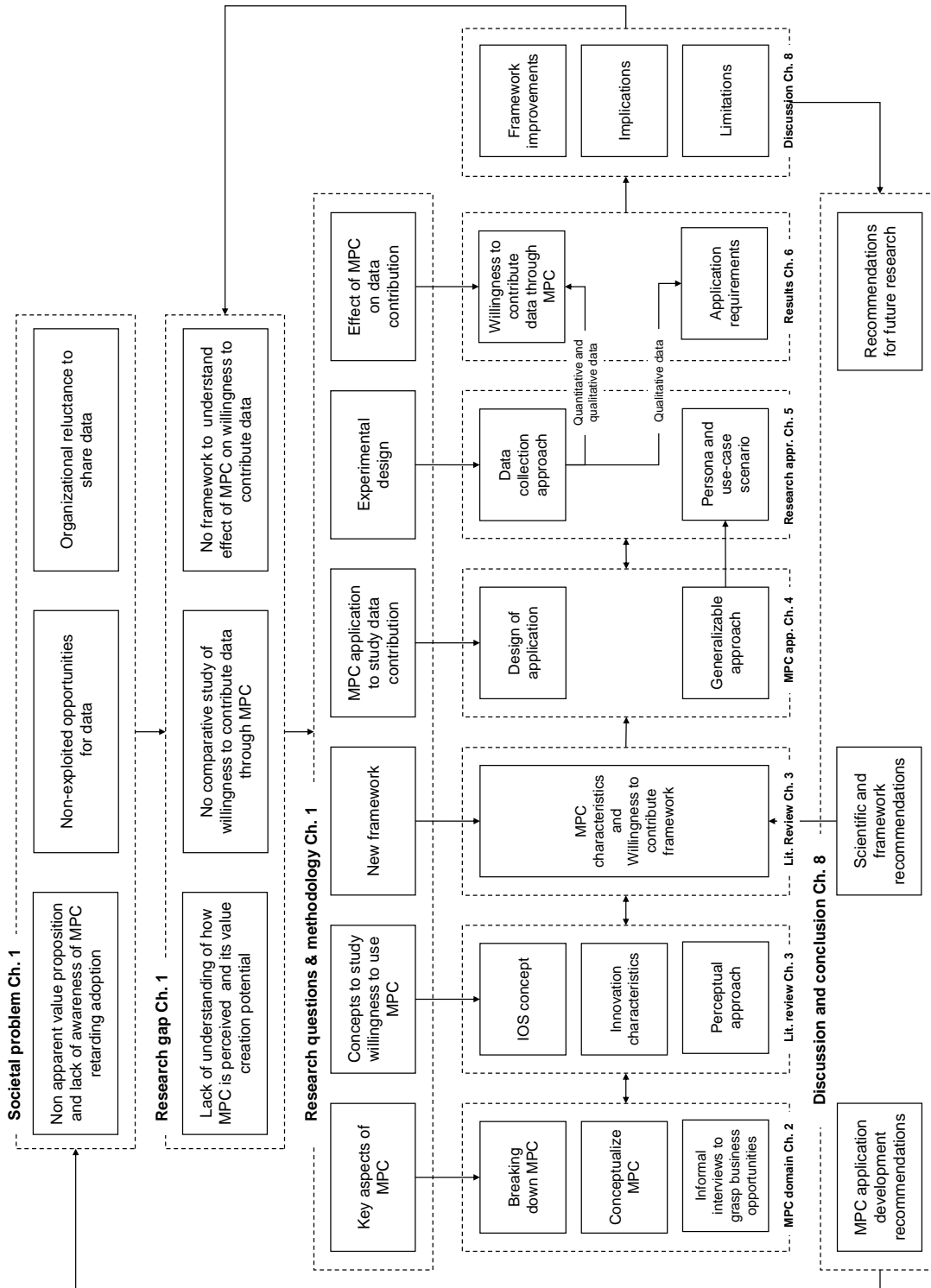
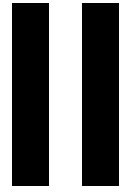


Figure 1.2: Thesis structure



Literature research

2

MPC domain

In this chapter a thorough examination of MPC is performed in line with the research objective, and to answer SQ_1 : “What is MPC, and what are the key aspects concerning the contribution of protected data through MPC?”.

It is first described what MPC is, and several technicalities and practicalities of MPC are discussed (2.1). Literature is then synthesized in order to understand how MPC works (2.2). Aside from providing clarity on how MPC is deployed in practice, this part also enables the researcher to communicate MPC consistently with organizations. Moreover, MPC is described in the form of characteristics (2.3). These characteristics should make clear the context in which MPC is deemed suitable. Several potential MPC application use cases in SC are derived through these characteristics (2.4). At the highest level of abstraction, several MPC research domains are identified; however, it remains unclear how the different parts add to the whole concerning the application-oriented domain. Therefore, an overview is established of the various items related to MPC adoption (2.5). This is used to describe the area of focus in this thesis. Moreover, this makes clear the reasoning behind the project scope.

2.1. Introduction to 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 $P_i (i = 1, \dots, n)$, each with a concealed dataset x_i , whereby they jointly and interactively compute an objective functionality $f(x_1, \dots, x_n) = (y_1, \dots, y_n)$ (application oriented task such as electronic voting) based on their inputs (Zhao et al., 2019) (see Figure 2.1.).

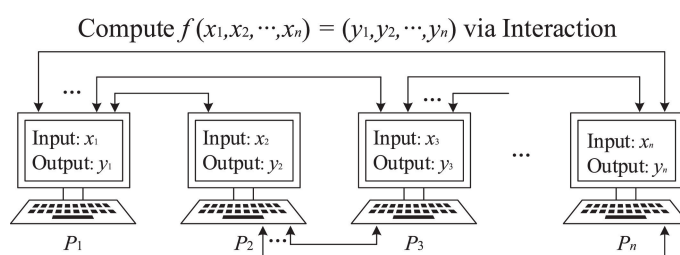


Figure 2.1: Diagram of Secure Multi-Party Computation. Adapted from Zhao et al. (2019)

The following example provides a case that is recognizable and is easy to enact. Assume several wine distributors (parties) that wish to compare their labor and capital cost over the number of produced goods to benchmark their performance. Each IP provides input data as a set in the following format: $x_i = (L, N)$, with:

- L is labor cost in euros;
- N is number of bottles dispatched.

```

input : Array of set of L and N
output : ALP
Function calculate_alp(X):
  sb ← 0 // sum bottles
  slc ← 0 // sum labor costs
  L ← length(X) // length of array
  for i ← 1 to L do
    // loop trough each party's dataset
    l ← X[i][0] // index 0 is labor cost value
    n ← X[i][1] // index 1 is number of dispatched bottles value
    sb ← sb + n
    slc ← slc + l
  end
  ALP ←  $\frac{sb}{slc}$  // Average Labor Productivity
  return ALP

```

Functionality 2.1: Arbitrary benchmarking functionality

The parties compare Labor Productivity (LP) through functionality 2.1. Functionality 2.1 is an arbitrary functionality¹. The function can be further extended with any other sub-function—it is solely meant to illustrate a function that requires firms to ‘share’ sensitive data. Needless to say, none of the warehouses wish to reveal their data. However, when parties collude, it is clear that the colluding parties can extract information from other parties, even when the application is *secure*. This vulnerability is a simple explanation of an example of what scholars refer to as the threshold of the adversary’s corruption capability (Maurer, 2006).

Functionality 2.1 also depicts a similar problem reported by Zare Garizy et al. (2018). That is, more data would be required to draw correct conclusions. In the case described here, more data is required to draw correct benchmarking conclusions. That is because comparing one’s average labor productivity against the aggregate average labor productivity will lead to misleading conclusions. Other information such as type of goods, use of capital, and order picking units are also needed. However, such information brings one closer to the possibility of linking results to IPs, for example, market leaders within a branch). This brings to surface an important aspect. While a protocol can be secure, the computation itself can leak information about the inputs.

¹An SMPC protocol that can compute arbitrary functionalities is referred to as a generic MPC protocol.

These challenges concern requirements that MPC protocols must satisfy to cover possible adversarial attacks related to privacy, correctness, independence of input, guarantee of output, and fairness (Zhao et al., 2019). Thereby several security models for MPC are defined. Based on the behaviour of the adversary, security models can be categorized into *semi-honest or passive* adversary model (i.e. users execute protocol as provided but may attempt to glean information from the output); *malicious* adversary model (i.e. corrupted participants may arbitrarily deviate from the protocol's specifications based on the adversary's instructions) (Bestavros, Lapets, & Varia, 2017; Catrina & Kerschbaum, 2008); *covert* adversary model (i.e. user who cheat only if 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); and *rational* adversary model (i.e. user will only cheat the protocol in order 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 is able to resist any adversarial attacks under the corresponding security model” (Zhao et al., 2019). However, MPC is still in its infancy (Choi et al., 2019), and to date, not all technical challenges have been practically solved (Zhao et al., 2019). Besides performance limitations, several implementation challenges are identified (e.g. see challenges addressed by Toldsepp, Pruulmann-Vengerfeldt, and Laud (2012), the *Usable and Efficient Secure Multiparty Computation* (UaESMC) project²). 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) argues that weak adversary models—which are technically more efficient—can still be satisfactory when considering incentives behind the collaboration. Other forms to cope with these challenges are applications which 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)³.

Trust is also an important factor. Faujdar, Agahari, de Reuver, and Fiebig (2020) examines the role of MPC on perceived security and trust, in respect of 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 enhanced security does not necessarily imply consent. Meanwhile, when considering the usage of MPC, the benefits of information sharing depend on one's ability to use the algorithm's output. Hence, this requires a function backed by win-win scenarios.

2.2. MPC architecture fundamentals

MPC can be deployed in many ways. In essence, MPC is deployed in a distributed computing environment. Figure 2.2 illustrates an example of an architecture. This section gives a brief explanation of this. In general, MPC comprises input parties (IP) delivering concealed data (i.e. sensitive, confidential, private) to the confidential computation; the result parties (RP) receiving results (or partial results) from the confidential; and, the *independent* computing parties (CP) jointly computing the

²<https://cordis.europa.eu/project/id/284731>

³See whitepaper on <https://www.unboundtech.com/>

confidential computation (Archer et al., 2018)⁴.

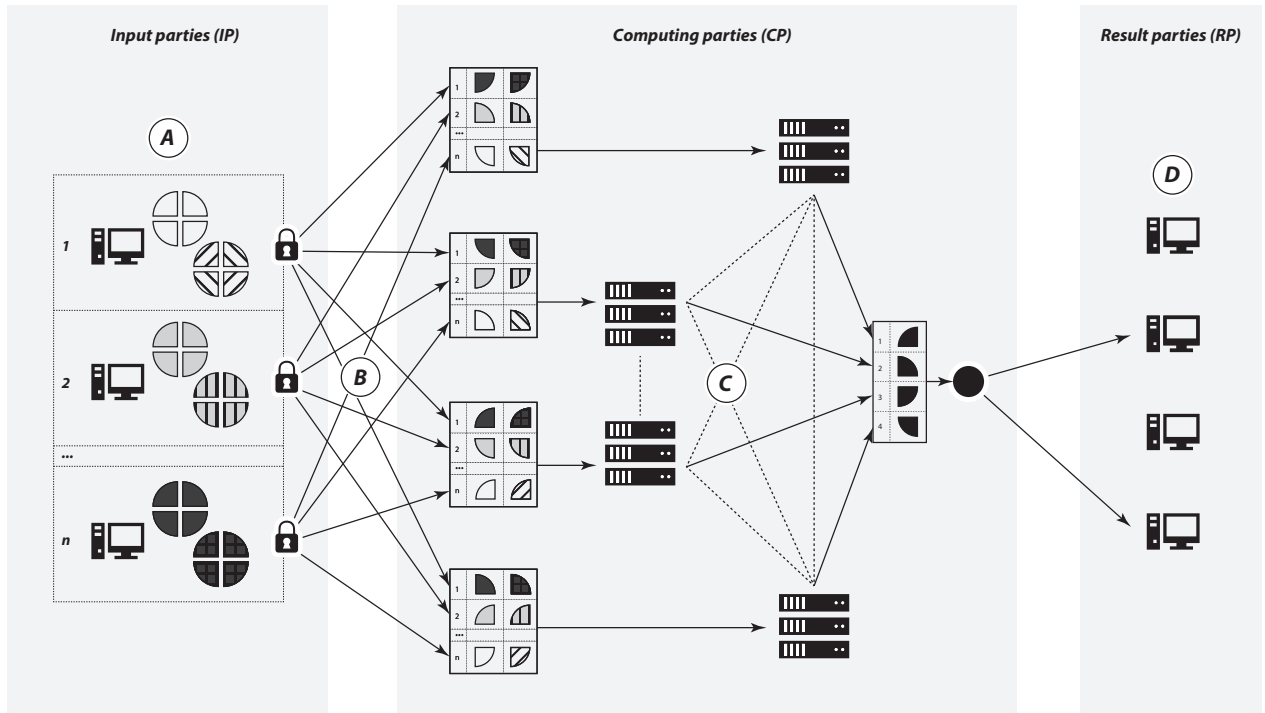


Figure 2.2: Example MPC application architecture with data flow. This diagram is based on building blocks drawn from the architectures of [Bogetoft et al. \(2009\)](#) and [Bogdanov et al. \(2012\)](#), and MPC working principles of [Bestavros, Lapets, Jansen, et al. \(2017\)](#).

In its most basic form (e.g. Figure 2.1), application users hold roles of IP, CP and RP). In practice, when considering inter-organizational collaboration, this is unlikely to be the case for several reasons, which become more clear throughout this thesis. In brief, from a technical view, most real-life applications require heavy computation servers for the computation process. Requiring many organizations to take the role of CPs places a burden on resource requirements to these organizations, which hinders adoption.

The data contribution process comprises two phases. The first phase comprises submitting and distributing the input (indicator A and B in Figure 2.2). 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 the case of [Bogetoft et al. \(2009\)](#) (applet), 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 channel⁵. Each interface has different perceived benefits; for example, a web-based form allows application-users

⁴Each MPC protocol has different properties (i.e. the number of CPs, number of input shares, limitations of CPs, etc.) that define the security, efficiency and robustness. [Archer et al. \(2018\)](#) provides a comprehensive overview of the important properties.

⁵For web-based forms; there are JavaScript libraries to turn user input into secure input source for MPC. See [Hastings, Hemenway, Noble, and Zdancewic \(2019\)](#) and corresponding GitHub repository at <https://github.com/MPC-SoK/frameworks> for an overview of open-source MPC frameworks. Also see <https://github.com/rdragos/awesome-mpc>.

to authenticate themselves to the application and benefit from the public internet.

The second phase (indicator C and D in Figure 2.2) comprises the multi-computation part and distribution of the 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; for example, through private and public keys). A requirement is that CPs must be independent and incentivized not to collude. This is also the case for the IPs.

2.3. MPC landscape

MPC can be deployed in different frames of reference. Applications can be deployed between companies within the same domain; for example, for assessing common customers between organizations for marketing purposes; it can be deployed across different units within the same company; for example, for cross-selling, which may be inhibited by data regulations; and it can be deployed across supply chain tiers; for example for streamlining manufacturer-supplier SC. Information sharing within these contexts can lead to enhanced information integration. As previously discussed, the challenge is that in a decentralized system, each party (can) act based on its separate objective functions. As a result, when information is shared within a network, once shared, the incentive between the companies could dissolve due to information asymmetry. This issue may result in the so called "one-shot game"⁶). 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. This is also necessary to understand the (supply chain) domains in which it is of interest. We characterize (*C*) MPC context by an environment where:

- C_1 A trusted third party (TTP) may be needed as a trusted middleman;
- C_2 A data protection regime inhibits data-sharing, or;
- C_3 data usage goes beyond legitimate purpose;
- C_4 Collusion is impractical or futile;
- C_5 Exposure from traditional non-mpc data sharing practices can lead to a *one-shot game*;
- C_6 Parties can agree on a computation function, while;
- C_7 all parties can gain from the output, and;
- C_8 are able to distill and provide corresponding input data at the required level of quality.

A noteworthy mention is that C_4 is not relevant for all adversary models.

⁶A party or parties have an incentive to behave opportunistically or in self-interest, which results in a single transaction, with no repercussions

2.4. Potential MPC application supply chain use case scenarios

This section presents several general supply chain scenarios that fit the characteristics described in the previous section. These scenarios are derived from literature research and extended based on informal interviews with supply chain professionals or derived only from the latter (also see [Toldsepp et al. \(2012\)](#) for other generic use cases and apparent industry requirements).

Collaborative distribution (DC)

In general, a distribution center (DC) is a warehouse (also referred to among other names as order fulfillment center), which is stocked with products (goods) to be distributed to other parties. A DC is the order processing element of the entire order fulfillment process. Traditionally, DCs process sets of products offered by the organization. Some DCs experience (high) fluctuations in demand, for example, seasonal demand. The use case here leverages on this issue. If a DC (company A) allows another DC (company B) to process their goods and redistribute them, it enables better utilization of capacity and more stable allocation of resources—through an additional stream of income. We refer to this delegation as collaborative distribution consistent with [Phillips \(2015\)](#). This notion is found particularly of interest for goods that are (only) sold in bulk by the supplier; have a short turn around time and require simple processing; can be easily delegated—for example, a bulk of goods transported to a DC which is broken up into smaller amounts and subsequently redistributed to retailers). An MPC application allows organizations to outsource only when there is a match. It does not send out requests ‘publicly’ and thus not giving away information such resource constraints or strategies used.

Problem:	Fluctuations in demand cause unstable use of capacity and allocation of resources, and; a non-utilized stream of income.
Solution:	Dynamic distribution capacity and resources among warehouses.
Requirement:	Share information with other parties about demand, resource, and capacity.
MPC need:	Through bidding, provide information only when there is a match.

Freight bidding

Freight bidding refers to the process of submitting proposals to both incumbent and prospective carriers. In seeking transportation services, shippers typically tender request for quotes (RFQ)—in a highly competitive environment. In broad terms, shippers open bid processes, follow a bid-analysis exercise and issue contracts to winning carriers ([Guo, Lim, & Rodrigues, 2003](#)). Some shippers outsource this process to TTPs to secure high-quality carriers while controlling the costs. The trusted role of the TTP herein is to procure carriers while not disclosing bids to any parties. This use-case is in several aspects similar with trade production contract exchange deployed by [Bogetoft et al. \(2009\)](#). This use-case relates to secure auctions—an emerging field of MPC research ([Brandt, 2001](#); [Brandt & Sandholm, 2005](#); [Chen et al., 2019](#); [Franklin & Reiter, 1996](#); [Lipmaa, Asokan, & Niemi, 2003](#); [Naor, Pinkas, & Sumner, 1999](#); [Wang, Leung, & Wang, 2004](#)).

- Problem: In a highly competitive environment carriers and shippers attempt to match bid and ask prices.
- Solution: Share data through a trusted third party.
- Requirement: Share price and capacity information.
- MPC need: Match bid and ask prices and release information only when there is a match—without the need of a trusted third party.

Demand and production coordination

This use case builds on the notion of integration of the supply chain partners. Vertically and horizontally integrated supply Chains can reduce inefficiencies in forecasting (Merkuryeva, Valberga, & Smirnov, 2019), mitigate the bullwhip-effect (J. Li & Shaw, 2001), and prevent double marginalization (Guan et al., 2020). Integrated supply chains become even more feasible with advancements in internet-of-things (IOT); see, for instance, Zheng, Wu, Sun, and Pan (2019) for demand and production coordination in an industry 4.0 supply chain context). Since parties wish to find, for instance, optimal output levels, this use case relates to *private set-intersection* in the multi-party setting (Kolesnikov, Matania, Pinkas, Rosulek, & Trieu, 2017). It should be noted that this use case requires a compliance regime (Cachon & Lariviere, 2001).

- Problem: Lack of information synchronization between supply chain members results in inefficiencies in the supply chain.
- Solution: Build trust networks and share information required to reduce inefficiencies.
- Requirement: Share sensitive information such as prices, forecasts, demand, and stock.
- MPC need: Calculate optimal output levels for each member without seeing the underlying data coming from supply chain members.

Group purchasing

Group purchasing organization (GPO) refers to an organization in which cooperative purchasing processes take place. It consists of dependent or independent organizations that bundle together to attain, among other benefits, reduced workload, lower purchasing prices, lower transaction costs, and reduced supply chain risks. While GPOs are believed to provide benefits, there are cases where it does not (Schotanus, 2007). Zhou, Dan, Ma, and Zhang (2016) argues that under a common wholesale price contracting scheme, information sharing has a negative effect in exacerbating double marginalization resulting in no incentives to share information, subsequently eliciting group purchasing harmful to the supply chain. However, the premise under the assumption of information asymmetry is unlikely to hold in an MPC setting. Because information is not ‘shared.’

- Problem: Group Purchasing Organizations (GPOs) serve as an intermediary in aggregate purchasing volume. That is, the GPO has information about market supply and demand and pricing, giving bargaining power resulting in higher costs to the buyer.
- Solution: Direct aggregate price.
- Requirement: Share demand information; and bid price.
- MPC need: Without a middle man, fair bidding and selling can take place.

Inventory sharing

Suppose two or more companies sell the same (or similar) merchandise in the same region, in (close) proximity, or areas of interest. In that case, these companies are better off when they combine their inventory. Benefits include improvements in dispatch speed, lower transportation costs, and better coverage. Combining inventory is an interesting area because of the limitation of distribution centers (DC). DCs are typically positioned at locations that yield the best distribution strategies. To expand coverage while maintaining dispatch commitments—such as customer delivery times—, organizations can, among other options, utilize more DCs. This is a capital commitment that requires careful planning.

An MPC platform can allow firms to combine their head and long-tail stock only when necessary. Revenue and costs can be subsequently shared, without openly giving away protected data such as buy-in-prices. An underlying motive is the increasing interest in *same-day* delivery. No literature has been found for the concept of inventory sharing.

Problem:	High demand variations may require ineffective warehouse expansions.
Solution:	Deploy a warehouse-space-sharing system.
Requirement:	Share capacity information; and prices.
MPC need:	Match storage request with capacity, bid and ask prices; and release information only when there is a match—without the need of a trusted third party.

Performance benchmarking

When companies benchmark their performance, they gain insights in performance gaps, identify areas of improvement, formulate better industry performance metrics, and so forth (Bogetoft & Otto, 2011). The challenge with this use case is the need for common standards. However, when this challenge is solved, firms are better able to attain continuous improvement. An MPC platform can, as previously elaborated through functionality 2.1, serve as a means to benchmark without giving away protected data. The COBE project⁷ (COntidential BEnchmarking) is an actual deployment of MPC for benchmarking. Benchmarking is an active field of MPC research (Damgård et al., 2017).

Problem:	Benchmarking requires organizations to share sensitive data.
Solution:	Build trust networks or make use of a trusted third party.
Requirement:	Share sensitive organizational data (depending on the metrics).
MPC need:	Calculate benchmarking metrics without each party seeing the underlying data.

Supply chain network risk analysis

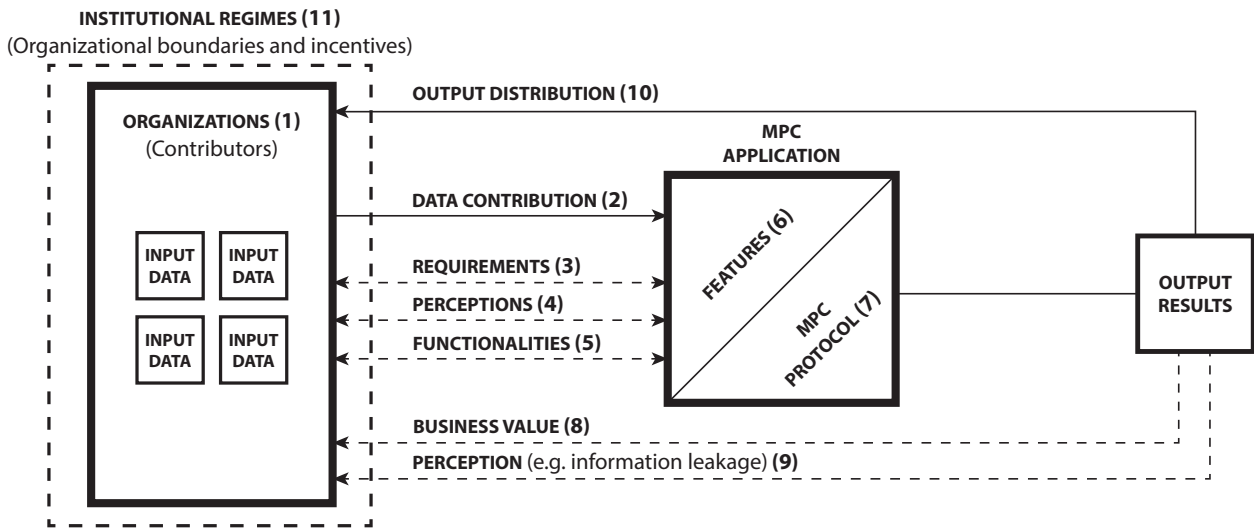
Some scholars consider data sharing to elicit risks in supply chains due to the increasing complexity of SCNs as a result of globalization and new business models, see, for example, Zare Garizy et al. (2018)). However, this scenario requires sharing protected data. MPC can serve a means to calculate risks in the network without giving away protected data. For instance, see Adhikari, Bisi, and Avittathur (2020), which describes possibilities to deal with supply and demand uncertainties.

⁷<https://alexandra.dk/uk/cases/cobe-confidential-benchmarking>

- Problem: Uncertain market developments result *unknown risks* for producers and suppliers.
- Solution: Coordinate efforts in order to reduce mutual risks.
- Requirement: Share sensitive organizational data.
- MPC need: Allows sensitive information to be shared without resulting in information asymmetry.

2.5. Assumption, scope, and terminology

This section provides an integrative overview of MPC aspects. Figure 2.3 illustrates this overview. Some of the aspects herein are already described in this section, and some are not. This overview is not meant to provide a list of all literature concerned with each aspect, nor is it our intent to give credit in this way.



1	Bestavros, Lapets, and Varia (2017)	2	Bestavros, Lapets, Jansen, et al. (2017)
3	Kanger and Pruulmann-Vengerfeldt (2015)	4	Fajdar et al. (2020)
5	Bestavros, Lapets, Jansen, et al. (2017)	6	(<i>ibid.</i>)
7	Archer et al. (2018)	8	Kanger and Pruulmann-Vengerfeldt (2015)
9	Zare Garizy et al. (2018)	10	Bestavros, Lapets, and Varia (2017)
11	Atallah et al. (2004); Bestavros, Lapets, and Varia (2017)		

Figure 2.3: MPC aspects identified

Arguably, an MPC application is a deployment of a protocol (7) integrated with several features (6), which provides functionalities (5) to organizations⁸ (1) depending on their requirements (3). What organizations are ‘allowed’ to do with their data is, in a broad sense, determined by institutional regimes (11). In addition, depending on the class of data shared, such as sensitive, private, confidential, secret data, organizations determine how critical the data in question is and the level of protection needed to safeguard it. Before organizations *contribute* (2) their input data (i.e. not share) several aspects come into play.

⁸organizations is used interchangeably with firms, companies, and enterprises in this document.

While organizations might have requirements themselves, the application itself could also pose requirements for them. Whether the organization will ultimately contribute its data depends on two main perceptions. One concerns perceptions regarding the MPC application itself (4). And the second concerns perceptions of the output (9). MPC can be viewed as a box comprising an input part and an output part. Which one is considered more important depends on the innovation phase (discussed later) and is likely to vary across organizations.

First, we consider the output part. The main item of interest herein concerns the information that may be leaked by the output of the MPC application itself *and* the value the output or the contribution as a whole provides value to the organization. This part taps into the question of *why* one should contribute data and at what risk—assuming a safe input in an ideal world. The first part (i.e., the input part of the application) concerns the perceptions of the input side of the application since MPC runs “under the hood” (users are unable to detect the running of MPC). The input part taps into *what* is needed for the output to be generated and *how* the output comes to place (the computation part). Thus while an MPC application may be perfectly safe, whether one feels it is safe is determined by how the information concerning the protocol is conveyed. In turn, the functionalities provided by the application makes it usable.

The distinction between input and output part is important because security is likely not the primary goal of the users, but the secondary since users pursue value from the output. Therefore, let us elaborate more on why the input and output parts should be approached as separate parts. The output is expected to be sensitive to the value it provides. This encompasses the business model aspect of the application. In addition, the output itself could also leak data. As a result, our conjecture is that perceptions related to aspects such as security and confidentiality depend on several factors. For instance, the output of an aggregate analysis may be needed for the organization to run its business, thus potentially resulting in higher risk-taking postures. Also, while one party may have analytical skills to ‘learn’ (glean) information from the output, others may not.

As a result, whether the perceptions of the application are positive or negative needs to be researched. Thus, how the final output must be shaped warrants a separate study. A study of perceptions of both the input and output part would likely results in a large experiment—at the current stage of research development. Hence, for this study, we limit our scope to the input part. To reiterate for the sake of clarity; in this study, we look into organizational perceptions of MPC applications with respect to features—which covers requirements and functionalities. As a result, the primary goal of users is confidentiality and not the value of the output.

For this study, the technical characteristics such as scalability, are less relevant. Rather, in line with the research goal, our study concentrates on the belief that MPC is optimal for its intended purpose. Thus, for this study, an environment is considered that allows for this assumption.

2.6. Conclusion

In sum, this chapter discusses what MPC is; which practical and technical aspects warrant attention in terms of willingness to contribute data; how a practical deployment of MPC looks like; how MPC can be applied to real-world problems; what the research areas of MPC are; and finally, describes the focus and boundaries set for this study. Altogether, this provides an answer to SQ_1 . This chapter

concludes the baseline for the study.

3

Willingness to contribute data

There is a lack of literature concerned with the adoption or implementation of MPC application. Therefore the problem is approached as follows. In the first section (3.1) literature is reviewed to understand interorganizational systems (IOS) used by organizations to exchange information. The vast body of literature available for this concept enables a better understanding of the issues related to systems used for data and information exchange between organizations. Then, we view MPC as an innovation and break it down into relevant attributes (3.2). This is performed through the use of innovation characteristics research. These attributes are derived from IOS, MPC, and innovation characteristics research literature. Through these attributes, the aspects that are addressed by companies when considering willingness to contribute protected data through MPC, become clear (3.3). The attributes are conceptualized in context of MPC comprising three constructs: perceived trustworthiness (3.4), perceived security (3.5), and perceived relative advantage (3.6). Finally, in order to answer RQ hypotheses are formulated (3.7). To test the hypotheses a simple conceptual model is developed (3.8).

In the subsequent chapter we operationalize willingness related aspects into measurable elements (3.9). This operationalization process is further extended with elements that enhance our understanding of MPC; more specifically, this concerns elements related to the attributes defined in Section 3.3. Altogether, this approach allows us to understand the importance of perceived trustworthiness, security, and relative advantage on willingness to contribute; it allows us to understand the effect of MPC on these aspects; and it allows us to understand how MPC affects perceptions concerned with MPC-defined attributes defined in section 3.3. This multi-faceted approach allows us to properly answer SQ2 and SQ3.

3.1. Interorganizational systems (IOS)

3.1.1. Introduction to IOS

In the previous chapter, several examples are given that show the benefits of information sharing in SC. Herein, information systems (IS) play a vital role. An SC with interlinked members (i.e. distributors, suppliers, etc.) through ISs is referred to as an IOS. IOS enables the movement of information across organizational boundaries (Johnston & Vitale, 1988). It provides the ability for computer-to-computer communication of business transactions, which in general has four levels of sophistication—communication, coordination, cooperation (Premkumar, 1999), and collaboration (Ali, Kurnia, & Johnston, 2008). Literature is not consistent with the description of these terminolo-

gies, however. For example, (Premkumar, 1999) refers to cooperation in IOS as “two business partners share common goals” while this is referred to as collaboration by Ali et al. (2008). Hence, a clear definition is in order.

Communication refers to a ‘simple’ electronic transfer of information. With coordination, information is exchanged (ad-hoc) amongst parties in support of a pre-defined objective. With cooperation, relevant information is exchanged in support of each party’s goal. With collaboration, all parties work together in line with a common shared goal; thus, for collaboration, cooperation is needed. With respect to the research questions, ‘collective purposes’ refers to cooperation and collaboration.

Application examples of IOS are Electronic Data Interchange (EDI) (communication infrastructure, see Choudhary, Pandey, Nayak, and Mishra (2011)) and Collaborative Planning, Forecasting and Replenishment (CPFR) (cooperation and collaboration infrastructure, see Zhongwen (2010)). IOSs can be classified as horizontal (companies that operate at common stages of the value chain performing similar value-adding activities), vertical (linking tiers such as distributors and manufacturers within the SC), and cross-linkage (spanning both vertical and horizontal dimensions linking the aforementioned parties with each other at different stages in the value chain) (Hong & Changsu Kim, 1998).

3.1.2. Interoperability problems raised by IOS

When discussing IOS, the classification of interoperability problems is needed. These are problems that arise from requirements to allow firms to operate between one another. An understanding of the problems makes clear the degree of resource investment needed to enable interoperability (Panetto, 2007). Interoperability is a technical issue and is a means to achieve integration. Panetto synthesizes several models that take different perspectives. Interoperability can be related to the kinds of systems (technical interoperability and the complexity of interoperations) between systems. It can also be related to the ability of firms to interoperate. This can be further related to the type of content of the exchange flows, which considers structuring and automating the exchange and interpretation of data to enhance the operational effectiveness of the exchange. Finally, it can be related to the availability of interface.

Thus, application interoperability spans organizational, semantic, and technical aspects. Organizational interoperability concerns issues that contribute to the construction and maintenance of interoperable systems. Technical interoperability concerns the ability of systems to interoperate. Semantic interoperability concerns issues for ensuring that data can be exchanged, understood, and processed in a meaningful way. Further, classification concerns diachronic interoperability (processes changing over time) and synchronic interoperability (processes occurring or existing at the same time). The former comprises applications that exchange models with similar semantics but need to be syntactically transformed before being exchanged, such as communication between disparate data repositories). The latter comprises issues where applications exchange models defined by compatible languages (the same syntax) but with different semantics, in a synchronous way. The key take-away derived from the work of Panetto is that interoperability may require the internal exchange of data on top of the MPC application—for example, collecting data internally from

bottom (i.e., at the shop level) to top (i.e., the business level). In this process, semantic alignment and syntactic (model transformations) may be required.

When the problem of interoperability is solved, the focus shifts towards the degree of the interdependent relationship between the activities of the firms (Kumar & van Dissel, 1996). Herein the greater the level of interdependency, the greater the intentional or accidental harm one unit can inflict on another (ibid.). Through this lens, different IOSs are distinguished, which inherit different types of risk of conflict, for example, opportunistic behavior (ibid.). Herein, there are transaction costs. These are “costs of managing the interaction while keeping the opportunistic behavior under control so that ongoing cooperation between the units can be sustained” (ibid.). These costs require risk management through mechanisms such as trust, to identify, assess, and manage dynamically occurring risks (Lei & W., 2005).

It is now clear that IOS implementation is faced with a complex adoption process, requiring interorganizational dependency. A review of relevant literature reveals that IOS adoption and implementation factors studied in the literature related to integrity (trust, risk, dependency, goal, verifiability, governance, quality, security), resources (cost, compatibility), and advantage (performance, improvement) (see Appendix A.3).

3.1.3. Implications of IOS for the study of MPC

Prior to IOS adoption, participating parties are known. This is not necessarily the case with MPC, however. This aspect makes the concept of IOS in its current form (i.e., in existing literature) in several respects different from MPC. Sendhil Kumar and Pugazhendhi (2012) and Ham and Johnston (2006) introduce the notion of unfavorable relationships, which we can apply to the characteristics of MPC. Herein, MPC, as a mediation agent, should weaken interdependency (degree of relationship) due to control limitations. This finding is consistent with the results of Ham and Johnston (2006), which from the perspective of interorganizational innovation adoption as an emergent process, explains the slow adoption of Inter-organisational Supply Chain Management (IOSCM) initiatives because each type of IOSCM affects the extent of interorganizational structure which is linked to a degree of relationship intimacy.

Given that with MPC participants compute a pre-defined function, we view MPC *applications* from an IOS perspective as an IOS system with a ‘protective’ layer with limited and controlled functionality. The IOS concept highlights adoption elements at an organizational level. However, there are several implications that need to be considered. Because information and control are managed in most real-world supply chains, “not by a single decision-maker, but by several decision-makers, each with their own, often incompatible, objective functions, and each using her/his own proprietary information” (Atallah et al., 2004). Thus, IOSs are used in decentralized systems.

However, when an SC is conceptualized as a centralized system (a single entity controls all parties within the SC), many factors carry a different weight when compared to a decentralized system. In MPC context, an SC is, in a theoretical sense, a centralized system. Herein, openness, transparency, and visibility are pre-defined¹ and perceptions herein differ between users. Thus, in the case of MPC, organizational behavior lies mainly on perceptions of the application, while in

¹When considering an MPC application built for a specific purpose

the case of IOS, the behavior is shaped by formal agreements. As a result, per this view, we also conclude that *trust* carries a different meaning when viewed from an IOS or MPC perspective (i.e., dyadic trust versus application trust).

A final remark is that when developing a solution by means of MPC, one needs to understand the interoperability issues arising with respect to data requirements laid out for participating members. Herein interoperability refers to the link between enterprise systems and the MPC application. Determining the requirements for input data warrant close attention, for it can cause interoperability challenges, which may induce negative interoperability perceptions hindering acceptance of the application. Since applications are expected to have different organizational impacts, rather than trying to understand which specific changes are needed, an understanding of the degree of changes needed for interoperability is expected to provide more meaning.

3.2. Innovation Characteristics

3.2.1. Innovation characteristics research

To understand an organization's innovation adoption behavior, scholars argue that there are many dimensions of the organization that might be affected by an innovation, which depends on the type of innovation (Afuah, 2003). An understanding of the innovation's attributes is deemed necessary for understanding firms' behavior in adopting innovations Downs and Mohr (1976).

Downs and Mohr distinguish primary and secondary attributes of innovation. Primary attributes are inherent to the technology or innovation and invariant across settings and organizations, for example, size or cost. Secondary attributes are perceptually based characteristics, for example, relative advantage or complexity). That is, the attribute "depends on the organization that is contemplating" (Downs & Mohr, 1976, p. 702). Use of primary attributes increases the stability of the determinants to make research effort more cumulative (Downs & Mohr, 1976, p. 701).

They suggest that much of the instability in innovation research was due to many perceptually based innovation attributes; therefore, it is organization-specific, which confounds and dilutes generalization research outcomes. In contrast to Downs and Mohr, Tornatzky and Klein (1982) argue that perceptually based characteristics have utility, thus *can* predict the adoption and implementation of various innovations, with some degree of consistency. This relates to innovation characteristics research. "Innovation characteristics research describes the relationship between the attributes or characteristics of an innovation and the adoption or implementation of that innovation" (ibid.).

Nevertheless, Tornatzky and Klein are also concerned with the lack of specificity in innovation research resulting in methodological weaknesses. Therefore, to allow generalizability and replicability (Sekaran & Bougie, 2010), their suggestion to clearly articulate (specify) characteristics is taken on board. In addition, the value of innovation characteristics must be obtained by actual perceptions of potential adopters. It is suggested that the characteristics be measured prior to the *decision makers* adoption decision (Tornatzky & Klein, 1982, p. 29). Because most retrospective (assuming what other's perceive) data gathering approaches are likely to give a distorted view of "prediction" (Wolfe, 1994).

The term decision-maker used in the previous paragraph requires elaboration. A decision-maker is an individual who represents an organization. However, unless a single individual represents an organization, adoption-decisions are not taken at an individual level (Rogers, 2003, Chapter 5). “It is not logical to attempt to generalize from the individual adopter to the organizational innovation process as the two processes are quite different” Tornatzky & Klein, 1982, p. 30. For organizations (not ran by a single individual), it is suggested that adopters need to represent decision-making individuals, hence decision-makers. In the best case, the selection of respondents (seeking the “dominant coalition) requires multiple respondents; for example, from several echelons of the organization, within each of the organizations under study (ibid).

3.2.2. MPC as innovation: MPC attributes

Attributes as dimensions

Kanger and Pruulmann-Vengerfeldt (2015) addresses five baseline conditions that need to be met for MPC to be adopted. These baselines provide a valuable point of departure. The baselines are formulated in a broad way, however. For instance, ‘sufficiently informed’ (“A sufficient understanding of the nature and possibilities of MPC is needed”). The term *sufficient* raises the issue of ambiguity (Wolfe, 1994). When is one sufficiently informed, and what aspects should be covered for them to feel sufficiently informed? Thus, this problematic for it does not provide a viable measure. Also, the description of *information* covers multiple aspects (i.e., nature, possibilities, and business case). This multi-barreled summation of considerations is found for all baselines. Nevertheless, the insights provided are integrated into attributes. For each attribute, a definition is given to cope with the issue raised by Wolfe (1994) and Tornatzky and Klein (1982) on the lack of consistent use of definitions in the literature.

Relative advantage (Rogers, 2003, p. 213) refers relative advantage as “degree to which an innovation is perceived as being better than the idea it supersedes” . It is such a general notion however, that Tornatzky and Klein (1982) considers 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 (see Section 2.3). Therefore, for this study, 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.

Compatibility (Rogers, 2003, p. 223) refers compatibility as “the degree to which an innovation is consistent with the existing values, past experiences, and needs of a potential adopter”. This definition concerns compatibility with values and beliefs; compatibility with previously introduced ideas; and compatibility with needs (ibid.). Thus, a normative and cognitive aspect on the one hand, and a practical and operational aspect, on the other hand. Since the output part of MPC (see Section 2.3) from the research scope, compatibility refers to the degree to which requirements imposed by MPC can find “fit” within organizational processes.

Trustworthiness Trustworthiness refers to the extent to which the MPC is perceived as suitable for providing its stated functionalities according to agreed-upon norms. The definition of trustworthiness is discussed and made clear in Section 3.4.

Security Security refers to the degree to which protective measures provided by the technology are perceived to ensure the confidentiality of the information being processed, stored, or transmitted despite risks posed by outside threats. It is based on the definition of CNSSI 4009 Committee on National Security Systems (CNSS) Glossary², which define security as “a condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise’s risk management approach.”; and the definition of security requirements (CNSSI-4009): “Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.” The concept of security is discussed and made clear in Section 3.5.

The four previously described dimensions are listed in Table 3.1 for clarity.

Dimension	Description	Reference
Relative advantage	refers to the extent to which MPC can be used as a solution to data-sharing cases relative to non-MPC solutions.	Definition of (Rogers, 2003, p. 213) altered due to dynamics of MPC (see Section 2.3) and framed in line with Kanger and Pruilmann-Vengerfeldt (2015).
Compatibility	refers to the degree to which requirements imposed by MPC can find fit within organizational processes.	Definition of (Rogers, 2003, p. 223) adjusted due to scope of research (see Section 2.3).
Security	refers to the degree to which protective measures provided by the technology are perceived to ensure the confidentiality of the information being processed, stored, or transmitted.	A combined definition of security and security requirements adapted from CNSS (2015) Committee on National Security Systems (CNSS) Glossary.
Trustworthiness	Refers to the extent to which the MPC is perceived as suitable for providing its stated functionalities according to agreed-upon norms.	Derived from the work of Pavlidis (2011) and Harrison McKnight and Chervany (2001).

Table 3.1: MPC dimensions

The four previously described dimensions are listed in Table 3.1 for clarity. The underlying factors concerning these dimensions are discussed next. It should be noted that while the results of the meta-analysis performed by Tornatzky and Klein (1982) shows that only compatibility, relative advantage, and complexity (complexity is at a near-acceptable level of statistical significance) was shown to be consistently related to adoption, it is also explained that this is related to failure of ad-

equate measures (Tornatzky & Klein, 1982, pg.40-42). Therefore six factors in total are considered due to their relation with MPC-specific (exploration) findings (e.g. Faujdar et al. (2020); Kanger and Pruulmann-Vengerfeldt (2015)).

Factors behind the dimensions

The relative advantage dimension comprises the factor simplification and cost advantage.

Simplification refers to the extent to which MPC eases and thus improves secure knowledge sharing over conventional non-MPC-based solutions. This definition is derived from the work of Kanger and Pruulmann-Vengerfeldt (2015). This factor considers the effort put in the “data contribution” process compared to conventional “data-sharing” solutions. This comprises setting up and maintaining data agreements, in comparison to the MPC in the same respect.

Cost advantage Cost advantage refers to the difference in perceived transaction between data contribution through an MPC solution and a non-MPC based solution. This factor is derived from the notion behind transaction cost by (Lei & W., 2005) discussed in Section 3.1.

Factor	Description	Reference
Simplification	Refers to the extent to which MPC eases and thus improves secure data contribution over conventional non-MPC-based solutions.	Derived from the work of Kanger and Pruulmann-Vengerfeldt (2015)
Cost advantage	Refers to perceived difference between transaction costs of data contribution through an MPC solution and a non-MPC based solution.	Derived from Lei and W. (2005) and Kumar and van Dissel (1996).

Table 3.2: Relative advantage determinants

The trustworthiness dimension comprises the factors of complexity, observability, divisibility and integrity:

Observability (Rogers, 1995; Tornatzky & Klein, 1982, p. 18) refers to observability as “degree to which the results of an innovation are visible to others”. The visibility of the results of an innovation is positively related to adoption and implementation (Tornatzky & Klein, 1982). One of the difficulties concerning this dimension is its potential for confounding with other perceived attributes such as observability of cost (or profit), observability of compatibility, etc. In terms of MPC, we view observability in terms of the visibility of the transaction. Consequently, we refer to observability as the degree to which the application’s components, which define the transaction process, are visible to others. In this respect, this considers the extent to which one can acknowledge that they are able to verify the true data transaction process with respect to the output. This is different than the above definition by Rogers and Tornatzky and Klein which relate to the (out-of-scope) output part of MPC applications discussed in Section 2.5. Our definition of observability is used as a collective term that one is able to describe what is happening on the inside of the system just by observing the outside of the system—consistent with (Honeycomb.io, n.d.).

Complexity (Rogers, 2003, p. 230) refers to “the degree to which an innovation is perceived as relatively difficult to understand and use”. This definition must be made clearer. With regard to complexity, a clear distinction must be made between MPC protocol and MPC-enabled applications.

Protocols require specific knowledge, and complexity herein lies in an understanding—in terms of security—of the protocol (framework) with respect to the intended purpose, such as underlying principles, intricacies, paradigms, deployment, and integration. These issues tap into aspects such as traceability and verifiability of the functioning of an application. Complexity then refers to the usability of the protocol in terms of security and privacy requirements (Lapets, Volgushev, Bestavros, Jansen, & Varia, 2016). From a different view, adopters can also view complexity with respect to the different phases of development and deployment of the final application. As a result, complexity can be viewed in any of the respective phases; for example, implementation complexity and usage complexity.

On the other hand, the complexity of MPC-enabled applications relates to the ‘total package’. Then instead, (assuming a stand-alone application) complexity of the application itself is assumed. Or, in other terms, the simplicity of the process. This process concerns completing a task through the application while understanding the activities occurring in the back-end. Hence while complexity concerns both views of MPC; however, when referring to the complexity of MPC, it is important to specify the unit of observation. Nevertheless, for both cases, complexity extends to the specification of policies governing proper uses of data (ibid.). For this study’s purposes, complexity refers to the degree to which a system or component has a design or execution that is challenging to comprehend and verify (IEEE, 1990).

Divisibility Kivlin (1967) refers to divisibility as the “extent to which an innovation can be tried (on a small scale) prior to adoption”. On another note, Rogers 2003, p. 223 refers to trialability as “the degree to which an innovation may be experimented with on a limited basis”. Divisibility is in favor over trialability for three reasons. First, is the ‘limited basis,’ which only complicates the measurement of this attribute. Second, the definition of divisibility is better suited in terms of the innovation stage (i.e., pre-adoption). Trialability, on the contrary, concerns trials “on the installment plan” (i.e. implementation) (Rogers, 2003, p. 231). Third, divisibility takes into account that the technology can be ‘open,’ taking into account (open-source) frameworks available for MPC.

Divisibility has been frequently used as a means to reduce risk (Kivlin, 1967, p. 87). When a system can be experimented with (tried), it allows one to increase their knowledge of the system. Knowledge shapes one’s beliefs in the trustworthiness of the system. Whether this affects trustworthiness in a positive or negative way depends on the architecture of the application. Because, “trustworthiness cannot be derived from the knowledge of the current system configuration alone. An initial assessment is required to enable the decision which components need to be included in the configuration. The consideration if a system is trustworthy, is carried out based on these values.” (Feller, 2014, p. 21). The divisibility of an application determines the extent that such a process can take place.

If the three above factors seem overlapping, we clarify this as follows. Whereas observability relates to honestly showing the presence of components (relating to being transparent); complexity refers to the comprehensibility of the components (understanding what is being shown); while divisibility concerns providing access to the component (being open).

Integrity refers to the extent to which one feels that the aggregate analysis is executed with input data per the given quality standards. This definition combines the notion of foolproof and the notion of incentives discussed in the previous chapter (i.e., incentives that prevent intended deviation from the desired norm). The concept of integrity is discussed further in Section 3.4.2. Foolproof takes into account that humans can make errors. A foolproof system mitigates the likelihood of errors—this prevents erroneous data weakening the value of the output. On the other hand, incentives acknowledge that participants may have malicious intent but are not aware of consequences, such as legal consequences, or that their intent reaps no benefits. On the contrary, it destroys the value of the output.

Factor	Description	Reference
Observability	Refers the degree to which the components of the application, that define the transaction process, are visible to others.	Based on Honeycomb.io (n.d.)
Complexity	Refers to the degree to which a system or component has a design or execution that is challenging to comprehend and verify.	IEEE (1990)
Divisibility	Refers to the extent to which an innovation can be tried on a small scale prior to adoption (Kivlin, 1967).	Kivlin (1967)
Integrity	Refers to the extent to which one feels that the computation is executed with input data per the given quality standards.	The definition of Chiregi and Navimipour (2016) framed in terms of MPC.

Table 3.3: Trustworthiness determinants

The compatibility dimension comprises the factors of adaptability and interoperability:

Adaptability ([Tornatzky & Klein, 1982](#)) refers to adaptability as the ability to refine, elaborate, and modify an innovation according to the needs and objectives of the implementor. It is a characteristic which describes whether the system is robust to changes, for example, changes in demand and requirements, over its lifetime. However, adaptability strongly relates to the architecture of the application (the protocol in this case), which is a research domain of its own. To understand the role of adaptability of an MPC *application* (not protocol), we adopt two notions by [Fayad and Cline \(1996\)](#). The issue of adaptability is then approached using the notion of “building the right thing” and “supporting the next thing”. Build the right thing corresponds to validation (i.e., figure out what the right thing really is).

We can then refer to adaptability as the degree to which the application allows the system’s capabilities to be changed in amount (easy to add another module, or extensibility) and in kind (easy to convert, or flexibility). This can be confused with a factor under relative advantage. However, adaptability allows a system to be compatible within a given user base. Hence compatibility is not viewed as a relative advantage, but rather a means to achieve pervasiveness because it is compatible within a network of potential participants. Therefore this is an attribute of the application, and not a relative advantage of MPC (only the protocol) per se.

Interoperability Interoperability refers to the level of organizational and technical issues arising from the requirements imposed by the application. The reader should refer to Section 3.1 for an understanding of this definition.

Factor	Description	Reference
Adaptability	Refers to the degree to which the application allows the system's capabilities to be changed in amount (easy to add another module, or extensibility) and in kind (easy to convert, or flexibility).	Based on notions of Fayad and Cline (1996) .
Interoperability	Interoperability refers to the level of organizational and technical issues arising from the requirements imposed by the application.	Based on the work of Panetto (2007)

Table 3.4: *Compatibility properties*

The security dimension comprises the factors of perceived risk and perceived control. Both of these factors are discussed in Section 3.5. For the sake of completeness of this chapter, the definitions are listed in Table 3.5.

Factor	Description	Reference
Risk	The extent to which one perceives a possibility of organizational damage when contributing protected data.	Based on the work of Chang (2010) ; Fisk et al. (2015) ; Singh, Rishiwal, and Kumar (2018)
Control	The extent to which one perceives having control of the information being processed, stored, or transmitted.	Based on Chang (2010) ; D. Huang, Rau, Salvendy, Gao, and Zhou (2011) .

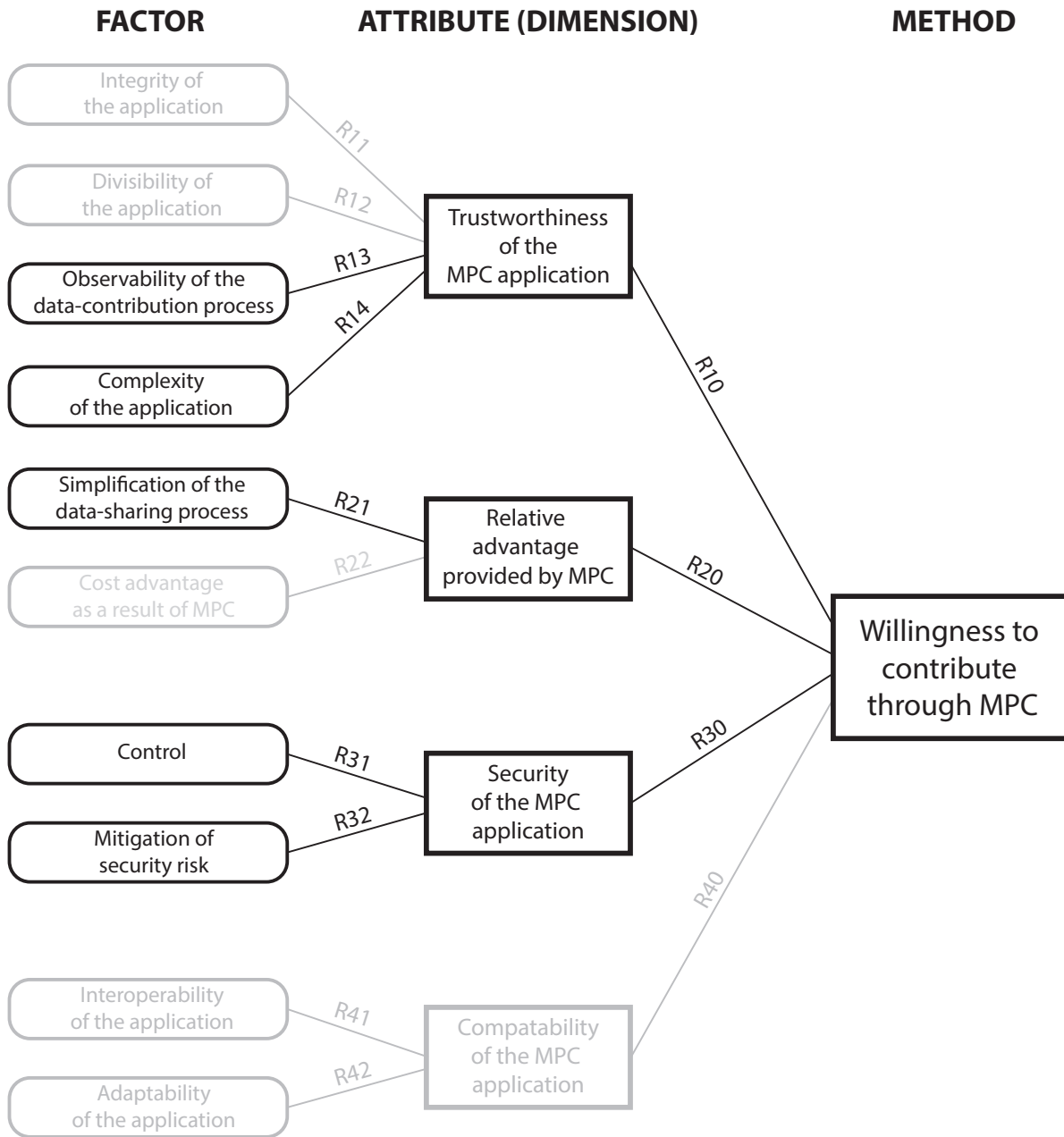
Table 3.5: *Security determinants*

3.3. An overview of MPC related attributes and determinants

In the previous section, MPC is broken down into four dimensions. Each dimension is broken down into attributes. Companies interpret MPC based on these attributes. Their judgment on whether they will contribute protected data or not will likely be based on their perceptions of these attributes. In this section, the attributes are combined into an overview (see Figure 3.1). The greyed out parts are dimensions or attributes which are removed from the scope of this study. The scoping process is described step by step in this section.

First, it must be asked by whom the attributes are rated. Companies are represented by individuals at various levels. These individuals determine the assimilation of new technologies within their organization to maintain or increase the organization's value. Herein, two types of individuals are distinguished: 'decision-makers' and 'end-users.' For this study, only the former is relevant since the influencing role of the latter increases post-adoption. Decision-makers decide whether to adopt a technology. The end-users, in turn, determine the internal rate of diffusion.

Thus, decision-makers are claimed to be the ones rating the MPC application based on the attributes. Then, it must be asked how they will rate the technology. This question is important because not all attributes are as important. This is because different pre-adoption phases exist, and



R10	Feller (2014); Pavlidis (2011); Reid, Nieto, Dawson, and Okamoto (2003), see section 3.4	R11	Grandison and Sloman (2000); C. Lai (2009); Reid et al. (2003); Schrieck, Hein, Wiesche, and Krcmar (2018)
R12	Kivlin (1967); Rogers (2003)	R13	Faujdar et al. (2020); Honeycomb.io (n.d.); Sridharan (2018)
R14	Feller (2014); Kivlin (1967)	R20	Kanger and Pruulmann-Vengerfeldt (2015); Rogers (2003)
R21	Kanger and Pruulmann-Vengerfeldt (2015). Also based on notions of Ham and Johnston (2006); Sendhil Kumar and Pugazhendhi (2012)	R32	Kanger and Pruulmann-Vengerfeldt (2015)
R40	Kanger and Pruulmann-Vengerfeldt (2015)	R41	Ham and Johnston (2006); Panetto (2007)
R42	Kanger and Pruulmann-Vengerfeldt (2015)		

Figure 3.1: Overview of MPC attributes and determinants

within each respective phase, more weight is put on the different attributes. For this, stage models are used. Stage models conceptualize innovation as a series of stages that unfold over time. Wolfe (1994) provides a comprehensive synthesis of research stage models of organizational innovation, which helps explain the pre-adoption phases. In abstract terms stage models tend to be a variant of *awareness* (organization becomes aware of an innovation's existence); *matching* (a problem or opportunity is matched to the innovation); *appraisal* (costs and benefits are appraised); *influencing* (sources of support and/or opposition attempt to influence the process); *adoption (or rejection)* (a decision is made to implement or not); *implementation* (the innovation is implemented); *confirmation (or reversal)* (the innovation-decision is reviewed); and *routinization* (the innovation becomes accepted as routine) (Wolfe, 1994, pg. 411). Although innovation processes are rather non-linear, complex iterative processes, having many feedback and feedforward cycles (Wolfe, 1994) these stages make clear the aspects considered during the different phases.

For this study, that is, the research question, the phases of interest are *awareness* and *matching*. That is, making an organization aware of the technology and allowing them to evaluate whether the technology can provide utility. This is because these phases are in line with the assumed newness of MPC in organizational settings, and thus organizations become aware of its existence and try to match it with perceived problems or opportunities.

Per this approach, the attribute interoperability can be discarded. This is because interoperability can be decoupled from the MPC application itself. From this view, this concerns issues arising later in the pre-adoption process ("can we and how will we solve interoperability issues of the application"), which are considered part of the appraisal phase. Concerning the attribute adaptability; when considering the flexible nature of MPC³, we can assume that a common goal can be established for a given MPC application and that its interface can be adapted to fit the network of prospects. As a result, the issue of adaptability is also solved. As a result, the dimension of compatibility is discarded.

In a similar vein, the problem of cost advantage can also be dismissed. Cost advantages (not fully apparent in the case of MPC) are likely to be addressed later in the pre-adoption phases (appraisal phase) to the extent that it might be coupled with the output of the application. The reason for removing this attribute from the scope is also related to difficulty in rating it. In the process of designing an experiment, it was found that the questions needed for rating cost advantage (i.e., the perceived difference between transaction costs of data contribution through an MPC solution and a non-MPC based solution), it was found that some experience with TTPs—as the non-MPC based solution—was needed in order to rate this attribute properly. In addition, this made the narrowed the number of eligible participants, which increased the risk of exceeding of the time requirements laid out in the TU Delft master thesis requirements.

The scope is narrowed down further. The concept of divisibility is removed due to its complexity—because it comprises other (complex) underlying concepts such as auditability of the code along with traceability, verifiability, testability, and trialability. In terms of criteria, such examination is outside the scope of the MOT domain. The same is true about integrity. For instance, many features can be used to increase and maintain quality standards. How these are perceived is achieved by

³In fact, anyone can create any application they desire within MPC boundaries that is.

means of effective interface design features; see, for example, [Yee \(2003\)](#). This is also outside the scope of the MOT domain. In addition, both of these concepts.

An assumption built in this overview is that the technology provides optimal performance for its intended purpose. This is needed since it is difficult to make any claims about how a system would perform in practice. An application with poor performance would be likely to have a negative effect on the willingness to participate in the data contribution process.

3.4. Trust and trustworthiness

There are various definitions of trust, and its meaning is context dependant. It is a composition of many different attributes: reliability, dependability, honesty, truthfulness, competence, and so forth ([Chiregi & Navimipour, 2016](#)). Which attributes are considered, depend on the environment in which trust is being specified ([Grandison & Sloman, 2000](#)). An MPC application can be seen as a platform. As a platform, it both the remote system that needs to be trusted and interactions over underlying services ([Grandison & Sloman, 2000](#)). Also, recall from Section 3.1, where trust is delineated by dyadic trust and application trust. In this section, we refer to application trust as the trustworthiness of the system. Trust and trustworthiness are concepts overloaded with meanings, however. The reader is therefore reminded that these concepts are discussed from the perspective of willingness to use.

In order to understand the role of trust in willingness to contribute, we follow a two-sided approach— which are termed *approach 1* and *approach 2*, representing two situations: an MPC application with *known* participants, and an MPC application with *unknown* participants. Assuming the former, the importance of trust lies in interpersonal aspects (discussed in Section 3.4.1). This is based on the assumption that one can damage its reputation when violating one's trust. When assuming the latter, the importance lies in the trustworthiness of the application (discussed in Section 3.4.2). This is based on the assumption that users focus on the workings of the application itself in this case. In such case, one needs to rely on the way the application shapes correct behavior.

3.4.1. Trust

In this study, trust is viewed from an interorganizational perspective. That is, trust is viewed from the prospect's perspective in the context of interorganizational cooperation and collaboration. Trust in *data sharing* represents "trust-related behavior because it makes one vulnerable to the actions of the trustee with respect to the information" ([Harrison McKnight & Chervany, 2001](#)). Trust-related behavior means "that a person voluntarily depends on another person with a feeling of relative security, even though negative consequences are possible" (*ibid.*). This generic definition of trust captures the social relationship (interdependency) of members within a network.

There are various aspects around MPC that relate to this view of trust. For instance, attempts to glean information from the output. Also, as seen in the case of [Zare Garizy et al. \(2018\)](#), complex MPC architectures could require participants to disclose certain (sensitive) information in favor of usefulness (in terms of new knowledge) of the output. For this case, the output, and what RP can do with the output, requires IP to trust others not to exploit their vulnerabilities. Moreover, IPs trust other IPs to behave in conformance with the application requirements; for example, submitting data that meets the quality requirements. In fact, the IPs want all parties taking part in the application

environment to operate with integrity.

For *approach 1* the notion of integrity (of participants or input parties), benevolence, predictability (or faith (Raj, Sarfaraz, & Singh, 2014)) (Harrison McKnight & Chervany, 2001; Mayer, Davis, & Schoorman, 1995), credibility (Quinn, Lewis, O'Sullivan, & Wade, 2009) and interdependency (Kumar & van Dissel, 1996) are relevant. Benevolence refers to the extent to which one is believed to act in the other's interest rather than acting from an egocentric or opportunistic profit motive. Predictability refers to actions that are consistent enough to be forecasted in a given situation. Integrity refers to fulfilling agreements made in agreed-upon ways. Interdependency refers to the extent of exposure to being exploited. A noteworthy mention is that these factors are influenced by the incentive system (Harrison McKnight & Chervany, 2001; Mayer et al., 1995; Quinn et al., 2009). These incentives refer to motives for collaboration. Incentives can also be motives to prevent misconduct. For example, institutional mechanisms and legal incentives to prevent unlawful behavior (Bestavros, Lapets, & Varia, 2017). Alternatively, when taking (open) game theory (Ghani, Hedges, Winschel, & Zahn, 2018) into account, it is imperative to elaborate on the incentives behind the interaction (H.-J. Li, Wang, Liu, & Hu, 2020; L. Li, 2002; Srikwan, Jakobsson, Albrecht, & Dalkilic, 2006).

3.4.2. Trustworthiness

In the previous subsection, trust is viewed from trustor to trustee. In this view, 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, then it meets a prerequisite for 'acceptance' (Pavlidis, 2011). In terms of MPC, trustworthiness is an essential concept because its presence is not apparent to the IP—thus requiring the IP to rely on its perceptions of the system as a whole. Thus, trustworthiness should be a verifiable property of the system (Feller, 2014).

For instance, active security with abort, is an MPC property which could result in unexpected opportunistic behavior (Archer et al., 2018). While this can be dealt with through the protocol or infrastructure of the MPC environment, 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 perceived trustworthiness of the application since it requires one to first understand the meaning of active security with abort and then understand how this is dealt with by the application, and finally deciding if this suffices their requirements.

For *approach 2* the concept of integrity (of the application) (Chiregi & Navimipour, 2016) is pointful. Integrity concerns beliefs behind norms, standards, platform rules, the configuration of the platform, which practically forces one to behave in a trustful way.

Trustworthiness is associated with risk (Hart & Saunders, 1997). In the context of MPC we consider the risks perceived by potential adopters with trying "something new". This encompasses risks associated with uncertainties due to the complexity of the application, and the divisibility and observability of the application. 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.

In sum, following a two-sided approach, it is argued that the concept of the trustworthiness of the

system is imperative for an understanding of willingness to use the MPC application. This is based 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. In addition, the system's trustworthiness is expected to increase the level of trust one lays in the behavior of other (unknown) contributors. For instance, system integrity prevents inconsistencies, which positively affect the predictability of others (Raj et al., 2014).

3.5. Security

At a fundamental level, usually, security concerns protecting assets that are of value to an organization. In the context of MPC, security is defined from the view of possible attacks (adversarial attacks discussed in Section 2.2). The purpose of adversarial attacks may be to discover the sensitive information of others 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 a number of 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. It follows a formal technical definition, and the reader who is interested is advised to read the full description of (Zhao et al., 2019, p. 360).

However, unlike real or technical security, perceived security is a psychological concept. From a physiological perspective, perceived security plays a vital 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 context of MPC, it is assumed that general (cognitive) determinants of perceived security in information systems can be applied.

D. 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 to a great extent (Chang, 2010; Wu, Wang, & Huang, 2010). Besides, with MPC it is assumed that (non-technical) users do not fully understand the technical mechanisms of security control. This may sound vague since organizations are assumed to have a good understanding of the technical mechanisms. However, as will become apparent later in this chapter, our assumption is important given the innovation phase under analysis (*awareness* and *matching*):

Assumption 1: In the *awareness* and *matching* pre-adoption phases, it is assumed that users do not fully understand the technical mechanisms of security controls provided by MPC—given its newness, and therefore lack familiarity with MPC. As a result, prospects' view of the technology is perceptually based and not based on 'real' (or actual) security.

Thus, perceived control is determined by the information or functions provided by the interface (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). Faujdar et al. 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, and therefore, risk is becoming more perceptually based (Stewart, 2004). Perceived risk, as introduced by Mitchell (1992), however, is viewed from a buyer consumer perspective, making it not suitable for the study. Chang (2010) adapted this theory to help understand managerial behavior in terms of the adoption of 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 the protection of organizational assets (the protected data) from loss or disclosure.

3.6. Relative advantage

In this thesis, relative advantage refers to the extent to which MPC can be used as a solution to data-sharing cases relative to non-MPC solutions. This description of relative advantage, shares several similarities with the description given by Kanger and Pruulmann-Vengerfeldt (2015) for task-technology fit. To increase our understanding of the role of relative advantage on willingness to contribute organizational postures are formulated.

These postures are derived by considering the pre-adoption phases presented at the beginning of Section 3.3. Three types of postures are distinguished: openness to use, willingness to contribute, and willingness to adopt⁴.

Openness to use Each type (class) of data can result in different degrees of damage to the organization when disclosed (intended and unintended). Openness to use, therefore, refers to the state of a person being clear to use the platform depending on the system's perceived security with respect to the type of data shared (Figure 3.2). A prospect views the security of an MPC application as satisfactory up to a certain degree depending on the damages he/she believes may be caused when information is disclosed to external parties. Intuitively, one may be willing to contribute through the application, *however*, depending on the type of data in question. This is reasoning is consistent with Singh et al. (2018). They have addressed this from an order of impact (e.g., financial loss) and data class. In a similar vein, Chang (2010) argue that "risk perception is based on a decision-maker's assessment of the risk inherent in a situation". This is viewed from the notion of risk propensity which refers to "the notion that many decision-makers consistently tend to either take or avoid actions they perceive as risky".

Willingness to use The required security is relative to type (or class) of data being shared. However, when assuming a secure platform for data exchange, strictly speaking, this platform is not

⁴Willingness to adopt is not discussed in further detail since it is outside the scope of this study

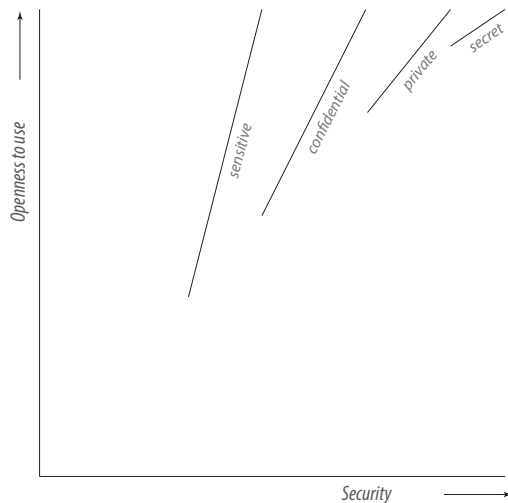


Figure 3.2: Increasing data class requires higher levels of security. The higher the sensitivity of a input data, the greater the consequences, the higher the risks, the greater the degree of restrictions, thus requiring higher levels of security (Jr et al., 1991). Perceived sensitivity of the input data depends on external factors (e.g. institutional regimes).

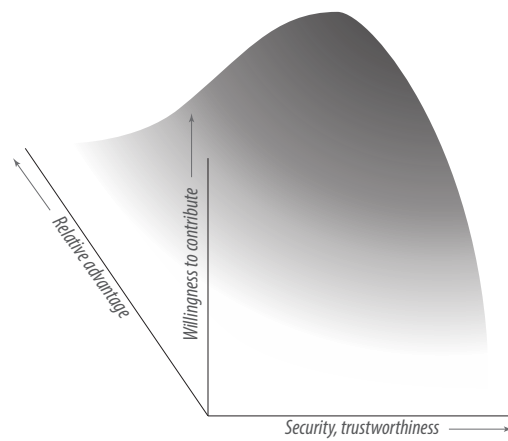


Figure 3.3: In absolute terms, MPC with trustworthiness and security level X , may be used for activity Y , but not for activity Z . The plot illustrates an arbitrary set of combinations of trustworthiness and security (indifferent) levels on the X-axis relative to relative advantage. Since perceptually based, each type of input data has its own plot.

used since the advantage it provides with respect alternatives is not defined (not known to users). This is in line with Kanger and Pruulmann-Vengerfeldt (2015) which points out that organizations might perceive other solutions as a better alternative. Thus, while the application might be trustworthy and secure willingness to contribute is also affected by the relative advantage provided by MPC. Willingness to contribute therefore 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 (Figure 3.3). Thus, in comparison to openness to use, the dimension of relative advantage and trustworthiness is added. Thus, 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 considered a solution for the given activity.

3.7. Hypotheses development

In this thesis, MPC is discussed as an enabler for contributing protected data. Given MPC's main purpose and given several successful deployments of MPC, as discussed in Section 2.2, it is expected that MPC will increase ones willingness to contribute data—when properly presented:

H1_A¹ : Willingness to contribute protected data through MPC is greater than willingness to contribute protected data over TTP.

For the development of hypotheses for trustworthiness, security, and relative advantage, a two-directional approach is followed. First, we ask what the effect of MPC is on an attribute. Then we ask what the importance is of that attribute on willingness to contribute protected data through MPC. The direction affects the hypotheses that can be derived.

3.7.1. Trustworthiness

What is the effect of MPC on perceived trustworthiness?

To answer this question, MPC is compared to a conventional data sharing application which 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. Thus, if the application is perceived as trustworthy, then the service provider becomes less relevant. This can be stretched to the point that the application can be perceived as trustless consensus (one trusts the application regardless of the parties involved).

These two aspects laid on a spectrum. At one end is "untrustworthy application" (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 name put and used within an experiment can confound research results. Therefore, for this study, an assumption is needed to cope with this issue:

Assumption 2: The application resides within and controlled by a nameless entity, which shapes its own perception of trustworthiness based on the overall perceived trustworthiness of the application.

This is needed because the trustworthiness is to be measured by perceptions related to the application and not by the company behind the application. After all, this will bias their perceptions. What is more, the factors behind trustworthiness are also not admissible—since it is implicitly suggested that the party behind the application is trustworthy. Per the above assumption, the emphasis on the service provider of the application is reduced. Since prospects have different ways of making judgments, we acknowledge that participants may still require this information even if the application is felt as trustworthy.

Based on the above answer, a hypothesis can be formulated. Provided that assumption 1 holds, MPC enhances trustworthiness perceptions of data contribution applications. Therefore the hypothesis is:

H2_A¹ : Perceived trustworthiness of an MPC-enabled application is greater than perceived trustworthiness of a TTP based application.

What is the importance of perceived trustworthiness on willingness to contribute via MPC?

In information system literature, it is shown that trust are 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 untrustworthy. This is already clear from the data perspective (loss of data). It can also be explained through the lens of social exchange theory (Cook & Rice, 2006, ch. 3). 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 still limited to a dyadic relationship. Nonetheless, this is fundamentally the aspect being addressed.

Although we have argued that trust between the different contributors becomes less relevant—having taken *approach₂*, the application owner (or, "the MPC application service provider") is still important. 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) characterizes 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 a requirement for contributing data over an MPC application. However, it should be noted 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.

H2_A² : Perceived trustworthiness of a data contribution application is considered an important aspect.

What is the effect of MPC on perceived security?

Although MPC is used to protect confidentiality, as an emerging technology, when managers are presented an MPC application, the effect MPC has on perceived security—to a great extent—is determined by the way the technology is presented (Faujdar et al., 2020). MPC's effect on perceived security can be explained through the lens of the Communication Privacy Theory Management Theory (CPMT). CPMT, is a rule-based theory and posits costs (e.g., risk) and benefits (e.g., usefulness) which *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 thesis, MPC is perceived by the author as a technology which is greatly dependent on network-effect. The higher the number of *responsible* MPC application, the more popular it becomes, fostering further diffusion of the technology and more acceptance—in case of high success factors. At the same time, 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 familiarity with MPC amongst respondents (see assumption 1 on page 45). Altogether, provided that assumption 1 holds:

H3_A¹ : Perceived security of an MPC-enabled application is greater than perceived security of a TTP based application.

What is the importance of perceived security on willingness to contribute via MPC?

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

contribution of data. 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 willingness to contribute via MPC:

H3_A² : Perceived security of a data contribution application is considered an important aspect.

What is the effect of MPC on perceived relative advantage?

A person may contribute protected 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 with respect to alternatives (i.e., relative advantage of MPC). However, if one is not familiar with conventional data transactions or interoperability issues, they may, as a result, not perceive advantage from the use of MPC. Because 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 willingness to contribute through MPC. Since there is no clear direction on the effect of MPC on relative advantage, the following hypothesis is adopted:

H4_O¹ : Perceived relative advantage of an MPC-enabled application is equal to perceived relative advantage of a TTP based application.

What is the importance of relative advantage on willingness to contribute via MPC?

Like the previous question, the answer to this question depends on the degree of familiarity with conventional data transactions or interoperability issues. What can also have an effect is the degree to which a party has a need to share, but is faced with technological barriers. As [Kanger and Pruulmann-Vengerfeldt \(2015\)](#) points out, if the perceived advantage of MPC does not seem pressing to the organization, they might not consider MPC for the given task. This is to some degree similar to “perceived benefits” in the aforementioned boundary rule formation ([Petronio, 2013](#)). In the context of [Petronio](#) perceived benefits effects willingness to disclose personal information. Therefore the following hypothesis is formulated:

H4_A² : Perceived relative advantage of a data contribution application is considered an important aspect.

3.8. Conceptual framework

The conceptual model is shown in [Figure 3.4](#). In this section, we operationalize the constructs. The measurement model is shown in [Figure 3.5](#). The operationalization process is based performed through an iterative process. The questions were uploaded on Google Forms—which provided an easy method to distribute, discuss, and modify questions—and subsequently tested through four iterations with acquaintances. In addition to the literature discussed in [Section 3](#), items related to the construct are also derived from the literature of cloud storage and computing, Information Technology, and Software-as-a-Service(SaaS). [Appendix A.4](#) provides the full list of questions that were initially considered for the constructs.

3.9. Perceptions of MPC

A measurement model is used to get a better understanding of MPC perceptions. [Figure 3.5](#) provides an overview of the items included in the model. This model will help in developing a questionnaire which will be administered to respondents. In total, 25 perceptually based items are derived

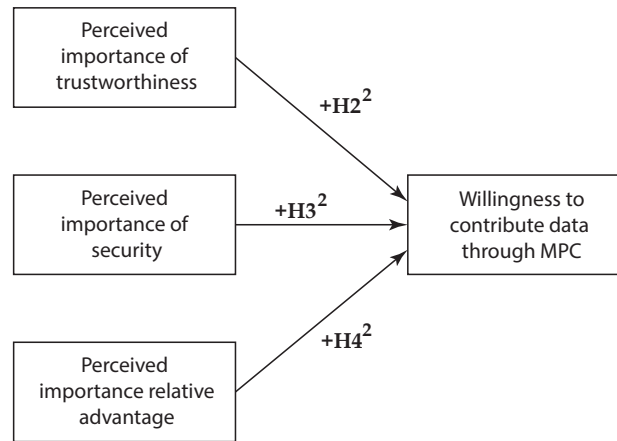


Figure 3.4: Simple conceptual framework

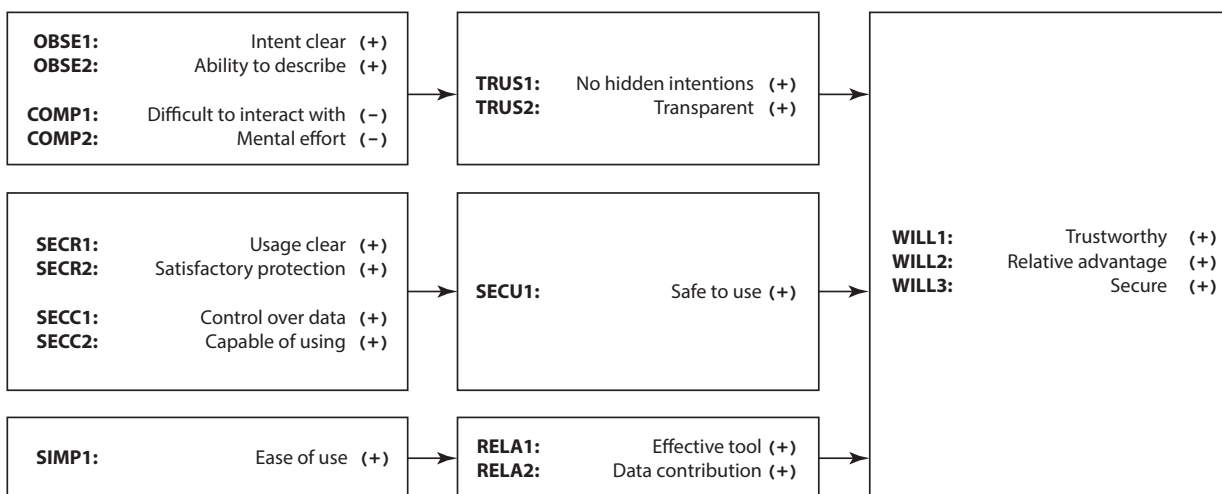


Figure 3.5: Measurement Model

from the measurement model. These are listed in Table 3.6. Several can only during the post-test. These items are marked by an asterisk. The word METHOD (in uppercase) must be replaced with MPC or TTP for each respective solution. It should be noted that the items are derived from our findings

3.9.1. Elements of observability of the data contribution process (OBSE)

Observability refers to the degree to which a system or component has a design or execution that is challenging to comprehend and verify. Following this definition, two types of people are distinguished: technical and non-technical persons. In terms of observability, both parties need to be served, and it is expected that perceptions differ between the two types. Two items are used to measure the construct: clarity of the intent of the application (similar to aim, (Heurix, Zimmermann, Neubauer, & Fenz, 2015), and one’s ability to describe the data contribution process.

Elements of complexity (COMP) Complexity refers to the degree to which the application has a design or execution that is challenging to comprehend. It is expected that “security savvy” adopters have a higher need for explicit information concerning security requirements. Such adopters could

be satisfied by, for instance, using technical jargon such as zero-knowledge proofs, dishonest majority, and threshold levels—or by including explicit information of terms and agreements. However, even when such information is included. It is uncertain whether this leads to an increase in willingness to contribute. Since, for example, not all terminologies are widely accepted; see, for example, [Hazay and Lindell \(2010\)](#) for discussion on the definition of adversaries. This may (unexpectedly) lead to lack of clarity still leading to confusion.

Furthermore, technical jargon is expected to add no value to non-technical persons. This is also the case when made use of explicit terms. It is expected that this may also create confusion ([Faujdar et al., 2020](#)). Non-technical people are more likely to build their perceptions based on comprehensible information, which shapes intuition. Two items are used to measure the construct: clarity of interaction and complexity of the application and content.

Elements of trustworthiness (TRUS) Trustworthiness refers to the extent to which the MPC is perceived as suitable for providing its stated functionalities according to agreed-upon norms. There are many factors that may influence the perceived trustworthiness of the application. For instance, one may validly call into question whether the referenced information is indeed used for the application's underlying functioning. This taps into the issue of distrust. This is because, for instance, a malicious service provider could also claim to use and make reference to another one's—open and honest—source code, while in reality, another code is used. While there may be potential solutions to deal with, this is left open to the respondent's perception. Hence we need also need to look into the degree to which the application is felt as honest and transparent (consistent with [Faujdar et al. \(2020\)](#)). Two items are used to measure the construct: clarity, the accurateness of claims, and transparency.

Elements of perceived risk (SECR) Risk refers to the extent to which one perceives a possibility of damage when contributing protected data. Two items are used to measure the construct: feeling of safety and security assurance, which are derived from [Benlian and Hess \(2011\)](#); [Featherman and Pavlou \(2003\)](#).

Elements of perceived control over input data (SECC) Control refers to the extent to which one perceives having control of the information being processed, stored, or transmitted. Two items are used to measure the construct: access to contributed data, and being capable of using the application.

Elements of perceived security of the application (SECU) Security refers to the degree to which protective measures provided by the technology are perceived to ensure the confidentiality of the information being processed, stored, or transmitted. One item is used to measure this construct: the perceived security MPC provides.

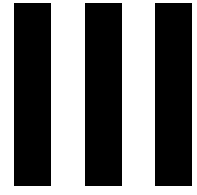
Elements of simplification of the data contribution process (SIMP) Simplification refers to the extent to which MPC eases and thus improves secure data contribution over conventional non-MPC-based solutions. Four elements are derived examine the construct: organizational involvement, rate of exposure when participating (tracing participants), and resolution.

Elements of relative advantage (RELA) Relative advantage refers to the extent to which MPC can be used as a solution to data-sharing cases relative to non-MPC solutions. One item is used to measure the construct: the degree to which MPC solution provides a (simple) solution to the challenge of secure data contribution.

Willingness to contribute (WILL) Willingness to contribute data protected data refers to the extent to which an organization is willing to contribute protected data through an MPC application. One item is used to measure this method: the overall perception to contribute protected company data over the application.

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.
	Perceived security of the application	My data cannot be accessed by other contributors.
I am satisfied with the security the METHOD provides.		
Rel. advantage	Perceived simplification of data contribution 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 3.6: Variables measured



Experiment

4

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 (re-remotely) access the content for treatments. In the first section of this chapter (4.1), the overall goal of the demonstration platform is described. Through a persona, respondents see the workings of the application in practice. Hence, the content is framed in line with the use-case (4.2). The application (based on the use-case) is a working mock-up, thus a non-operational application (4.3). The mock-ups' final design is described, including every difference between the two (4.4). The final section describes the development process (coding) of the whole demonstration platform (4.5).

For replicability and reproducibility, the demonstration platform is publicly available (see Appendix A.2).

4.1. Goal

The purpose of this study is to understand how MPC affects willingness to contribute protected data. However, there is a lack of case studies 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 \(2013\)](#).

4.2. Use-case

A use-case is a deployment of an MPC application (such as those described in Section 2.4). 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 2.4) is suited for this purpose.

The problem addressed An objective overview that showcases DC performance with respect to the different compositions of machine, 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. This is argued from the standpoint of quality and insights and not the number of comparison reports available on the market. For instance, Curtis Barry & Company¹ compare ratio based indicators. However, such approaches are considered highly misleading (ISyE, 2003). Warehouses wishing to improve usually approach solution providers with their wishes and demand. Each solution provider ‘sell’ their solution, however. As a result, the proposals may be biased. An objective overview of how different solutions (actually) perform lacks, however.

Which alternative information sources are there and what value do they add? Two primary sources concerning the problem addressed are distinguished. First are benchmarking (or performance) reports. We did our best to seek reports that provide an objective overview, as previously discussed. However, they were perceived as having limited value. For instance, we took example survey questions² and the top 5 metrics of the study and asked five mid to top managers to share their perceptions of the contribution of such study (in an informal voice call). The main findings were that (i) they felt the questions were ambiguous, affecting the end-results; and (ii) the pamphlet³ do not give a sense of direction on ways to improve performance⁴. That is because while overall poor performance could be identified, it is difficult to make any claims on what may be the cause or if it is related to other factors; for example, the type of resources used, and industry specific unit of measurement. We also asked for them to describe which sources of information they use to keep track of performance trends. This question is related to the second source: consultancy firms.

Before discussing the second source, it is worth mentioning that two managers did not actively keep track of their environment (i.e., whether there are better alternative solutions available). The other three of the managers did invest resources related in attempts to get a better view of industry performance and technological solutions. We were shown by means of real reports the shortcomings. Three reports were shown to us. Due to strict confidentiality agreements, the reports shown to us can not be shared in this report. Two of the reports discussed were studies performed by well-known international consulting firms. Our finding is that these reports provide concrete advice on what decisions to make (e.g., advice regarding expansion or synergies). Another finding concerns the initiative to the underlying reason to hire a consultancy firm. That is what led to hiring the consultancy firm. All of the firms hired consultancy firms due to a form of ‘push.’ For instance, a need felt to increase capacity following an increase of orders over the years to avoid a volume capacity constraint in (near) future. The information used was either from internal data or based on (generic) reports on trends (acquired through other consultancy firms).

What is our proposed output? The proposed output 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 4.1). This graph is meant to give a concrete example of the output. A complete study is needed to properly address the issue of *insight versus information leakage* (as explained in Section 2.5. The

¹<https://www.fcbbc.com/blog/bid/156213/benchmarking-metrics-of-warehouse-operations>

²<https://werc.org/page/DCMeasuresSurvey>

³WERC annual survey and report on industry metrics, DC measures – 2020 Snapshot in Time.

⁴These were based on a quick (~15 min) assessment

list of metrics comprises both throughput information, resource, capacity, and financial information. The full list of metrics can be viewed in the excel template file stored on GitHub (see Appendix A.2).

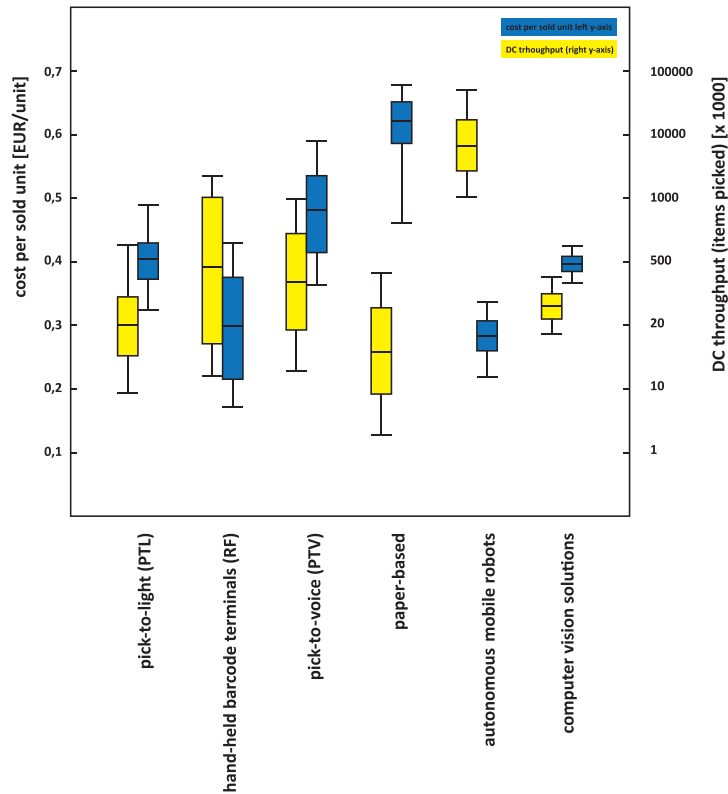


Figure 4.1: For illustrative purpose only: an exemplary plot of output generated by the MPC application.

What is the value of this output? In conclusion, an objective overview showing the performance of different warehouse configurations for supply chain professionals lacks. Based on the interviews, such information is felt missing and could well serve as a valuable instrument for factual judgment. This conclusion was drawn based on the following reasoning. We showed *exemplary* Figure 4.1 to three of the managers (previously mentioned managers) and asked whether (i) they have (ever acquired) such information and (ii) whether such information adds value. To item (i) none of them did, and to item (ii), all three felt it did provide value. One manager asked for the whole ‘report.’ However, this was not provided since this is not available⁵. This manager suggested that a report with such content—covering DC dimensions—would serve as a valuable instrument provided it is based on a great number of industry players. The information would allow him to make a better initial assessment before turning to external parties. It also allows him to juxtapose proposals and advise with industry performance. The other two managers mentioned overlapping opinions similar to the other; however, while they were positive, they were somewhat specific to the example given. We stressed that a clear mention was made that this is an illustration and not a plot based on real data.

⁵such a full report warrants an extensive depth study

What is the problem MPC solves? 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 computations needed 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.

What is the goal of the application? The goal of the application is to enable corporate decision-makers to become more proficient in assessing the value of efficiency-enhancing technologies; are better capable in identifying performance gaps; are better capable of re-engineering warehousing operations, and; are better capable in assessing actual industry performance.

4.3. Mock-up design

As mentioned in the first section of this chapter 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 distribution center (DC) performance indicators – as previously described. The aspects covering the design of the mock-up are grouped into design considerations (4.3.1), application-features that need to be embodied in the mock-up (4.3.2), and explicit information that must be displayed within the mock-up (4.3.3).

4.3.1. Design considerations

In terms of (general) design considerations, comprehensibility and deployment of the mock-up are considered.

Comprehensibility The mock-up represents a working application. For the application, non-technical descriptions are used to allow the contributor to understand the functionalities of the features. Visualizations are also used since this is expected to positively affect trust perceptions (Faujdar et al., 2020). Based on this finding interactive web browsing features are used to simplify information further. For instance, animated SVG diagram is used (see Figure 4.2).



Figure 4.2: Screenshots of animated illustration used to depict the process behind “what happens after you submit your data”

MPC deployment The MPC application is displayed as the deployment of a web-based service to show that no new software needs to be installed within corporate environments (see Bestavros,

Lapets, Jansen, et al. (2017)). Using web-based services (through browsers) allows easy customization of the user interface without requiring significant updates. Herein, “poka-yoke”⁶ measures can be implemented to avoid human errors.

4.3.2. Features

Faujdar et al. (2020) found that real-time display of contributors may induce adverse effects. For this reason, for this mock-up, a different approach is adopted. Other functionalities are used instead: contributors are provided with a time window for data submission (i.e., a deadline is imposed). The features used for this are idempotent re-submission and an analyzer interface. These provide better functionalities to organizations.

Idempotent re-submission is a feature that provides input parties the ability to resubmit their data (Bestavros, Lapets, Jansen, et al., 2017). This allows the input party to resubmit multiple times without changing the result. This is possible until the computation is instantiated (i.e., until the submission deadline). Information is provided on the possibility of re-submission till the due date. Input parties are provided a unique submission ID. This ID is hashed on the client-side, and this hashed value is stored in the server database and used only as an index into the server database allowing participants to resubmit (update) input data more than once in a session (overwriting their previous submissions). This allows input parties to rectify errors (or corrupted data) discovered after input is submitted. These aspects relate to integrity since it is included to assure correct input data (quality standard). This feature is described in the application as follows: “*After you hit submit, two things occur. (1) your input ... (2) Your submission ID is hashed (one-way hashing) and stored in our server database. This hashed value is the only information that 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.*”

An analyzer interface provides a fail-safe mechanism to stop the analyzer (computation server) to compute the final aggregate data when too few participants have submitted their data (Bestavros, Lapets, Jansen, et al., 2017). In this condition, the service provider (or application owner) will not allow the analyzer to compute the final aggregate data. This prevents the possibility of disclosing information due to a low number of participants. This functionality runs in the backend. Hence, we need to provide explicit information on this functionality. This feature is described in the application as follows: “This application makes use of a so-called analyzer interface. This allows us only to 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.”

Input data file The application requires over a hundred input fields. To ease the data collection process, we make use of an excel template file. This is based on Bestavros, Lapets, Jansen, et al. (2017). This file allows the input party to save their input (locally) on their machines (since storing on the web platform defeats the purpose of MPC). The template can be parsed (‘read’) by the web browser as a quick method to input data. In this way, input parties also maintain a copy of their input. This feature is provided considering the usability of the application (ibid.). The design is shown in Figure 4.3. This is to make the application “realistic”; however, it is not an aspect under study.

⁶Poka-yoke is a Japanese term that means “mistake-proofing” or “inadvertent error prevention”

Input your data

Please make sure your 2020 submission ID and participation code match the ones provided in the email sent to you by the organization. You will not be able to submit your input if this information is incorrect. Drag and drop your completed template file in box below to encrypt and include your submission in the aggregate data. All selection fields below have search functionality.

ID:

Code:

Location:

Channel:

Goods:

Diversity:

Market:

Completed Excel template only

Drag and drop your completed template file here in this box or click here to select file

As shown in the illustration, this part runs in your web browser. At this point, when you enter your data your files do not leave your machine.

ⓘ 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.

Figure 4.3: The input panel makes use of input fields with search functionality. A drag-and-drop box allows easy uploading of the data file. The side-panel describes that data entered is not yet submitted at this stage.

Data review and input validation Input validation (or input feedback) prevents spurious data seeping into the analytic. It should identify and highlight incorrect or malformed data – this highlighting functionality is, however, not built into the mock-up. A panel for review allows the input party to ‘check’ input supplied to prevent improperly formed data entering the computation. Therefore the mock-up features a panel that allows input parties to view their data before submitting. As mentioned, this panel should have input validation features that aid in identifying (potential) erroneous user input; however, it is not included in this mock-up. This makes part of *integrity*, which is scoped out.

4.3.3. Information to be displayed

Roles This aspect makes clear to the input parties the roles that make part of the whole MPC ‘system.’ Three roles are considered: (i) an m (unknown) number of contributors (IP) who contribute protected data for the calculation; (ii) an n (known) number of automated, publicly-accessible service provider (CP) that sees only shares of encrypted data and connects all other participants without requiring them to maintain servers (or even to be online simultaneously); and (iii) an m number of (same number as input parties) analyzers (RP) who receive the output of the analytic. Information concerning the different roles is implicitly mentioned.

Source code accessibility The source code of the MPC application is open-source. This allows contributors to assess the application in their own environment. A link is made to the source code. However, this brings the contributor to a page that asks them to assume that the code is available. This is because the dimension of divisibility is scoped out. In addition, in this way, focus on the research is maintained.

Data falsification (and data quality) ⁷This aspect concerns information needed to avoid falsification of input data. For the given use-case, the participating organizations lack the incentive to falsify

⁷Estimations are based on abstract reasoning.

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 thru Sh. 10). All input fields are highlighted yellow.

Sh. 1 Sh. 2 Sh. 3 Sh. 4 Sh. 5 Sh. 6 **Sh. 7** Sh. 8 Sh. 9 Sh. 10

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. This 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 4.4: Panel to review input data. The input fields reflect the excel template file. This example shows the seventh sheet.

results. The output of the results is as good as the input – “garbage in is garbage out.” Inputting false data makes the results useless. From this line of reasoning, falsification is deterred by the treat of the algorithm providing useless output. This is included in the mock-up through the following statement in the information panel: *“The purpose of this panel is to allow you to check the quality of your data before submitting it to the computation server. This 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”*.

Collusion ⁸This aspect concerns information needed to make clear the adversary model adopted and measures embodied to prevent malicious acts (i.e., collusion). With regards to collusion (colluding or actively deviating from the protocol), we ask ourselves, “is there an incentive that deters collusion” or “is there a reason *not* to know”? The answer to this question is two-fold when considering collusion is possible between IPs and between CPs. Given that the application requires a sufficient number of IPs and that the IPs are unknown, it is expected the collusion among IPs up to the threshold level (assuming a certain level of input parties required for the computation) does not pose a significant risk since this requires a great deal of resource investment and the investment does not amount to the expected returns ⁹. Concerning an incentive that deters collusion between CPs, we need to make statements about the number of CPs. On the one hand, when encrypted data is distributed to more than one CP in a permuted order, then, when the data is decrypted (unauthorized), it does not convey much more information than what is conveyed by the result

⁸Estimations are based on abstract reasoning.

⁹this issue requires in-depth analysis with respect to the protocol used, however, is outside the scope of this study

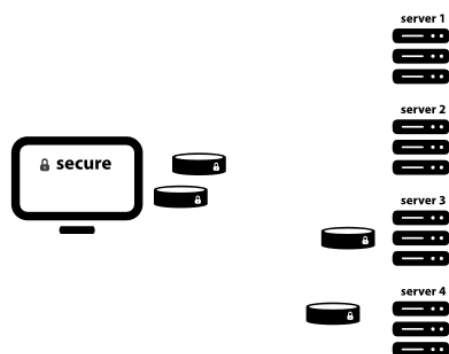
since the parties do not know which data share belongs to which party. At the same time, the CPs are assumed not to collude. However, for the same reason behind assumption, 2 no statements are made of the organization maintaining the CPs.

Given the assumed lack of familiarity with the technology among contributors, we propose the use of several CPs. The CPs are assumed to be known and have conflicting interests, thus removing the incentive to collude. In sum, while collusion is possible, it is unlikely, and when collusion occurs, the information gleaned does not possess significant value since the owner is unknown to the CPs. Finally, based on this reasoning, a semi-honest adversary model suffices. Given the number of input fields, pre-processing is used to lower online MPC computational costs.

After careful consideration, however (reviewing the mock-up with testers), it was noted that the above terminologies only increase complexity whilst not adding clarity. Therefore, this information is left out from the use-case and mock-up since it is expected not to provides significant value whilst making the content harder to digest.

It should be noted that an explicit mention of risks associated with collusion is not made. This could induce fear unnecessarily. Sufficient information is provided on the workings of the system and allows one to make their own fair judgments based on their perceptions. The above information is embedded in the mock-up as follows: “After you hit submit, two things occur. (1) your input is split into four shares. Each share is randomly distributed encrypted to a computing server over a secure HTTP channel. (2) Your submission ...after submission”.

The final perception lies with the respondent. This is also the case for the non-MPC solution (discussed in the next chapter), where we do not make any statements about risks related to the use of TTP; for example, feeling that a TTP might use data for other purposes than stated).



After you hit submit two things occur. (1) your input is split in four shares. Each share is randomly distributed encrypted to a computing server over a secure HTTP channel. (2) Your submission ID is hashed and stored in server database. This functionality allows you to resubmit your data in case you find any errors in your input data after submission.

Figure 4.5: Information displayed concerning Computation parties

4.4. Final design

As will become apparent in the next chapter, two applications are required. This follows an experimental design that is used. The application is used as a treatment herein. 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. This is 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 a description of the content.

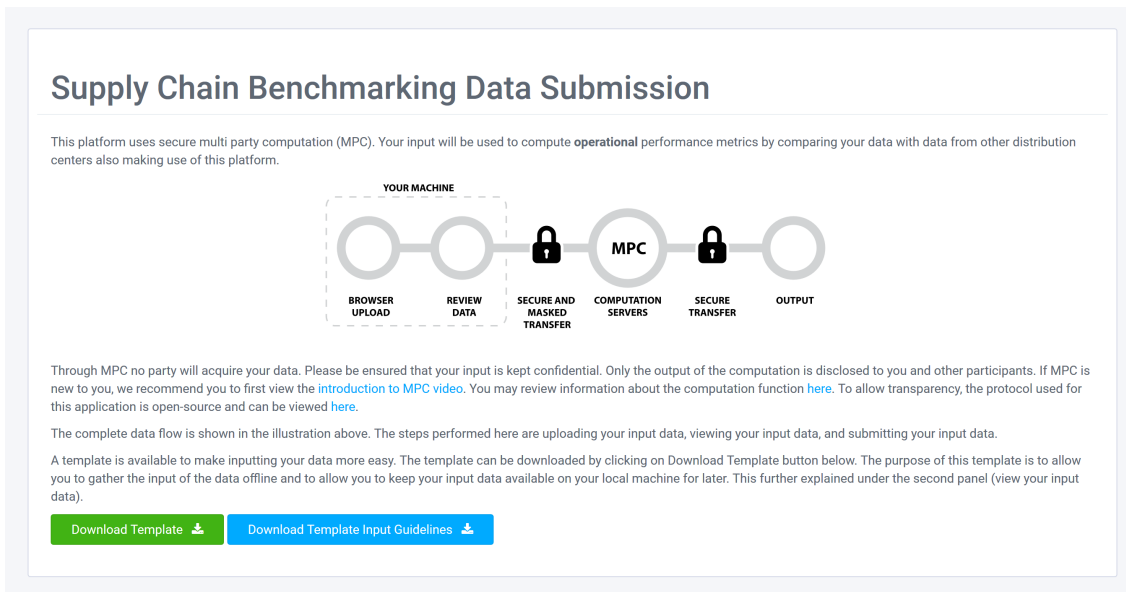


Figure 4.6: Start panel screenshot for MPC application

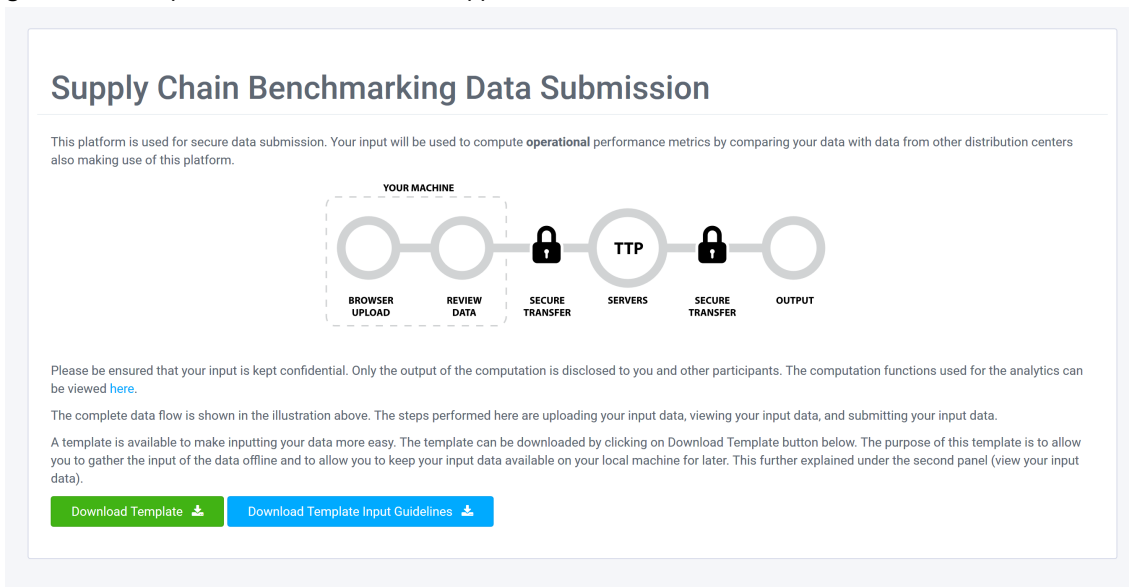
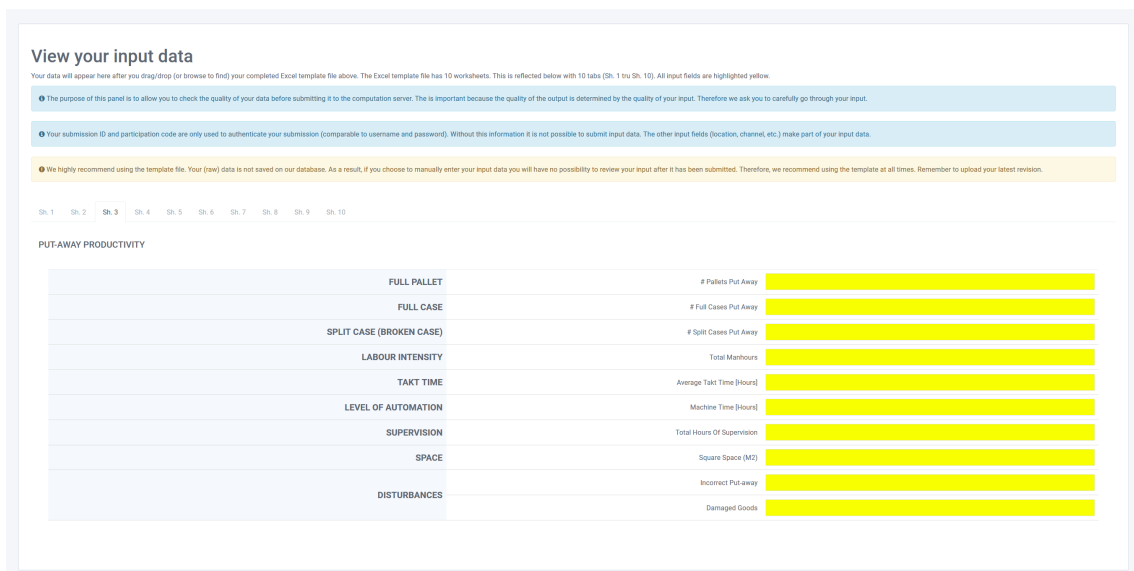


Figure 4.7: Start panel screenshot for TTP application

Structure The structure for the two treatments are identical. Both treatments have four panels. The first panel provides a description of 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. The content of these panels 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.

Content In the first panel, a description is provided of the sources behind the application and the data flow. See Figure 4.6 and Figure 4.7 for a comparison between the panels. As can be noted, we have attempted to mirror both cases. This is done by adopting the following protocol: “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 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. This 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 to Sh. 10). All input fields are highlighted yellow.

• The purpose of this panel is to allow you to check the quality of your data before submitting it to the computation server. This 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.

• 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.

Sh. 1 Sh. 2 Sh. 3 Sh. 4 Sh. 5 Sh. 6 Sh. 7 Sh. 8 Sh. 9 Sh. 10

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 (M ²)	
DISTURBANCES	Incorrect Put-away	
	Damaged Goods	

Figure 4.8: 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. 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. This makes sense 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.

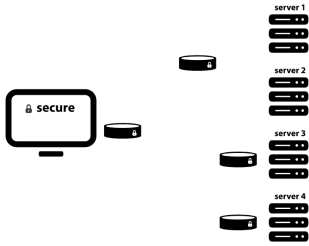
The second (see Figure 4.4) and third panel (see Figure 4.8) is the same for both groups. The data panels are the same for the two groups since the features used to provide functionality for both MPC and non-MPC based applications.

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]	

[Submit](#)



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.

- 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.
- 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 4.9: 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]	

[Submit](#)

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

- 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 4.10: 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 4.9 and Figure 4.10. Although it makes sense in the case of MPC application that the service provider does not keep a copy of the raw data on its servers (in fact, some consider this a requirement), we see no reason why such a feature would not make sense for the TTP-based application.

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 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 since this such feature does not make any sense since the service provider has the raw data upon submission.

4.5. Demonstration platform development

4.5.1. Platform

An existing platform for the demonstration suitable for the demonstration platform was not found. Platforms found that provide the needed functionalities are generally designed for "online-courses," having as a result to "many bells and whistles." However, a straightforward platform is needed. As a result, a new platform is built from scratch¹⁰. The architecture of the platform is depicted by Figure 4.11.

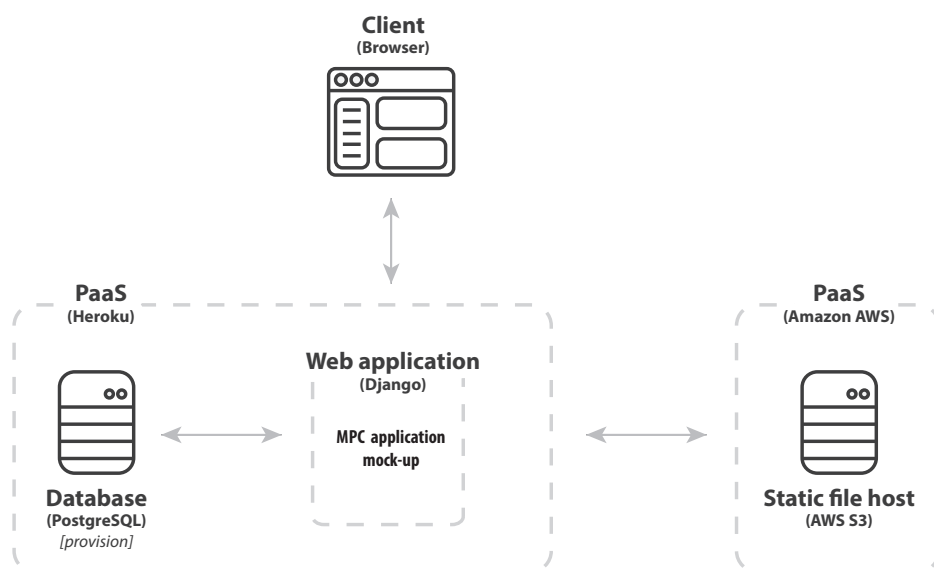


Figure 4.11: Demonstration platform architecture

For the development of the platform, open-source tools are used. The platform is built using python and python-based Django framework. Python is a popular multi-paradigm programming language and has a strong supporting community. The Django framework is a python based (web) framework that is built for the development of web applications. It is used because it provides an extensible authentication system and an administrative interface (eases the development process). Django (officially) supports several database backends. The backend used for the platform is PostgreSQL. This is a relational database management system. Relational databases represent and store data in tables and rows. It uses a structure that allows identification and access data in relation to another piece of data in the database. This suffices over a non-relational database since there is a clear structure.

4.5.2. Mock-up

For the mock-up, Hypertext Markup Language (HTML), Cascading Style Sheets (CSS), JavaScript (JS), and JQuery are used. A CSS and JS Bootstrap framework is used. HTML, CSS, and JS are used for the layout of the web pages. In simple terms, HTML is used to define the structure,

¹⁰for some parts (the front-end in particular), existing templates, themes, and plugins are used.

CSS for the presentation, and JS for the front-end behavioral aspects. jQuery is used for more straightforward finding, selecting, and manipulation of Document Object Model (DOM) elements. An additional plug-in is used. Sheets.Js¹¹ is used for client-side reading of to-be-uploaded input (parsing the excel template file). Finally, animated SVG is also coded to enhance visualization of information.

4.5.3. Deployment

The demonstration platform is only accessed by participants making part of the experiment. As a result, low traffic is expected. Moreover, access to the platform is “short-lived” (i.e., taking the duration of the study). Heroku is used as the hosting provider. Heroku is a cloud-based PaaS service. As a PaaS, the needed web infrastructure is taken care of (e.g., proxy servers). Heroku’s free tier has many limitations with regard to scaling, however. One of the limitations are Dyno’s that sleep after 30 minutes of non-activity. It then takes approximately 10-15 seconds for the Dyno to wake up. Because during testing of the experiment, one respondent indicated that the site was not working—due to a sleeping dyno—it was decided to use a paid dyno to prevent this from occurring. The static files were served from Amazon AWS S3.

¹¹<https://github.com/SheetJS>

5

Experiment design

This research aims to explore the effect MPC has on data sharing towards data contribution. Hence a “cause-and-effect” methodology is needed. Therefore our research aim requires a high internal validity in order to lay confidence in our findings. At the same time, this study is conducted 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. In Chapter 3, it has been discussed that the unit of observation is the decision-maker or a person that affects decision making processes within organizations. Therefore this chapter first starts (5.1) with participant selection criteria for target respondents. Then in the next section (5.2), the pool from which the respondents are acquired is described. Then, the the experimental design and setup is discussed in detail (5.3). This chapter concludes with describing the experiment procedure (5.4).

For replicability and reproducibility, the experiment is publicly available (see Appendix A.2).

5.1. Participants

In Section 3.2.2, it is discussed that rather than inferring perceptions ourselves, these need to be rated by direct measurement of the adopter’s perceptions or expert judges not directly involved in the innovation process. Any inferences made puts the reliability of the results to question (Tornatzky & Klein, 1982). Furthermore, direct measurement allows replicability (ibid.). As discussed in Chapter 3.2.1, organizations are represented by individuals. More specifically, the organization is, in fact, a representative of the actual individuals making adoption decisions. Herein, an organization is an enterprise not ran by a single individual.

The occupation and level of involvement in the evaluation, adoption, or implementation of these individuals are important factors to consider in the selection criteria. In *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 decisions-makers with roles such as technology managers, business strategists, improvement managers, IT advisors, program managers, project managers, and project engineers.

5.2. Data collection

We consider the best case focus group (batches) discussed in the previous section as the “holy grail”. Requiring 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 more¹ time. This is due to the experimental setup² used for this study (discussed in the next section).

On the other hand, crowd-sourcing platforms make data acquisition more attainable in terms of costs³. 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 collections. The first collection comprises a proxy group. The second collection comprises the “holy grail”.

The first collection will be performed using Prolific. Prolific⁴ is 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. In order to increase the participation rate (response rate), we opt to perform the experiment at the respondent’s location. Further information is not provided in order 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.

5.3. Experimental design

5.3.1. Quantitative study

Experimental research is suitable for our research objective. A pre-test and post-test experimental and control group design is adopted. A pre-test and post-test methodology allow comparison of participant groups and measurement of the degree of change stemming from the treatment.

Participants will be assigned randomly (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 5.1.

Treatment (X_1) will represent an MPC application with all features discussed in the previous chapter. Treatment (X_2) represents a “conventional” data sharing application. By conventional, we

¹with respect to time requirements of the master thesis

²Also challenging due to COVID-19 induced challenges

³Also more feasible due to complications imposed by COVID-19

⁴a crowd-sourcing platform for research purposes (see <https://www.prolific.co/>)

Groups	Pre-test	Treatment	Post-test
Group 1 R_1	O_1	X_1	O_3
Group 2 R_2	O_2	X_2	O_4

Table 5.1: Pre-test and post-test experimental and control group design

refer to a data transfer through a trusted third party (TTP). The difference between the two is, needless to say, that (X_1) contains MPC-only related features and information, whereas (X_2) contains TTP related information—making it a data-sharing platform. Still, both treatments follow a common tread and are identical in terms of information displayed and look and feel. This is discussed in the previous chapter.

Per the above setup and research aim, the statistical test will be a comparison of means. Respondents will rate their score using a 5-point Linkert scale. A 5-point Linkert scale is used because during testing of the experiment, a 7-point Linkert 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.

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

5.3.2. Experiment setup

In this section, we describe the design of the experiment. At the highest level of abstraction, the experiment comprises four parts:

The first part is the pre-test. The pre-test is *exactly* the same for the two groups. In the pre-test, perceptions are measured based on expectations for a data contribution platform. This provides an indication of the respondent's initial anchor point and a reference that allows measurement of the interaction effect as a result of 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. This is approached with care, however. All features that would be possible even 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. This part is 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. This is because, upon testing, the experiment was found to require concentration. Presenting 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 end of the questionnaire.

5.4. Procedure

The complete experiment process flow is shown in Figure 5.1. First, participants are provided with an introduction to the study and provided with terms for conducting the experiment. Then all respondents are presented 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.

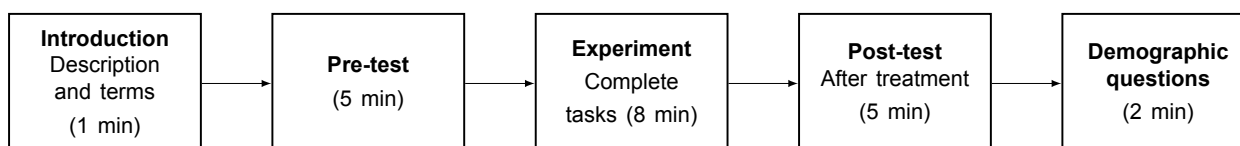


Figure 5.1: The (online) experiment process flow. Time for completion is approximately 20 min.

The measurement instrument used for the experiment is a questionnaire. Qualtrics^{XM} is used for the questionnaire. The above setup is configured as depicted by Figure 5.2. The Qualtrics^{XM} randomizer function is used⁵. Only one of the blocks ('element') is presented to the respondents. The checkbox for *Evenly Present Elements* is checked to present each element (roughly) an equal number of times across all respondents. Using this feature, respondents can not go back to block 1 (pre-test) after the randomizer is initiated. The main reason for using Qualtrics^{XM} is that it is GDPR compliant⁶ and the functionalities it provides⁷ (e.g. the previously described randomizer).

The lab experiment is set up as shown in 5.3. The last block intends to ask questions on observations from the results and findings.

5.4.1. Persona

The treatment comprises a use-case that makes use of a persona, which is provided to the respondents. A persona is used in order 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 for 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.

⁵<https://www.qualtrics.com/support/survey-platform/survey-module/survey-flow/standard-elements/randomizer/>

⁶<https://www.qualtrics.com/gdpr/>

⁷<https://www.qualtrics.com/>

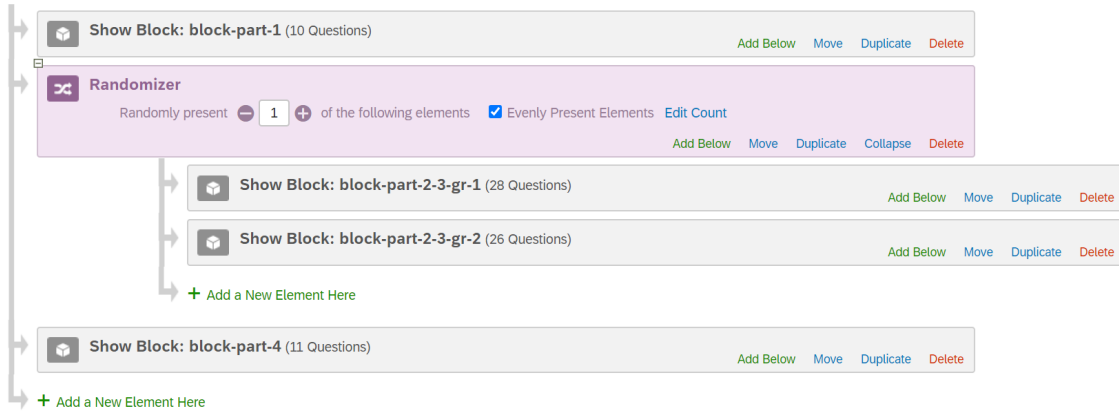


Figure 5.2: Survey flow: randomization applied using Qualtrics^{XM} survey flow feature.

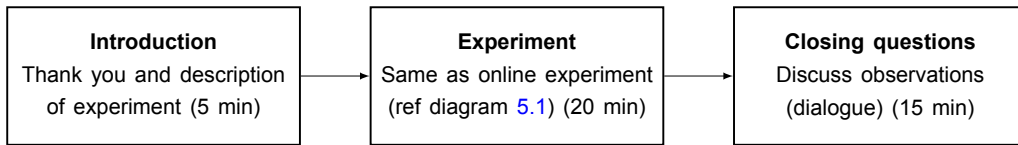


Figure 5.3: The lab experiment procedure

The persona is based on a similar role of the people that were interviewed (discussed in the previous chapter). That is, it is based on decision-makers, i.e., professionals, in distribution centers. They seek optimal warehouse configurations. This is based on the role of the interviewees. Their roles have been checked with similar roles on LinkedIn. Here we found sufficient evidence that the role of improvement manager (or similar positions) is a role that is recognizable within organizations. Hence, although we only talked to three ‘improvement-like’ managers, we find sufficient evidence that this is a widely adopted position by organizations. Thus, this role resembles the decision-makers needed for the performance benchmarking application. The persona description includes the role of an adopter and the problem this person faces.

As discussed in Chapter 2.2, seeking improvement is an industry-wide problem. The persona for both experimental groups is the same. 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.

5.4.2. Use-case scenario

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 allows us to design in line with the scope defined in Section 2.5.

Recall from this section that we excluded the output part from the research scope. A description of how the focus is laid on the input part is in order. To account for this, in the use case, an explicit statement is included so that users focus on the input part. This is explicitly suggested by the following statement in the second paragraph: *"The company offering the benchmarking services, provided a booklet with an example of the output generated (see below). This is exactly the kind of information you need."* The respondent must then accept that his/her personal preferences of the output and valuation of the output are not part of his own actual concern.

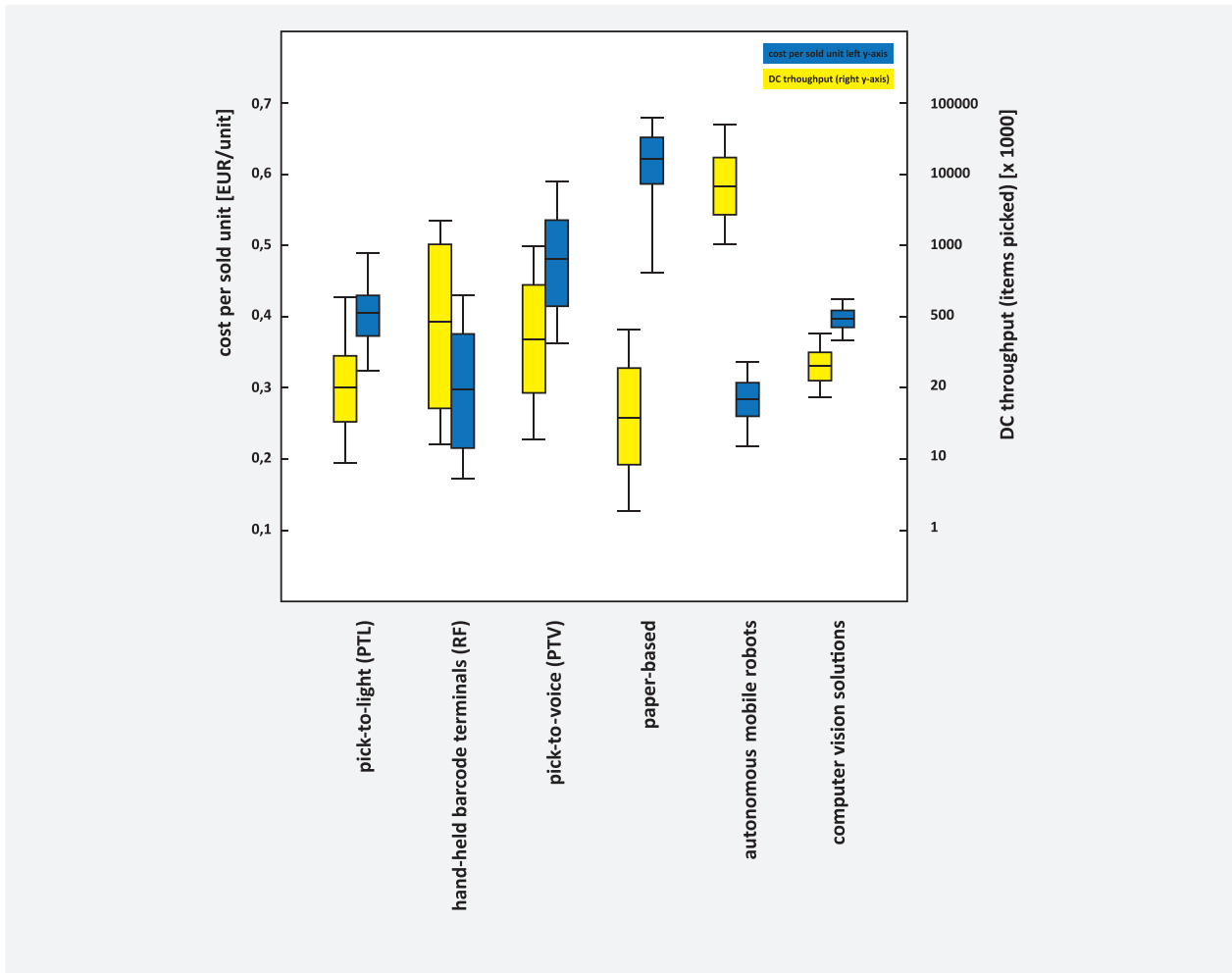
The use-case scenario description for the two experimental groups differ. Differences are highlighted cyan for group 1 (MPC) and pink for group 2. Herein, texts with the same numbering replace each other for the respective group, whereas non-highlighted text is used for both groups. We attempted to provide the same level of objectiveness for both groups.

You found a ¹multi party computation ¹a trusted third party (TTP) application called PEBE (PErformance BEenchmarking) available for distribution centers. ²You know that multi party computation applications allow participants to share knowledge without sharing the underlying data. As a results multi party computation users contribute data and do not share their data - they only share knowledge, and their data is confidential by design. ²You know that TTPs work under contracts or agreements to ensure confidentiality.

This application requires contribution of sensitive internal company data 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 5.1, respondents are given a number of steps and tasks that need to be performed. These steps allow sufficient interaction with the application. In order to assure that respondents have indeed performed the steps, they are provided a “code” after completion. Participants input this code in the questionnaire. This indicates that the respondent has performed the steps. The questionnaire, as presented to the respondents, is provided in Appendix A.11.

6

Results

This chapter presents the results of the experiment. First, the data collection process is described, along with the steps taken to ensure reliable data (6.1). Three channels were used to collect data. It is therefore needed to attest whether these datasets can be merged (6.2). Then, the data is prepared for tests and reviewed to get a sense of the data (6.3). After the dataset is established, several checks are performed to evaluate the extent to which the respondents meet the profile of decision-makers (6.4). The subsequent chapter reports the results of the correlation analysis (6.5). The results of the analysis are used to test the *importance* related hypotheses. This comprises the importance of the difference dimensions of willingness to contribute. In the subsequent chapter the *TTP-MPC related hypotheses* are tested (6.6). Next, the treatment effects on each item is examined (6.7). This provides a better understanding in the effect of MPC on the different aspects. In addition to the quantitative assessment a qualitative assessment is performed (6.8). Finally, a conclusion is drawn (6.9). The results of this chapter can be used to answer SQ3.

For the statistics discussed in this chapter the following software is used: IBM SPSS Statistics version 26; Factor Analysis software Release 10.10.02 64 bit (Baglin, 2014), and R3.5 (R Core Team, 2013).

For replicability and reproducibility, the dataset is publicly available (see Appendix A.2).

6.1. Data collection and data reliability

In total, 117 responses are collected. This comprises three datasets (see Table 6.1).

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

Table 6.1: Collected datasets. Total N is 117.

Data collection commenced at 15:00 (local time) July 7, 2020, using Prolific. The average reward per hour was £9.10/hr, with 10,824 of 131,703 eligible participants and a hundred open positions. After the questionnaire was published, we observed (real-time) how the progress proceeded.

During this process, we evaluated the responses using a protocol (see Table 6.2)—for quality and reliability assurance.

Data collection through Prolific took approximately 11 hours in total. In total, 12 responses were

Item	Criteria	Description
P1	Did the participant enter valid experiment codes?	At the end of the treatment participants are presented with the following question: "You have been provided a code (example J86) after you have completed all tasks. Enter this code here". If invalid codes are provided then the response is rejected since it indicates that the respondent did not perform the tasks – making the results not reliable. These results are destroyed since this experiment is—to a great extent—conducted without supervision. This is in particular important for the Prolific part since there is an incentive for participation.
P2	Is the time taken to complete reasonable (longer than 14 min for Group 1 and longer than 10 min for group 2)	Upon testing it was found that a reasonable time to complete is 20-25 min. However it could also be completed in 14 min for group 1, and 10 min for group 2 (time difference is due to the 3 minute video for group 1). Any response where the time taken to complete is shorter than the aforementioned times are destroyed. This minimum time is required for a proper understanding of the questions and experiment. Taking less time indicates unreliable responses.
P3	Does the respondent meet the demographic requirements (educational and occupation requirements)?	The majority of the participants make part of the proxy group. The respondent must therefore meet the educational and occupation requirements. Responses that fail to meet these requirements are destroyed.
P4	Did the respondent provide consistent answers?	When answers to questions are not consistent they are destroyed. For instance, a respondent which perceives the process as complex is unlikely to respond that the process does not require a lot of his/her mental effort.

Table 6.2: Quality control protocol

destroyed during the time: four responses were rejected and destroyed based on *P1*, two due to *P2*, four due to *P3*, and two due to *P4*. Upon rejection, this opened up new positions for other participants.

To make the assessment of consistency more clear, we explain this using the following example. A participant that was administered X_2 responded "*I have absolutely no idea what was going on at all*". While this response provides little meaning, it is also in contradiction with other responses such as *strongly agreeing* with the statement "*Understanding how the data is processed does not require a lot of my mental effort*".

We missed identifying two responses that failed to meet criteria *P3*. 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 *P3*: the participants have lower than undergraduate education, are skilled laborers (not skilled professionals), and difficulty understanding the application. This was

examined using SPSS syntax [A.5.16](#).

The questionnaire was also published within the author's own network. In total, 11 responses were collected. From this, two responses were destroyed due to failing protocol item *P1*, leaving nine valid responses. In the period before data collection (one month) and during data collection, no events took place—of which we are aware of—that might have had an influence on the research results.

6.2. Establishing the dataset

Three datasets are collected through three channels (see [Table 6.1](#)). The question remains whether the three datasets can be merged into a single dataset. In order to answer this question, we check whether the means are the same (between each dataset). First step: in the dataset, a new variable is created (*DatasetId*), and each dataset is assigned the respective value per the ID column values of [Table 6.1](#).

A one-way ANOVA is then used to compare the means of the three datasets for the variables. This is done using the SPSS syntax [A.5.1](#). From the output of the three datasets it is concluded that the three datasets can not be merged. The three datasets are considered significantly different on eighth variables. Upon further examination of the means, it is found that the third dataset is the cause. Herein, trustworthiness related variables (for MPC group) have been rated higher by the respondents in the third group. This dataset is therefore removed. The same test (comparable with an independent t-test) is then repeated for dataset 1 and 2. The output of this test shows a far from significant difference of means. It can therefore, be assumed that dataset 1 and 2 comprise participants from the same population. This dataset is further used for this study. SPSS outputs [??](#) provides an overview of the descriptive. SPSS outputs [6.26](#) through [6.26](#) provide a visualized version hereof.

Descriptives statistics on next page →

		I am satisfied with the trustworthiness of the METHOD				I would be willing to use this application based on its trustworthiness			
		2.00	3.00	4.00	5.00	2.00	3.00	4.00	5.00
The intent of the application is clear to me	1.00	2	1	1	0	2	1	1	0
	2.00	2	5	2	0	1	6	2	0
	3.00	1	3	7	0	2	3	5	0
	4.00	4	19	37	7	1	20	33	13
	5.00	1	1	11	3	1	1	12	2
The application clearly describes how my data is processed from data submission to output	1.00	1	0	0	0	0	1	0	0
	2.00	3	6	1	1	3	6	1	1
	3.00	3	8	9	0	3	8	8	0
	4.00	2	11	36	4	0	14	30	9
	5.00	1	4	12	5	1	2	14	5
The application provides a complete and detailed description of how METHOD is used to protect my data	1.00	4	0	0	0	2	2	0	0
	2.00	2	11	9	0	2	10	7	3
	3.00	1	10	8	1	0	11	8	1
	4.00	3	8	32	6	3	7	29	9
	5.00	0	0	9	3	0	1	9	2
Interaction with the application is clear and understandable	1.00	1	0	1	0	1	0	1	0
	2.00	2	9	3	0	2	9	2	1
	3.00	0	2	6	1	0	2	5	2
	4.00	5	15	34	6	3	16	32	8
	5.00	2	3	14	3	1	4	13	4
The descriptions of METHOD are complex	1.00	2	3	4	1	2	2	4	2
	2.00	2	6	11	0	1	6	11	1
	3.00	4	12	24	2	3	13	22	4
	4.00	1	7	19	6	0	9	15	8
	5.00	1	1	0	1	1	1	1	0
Understanding how the data is processed does not require a lot of my mental effort	1.00	1	3	2	0	1	3	2	0
	2.00	5	7	8	1	3	9	7	2
	3.00	2	8	12	1	1	8	13	1
	4.00	0	10	32	7	1	9	28	10
	5.00	2	1	4	1	1	2	3	2
Claims made by the application are clear and accurate	1.00	1	1	1	0	1	1	1	0
	2.00	2	0	3	0	1	1	3	0
	3.00	3	13	7	0	3	13	7	0
	4.00	3	15	38	6	1	16	34	10
	5.00	1	0	9	4	1	0	8	5
The application is open and transparent in how it protects my data	1.00	3	0	1	0	2	1	1	0
	2.00	2	4	6	0	2	4	6	0
	3.00	2	13	13	1	1	14	10	3
	4.00	3	11	33	4	2	12	29	8
	5.00	0	1	5	5	0	0	7	4

Table 6.3: Trustworthiness descriptive statistics

		METHOD provides a simple solution to secure data contribution				I would be willing to use METHOD based on the solution it provides to secure data contribution			
		2.00	3.00	4.00	5.00	2.00	3.00	4.00	5.00
It feels safe contributing sensitive company data over the application	1.00	0	2	2	0	0	2	1	1
	2.00	3	4	15	1	1	7	15	0
	3.00	1	5	14	2	0	6	13	3
	4.00	1	4	37	9	0	7	31	13
	5.00	0	1	3	3	0	1	4	1
The use of METHOD gives me a feeling of security assurance	1.00	0	1	1	0	0	1	0	1
	2.00	3	5	12	1	1	8	12	0
	3.00	2	5	13	3	0	7	12	4
	4.00	0	5	40	6	0	7	35	9
	5.00	0	0	5	5	0	0	5	4
Only I am able to view my contributed data	1.00	0	0	1	0	0	0	0	1
	2.00	1	3	9	0	0	5	7	1
	3.00	2	5	15	2	0	7	13	3
	4.00	2	7	41	9	1	10	37	11
	5.00	0	1	5	4	0	1	7	2
The service provider cannot examine my data beyond my control	1.00	0	2	3	1	0	2	2	2
	2.00	1	3	12	1	0	4	9	4
	3.00	3	10	20	3	0	14	17	4
	4.00	1	0	32	6	1	2	31	5
	5.00	0	1	4	4	0	1	5	3
I feel capable of using the application	1.00	1	0	1	0	0	1	1	0
	2.00	1	2	1	0	1	2	1	0
	3.00	1	6	7	1	0	9	5	1
	4.00	1	5	43	8	0	9	39	9
	5.00	1	3	19	6	0	2	18	8
My data cannot be accessed by other contributors	1.00	0	0	1	0	0	0	0	1
	2.00	1	3	5	0	0	4	3	2
	3.00	3	8	15	0	0	11	13	2
	4.00	1	5	37	8	1	8	34	8
	5.00	0	0	13	7	0	0	14	5

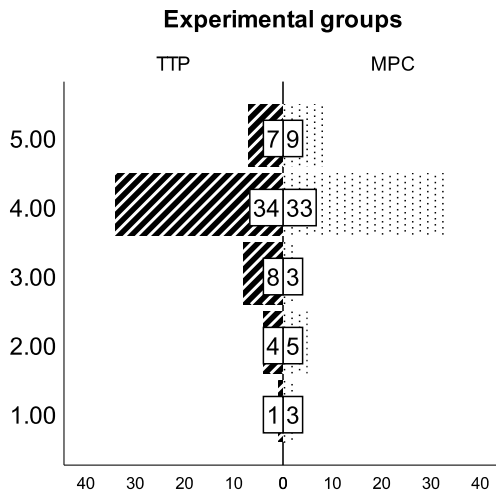
Table 6.4: Relative advantage descriptive statistics

		I am satisfied with the security of the METHOD				I would be willing to use this application based on the security provided by METHOD				
		2.00	3.00	4.00	5.00	1.00	2.00	3.00	4.00	5.00
It feels safe contributing sensitive company data over the application	1.00	1	2	0	1	0	2	1	0	1
	2.00	0	4	9	10	0	0	14	7	2
	3.00	0	3	7	11	1	2	9	9	2
	4.00	0	1	6	38	6	1	11	25	14
	5.00	1	0	1	3	2	1	0	4	1
The use of METHOD gives me a feeling of security assurance	1.00	1	1	0	0	0	1	1	0	0
	2.00	0	6	5	10	0	1	11	6	3
	3.00	0	2	13	7	1	3	13	6	1
	4.00	1	1	4	42	3	1	10	29	11
	5.00	0	0	1	4	5	0	0	4	5
Only I am able to view my contributed data	1.00	0	1	0	0	0	1	0	0	0
	2.00	1	3	3	6	0	2	6	4	1
	3.00	0	2	8	12	2	1	10	11	1
	4.00	1	4	9	38	7	2	16	24	17
	5.00	0	0	3	7	0	0	3	6	1
The service provider cannot examine my data beyond my control	1.00	0	2	1	3	0	1	2	3	0
	2.00	1	4	6	6	0	1	11	4	1
	3.00	0	4	13	17	2	3	16	14	2
	4.00	0	0	2	33	4	0	5	21	13
	5.00	1	0	1	4	3	1	1	3	4
I feel capable of using the application	1.00	0	1	0	1	0	0	1	1	0
	2.00	0	0	2	2	0	0	3	1	0
	3.00	1	2	3	8	1	2	7	5	1
	4.00	0	3	13	38	3	2	15	24	16
	5.00	1	4	5	14	5	2	9	14	3
My data cannot be accessed by other contributors	1.00	0	1	0	0	0	1	0	0	0
	2.00	1	2	1	4	1	2	2	4	1
	3.00	0	5	8	12	1	2	13	11	0
	4.00	1	2	10	37	1	1	16	19	15
	5.00	0	0	4	10	6	0	4	11	4

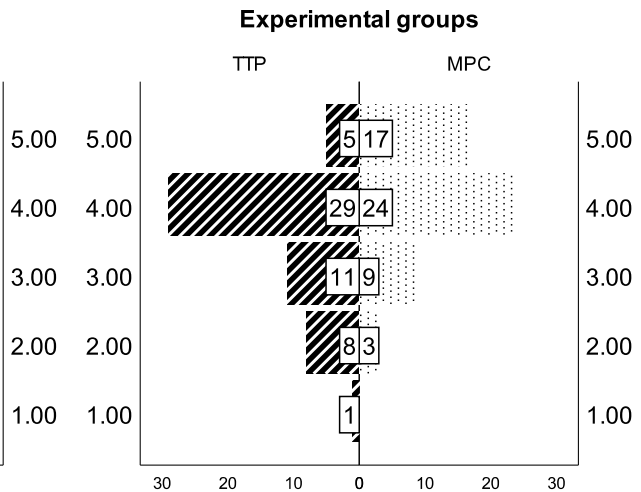
Table 6.5: Security descriptive statistics

		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			
		2.00	3.00	4.00	5.00
METHOD provides a simple solution to secure data contribution	2.00	1	3	1	0
	3.00	2	9	4	1
	4.00	2	15	48	6
	5.00	0	0	10	5
I would be willing to use METHOD based on the solution it provides to secure data contribution	2.00	0	1	0	0
	3.00	3	11	9	0
	4.00	0	13	42	9
	5.00	2	2	11	3
I am satisfied with the trustworthiness of the METHOD	2.00	4	5	1	0
	3.00	0	20	8	1
	4.00	1	2	47	8
	5.00	0	0	7	3
I would be willing to use this application based on its trustworthiness	2.00	2	4	1	0
	3.00	3	20	8	0
	4.00	0	3	42	8
	5.00	0	0	11	4
I am satisfied with the security METHOD provides	1.00	1	1	0	0
	2.00	4	4	2	0
	3.00	0	15	8	0
	4.00	0	7	49	7
I would be willing to use this application based on the security provided by METHOD	5.00	0	0	4	5
	2.00	3	2	1	0
	3.00	2	22	11	0
	4.00	0	3	35	7
	5.00	0	0	15	5

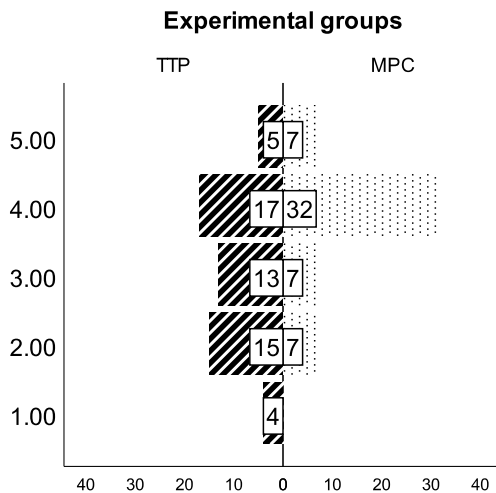
Table 6.6: Willingness descriptive statistics



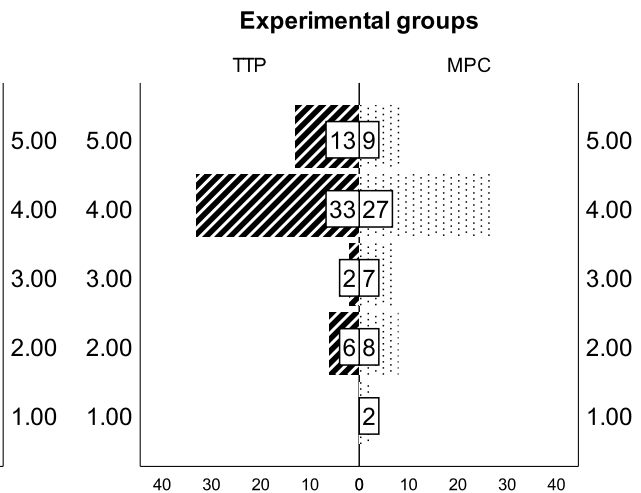
SPSS Output 6.1: *The intent of the application is clear to me*



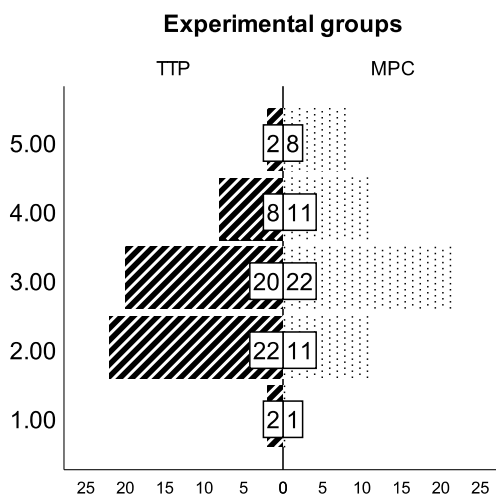
SPSS Output 6.2: *The application clearly describes how my data is processed from data submission to output*



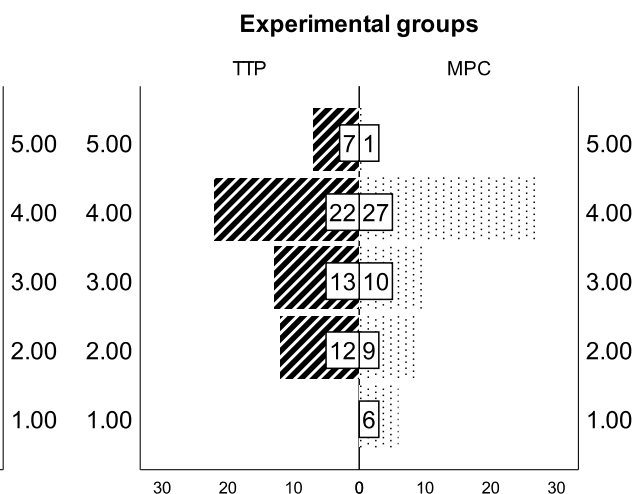
SPSS Output 6.3: *The application provides a complete and detailed description of how METHOD is used to protect my data*



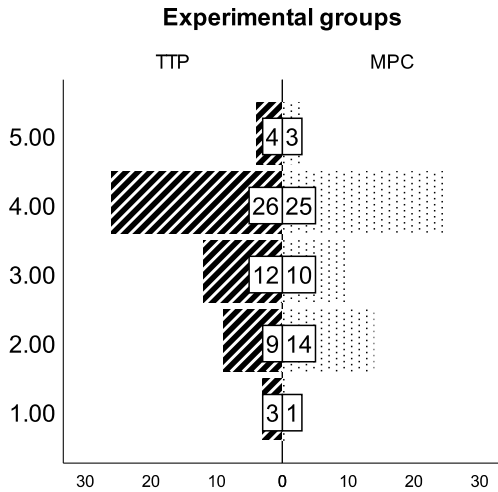
SPSS Output 6.4: *Interaction with the application is clear and understandable*



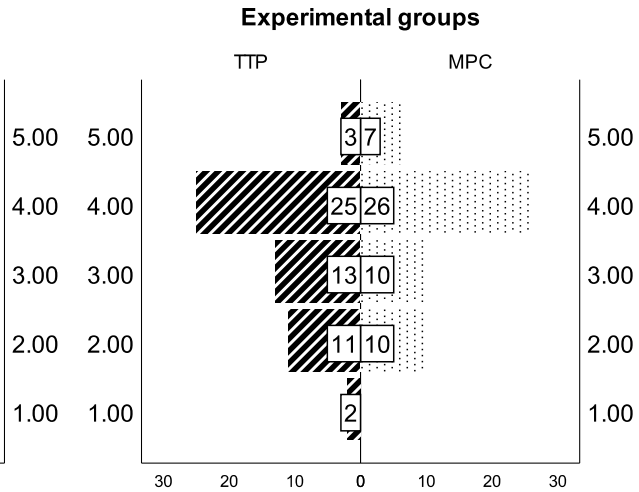
SPSS Output 6.5: *The descriptions of METHOD are complex*



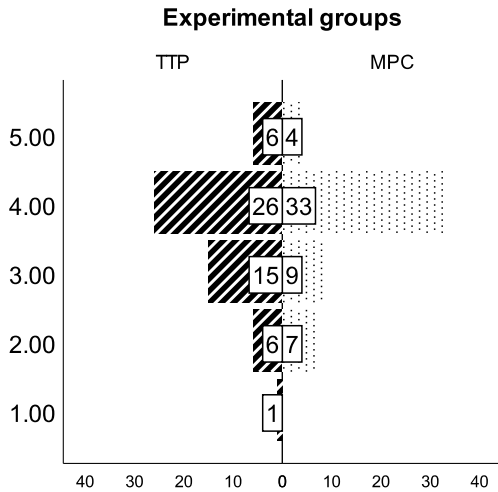
SPSS Output 6.6: *Understanding how the data is processed does not require a lot of my mental effort*



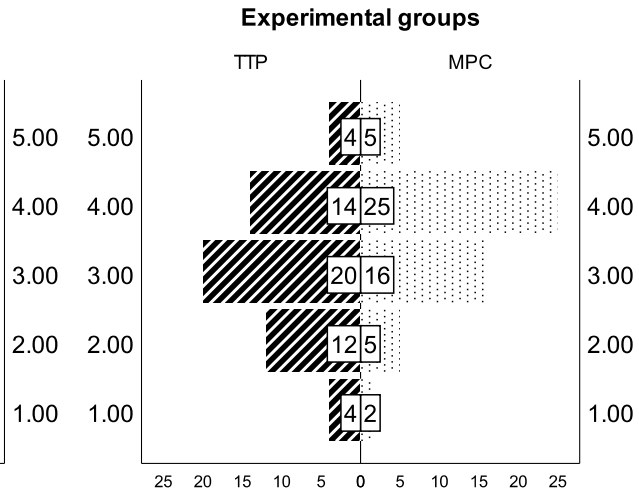
SPSS Output 6.7: *It feels safe contributing sensitive company data over the application*



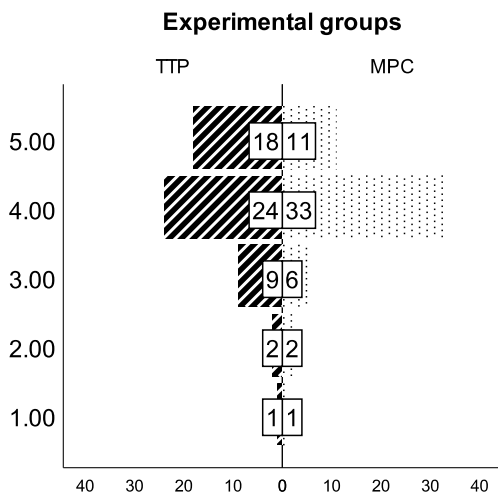
SPSS Output 6.8: *The use of METHOD gives me a feeling of security assurance.*



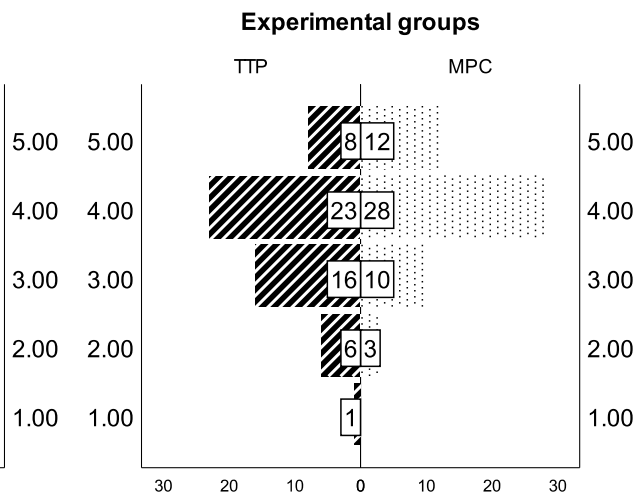
SPSS Output 6.9: *Only I am able to view my contributed data*



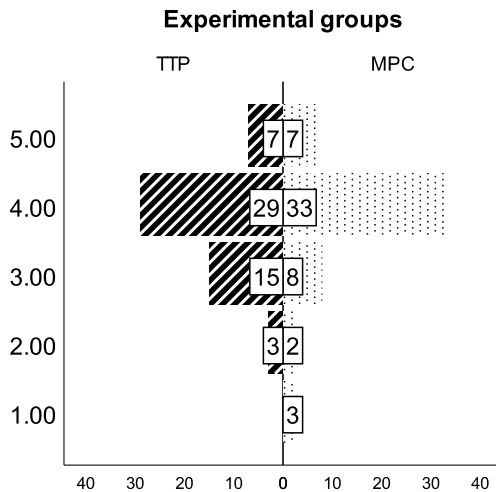
SPSS Output 6.10: *The service provider cannot examine my data beyond my control*



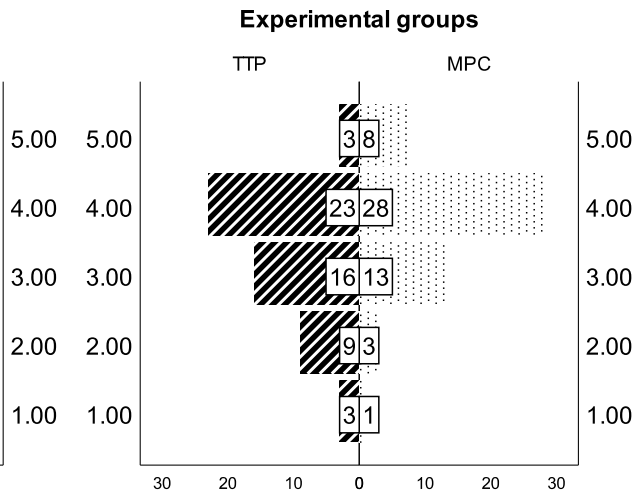
SPSS Output 6.11: *I feel capable of using the application*



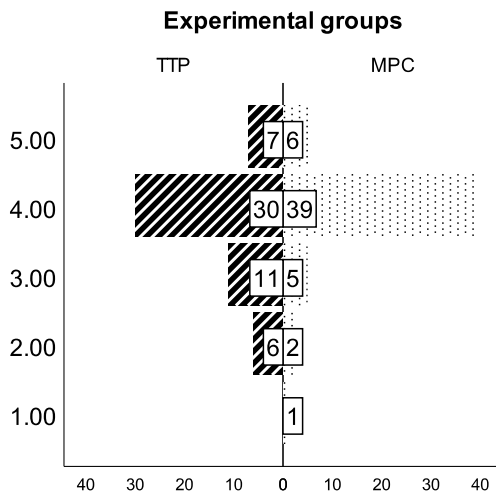
SPSS Output 6.12: *My data cannot be accessed by other contributors*



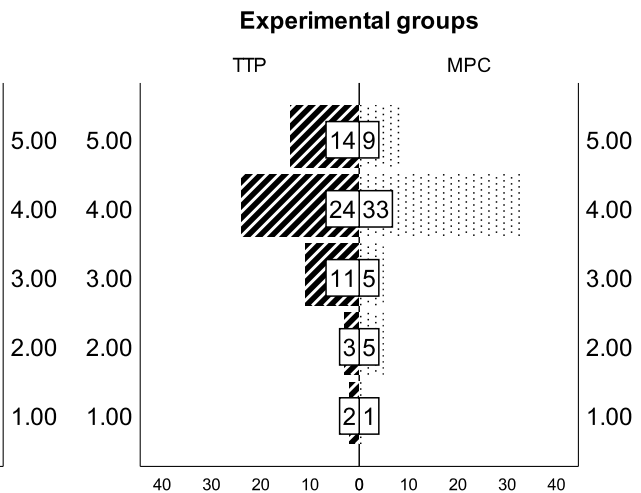
SPSS Output 6.13: Claims made by the application are clear and accurate



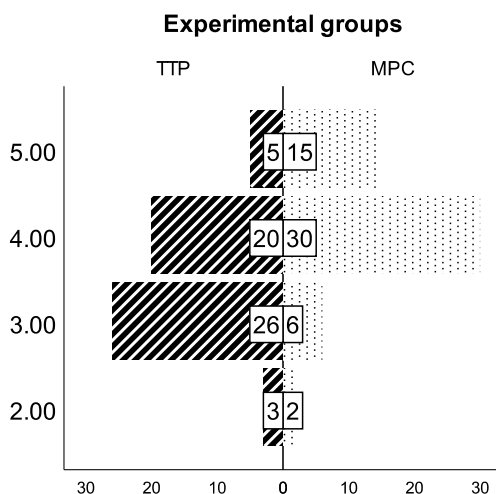
SPSS Output 6.14: The application is open and transparent in how it protects my data



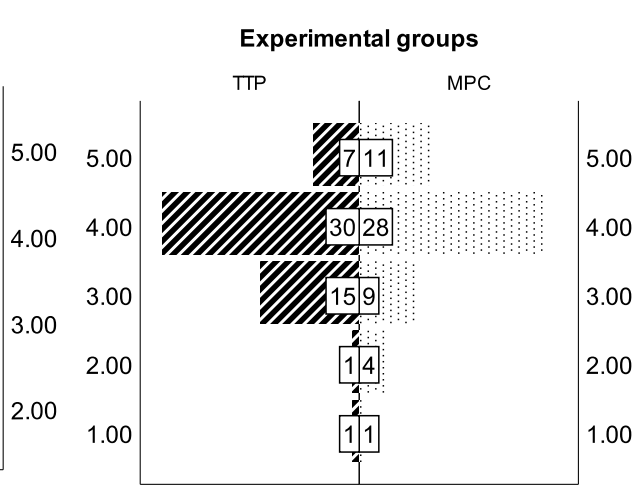
SPSS Output 6.15: The application provides a simple way to securely contribute data



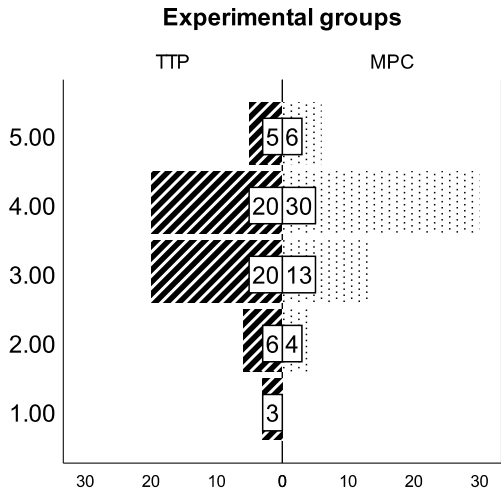
SPSS Output 6.16: The application does not require expertise from multiple organizational departments



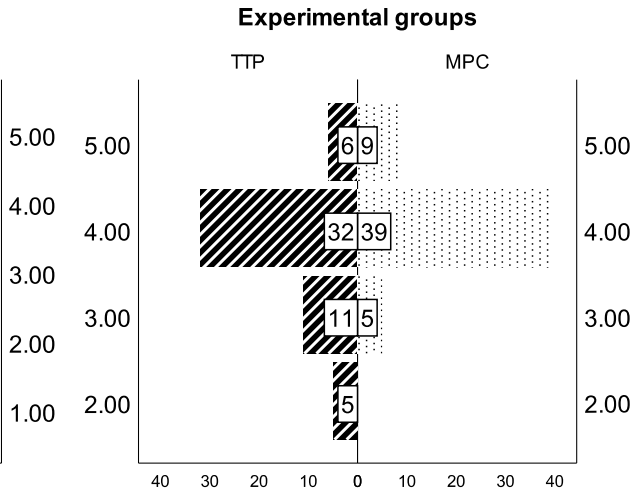
SPSS Output 6.17: The application provides an advantage over conventional data sharing practices



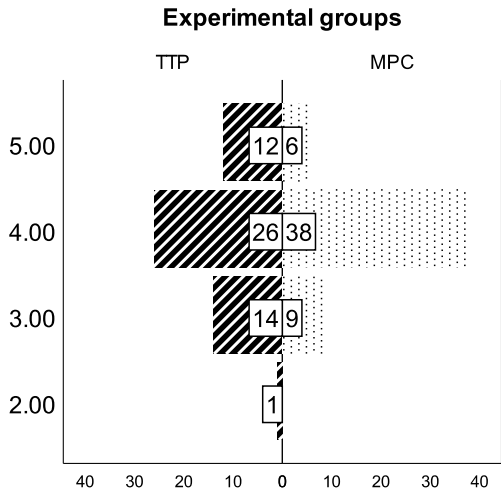
SPSS Output 6.18: When contributing data, no other party knows about my participation



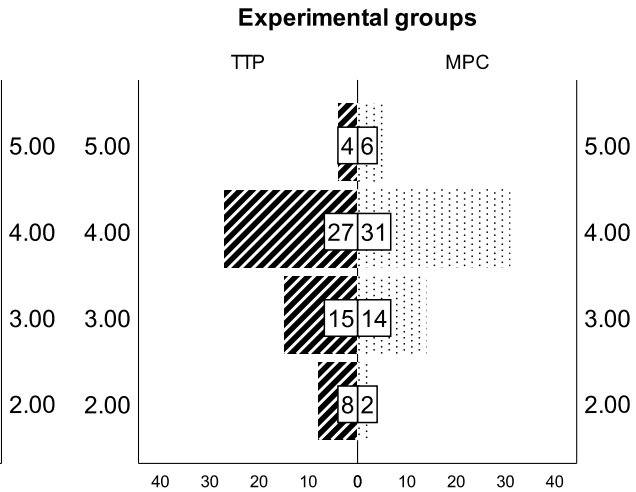
SPSS Output 6.19: I feel less hesitant with contributing sensitive company data when using this mpc application



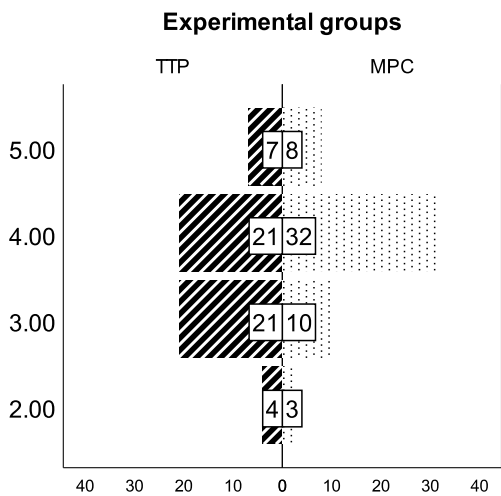
SPSS Output 6.20: METHOD provides a simple solution to secure data contribution



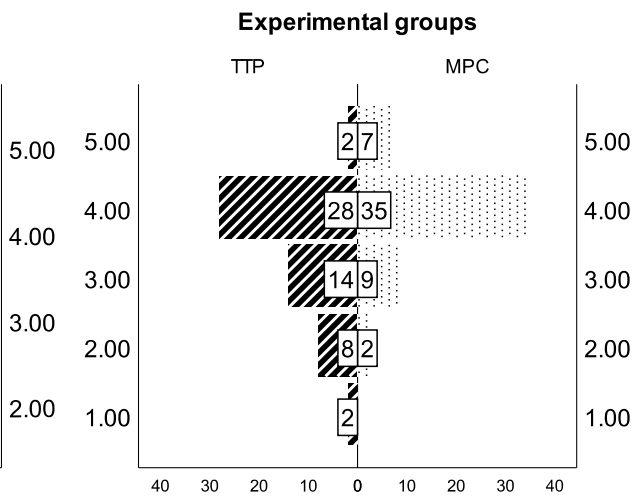
SPSS Output 6.21: I would be willing to use METHOD based on the solution it provides to secure data contribution



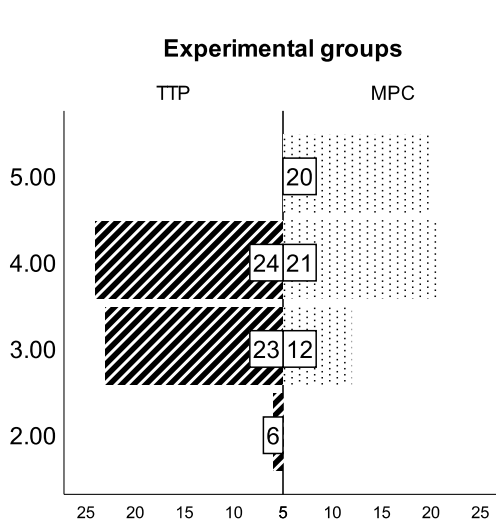
SPSS Output 6.22: I am satisfied with the trustworthiness of the METHOD application



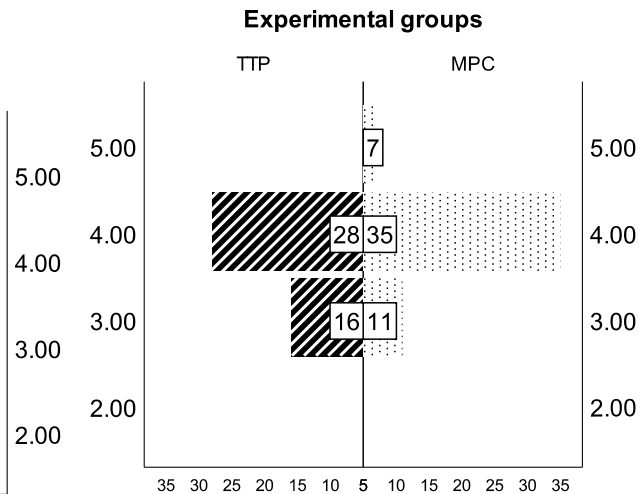
SPSS Output 6.23: I would be willing to use this application based on its trustworthiness



SPSS Output 6.24: I am satisfied with the security the METHOD provides



SPSS Output 6.25: I would be willing to use this application based on the security provided by METHOD.



SPSS Output 6.26: Overall, if the output (the analytic) of the application provides sufficient value to my organization, then I would be willing to contribute sensitive company data over a METHOD application.

6.3. Data preparation in SPSS

The first change to the dataset is the inclusion of an experimental group column. The two experimental groups must be reflected in the dataset. Group R_1 is categorized as MPC and group R_2 as TTP. This is done using the SPSS syntax [A.5.2](#).

Several variables are classified as ORDINAL but are, in fact, NOMINAL variables. Variable Q4.2 and Q4.8 through 4.10 are changed to NOMINAL. This is done using the SPSS syntax [A.5.3](#) (example shown is for Q4.2).

Then we use a boxplot to search for birth year outliers. This is done to find invalid responses. For instance, several participants entered age instead of birth year, and some provided invalid birth year (e.g., 19991). These are changed. Then, age is computed. This is done using the SPSS syntax [A.5.4](#).

Because of the blocks used in Qualtrics^{XM}, each group's responses are captured in individual columns. Thereby we need to merge these together in order to perform certain tests. This is done using the SPSS syntax [A.5.5](#).

The occupation of the participants have been grouped into several categories: upper management (e.g., operations manager), middle Management (e.g., shift manager), skilled professional (e.g., IT engineer), and skilled laborer (e.g. administrative employee). A new variable is created, and these values have been entered manually (see variable IndustryRole). The same process is repeated for categorizing industry functions such as Information Technology and software, Education, Sales, Marketing and Media (see variable IndustryFunctionCategory).

6.4. Participant demographics

The average age of the participants is 33. The 107 participants in the sample displayed an age median of 31, mode of 29, minimum of 21, and a maximum of 54, with IQR_1 at 27, IQR_2 at 31 and

IQR_3 at 36 (see SPSS output 6.27). The age distribution is shown by SPSS output 6.28¹. This is done using the SPSS syntax A.5.10. From the role at work frequency table (SPSS output 6.29), we can see that the majority of all participants have a role at work, which is at a satisfactory level². The highest educational degree earned is also at a satisfactory level (SPSS output 6.30). This is done using the SPSS syntax A.5.11. The participants categorized as skilled laborers, and the participants with lower than undergraduate degree will be addressed later.

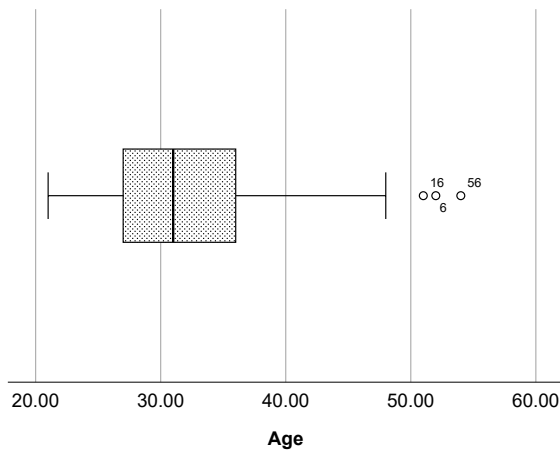
Next, we combine role at work with industry function (moved to the appendix due to its size. See SPSS output A.1). This is done using the SPSS syntax A.5.14. This output shows a homogeneous distribution of industry domains and level of seniority. Although the size of respondents in the technical domain comprises a large portion of the respondents' background, this is in favor of 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.

In the literature review, it is assumed that the familiarity of MPC amongst respondents is low. Then an 'educate' approach was followed. The participants who have been administered the MPC treatment are asked to rate their familiarity with MPC prior to taking part in the study. The results confirm our assumption (see SPSS output 6.31). This is done using the SPSS syntax A.5.15.

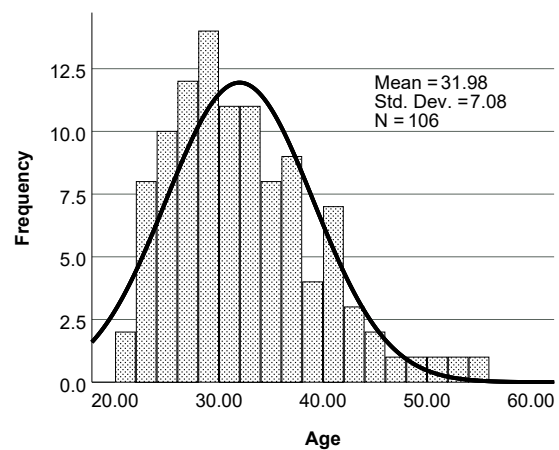
Finally, we create a pivot table grouping organizational size with education level (see SPSS output A.3). This is done using the SPSS syntax A.5.13. A pivot table is also created showing the involvement in innovation and role at work (see SPSS output A.2). This is done using the SPSS syntax A.5.12. These 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.

¹One participant did not enter age, hence N=106.

²We looked into the high number of respondents with an occupation level categorized as upper management—which seemed potentially dubious. We believe this might be due to the economic impact of COVID-19. That is, people seek other sources of income. On September 24, 2020, we re-evaluated the number of total eligible participants. Using the same participant-criteria, Prolific reported 19,718 matching participants (who have been active in the past 90 days), showing a significant increase when compared to 10,824 reported on July 7, 2020. Thus, we have no reason to call into question the high number of respondents categorized as upper management. Unfortunately, the information of total participants (including non-eligible participants) was omitted. This would have allowed us to compare the ratio further.



SPSS Output 6.27: Boxplot age distribution.



SPSS Output 6.28: Participant age distribution.

	Count	Table N %
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%

	Count	Table N %
Undergraduate (BA, BSc, other)	33	30.8%
High school diploma	4	3.7%
Graduate degree (MA, MSc, other)	52	48.6%
Technical/Community college	3	2.8%
Secondary education	2	1.9%
Doctorate degree (PhD, other)	12	11.2%
No formal qualifications	0	0.0%
Not applicable/I do not know	1	0.9%

SPSS Output 6.29: Role at work

SPSS Output 6.30: Education level

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not all familiar	32	29.9	60.4	60.4
	Slightly familiar	9	8.4	17.0	77.4
	Somewhat familiar	9	8.4	17.0	94.3
	Moderately familiar	3	2.8	5.7	100.0
	Total	53	49.5	100.0	
Missing	System	54	50.5		
Total		107	100.0		

SPSS Output 6.31: Level of familiarity with MPC

6.5. 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 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. This is possible because users were asked to rate their perceptions of the different aspects in 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 3.6.

Polychoric correlation (Olsson, 1979) is used for the correlation analysis. This is because of the limitations of PCA, which makes it not suited for Linkert scales, according to some scholars (Rigdon & Ferguson, 1991). Linkert 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 FACTOR³. The results are reported as listed in Table 6.7.

	Correlation	Page numbers	
		Factor analysis	Validity/fit
Trustworthiness	96	97-98	97-98
Security	99	100	100
Relative advantage	101	102	102
Willingness	103	N/A	103

Table 6.7: Overview of descriptive statistics and correlations

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. The descriptives, factor loading, reliability, and multicollinearity results (VIF, AVE, CR, and C- α) are reported in Appendix A.8.

6.5.1. PCA analysis, re-evaluation of constructs

For trustworthiness, several items 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.

³<http://psico.fcep.urv.es/utilitats/factor/index.html>

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. This is based on results of the qualitative assessment. We also found that the item “I feel capable of using the application” is also an inaccurate measure in terms 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.

6.5.2. Validity

As described in Section 6.1 a cross-sectional method is employed. As a result, Common Method Variance (multicollinearity) could be an issue. This is examined using two indicators. The first test employed is Harman’s one-factor test ((Tehseen, Ramayah, & Sajilan, 2017, p. 151)). Harman (1960) “uses exploratory factor analysis where all variables are loaded onto a single factor and constrained so that there is no rotation” (Eichhorn, 2014). CMV is an issue when the largest component explained is higher than 50% (Harman, 1960, ch. 7).

Also, the VIF values of the model are all well below 10, and the tolerance all well above 0.2. Moreover, from the correlation table, it is also clear that there are 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.

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.

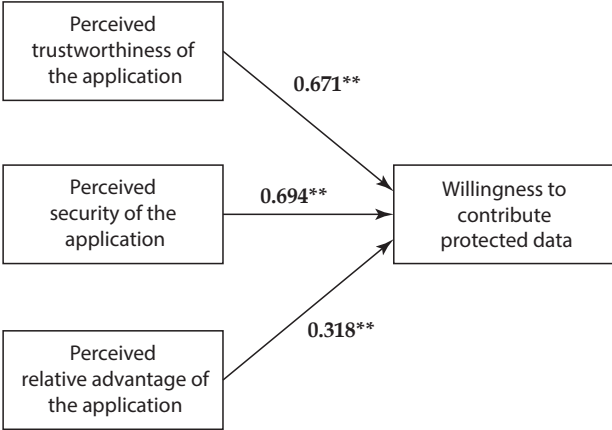
6.5.3. Results

A correlation of ($r=0,694$, $p < 0.001$) is reported between perceived trustworthiness and perceived willingness to contribute. A correlation of ($r=0,671$, $p < 0.001$) is reported between perceived security and perceived willingness to contribute. These are considered large effects ($r > 0.5$) (Field, 2017, ch.2) which reflect important aspects (our cut-off point).

However, a weak to medium correlation of ($r=0,318$, $p < 0.001$) 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, thus further indicating perceived relative advantage is not the primary concern. This also becomes clearer when comparing these values with the trustworthiness and security pairs.

An overview of the polychoric correlations is provided in Figure 6.32 on page 95. From the values reported we find evidence to support hypotheses $H2_A^2$ and $H3_A^2$; however, are unable to accept hypotheses $H4_A^2$ due to insufficient correlation.

Research model with polychoric correlations on next page →



** Correlation is significant at the 0.01 level (2-tailed).

SPSS Output 6.32: Research model: polychoric correlations for complete sample. N=106.

Perceived trustworthiness polychoric correlation results on next page →

		2	3	4	5	6	7	8	9	10								
1	The intent of the application is clear to me	Corr. Coefficient	.439**	.385**	.488**	.348**	.423**	.568**	.441**	.352**	.353**							
		Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000							
		Bias	0.000	-0.003	-0.001	0.000	-0.001	-0.001	-0.003	-0.002	-0.003							
		Std. Error	0.077	0.087	0.087	0.089	0.091	0.076	0.073	0.084	0.082							
		95% CI	Lwr. 0.277	0.203	0.301	0.170	0.229	0.409	0.285	0.171	0.182	Upp. 0.582	0.549	0.640	0.516	0.586	0.704	0.574
2	The application clearly describes how my data is processed from data submission to output	Corr. Coefficient	1.000	.490**	.297**	0.169	.351**	.395**	.493**	.411**	.437**							
		Sig. (2-tailed)	0.000	0.000	0.002	0.084	0.000	0.000	0.000	0.000	0.000							
		Bias	0.000	-0.002	0.000	0.000	0.000	0.000	-0.001	-0.001	-0.003							
		Std. Error	0.000	0.079	0.102	0.094	0.091	0.077	0.076	0.092	0.086							
		95% CI	Lwr. 1.000	0.327	0.092	-0.022	0.163	0.242	0.332	0.223	0.262	Upp. 1.000	0.639	0.496	0.353	0.521	0.533	0.626
3	The application provides a complete and ... of how METHOD is used to protect my data	Corr. Coefficient	1.000	.227*	0.116	.307**	.399**	.720**	.499**	.381**								
		Sig. (2-tailed)	0.000	0.019	0.236	0.001	0.000	0.000	0.000	0.000								
		Bias	0.000	0.000	0.003	0.002	-0.001	-0.002	0.001	0.002								
		Std. Error	0.000	0.087	0.103	0.098	0.074	0.057	0.074	0.088								
		95% CI	Lwr. 1.000	0.055	-0.084	0.114	0.245	0.591	0.353	0.198	Upp. 1.000	0.395	0.318	0.490	0.539	0.819	0.638	0.549
4	Interaction with the application is clear and understandable	Corr. Coefficient			1.000	.307**	.390**	.360**	.289**	.245*	.235*							
		Sig. (2-tailed)			0.001	0.000	0.000	0.003	0.011	0.015								
		Bias			0.000	-0.005	-0.002	0.000	0.002	0.000								
		Std. Error			0.000	0.098	0.086	0.101	0.084	0.093								
		95% CI			Lwr. 1.000	0.105	0.215	0.146	0.128	0.050	Upp. 1.000	0.485	0.545	0.555	0.456	0.421	0.421	
5	The descriptions of METHOD are complex	Corr. Coefficient				1.000	.335**	.257**	0.127	0.190	0.102							
		Sig. (2-tailed)				0.000	0.008	0.195	0.051	0.299								
		Bias				0.000	-0.002	-0.004	0.003	-0.001								
		Std. Error				0.000	0.097	0.099	0.108	0.100								
		95% CI				Lwr. 1.000	0.131	0.054	-0.079	-0.018	Upp. 1.000	0.512	0.438	0.339	0.379	0.292		
6	Understanding how the data is processed does not require a lot of my mental effort	Corr. Coefficient					1.000	.422**	.325**	.311**	.311**							
		Sig. (2-tailed)					0.000	0.001	0.001	0.001	0.001							
		Bias					0.000	-0.001	0.002	-0.002	-0.001							
		Std. Error					0.000	0.091	0.095	0.096	0.095							
		95% CI					Lwr. 1.000	0.225	0.140	0.112	Upp. 1.000	0.587	0.505	0.491	0.484			
7	Claims made by the application are clear and accurate	Corr. Coefficient						1.000	.511**	.427**	.445**							
		Sig. (2-tailed)						0.000	0.000	0.000								
		Bias						0.000	-0.001	-0.004								
		Std. Error						0.000	0.077	0.085								
		95% CI						Lwr. 1.000	0.343	0.247	Upp. 1.000	0.650	0.582	0.592				
8	The application is open and transparent in how it protects my data	Corr. Coefficient							1.000	.412**	.400**							
		Sig. (2-tailed)							0.000	0.000								
		Bias							0.000	0.001								
		Std. Error							0.000	0.085								
		95% CI							Lwr. 1.000	0.234	Upp. 1.000	0.575	0.556					
9	I am satisfied with the trustworthiness of the METHOD	Corr. Coefficient								1.000	.859**							
		Sig. (2-tailed)								0.000	0.000							
		Bias								0.000	-0.001							
		Std. Error								0.000	0.042							
		95% CI								Lwr. 1.000	0.766	Upp. 1.000	0.930					
10	I would be willing to use this application based on its trustworthiness	Corr. Coefficient									1.000							
		Sig. (2-tailed)									0.000							
		Bias									0.000							
		Std. Error									0.000							
		95% CI									Lwr. 1.000	Upp. 1.000						

** Correlation is significant at the 0.01 level (2-tailed). * Correlation is significant at the 0.05 level (2-tailed).
 Bootstrap results are based on 1000 bootstrap samples.
 N=106 for all items, except item 10, N=105 (missing value).

Table 6.8: Correlation: trustworthiness and willingness to contribute

Determinant of the matrix	0.116
Bartlett's statistic	221.5 (df =6; P<0.001)
Kaiser-Meyer-Olkin (KMO) test	0.73216; (fair, see (Kaiser, 1974, pg.35))
BC Bootstrap 95% confidence interval of KMO	[0.644,0.812]

Table 6.9: Adequacy of the polychoric correlation matrix

Item	Rotation 1		Rotation 2		Bca	
	Component		Component		Lwr.	Uppr.
	C1	C2	C1	C2		
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
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; small difference in factor loading between components.

Factor loadings are suggested at least 0.60 and ideally at 0.70 or above (Chin, 1998).

Table 6.10: Perceived trustworthiness: Factor loadings. Test is run using FACTOR.

Component	Variance	Proportion of variance	Reliability	Factor Determinancy Index
1	2.539	0.363	0.926	0.962
2	2.317	0.331	0.859	0.927

Table 6.11: Perceived trustworthiness: Explained variance and reliability of rotated components.

Var	Eigenvalue	PoV	Cumulative PoV
1	3.491	0.499	0.499
2	1.363	0.195	0.694
3	0.640	0.092	
4	0.503	0.072	
5	0.474	0.068	
6	0.358	0.051	
7	0.167	0.024	

PoV = Proportion of variance

Table 6.12: Perceived trustworthiness: Explained variance of eigenvalues.

	C1	C2
C1	1	
C2	0.433	1

Table 6.13: Perceived trustworthiness: inter-factors correlation.

Continued on next page →

	Fitted	Standardized
Smallest Residual	-0.1934	-1.99
Median Residual	-0.0400	-0.41
Largest Residual	0.1120	1.15
Mean Residual	-0.0496	-0.51
Variance Residual	0.0052	
Root Mean Square of Residuals (RMSR)	0.0877	
BC Bootstrap 95% confidence interval of RMSR	[0.070,0.101]	
Expected mean value of RMSR for an acceptable model	0.0971	
Weighted Root Mean Square Residual (WRMR)	0.0858	
BC Bootstrap 95% confidence interval of WRMR	[0.068,0.098]	

Table 6.14: *Perceived trustworthiness: distribution of residuals.*

Perceived security polychoric correlation results on next page →

		2	3	4	5	6	7	8	
1	It feels safe contributing sensitive company data over the application	Corr. Coefficient	.797**	.360**	.334**	0.168	0.172	.455**	.334**
		Sig. (2-tailed)	0.000	0.000	0.000	0.085	0.078	0.000	0.000
		Bias	-0.001	-0.001	0.002	-0.003	-0.003	-0.003	-0.004
		Std. Error	0.041	0.089	0.093	0.102	0.103	0.089	0.095
		95% CI Lower Upper	0.707 0.867	0.178 0.528	0.150 0.506	-0.037 0.364	-0.037 0.362	0.270 0.613	0.140 0.512
2	The use of METHOD gives me a feeling of security assurance	Corr. Coefficient	1.000	.347**	.423**	0.162	.274**	.566**	.459**
		Sig. (2-tailed)		0.000	0.000	0.097	0.005	0.000	0.000
		Bias	0.000	-0.003	-0.001	-0.004	-0.004	-0.004	-0.004
		Std. Error	0.000	0.085	0.084	0.101	0.098	0.077	0.084
		95% CI Lower Upper	1.000 1.000	0.177 0.507	0.243 0.574	-0.036 0.353	0.080 0.458	0.405 0.703	0.282 0.615
3	Only I am able to view my contributed data	Corr. Coefficient		1.000	.439**	.287**	.546**	.219*	.272**
		Sig. (2-tailed)			0.000	0.003	0.000	0.024	0.005
		Bias	0.000	0.000	0.002	-0.004	-0.001	-0.002	-0.001
		Std. Error	0.000	0.000	0.091	0.100	0.083	0.095	0.090
		95% CI Lower Upper	1.000 1.000	0.262 0.613	0.086 0.474	0.379 0.699	0.021 0.397	0.090 0.444	
4	The service provider cannot examine my data beyond my control	Corr. Coefficient			1.000	0.014	.436**	.469**	.466**
		Sig. (2-tailed)				0.885	0.000	0.000	0.000
		Bias	0.000	0.000	0.000	0.002	0.000	-0.004	-0.003
		Std. Error	0.000	0.000	0.109	0.088	0.084	0.083	0.083
		95% CI Lower Upper	1.000 1.000	-0.194 0.232	0.265 0.609	0.292 0.625	0.296 0.624		
5	I feel capable of using the application	Corr. Coefficient				1.000	0.098	0.112	0.098
		Sig. (2-tailed)					0.316	0.253	0.319
		Bias	0.000	0.000	0.000	-0.002	0.003	0.001	0.001
		Std. Error	0.000	0.000	0.114	0.108	0.108	0.093	0.093
		95% CI Lower Upper	1.000 1.000	-0.137 0.320	-0.095 0.320	-0.089 0.282			
6	My data cannot be accessed by other contributors	Corr. Coefficient					1.000	.354**	.315**
		Sig. (2-tailed)						0.000	0.001
		Bias	0.000	0.000	0.000	-0.003	-0.002	-0.002	-0.002
		Std. Error	0.000	0.000	0.097	0.082	0.082	0.082	0.082
		95% CI Lower Upper	1.000 1.000	0.154 0.534	0.146 0.472				
7	I am satisfied with the security METHOD provides	Corr. Coefficient						1.000	.766**
		Sig. (2-tailed)							0.000
		Bias	0.000	0.000	0.000	-0.003	-0.003	-0.003	-0.003
		Std. Error	0.000	0.000	0.041	0.041	0.041	0.041	0.041
		95% CI Lower Upper	1.000 1.000	0.677 0.832					
8	I would be willing to use this application based on the security provided by METHOD	Corr. Coefficient							1.000
		Sig. (2-tailed)							0.000
		Bias	0.000	0.000	0.000	0.000	0.000	0.000	0.000
		Std. Error	0.000	0.000	0.000	0.000	0.000	0.000	0.000
		95% CI Lower Upper	1.000 1.000	1.000 1.000					

** Correlation is significant at the 0.01 level (2-tailed).

* Correlation is significant at the 0.05 level (2-tailed).

Bootstrap results are based on 1000 bootstrap samples.
N = 106 for all items.

Table 6.15: Correlation: Security and willingness to contribute

Determinant of the matrix	0.054
Bartlett's statistic	302.0 (df=10; P<0.001)
Kaiser-Meyer-Olkin (KMO) test	0.616 (mediocre, see (Kaiser, 1974, pg.35))
BC Bootstrap 95% confidence interval of KMO	[0.491,0.735]

Table 6.16: Adequacy of the polychoric correlation matrix

Item	Rotation 1		Rotation 2		Bca	
	Component		Component		Lwr.	Uppr.
	C1	C2	C1	C2		
1	It feels safe contributing sensitive company data over the application		0.988	0.988	0.914	1.067
2	The use of MPC gives me a feeling of security assurance		0.947	0.947	0.868	0.976
3	0.825	Only I am able to view my contributed data		0.825	0.498	0.928
4	0.588	The service provider cannot examine my data beyond my control		0.588	0.199	0.766
5	I feel capable of using the application**		0.591			
6	0.928	My data cannot be accessed by other contributors		0.928	0.743	1.022

**Item was removed; was not found not an accurate measure. This item fits the context of implementation. Factor loadings are suggested at least 0.60 and ideally at 0.70 or above (Chin, 1998).

Table 6.17: Perceived security: factor loadings. Test is run using FACTOR.

Component	Variance	Proportion of variance	Reliability	Factor Determinancy Index
1	2.026	0.405	0.97	0.985
2	1.949	0.39	0.885	0.941

Table 6.18: Perceived security: explained variance and reliability of rotated components.

Var.	Eigenvalue	PoV	Cumulative PoV
1	2.891	0.578	0.578
2	1.085	0.217	0.795
3	0.562	0.112	
4	0.383	0.077	
5	0.080	0.016	

PoV = Proportion of variance

Table 6.19: Perceived security: explained variance of eigenvalues.

	C1	C2
C1	1	
C2	0.393	1

Table 6.20: Perceived security: inter-factors correlation.

	Fitted	Standardized
Smallest Residual	-0.1583	-1.63
Median Residual	-0.0536	-0.55
Largest Residual	0.0594	0.61
Mean Residual	-0.0512	-0.53
Variance Residual	0.0053	
Root Mean Square of Residuals (RMSR)	0.0888	
BC Bootstrap 95% confidence interval of RMSR	[0.065,0.112]	
Expected mean value of RMSR for an acceptable model	0.0971	
Weighted Root Mean Square Residual (WRMR)	0.0957	
BC Bootstrap 95% confidence interval of WRMR	[0.072,0.123]	

Table 6.21: Perceived security: distribution of residuals.

Perceived relative advantage polychoric correlation results on next page →

		2	3	4	5	6	
1	The application provides a simple way to securely contribute data	Corr. Coefficient	.310**	.282**	.446**	.332**	.523**
		Sig. (2-tailed)	0.001	0.003	0.000	0.000	0.000
		Bias	-0.004	-0.006	-0.004	-0.005	-0.008
		Std. Error	0.101	0.115	0.086	0.103	0.079
		95% CI Lwr. Upp.	0.109 0.497	0.037 0.492	0.264 0.604	0.114 0.518	0.353 0.659
2	The application does not require expertise from multiple organizational departments	Corr. Coefficient	1.000	0.063	0.138	.322**	.343**
		Sig. (2-tailed)		0.521	0.157	0.001	0.000
		Bias	0.000	-0.004	-0.005	-0.005	-0.005
		Std. Error	0.000	0.107	0.103	0.097	0.088
		95% CI Lwr. Upp.	1.000 1.000	-0.157 0.266	-0.074 0.332	0.128 0.502	0.160 0.499
3	The application provides an advantage over conventional data sharing practices	Corr. Coefficient		1.000	.293**	.382**	.442**
		Sig. (2-tailed)			0.002	0.000	0.000
		Bias		0.000	0.000	0.000	-0.007
		Std. Error		0.000	0.095	0.099	0.087
		95% CI Lwr. Upp.		1.000 1.000	0.097 0.470	0.185 0.569	0.255 0.594
4	When contributing data, no other party knows about my participation	Corr. Coefficient			1.000	.420**	.373**
		Sig. (2-tailed)				0.000	0.000
		Bias			0.000	-0.002	-0.005
		Std. Error			0.000	0.078	0.083
		95% CI Lwr. Upp.			1.000 1.000	0.255 0.564	0.197 0.525
5	I feel less hesitant with contributing sensitive company data when using this mpc application	Corr. Coefficient				1.000	.393**
		Sig. (2-tailed)					0.000
		Bias				0.000	-0.006
		Std. Error				0.000	0.091
		95% CI Lwr. Upp.				1.000 1.000	0.196 0.553
6	METHOD provides a simple solution to secure data contribution	Corr. Coefficient					1.000
		Sig. (2-tailed)					
		Bias					0.000
		Std. Error					0.000
		95% CI Lwr. Upp.					1.000 1.000

** Correlation is significant at the 0.01 level (2-tailed).
* Correlation is significant at the 0.05 level (2-tailed).
Bootstrap results are based on 1000 bootstrap samples.
N = 106 for all items.

Table 6.22: Correlation: Relative advantage and willingness to contribute

Determinant of the matrix	0.376
Bartlett's statistic	101.5 (df =6; P<0.001)
Kaiser-Meyer-Olkin (KMO) test	0.70183 (fair, see (Kaiser, 1974, pg.35))
BC Bootstrap 95% confidence interval of KMO	[0.570,0.802]

Table 6.23: Adequacy of the polychoric correlation matrix

Item		Rotation 1		Rotation 2		Bca	
		Component		Component		Lwr.	Uppr.
		C1	C2	C1	C2		
1	The application provides a simple way to securely contribute data	0.752	N/A	N/A	N/A	0.463	0.854
2	The application does not require expertise from multiple organizational departments**		N/A	N/A	N/A	N/A	N/A
3	The application provides an advantage over conventional data sharing practices	0.656	N/A	N/A	N/A	0.263	0.805
4	When contributing data, no other party knows about my participation	0.815	N/A	N/A	N/A	0.687	0.886
5	I feel less hesitant with contributing sensitive company data when using this mpc application	0.785	N/A	N/A	N/A	0.640	0.864

**Item was removed; due to low factor loading (0.544).

Factor loadings are suggested at least 0.60 and ideally at 0.70 or above (Chin, 1998).

Table 6.24: Perceived relative advantage: factor loadings. Test is run using FACTOR.

Component	Variance	Proportion of variance	Reliability estimate
1	2.276	0.569	0.747

Table 6.25: Perceived relative advantage: Explained variance and reliability.

Var	Eigenvalue	PoV	Cumulative PoV
1	2.276	0.569	0.569
2	0.809	0.202	
3	0.528	0.132	
4	0.387	0.097	

PoV = Proportion of variance

Table 6.26: Perceived relative advantage: Explained variance of eigenvalues.

	Fitted	Standardized
Smallest Residual	-0.2152	-2.22
Median Residual	-0.2074	-2.14
Largest Residual	-0.0343	-0.35
Mean Residual	-0.1423	-1.47
Variance Residual	0.0056	
Root Mean Square of Residuals (RMSR)	0.1607*	
BC Bootstrap 95% confidence interval of RMSR	[0.116,0.223]	
Expected mean value of RMSR for an acceptable model	0.0971	
Weighted Root Mean Square Residual (WRMR)	0.1265**	
BC Bootstrap 95% confidence interval of WRMR	[0.091,0.171]	

*Violates criteria; see (Harman, 1960, pg. 21)

**Violates criteria; see(yun Yu, 2002, pg. 67-69)

Table 6.27: Perceived relative advantage: distribution of residuals.

Perceived willingness polychoric correlation results on next page →

		2	3	4	5	6	7	
1	METHOD provides a simple solution to secure data contribution	Corr. Coefficient	.706**	.611**	.601**	.476**	.544**	.487**
		Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	0.000
		Bias	0.000	-0.001	0.000	-0.001	-0.002	-0.002
		Std. Error	0.060	0.057	0.062	0.067	0.056	0.079
		95% CI Lower	0.581	0.491	0.465	0.337	0.426	0.316
		95% CI Upper	0.809	0.716	0.710	0.599	0.647	0.627
2	I would be willing to use METHOD based on the solution it provides to secure data contribution	Corr. Coefficient	1.000	.405**	.412**	.290**	.296**	.318**
		Sig. (2-tailed)		0.000	0.000	0.003	0.002	0.001
		Bias	0.000	0.001	0.001	0.002	0.002	0.000
		Std. Error	0.000	0.089	0.086	0.103	0.103	0.098
		95% CI Lower	1.000	0.225	0.240	0.085	0.093	0.117
		95% CI Upper	1.000	0.575	0.572	0.492	0.491	0.508
3	I am satisfied with the trustworthiness of the METHOD	Corr. Coefficient		1.000	.859**	.630**	.599**	.679**
		Sig. (2-tailed)		0.000	0.000	0.000	0.000	0.000
		Bias		0.000	-0.002	-0.003	-0.004	-0.004
		Std. Error		0.000	0.045	0.065	0.062	0.065
		95% CI Lower		1.000	0.760	0.491	0.467	0.538
		95% CI Upper	1.000	0.932	0.745	0.711	0.792	
4	I would be willing to use this application based on its trustworthiness	Corr. Coefficient			1.000	.600**	.618**	.694**
		Sig. (2-tailed)			0.000	0.000	0.000	0.000
		Bias			0.000	-0.004	-0.003	-0.004
		Std. Error			0.000	0.070	0.058	0.053
		95% CI Lower			1.000	0.442	0.496	0.584
		95% CI Upper			1.000	0.721	0.715	0.788
5	I am satisfied with the security METHOD provides	Corr. Coefficient				1.000	.766**	.686**
		Sig. (2-tailed)				0.000	0.000	0.000
		Bias				0.000	-0.004	-0.003
		Std. Error				0.000	0.041	0.059
		95% CI Lower				1.000	0.677	0.558
		95% CI Upper			1.000	0.835	0.793	
6	I would be willing to use this application based on the security provided by METHOD	Corr. Coefficient					1.000	.671**
		Sig. (2-tailed)					0.000	0.000
		Bias					0.000	-0.004
		Std. Error					0.000	0.052
		95% CI Lower					1.000	0.559
		95% CI Upper				1.000	0.764	
7	Overall, if the output ... willing to contribute sensitive company data over a METHOD application	Corr. Coefficient						1.000
		Sig. (2-tailed)						0.000
		Bias						0.000
		Std. Error						0.000
		95% CI Lower						1.000
		95% CI Upper					1.000	

** Correlation is significant at the 0.01 level (2-tailed).

* Correlation is significant at the 0.05 level (2-tailed).

Bootstrap results are based on 1000 bootstrap samples.

N = 106 for all items.

Table 6.28: Correlation: Perceptions and overall willingness to contribute

Determinant of the matrix	0.116
Bartlett's statistic	221.5 (df =6; P<0.001)
Kaiser-Meyer-Olkin (KMO) test	0.73216 (fair, see (Kaiser, 1974, pg.35))
BC Bootstrap 95% confidence interval of KMO	[0.644,0.812]

Table 6.29: Adequacy of the polychoric correlation matrix

6.6. Hypotheses testing

In this section we test the hypothesis with the aim to answer the last sub question: “To what extent does MPC change perception towards willingness to contribute protected data and what is its effect on the previously determined factors?”. The structure of this chapter follows the same sequence as the structure of the question. First, we analyze the extent to which MPC changes perception concerning willingness to contribute data (6.6.1). Then we analyze the extent to which MPC affects the perception of trustworthiness, relative advantage, and security. In the following sections, Cohen’s d is calculated using the following formula:

$$\text{Cohen's } d = \frac{M_2 - M_1}{SD_{pooled}} \quad \text{where: } SD_{pooled} = \sqrt{\frac{SD_1^2 + SD_2^2}{2}} \quad (6.1)$$

Upon running the independent t-test, in some cases Levene’s test indicates that the variances of the two groups is not equal. That is, the significance indicates 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).

6.6.1. Willingness to contribute

To recall, the trustworthiness hypothesis is:

H1_A¹ : Willingness to contribute protected data through MPC is greater than willingness to contribute protected data over TTP.

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) a Bayesian comparison of means is performed, and an independent samples t-test is used.

First, the Bayesian comparison of means is performed. This is done using the SPSS syntax A.5.17. The results Bayesian comparison of means is:

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 to 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, $BF_{01}=3.144$, suggested that the data were moderately more probable under the alternative hypothesis than the null.

Then, an independent t-test is performed. This is done using the SPSS syntax A.5.18. The results of the t-test using bootstrap is⁴:

⁴The values you get when running the syntax could differ because of the way bootstrapping works (sampling).

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 reject the null hypothesis and accept the alternate hypothesis.

6.6.2. Trustworthiness, relative advantage and security

Similar to *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.

Trustworthiness

To recall, the trustworthiness hypothesis is:

H2_A¹ : Perceived trustworthiness of an MPC-enabled application is greater than perceived trustworthiness of a TTP based application.

An independent t-test is used. This is done using the SPSS syntax [A.5.19](#). The results of the robust test is:

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.

To avoid making a type two error, a one-tailed approach⁵ is used to increase power. The critical values are $t(104)[one-tailed]=1.660$, and $t(104)[two-tailed]=1.983$ ⁶. In SPSS, an independent t-test is used with a 90% confidence interval (one end of the distribution). This is done using the SPSS syntax [A.5.20](#). The results of the one-tailed test are:

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 $t(104)=1.738$, $p=.043$ ^a (one-tailed). Thereby we accept the alternate hypothesis. A

⁵SPSS version 26 does not provide an option for one-tailed independent t-tests.

⁶The critical values are calculated using Excel's TINV function

Cohen's d effect of $d=0.408$ represents a 'medium' effect size.

^aone-tailed significance, calculated with Excel's TDIST function using SPSS output values.

Security

To recall, the security hypothesis is:

H3_A¹ : Perceived security of an MPC-enabled application is greater than perceived security of a TTP based application.

An independent t-test is used. This is done using the SPSS syntax [A.5.22](#). The results of the robust test is:

The homogeneity of variance assumption was met ($p=.550$). On average, participants given an MPC application perceive a higher level of 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 accept the alternative hypothesis. It represented a Cohen's d effect of $d=1.197$ (a 'very large' effect size).

Relative advantage

To recall, the relative advantage hypothesis is:

H4_A¹ : Perceived relative advantage of an MPC-enabled application is greater than perceived relative advantage of a TTP based application.

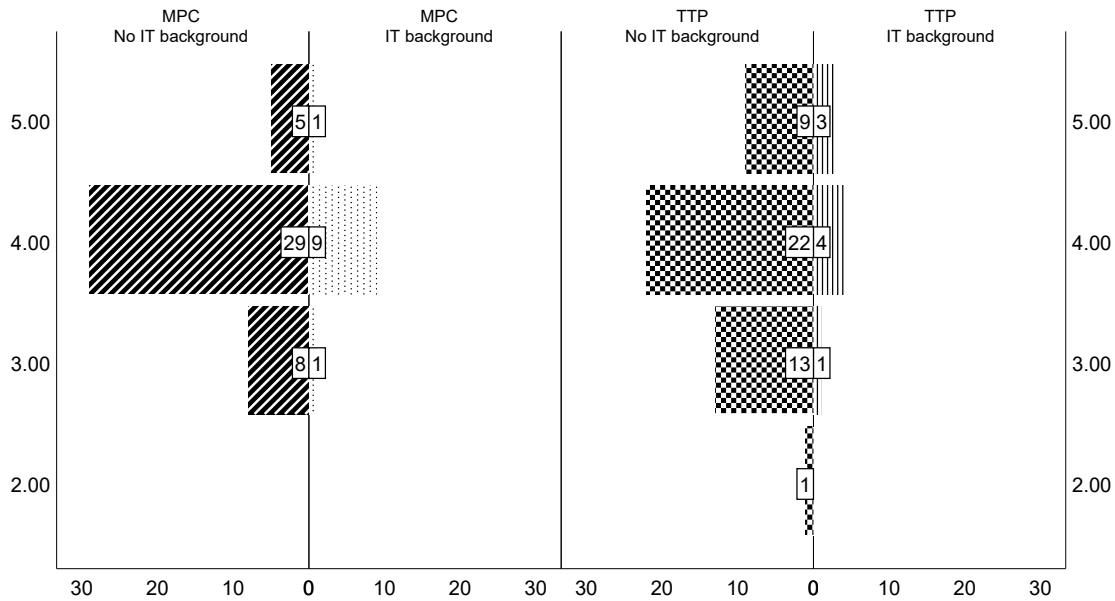
An independent t-test is used. This is done using the SPSS syntax [A.5.21](#). The results of the robust test is:

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 accept the null hypothesis. It represented a Cohen's d effect of $d=.03$ (negligible effect size).

Initially, our data indicate that MPC does not have an effect on 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. 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." Using a t-test, a significant difference was reported. This question concerns the application as a whole; however, whereas the question used for testing the hypothesis is specific to MPC. It is then evaluated whether the pre-test scores of *application-related* question

may be used for the *MPC-related question* the values are compared before drawing any conclusions (see Table ??). From this table, we can already 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.

Although at the cost of a smaller sample size, we further examined whether respondents with a background in IT have different perceptions. SPSS output 6.33 provides a visual overview of this group.



SPSS Output 6.33: Split plot of MPC and TTP participants with and without an IT background.

A t-test was run for MPC and TTP with an IT background despite the small sample size (Total N=19). The result is as follows:

On average, *participants with a background in IT* provided an MPC application (N=11) perceive more relative advantage (M=3.909, SE=.163), than those given a TTP application (N=8) (M=3.875, SE=.227). This difference, .034, bias-corrected and accelerated (BCa) 95% confidence interval (CI) [-0.511, 0.591], was not significant $t(13.55) = .122$, $p = 0.905$ (two-tailed).

Per the above, we have no indications that IT background affects the perception of relative advantage.

6.7. Interaction effect

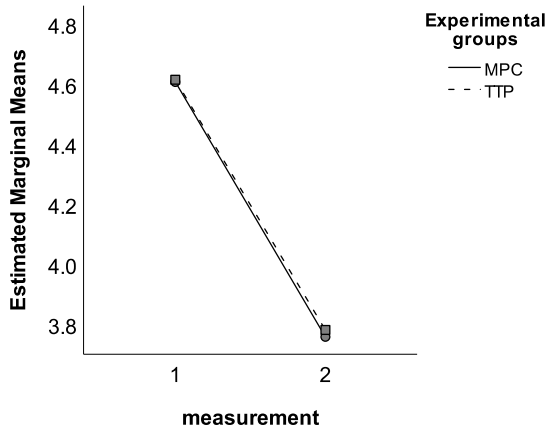
The interaction effect can be measured by $[(O_3 - O_1) - (O_2 - O_4)]$. This comprises a two by two matrix: one between-subject independent factor (experimental groups) with two levels (MPC and TTP), and two within-subject independent variables (pre-test score and post-test score). Hence,

a mixed-design analysis of variance model (Field, 2017, ch. 16) (also called split-plot or two-way repeated-measures ANOVA) is used. The SPSS plots for trustworthiness are shown in SPSS output 6.34 tru 6.41, relative advantage in SPSS output 6.42 tru 6.46, and security in SPSS output 6.47 tru 6.52. These plots allow us to gain some insight in the difference between means (unless noted, all p-values are values from Greenhouse-Geisser correction). Overall, it can be observed 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.

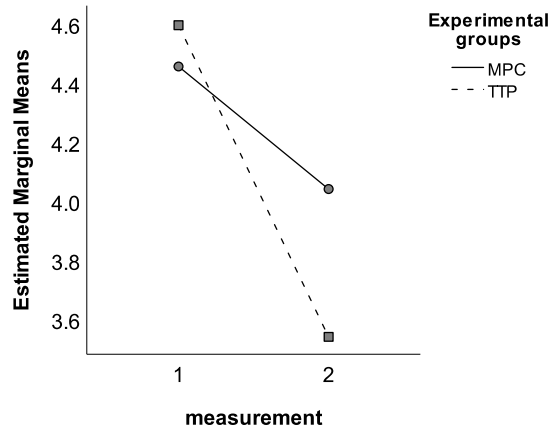
Next, we will discuss the outputs of trustworthiness and security-related variables. First, for trustworthiness, three variables indicated a significant interaction effect. MPC significantly interacted with the degree to which respondents perceived the complete data contribution process, $F(1,105)=8.017$, $p=.006$ (see SPSS output 6.35). MPC also significantly interacted with the degree to which respondents perceived the completeness of the information regarding the protection of submitted data, $F(1,105)=15.315$, $p<.001$ (see SPSS output 6.36). MPC also significantly interacted with the degree to which respondents perceived the transparency in protecting data, $F(1,105)=5.046$, $p=.004$ (see SPSS output 6.41). Second, relative advantage, MPC significantly interacts with perceived advantage over conventional data sharing application, $F(1,105)=9.813$, $p=.002$ (see SPSS output 6.44). MPC significantly interacts with the perceived simplicity of the application provides for secure data-contribution, $F(1,105)=4.541$, $p=.035$. Third and final, security, the difference between MPC and TTP for all of the separate items are not statistically significant.

An interesting finding is the comparison of 6.38 with 6.39. These two outputs, while there is no statistically significant interaction effect, 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 $F(1,105)=8.646$, $p=0.004$.

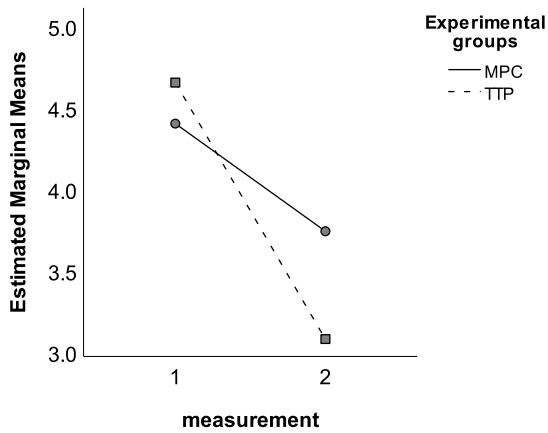
SPSS independent t-test outputs on next page →



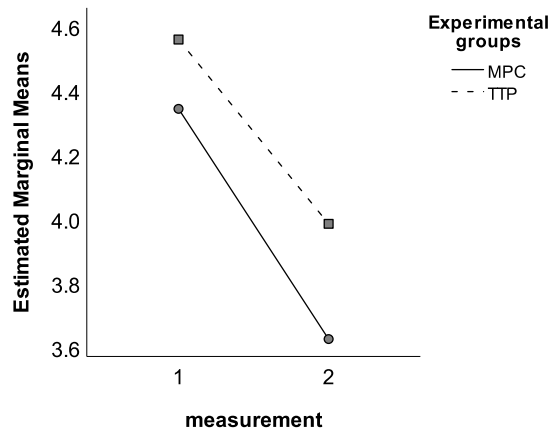
SPSS Output 6.34: The intent of the application is clear to me. $F(1,105)=.007, p=.934$



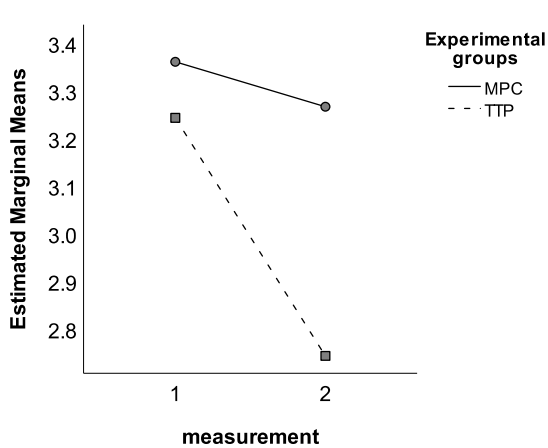
SPSS Output 6.35: The application clearly describes how my data is processed from data submission to output. $F(1,105)=8.017, p=.006$



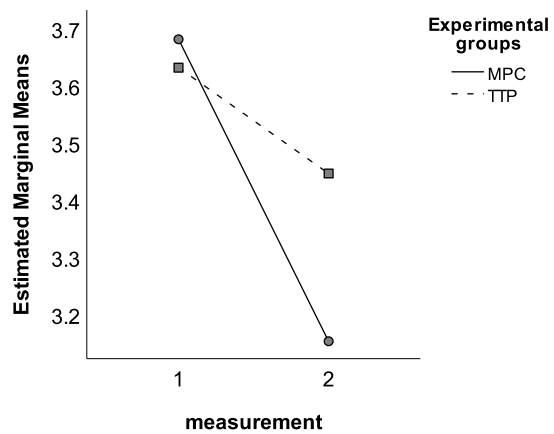
SPSS Output 6.36: The application provides a complete and detailed description of how METHOD is used to protect my data. $F(1,105)=15.315, p<.001$



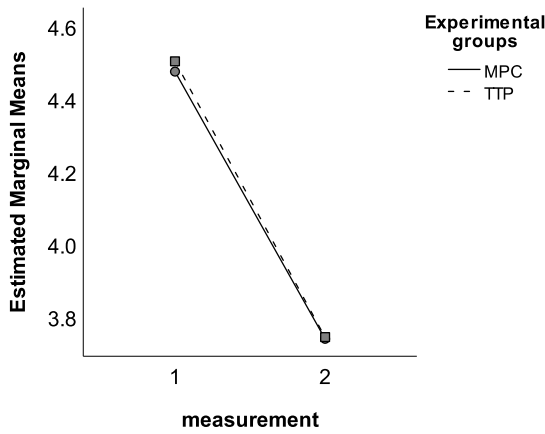
SPSS Output 6.37: Interaction with the application is clear and understandable. $F(1,105)=.531, p=.468$



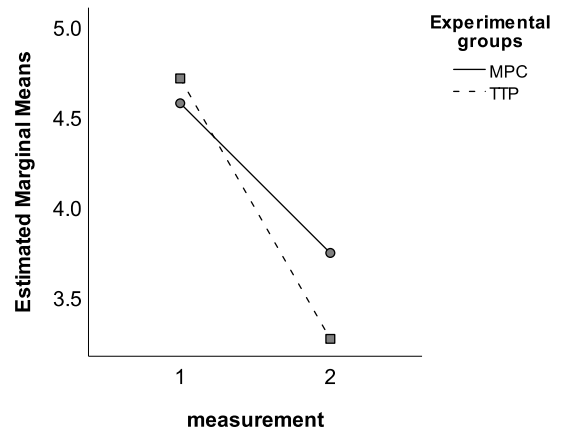
SPSS Output 6.38: The descriptions of the METHOD are complex. $F(1,105)=2.009, p=.159$



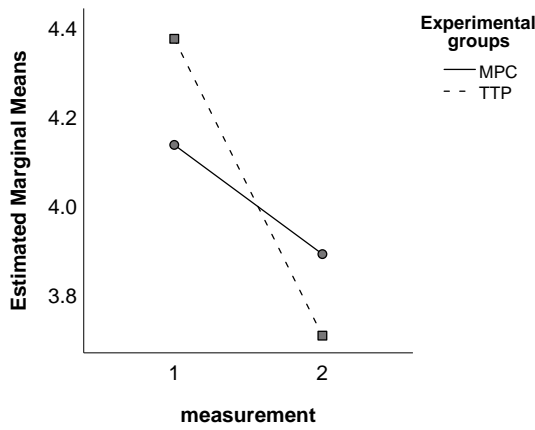
SPSS Output 6.39: Understanding how the data is processed does not require a lot of my mental effort. $F(1,105)=2.000, p=.160$



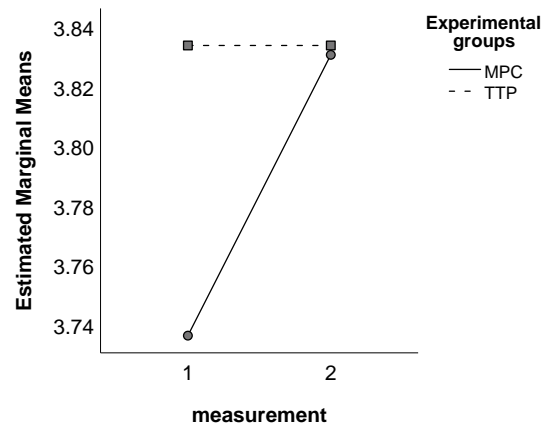
SPSS Output 6.40: Claims made in the application must be clear and accurate. $F(1,105)=0.018$, $p=.893$



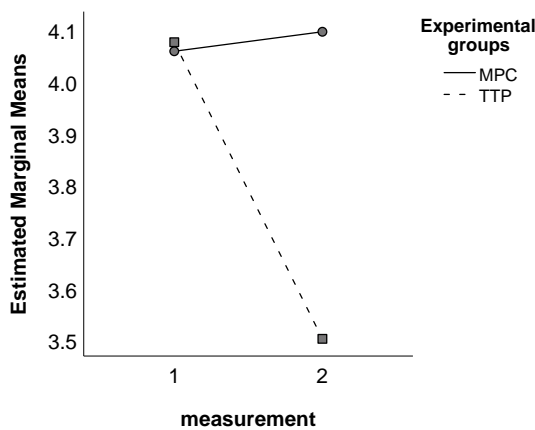
SPSS Output 6.41: The application is open and transparent in how it protects my data. $F(1,105)=8.629$, $p=.004$



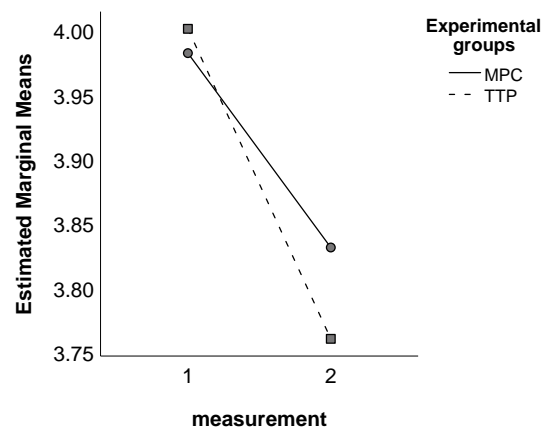
SPSS Output 6.42: The application must provide a simple way to securely contribute data. $F(1,105)=4.541$, $p=.035$



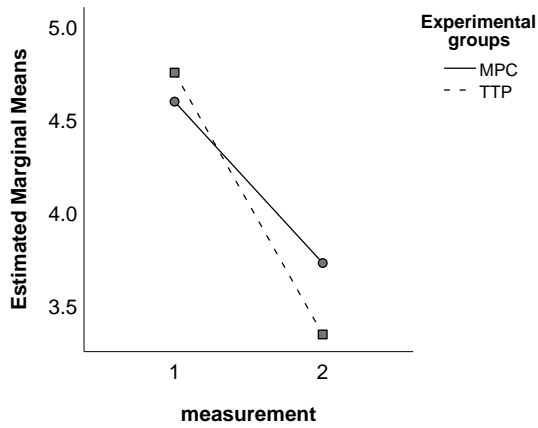
SPSS Output 6.43: The application must not require expertise from multiple organizational departments. $F(1,105)=.126$, $p=.723$



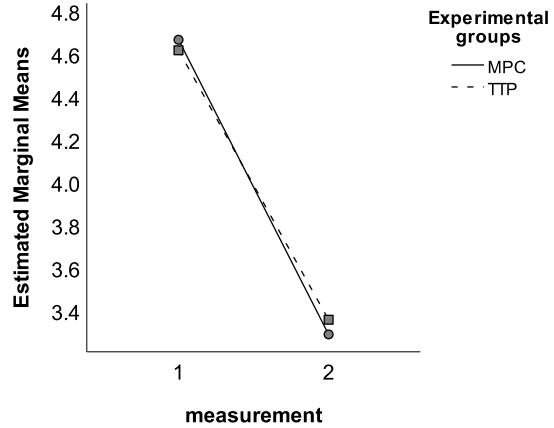
SPSS Output 6.44: The application must provide an advantage over conventional data sharing practices. $F(1,105)=9.813$, $p=.002$



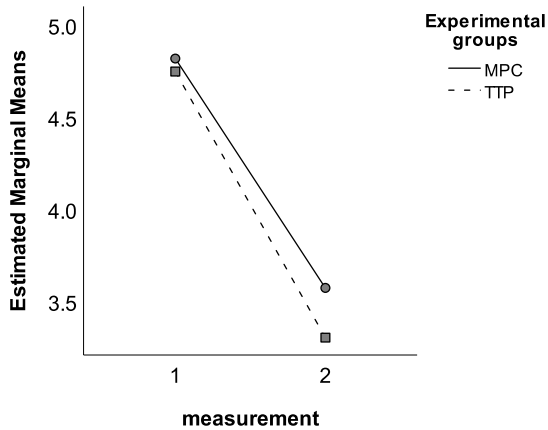
SPSS Output 6.45: When contributing data, no other party should know about my organization's participation. $F(1,105)=.134$, $p=.715$



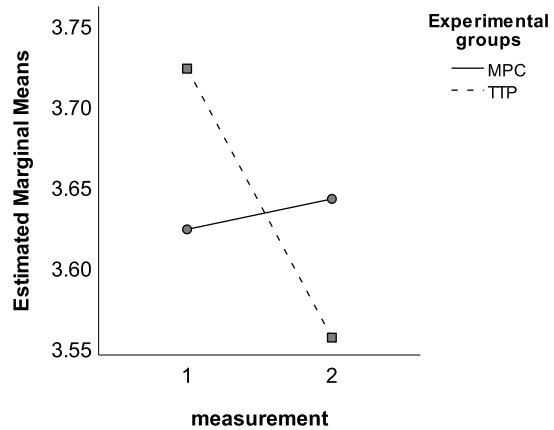
SPSS Output 6.46: Through the method I feel less hesitant to contribute sensitive company data through a web application. $F(1,105)=.X$, $p=.X$



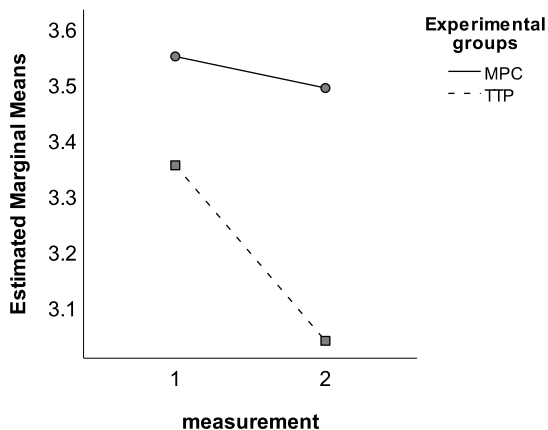
SPSS Output 6.47: It feels safe contributing sensitive company data over the application. $F(1,105)=.253$, $p=.616$



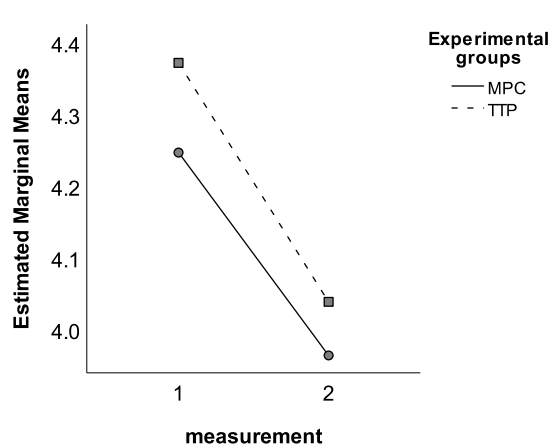
SPSS Output 6.48: The use of METHOD gives me a feeling of security assurance. $F(1,105)=.789$, $p=.376$



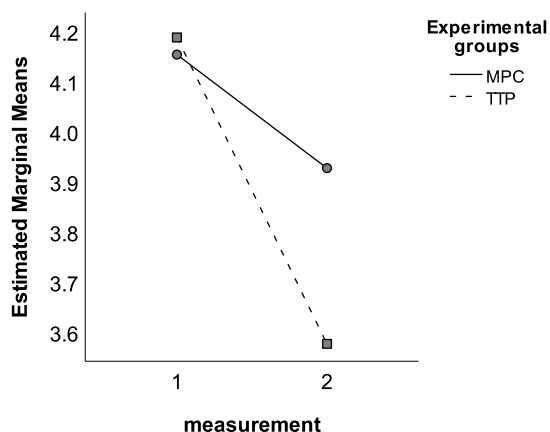
SPSS Output 6.49: Only I am able to view my contributed data. $F(1,105)=.530$, $p=.468$



SPSS Output 6.50: The service provider cannot examine my data beyond my control. $F(1,105)=1.167$, $p=.283$



SPSS Output 6.51: I feel capable of using the application. $F(1,105)=.072$, $p=.789$



SPSS Output 6.52: My data cannot be accessed by other contributors. $F(1,105)=2.233$, $p=.138$

6.8. Qualitative assessment

In this section, the results are further elaborated upon. This qualitative research helps in assessing potential reduction fallacy—since data is collected at an individual level (unit of observation) whilst drawing conclusions at an organizational level (unit of analysis).

At one of the companies (lab participants), during the observation, it was noted that while at an individual level participants differ in their rating, at a group level, through a dialogue, they weigh the perceived gains and burdens and draw a group perception. For instance, one of the managers was risk-averse when faced with protected data—due to 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.

On the other hand, his more-technical colleague criticized the trustworthiness and security of the application. On the other hand, 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, 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.

6.8.1. 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”. With respect to the lab participants, the main concern was related to knowing the organization behind the application. This is important, in particular, due to liability concerns and the ability to evaluate the organization’s credibility. In addition, 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 for-

mal approval. Thereby, trustworthiness perception is based on thorough evaluation.

One way of dealing with this issue—which was mentioned—is backing the application by an organization with a “respected (responsible) reputation”. The example given for the case was a TU Delft logo and cross-link to a forum on the TU Delft website. This forum should describe the activities concerning the MPC applications that are in use. However, in the case of an MPC application backed by a commercial company, then this company felt it needed to be taken aboard the development of the application (as an internal audit). Upon extending this question with divisibility, it was argued that an evaluation of the company is still needed 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.

6.8.2. 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”. With respect to the lab participants, the main concern was related to knowing the organization behind the application. This is important, in particular, due to liability concerns and the ability to evaluate the organization’s credibility. In addition, 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.

One way of dealing with this issue—which was mentioned—is backing the application by an organization with a “respected (responsible) reputation”. The example given for the case was a TU Delft logo and cross-link to a forum on the TU Delft website. This forum should describe the activities concerning the MPC applications that are in use. However, in the case of an MPC application backed by a commercial company, then this company felt it needed to be taken aboard the development of the application (as an internal audit). Upon extending this question with divisibility, it was argued that an evaluation of the company is still needed 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.

6.8.3. 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 still, many departments needed to be involved. In fact, it was mentioned that, initially, the resources needed for participation might be even more than would be the case in comparison to a straight-forward trusted third party. It was discussed, however, that if the company had “levers” to trace claims made by the application and evaluate the credibility of the application and the trustworthiness of the organization, than such an application is perceived to provide a relative advantage over third party data processing (non-MPC) based solutions.

In sum, it was not clear at this point the extent to which MPC provides an advantage over TTP. All parties did agree that the organization behind the application determines—to a great extent—the

way 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—given that 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.

6.8.4. Security

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

The majority that entered a low value for willingness to contribute data were security-related “Information protection is the first priority no matter if the results are positive”. Or, “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.”, Or, “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”, or “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—information which was missing in the application, however.

6.9. Conclusions

The quantitative and qualitative analyses show that MPC contributes to perceptions of willingness to contribute protected data. The results are reported in Table 6.30. It was 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 as a result of MPC. These aspects seem to be perceived as important aspects in terms of willingness to contribute protected data. This is 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, however, not negatively effecting perceived trustworthiness, however. 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. In comparison to trustworthiness and security, a weaker correlation between relative advantage and willingness to contribute is reported.

The qualitative assessment indicates that more information and features are needed in order for

MPC to enhance further the perceived relative advantage. Moreover, the observed participants advised several changes that should be considered with respect to trustworthiness.

Hypothesis	Quantitative Results	Conclusion
H1_A¹ : Willingness to contribute protected data through MPC is greater than willingness to contribute protected data over TTP.	A medium effect size (d=0.460, p=0.020) (two-tailed), is reported.	<input type="checkbox"/> H1₀¹ H1_A¹ <input checked="" type="checkbox"/> We accept the alternative hypothesis.
H2_A¹ : Perceived trustworthiness of an MPC-enabled application is greater than perceived trustworthiness of a TTP based application.	A medium effect size (d=0.408, p=0.043) is reported.	<input type="checkbox"/> H2₀¹ H2_A¹ <input checked="" type="checkbox"/> We accept the alternative hypothesis.
H2_A² : Perceived trustworthiness of a data contribution application is considered an important aspect.	A large correlation (r=0.660, p<0.01) is reported.	<input type="checkbox"/> H2₀² H2_A² <input checked="" type="checkbox"/> We accept the alternative hypothesis.
H3_A¹ : Perceived security of an MPC-enabled application is greater than perceived security of a TTP based application.	A very large effect size (d=1.197, p<0.001) is reported.	<input type="checkbox"/> H3₀¹ H3_A¹ <input checked="" type="checkbox"/> We accept the alternative hypothesis.
H3_A² : Perceived security of a data contribution application is considered an important aspect.	A large correlation (r=0.657, p<0.01) is reported.	<input type="checkbox"/> H3₀² H3_A² <input checked="" type="checkbox"/> We accept the alternative hypothesis.
H4_A¹ : Perceived relative advantage of an MPC-enabled application is greater than perceived relative advantage of a TTP based application.	A negligible effect size (d=0.03, p=.882) was initially reported. However, when taking into account pre-test scores, MPC does affect perceived relative advantage in comparison to TTP (F(1,105)=8.248, p=.005).	<input type="checkbox"/> H4₀¹ H4_A¹ <input checked="" type="checkbox"/> The null hypothesis should be accepted when considering post-test scores only. Upon using the results of a similar question, it is observed that MPC respondents had a lower anchor point in comparison to TTP participants. After manipulating the data, MPC does seem to enhance perceived relative advantage. We accept the alternative hypotheses.
H4_A² : Perceived relative advantage of a data contribution application is considered an important aspect.	A weak correlation (r=0.318, p<0.01) is reported. This weak correlation does not reflect an important item of consideration.	<input checked="" type="checkbox"/> H4₀² H4_A² <input type="checkbox"/> We accept the null hypothesis, however this depends on the background of the decision-maker.

Table 6.30: Summary of accepted hypotheses.

IV

Upshot

7

Discussions & Conclusion

In general, the findings suggest that organizational willingness to contribute protected data through a web application is mainly affected by perceived trustworthiness and perceived security. MPC positively enhances not only perceptions on both dimensions, but also perceived relative advantage, albeit to a lesser extent. These conclusions have been drawn by answering four SQs:

What is MPC, and what are the key aspects concerning the contribution of protected data through MPC?

To answer this question, a literature review was performed. Through SQ1, it becomes clear that a common language is needed for discussing MPC since it seems to be new in organizations. Two mediums were hence established: a diagram was created that explains the workings of MPC, and eight characteristics were formulated that describe the landscape in which MPC is of interest. These characteristics were then used (and indirectly tested) in informal interviews. Through these characteristics, the business potential of MPC can be made clear. Moreover, the informal interviews indicate that these characteristics aid in formulating new business opportunities, and they enabled the establishment of a practical approach for presenting MPC that also enhanced our intuition of organizational willingness to contribute protected data.

In this study, MPC is considered an enabler for secure data contribution. Since our aim is to understand its effect on organizational willingness to contribute protected data, we focus on MPC's application side and scope out all non-relevant and potentially confounding aspects. The conclusion is that a clear distinction must be made between the input and output components of MPC. This is because, fundamentally, security is likely not the primary, but the secondary goal of users, since they pursue value from the output (either direct or indirect). As a result, the key aspects that must be considered in terms of willingness to contribute are perceptions related to features that should reside in the application. These features should reflect organizational requirements, which allows them to assess the application's security mechanisms properly. Moreover, these features must make clear the presence of MPC in the data contribution application.

Along what dimensions would organizations evaluate an MPC application for the contribution of protected data, regardless of the value provided by the output of the application?

For this question, a thorough literature review was performed, and a conceptual framework was developed that used an IOS as its departure. IOS literature allowed us to understand the prob-

lems arising from software used for the movement of information across organizational boundaries. Then, innovation characteristics research was utilized to derive MPC-specific attributes that are considered by organizations. In this process, generic characteristics were sought, particularly from IS literature, and contextualized and framed in terms of MPC. Then, to examine only the aspects related to the given innovation phase of MPC, the method willingness to contribute was viewed from an innovation development process perspective.

Here, we found that willingness to contribute is the first concern addressed by organizations when presented with MPC as an emerging technology. However, we also found that compatibility, which was initially considered to be an important attribute of MPC, could be removed from the scope. The remaining attributes were integrated into a conceptual framework comprising three dimensions: trustworthiness, relative advantage, and security. These are second-order constructs. First, the trustworthiness dimension comprises the observability, complexity, integrity, and divisibility of the application. Integrity and divisibility have been removed from the scope due to their inherent complexity. Second, relative advantage comprises simplification of the knowledge-sharing process and cost advantage. Cost advantage was removed because it does not fit well with the research methodology since it requires some direct comparison with conventional data contribution solutions. Third, security comprises perceived control and perceived risk.

How is MPC perceived by organizations in terms of the previously defined dimensions?

The conceptual framework suggests that for organizations to contribute data through a web application, a positive perception of trustworthiness, a relative advantage, and security must be present. Literature suggests that 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.

Meanwhile, there is a lack of literature regarding the role of perceived advantage in the context of PETs in organizational settings. As a result, using [Kanger and Pruulmann-Vengerfeldt \(2015\)](#) argument of organizational and technological fit, it was conjectured that perceived relative advantage is important in the organizational process of considering willingness. This is similar to the perceived usefulness of PETs [Harborth, Pape, and Rannenberg \(2020\)](#), albeit at an individual level. Through abstract reasoning, it is argued that the application should provide relative advantage when considering willingness to contribute protected data.

However, the results revealed that relative advantage is not as important as initially proposed in this context. Aligning our results with [Harborth et al.](#), who studied usage of PETs at an individual level, the weight of relative advantage could increase later in pre-adoption phases. This is assumed because organizations stated that TTP does provide a viable solution in protecting confidentiality. However, the use of TTP as a solution is backed business cases and thorough assessments. This suggests that security is a secondary concern, which is consistent with conventional data-sharing literature. The primary concern remains the purpose for data sharing. Despite this fuzzy view of priority, when viewing MPC as a solution to foster the contribution of data beyond data sharing initiated as a result of cooperation and collaboration endeavors, 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 fully understand the data contribution process.

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 the application is not perceived as trustworthy, AND the organization behind the application is credible and traceable, AND the data contributor is able to 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 the development of the application or is not able to perform an internal audit.

Regarding the credibility of a organization, in this thesis assumptions have been made to address the issue of 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 credibility of the organization behind the application plays a vital role. We therefore emphasize that researchers attempting to understand the effect of MPC on organizational behavior should follow a similar approach. Nevertheless, credibility could further enhance the variance explained in 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).

What are the implications of the above findings in terms of the development of MPC?

MPC has been shown to have a significant effect on trustworthiness, while no claims or statements have been made on the service provider. We believe this is the result of a feeling of independence induced by MPC. When contributing data via a TTP, participants must place their trust in the entity and not in the contributors. With respect to IOS, this study suggests that MPC lowers interdependency. In terms of transaction cost theory (Lei & W., 2005), MPC reduces the costs of managing the data-sharing parties (contributors). However, the importance of perceived trustworthiness of the application increases.

The effect of MPC on trustworthiness could thus be the result of the feeling evoked by a platform that handles data "independently from the application owner or service provider." Hence, without MPC, there is a need to know more about the TTP, whilst with MPC, less emphasis is placed on the service provider. From an organizational perspective, however, companies have stressed the importance of, among other factors, knowing the details behind the application and the architecture of the MPC application. Such information is required to ascertain that claims are accurate.

The treatment used for the application was a mock-up, designed based on the contribution of scholars. Our findings can be linked to the look and feel of this mock-up, developed specifically for this study. The overall design was based on the that of a successfully deployed and currently used MPC application (Bestavros, Lapets, Jansen, et al., 2017; Bestavros, Lapets, & Varia, 2017). It was also based on prior studies that have examined how the presentation of information is perceived (Faujdar et al., 2020). These scholars suggest features that should be embedded in an MPC application and methodologies that can be used to elicit a trustworthy and usable MPC application. However, while Bestavros, Lapets, Jansen, et al. (2017) argue in favor of making the underlying code open source, our findings suggest that this method must be traceable; that is, organizations must be able to assert that the code is in fact the actual code used for the application. Furthermore, including a visualization (Faujdar et al., 2020) of the workings of MPC in the text was positively re-

ceived.

Based on the information acquired from companies, a link between trustworthiness and relative advantage is also suggested; However, this link was not included in our framework. An intuitive explanation is that TTPs have a reputation and are hired for their “guarantee” of confidentiality, and they are assessed in terms of trustworthiness—the extent to which the trusting party can lay confidence in the trustee regarding the trust they oversee. They provide an advantage over other trustees based on their capabilities and capacities concerning security and trustworthiness, or, more concisely, their integrity and credibility. This brings us back to the previously discussed credibility of the organization behind the application. However, as presented, the mock-up is not mature for examining this link. As our results suggest, relative advantage does not seem to be as important as perceived trustworthiness and perceived security with respect to willingness to contribute. Therefore, it is suggested that the recommendations laid out by the organizations should be embedded to further enhance perceptions.

7.1. Theoretical implications

Given the conceptual model and scoping of the research, we can agree that MPC is a broad research domain. This study offers principal implications and valuable contributions to the literature. First, a map is provided that articulates the practical intricacies of MPC. In addition, different architectures have been synthesized into a single diagram, which illustrates the building blocks of MPC well. We have consequently improved the contributions provided by (Bestavros, Lapets, Jansen, et al., 2017; Bestavros, Lapets, & Varia, 2017; Bogdanov et al., 2012; Bogetoft et al., 2009; Bogetoft & Otto, 2011). Moreover, MPC is framed in terms of characteristics, making it easier derive new potential business cases. This work thus provides a foundation and framework for future research.

Second, most research on MPC or PETs in this regard take an individual perspective; see, for example, (Dhagarra, Goswami, & Kumar, 2020; Gan, Chua, & Wong, 2019; Harborth et al., 2020). Although TAM provides a satisfactory framework at an individual level, it is not considered suitable in this thesis due to its limitations (as explained in Appendix A.1. In this study, a framework was developed—the first, to our knowledge—to assess willingness at an organizational level. In our quest, characteristics research was adopted and extended with empirical evidence in the context of an education and niche strategy. In doing so, we have improved the explanatory power of innovation characteristics research within the context of PETs. More specifically, through this methodology, considering the suggestions by Wolfe (1994) allowed us to carefully assess the technology under research. For instance, rather than simply considering trust, which Quinn et al. (2009) referred to as single-faceted, a multifaceted approach was followed: trustworthiness was contextualized in terms of MPC, and the underlying aspects were carefully arranged. Our study further contributes by having empirically tested the conceptual framework.

The concept of IOS is also extended in this regard. The findings indicate that the data-sharing complexities shift towards attaining trustworthy and secure applications when adopting PETs. That is, the importance of trust within a network becomes less relevant.

Third, the relative advantage of PETs is an under-researched concept. This study is one of the few to examine the role of relative advantage in terms of willingness to contribute and the effect

of MPC (or PET) on data contribution. As previously explained, scholars usually approach these subjects from a usefulness perspective at an individual level (i.e. decisions made for own personal needs). Although a strong correlation was not found, our results indicate that relative advantage seems to have an effect on an organization's willingness to contribute data.

An implication of the proposed framework is that an implicit requirement is built into the framework. This concerns relative advantage in particular. The requirement is that the unit of observation must have experience with data sharing to acquire the best results. For instance, it is difficult for one to perceive the relative advantage of MPC (i.e. a simple solution to secure contributions) if they do not have any experience with data sharing—since a reference point is then lacking. Nonetheless, our work provides a valuable stepping stone towards a more thorough examination of a phenomenon, which can help in defining new value propositions and enhancing perceptions.

Finally, this study makes a positive contribution to the Safe-DEED project. The use case scenario, mock-up, and empirical findings provide a valuable reference for the project, contributing to WP6 in particular. WP6 encompasses demonstrator scenarios for the review of the project, and our work provides developers with a means to grasp aspects that should be considered in the development of new applications and business models. This study is well aligned with the objective of WP6 in the sense that use cases are formulated, MPC attributes are derived and empirically tested, and both quantitative and qualitative explanation is provided on willingness to contribute protected data through MPC-enabled applications.

7.2. Practical implications

Following our literature research, a perceptually based approach was followed, and we found that people seem to rely more on their perceptions than on “real situations” or “facts.” The perceptual approach was found to be suitable given the newness of MPC and the lack of awareness among organizations. That is, perceptions are more important in the initial phases of the pre-adoption process, where a lack of awareness is likely to exist. The collected data confirmed that awareness of MPC in business settings is lacking. To address this, a 3-minute video introduction to MPC was made to educate respondents. The logical explanation for this decision is that one cannot be asked for their opinion about a technology that is completely unknown to them. This approach is based on an “educate niche strategy” (aimed at increasing customer knowledge) [Ortt et al. \(2013\)](#)), which has provided a pragmatic method to approach the problem. This strategy is consistent with [Kanger and Pruulmann-Vengerfeldt \(2015\)](#) argumentation of “sufficient information”.

The video introduction to MPC was generic to avoid bias. Nevertheless, in a real setting, a similar approach should be followed, and such a video should be included; however, it should be made more specific and incorporate further detail (e.g. the organizations where the computation servers reside). Prospects can then clarify the perceived risks, which will increase in importance in later phases of the pre-adoption process.

The value of MPC is preceded by different issues that warrant careful consideration. Since MPC is an enabler, perceptions are likely to be a matter of case-by-case evaluation. Nevertheless, the application must be built using a self-contained application philosophy—meaning it has all the information that allows one to carefully evaluate and assess the technology. This contributes

greatly to the way in which managers perceive this technology. This is important particularly when the organization behind the application is a commercial entity (a profit seeker or profit maximizer).

It is clear that MPC provides value, as demonstrated through several potential use cases for MPC in SCs: collaborative distribution, freight bidding, demand and production coordination, group purchasing, inventory sharing, performance benchmarking, and SC network risk analysis. However, MPC must be communicated in a proper way. By “looking around us,” we learned that new technologies are communicated in different ways. For instance, with regard to blockchain, a large number of sources (videos in particular) explain how blockchain works. From oversimplified to complex, in-depth material, any individual interested in blockchain can find an appropriate source. This was not the case with MPC. The implication is not that there are insufficient resources; however, since MPC already lacks in popularity, in a business setting easily digestible and complete information is lacking. Moreover, the videos *that do* explain MPC were found to be either oversimplified or lengthy (e.g. online classes and conference speakers) and not always clear on their contribution. As a result, it does not invite businesses to further look into motives to adopt MPC. Returning to the block chain comparison, blockchain is widely known for its trustless properties and for providing full transparency of transactions. When searching for MPC, however, the majority of content discusses cryptographic primitives but does not clearly articulate how it can be translated into value.

During the lab experiment, we learned that MPC is perceived to carry potential value from a managerial perspective. A video was found to be a more effective means of communicating the technology than a presentation. The video was said to be more compelling; it was used as an introduction and allowed for more effortless and meaningful discussions to take place. At the beginning of the study, PowerPoint presentations were used. It took more time to introduce the MPC. This was found particularly disturbing by the author since gold-collar workers, typically, have a limited time available. In this study, we found that the short video introduction to MPC greatly contributed to educating people, and in a discussion with the lab participants, several items were noted that should be added to “give it even more crisp.” The main item is the inclusion of an explanation of the randomization part, which would make the introduction to MPC complete.

To bridge the aforementioned gap, and given the fundamental problem addressed in this section, the video introduction to MPC was published on YouTube in our quest to contribute to the research community.

The elements included in the application (i.e. the video introduction to MPC, reference to the source code, reference to the computation function, and the Excel input file) were positively received. The organizations expressed their appreciation for the video and the reasoning behind the features that were less apparent, for instance the reasoning behind the Excel template file (i.e. offline data collection and not storing raw data). This induced a positive feeling regarding the decisions taken by the application owners. While some items made sense, others highlighted the implications of safe contribution. We extend the usability requirements addressed by [Bestavros, Lapets, Jansen, et al. \(2017\)](#) and information communication methods by [Faujdar et al. \(2020\)](#) with items from this study. For completeness, the list of items are summarized in Table 7.1. It should be noted that some of the items listed are based only on feedback received.

One item that a respondent mentioned as a remark is that the submissions ID, supposedly

provided via email and used to allow data submission, requires review. In his opinion, since this data was submitted along with the dataset, this made matching (using, for example, timestamps) of the input data with the data owner possible, hence increasing risks. Furthermore, the explanation of the utilized hash functionality was clear to the respondent; however, this case illustrates the way in which individuals shape their perceptions. In the mock-up, the use of hashing was described, but the full reasoning behind it was lacking.

The mock-up used for this experiment is effective to the extent that it allows companies to base their decisions on factual information—in particular, what is being claimed, whether the information is complete, and how it can be assured that the claims are real. The latter is referred to as the traceability of the information provided. While our analysis demonstrates that MPC positively contributes to perceptions of data contribution, we stress that developers must carefully assess traceability features. At the same time, to foster responsible development we urge organizations to carefully assess applications based on the above—to avoid providing data to malicious parties.

7.3. Limitations

This study has several limitations, which are discussed in this section. These may also be interpreted as a call for researchers to further address.

7.3.1. Methodology

The data landscape is evolving at a fast pace. For instance, the requirements imposed by the GDPR (data-protection regulation) have changed the possibilities of data acquisition and usage. Despite our results being robust to CMV, the cross-sectional method employed could pose a limitation since it is perceptually based. This is because perceptions today could change in the future. Nevertheless, our results are backed by findings from a lab experiment in two different organizational settings. The two organizations have moderate to highly stringent data policies, whereby both are mature in terms of adhering to GDPR regulation. Therefore, the suggestions laid out in this thesis provide a sound basis for MPC application development and a framework for assessing willingness to contribute protected data through a web application. Future research could further extend this study by integrating more attributes (e.g. divisibility, integrity, compatibility) and using a longitudinal approach.

7.3.2. Protocol

In this study, no mention was made of the protocol employed (e.g. semi-honest). Hence, we are unable to make any claims on the extent to which different adversary models are perceived or have an effect on our findings. Nevertheless, it is clear that although this information was omitted, MPC is perceived as a means to enhance trustworthiness and security. We believe that later in the innovation appraisal process, this information becomes more important. However, the website on which our mock-up is based does not include any supporting text, although the parties behind the application indicated that contributors have been part of or followed the development of the application. Thus, it is possible that specific information regarding the technicalities has been provided and communicated outside the application. Acknowledging that this is not always possible, extending our study with this information could provide valuable contributions to academia.

7.3.3. Prolific

The majority of responses were collected through Prolific. Scholars have demonstrated that Prolific is a reliable source [Palan and Schitter \(2018\)](#). 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 evaluation of the lab experiment, we observed that decisions may take place in groups, such as project teams. That is, groups of individuals together shape a unified perception. In fact, we believe that the presence of the author during the experiment might have even had an effect on (i.e. biased) perceived trustworthiness. To recall, the trustworthiness scores for the lab participants were significantly higher than the Prolific dataset (which is 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. We stress, however, that questions should be properly framed in the interest of the organization they represent. Nonetheless, we for researchers to perform case studies to enrich our general understanding of MPC adoption in organizational settings.

7.3.4. Framework

The main objective of this study was to determine the effect of MPC on data sharing towards data contribution. In establishing a framework, only items that were found to relevant in the awareness and matching phase were included. Our scoped framework is hence limited to the awareness and matching phase, but can be extended if desired. However, proper scoping is necessary to avoid pitfalls associated with having too many variables or acceptance of a study with a long duration.

While the cost advantage was removed from the scope, it must be noted that cost advantage is not always a requirement. That is, cost advantage suggests the contribution of data for beneficial purpose. The use of MPC extends beyond cost advantages, and advantages may also be intangible. For instance, the case of the Boston Women’s Workforce Council demonstrates that there may be other reasons to use MPC than purely a cost advantage or even the value of output to the organization in this regard. Acts based on corporate responsibility may go beyond direct or tangible gains. In addition, to measure cost advantage, one needs to be clear about not only the actual costs of the MPC application under study but also the costs incurred when deployed through a third party.

This study presented a use case driven by benefits. In terms of the abovementioned reasoning, the research results are not limited to clear benefit-driven (i.e. cost or profit) applications. First, this is because we measured willingness to contribute data based on the assumption that “the output provides value to your organization” through a generic question. Value herein does not implicitly or explicitly suggest the cost of profit. Thus, the results of this study can be generalized beyond benefit-driven applications, under the assumption that the output of the application provides value to the organization.

All of the concepts included in the framework are perception-based and therefore suffer from the fundamentally philosophical problem of perception: a sense perception that may or may not

be based on experiences. Our framework thus suffers from the same problem, which makes the framework susceptible to the dynamics of the individual's environment in which it is discussed. Therefore, this framework requires assumptions on a fundamental issue at play that stems from incentives, which can shape perceptions on their own regardless of the MPC application—inducing fear beyond the MPC application. In our framework, we took a subtle approach to dealing with incentives (use cases backed by a persona). Moreover, we have not viewed incentives as a dimension (at the same level as trustworthiness, security, and relative advantage). Rather, incentives (in our case incentives not to collude) were viewed as systematic phenomena.

Researchers must therefore clearly articulate the incentives behind the application. During our discussions with companies, the problem of collusion (both IP and CP) was not perceived as an issue for the given case. Both companies were positive about the computation servers residing in different environments. Nevertheless, a framework that can measure incentives, provides an even better understanding of the invisible hand behind perceptions.

7.3.5. Designed instrument

The mock-up was designed in accordance with 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 development of the application involved a lengthy discussion with many parties. As a result, these parties are more likely to be aware of the back-end prior to giving consent on their participation. To address this issue, more information was included than the reference application—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.

7.4. Further recommendations for future research

During the study, several important aspects were identified that were either absent in current literature or under researched. These aspects are described in this section:

Relative advantage. We propose that studies should measure organizational perception based on a confrontation of both a TTP and an MPC solution. A better understanding of relative advantage is likely to contribute to the development of MPC applications that clarify why MPC is the solution for the perceived risks associated with contributing data for an aggregate analysis. To provide a valuable reference point that is missing in current literature, such research should also include costs. That is, it should answer the question of how MPC would compare in total cost to other solutions. The insights would also provide a valuable instrument to determine cut-off points and a reference for the development of business cases—both small and large in this regard.

Divisibility of the application. This concerns many concepts, including but not limited to the auditability of the code, along with traceability, verifiability, testability, and trialability. These items merit their own study. However, the way in which these items should be conceptualized for MPC has not yet been researched. A study on this matter would provide a valuable contribution to the responsible development of under-the-hood technologies such as MPC. As previously mentioned, we

emphasize the importance of providing levers for organizations to have a clear view of the measures behind the application and assurance that they are the actual measures. A study that examines whether the presence of source code increases perceived trust is also suggested—comparable to [Arcand, Nantel, Arles-Dufour, and Vincent \(2007\)](#), who studied the effect of privacy statements on perceived trust.

Input, output and business case. In defining the scope of this research, we found that research is lacking on risk evaluation concerned with the output of the application (information leakage), and the output with respect to the input—more concisely, an MPC business model framework. In this study, several potential business opportunities have been described. A business case canvas conceptualized towards MPC would provide a valuable framework for assessing business cases. Such a framework can clearly indicate to entrepreneurs whether MPC provides a viable business case for the problem at hand.

Incentives behind the application. Incentives constitute another under-researched area. Although several scholars have mentioned the term, there is no framework that allows one to effectively assess the adversary model in comparison to the underlying risks within different contexts. It is clear that such a framework would offer great value in assessing the perceived risks and ways in which to cope with them. Therefore, we call for researchers to establish an integrative framework to determine suitable adversary models. This helps application developers in designing and embedding incentive systems to deter undesired behavior.

7.5. Conclusions

The RQ posed a difficult challenge, primarily due to the lack of research concerned with the application side of MPC. Drawing from innovation characteristics research and the IOS concept, we developed a conceptual framework to empirically investigate organizational willingness to contribute data through a web application. This framework allowed us to examine the extent to which MPC affects organizational willingness to contribute protected data. The conceptual framework was tested amongst respondents who met the proxy requirements for decision-makers. Our findings suggest that perceived trustworthiness and perceived security are the main aspects that explain organizations' willingness to contribute protected data. Now, only the main RQ remains: Now only the main research question remains:

To what extent does MPC affect organizational perception of the [contribution](#) of protected data?

MPC enhances organizational perceptions of data contribution, and it is thus found to significantly increase 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. That is, both are considered as the locus of willingness to contribute protected data through a web-based application. From our qualitative assessment, it is assumed that the positive contribution of MPC herein is because 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 the extent to which an organization is able to assert the trustworthiness of the application and the security measure used by the application. MPC also affects perceived relative advantage: a weak to medium correlation between perceived relative advantage and willingness to contribute protected data is reported, suggesting that relative importance is not perceived to be as important as perceived trustworthiness and perceived security with respect to willingness to contribute protected data. Nevertheless, it was also found that relative advantage becomes more apparent for MPC-based applications in combination with users with an IT background. While perceived security might seem to enhance perceived relative advantage, no evidence can be provided to support this hypothesis. Despite this finding, relative advantage is assumed to become more important later in the innovation appraisal process.

Finally, as a closing remark, this study began by viewing MPC as an enabler for secure data *contribution*, and while we (and scholars) argue that organizations do not share data, the organizations that were interviewed do still consider it data sharing, or, at the least, “releasing” data outside organizational boundaries. This position is based on the fact that even though an organization’s data is split in shares and encrypted, by definition, and regardless of how the data is sliced, it still passes the organization’s boundaries. Despite this unyielding view of “data contribution,” this term is preferred over “data sharing” to emphasize the way in which MPC changes how one should view their commitment in the knowledge-sharing process. It is emphasized that the organizations addressed the need for features that enable them to assess the credibility of the organization behind the application. These features should preferably be embedded into the application in a form that is traceable to the organization. Herein, MPC service providers should provide these organizations with levers that allow them to be certain about the claims being made.

7.6. Relevance with MoT programme

The research topic, RQ, research approach, and research methodology are aligned with the TU Delft Management of Technology thesis criteria. This thesis reports on a scientific study in a technological context. It demonstrates an understanding of technology as a corporate resource and has social and economic relevance, as discussed in Chapter 1. Therefore, it connects with several courses of the MoT curriculum.

This study considers methods to integrate (ethical) design processes into emerging technologies (MOT1412 Technology Dynamics), and it considers an organization’s innovation behavior herein (MOT1524 Leadership and Technology Management). It also considers organizational decision-making with respect to innovation processes (MOT1451 Inter- and Intra-organizational Decision-making). Furthermore, the study takes into account the external economic and societal environment in which MPC will be implemented (MOT2421, Emerging and Breakthrough Technologies), as well as organizational approaches supporting different types of innovations (MOT1435 Technology, Strategy, and Entrepreneurship), and Finally, methodologies for conducting research (MOT2312 Research Methods).

Aspect	Reasoning	Consideration
Data template file	This file allows for offline data collection and does not store raw data (Bestavros, Lapets, Jansen, et al., 2017).	Ensure that the data template file is foolproof and that a sufficient explanation is provided to ensure input data that meets the quality requirements.
Introduction to MPC video	Such a video makes it easier for prospects to understand the technology behind the application.	Supplement the video with information specific to the MPC application for readers who are interested.
Analyzer interface	This interface explains how one protects the interest of the data owner (Bestavros, Lapets, Jansen, et al., 2017).	Explain what the threshold levels are.
(Animated) illustrations	Visualizations enhance perceptions (Faujdar et al., 2020). Use of animated illustrations can further enhance perceptions (based on feedback received during development of the mock-up).	Use illustrations to enhance perception. Animated illustrations can be utilized for more complex descriptions.
Source reference	The source reference includes references to sources to clarify the functioning of the protocol underlying the application.	Ensure that sources are traceable (see section on traceability). Organizations should pay careful attention to closed-source MPC applications Bestavros, Lapets, and Varia (2017).
Idempotent re-submission	This enables users to rectify errors (or corrupted data) discovered after input is submitted—with the aim of ensuring correct input (Bestavros, Lapets, Jansen, et al., 2017).	Provide an explanation of how this is achieved.
Data verification	This helps with the review of the input data to prevent erroneous data and to prevent parties from destroying the results.	Include a description and reasons that deter the falsification of data (Bestavros, Lapets, Jansen, et al., 2017).
Output example	Depending on how a service provider promotes its application, output examples clarify what is generated from the input	When persuading companies to contribute data, provide a complete report of the analytics (as a preview).
Platform infrastructure	The platform infrastructure determines to a great extent whether participation will take place.	Provide information regarding, among other things, the location the computation servers, the companies behind the computation servers, and who has access to these servers.
Terms and agreements	It was suggested that terms and agreements were missing.	Consider including terms and agreements as well as disclaimers (Faujdar et al., 2020).
Regulations and analogies	A question was raised regarding whether MPC can be used as a means to deal with requirements (GDPR).	Consider including descriptions and references to respective regulatory requirements that are met by the application. This could serve as an alternative or addition to descriptions of adversary models.
Cognitive overload	Organizations suggested that additional information can be included in the application; however, this would be at the cost of information overload.	Use a synoptic panel that includes all sources (introduction video, source code, computation functions, input file)—for example as hyperlinked buttons—allowing for a clean presentation of the application features (less text).

Table 7.1: Items for considerations for MPC application developers and organizations

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. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0377221719307210> 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. Retrieved from <http://www.sciencedirect.com/science/article/pii/B978012381418000012> doi: <https://doi.org/10.1016/B978-0-12-381418-0.00001-2>
- Adom, D., Hussein, E., & Adu-Agyem, J. (2018, 01). Theoretical and conceptual framework: Mandatory ingredients of a quality research. *International Journal of Scientific Research*, 7, 438-441.
- Afuah, A. (2003). *Innovation management: Strategies, implementation, and profits*. Retrieved from <https://tudelft.on.worldcat.org/oclc/824603665>
- Ali, M., Kurnia, S., & Johnston, R. B. (2008, Jan). A dyadic model of interorganizational systems (ios) adoption maturity. In *Proceedings of the 41st annual hawaii international conference on system sciences (hicc 2008)* (p. 9-9). doi: 10.1109/HICSS.2008.18
- Arcand, M., Nantel, J., Arles-Dufour, M., & Vincent, A. (2007). The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust. *Online Inf. Rev.*, 31, 661-681.
- 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
- 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.
- Baker, J. (2012). The technology–organization–environment framework. In Y. K. Dwivedi, M. R. Wade, & S. L. Schneberger (Eds.), *Information systems theory: Explaining and predicting our digital society, vol. 1* (pp. 231–245). New York, NY: Springer New York. Retrieved from https://doi.org/10.1007/978-1-4419-6108-2_12 doi: 10.1007/978-1-4419-6108-2_12
- Benlian, A., & Hess, T. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of it executives. *Decision Support Systems*, 52(1), 232 - 246. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0167923611001278> doi: <https://doi.org/10.1016/j.dss.2011.07.007>
- Bestavros, A., Lapets, A., Jansen, F., Varia, M., Volgushev, N., & Schwarzkopf, M. (2017). Design and deployment of usable, scalable mpc..
- Bestavros, A., Lapets, A., & Varia, M. (2017, January). User-centric distributed solutions for privacy-preserving analytics. *Commun. ACM*, 60(2), 37–39. Retrieved from <https://doi.org/10.1145/3029603> doi: 10.1145/3029603
- 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.
- Bogetoft, P., & Otto, L. (2011). *Benchmarking with DEA, SFA, and r*. Springer New York. Retrieved from <https://doi.org/10.1007%2F978-1-4419-7961-2> doi: 10.1007/978-1-4419-7961-2
- Brandt, F. (2001, 07). Cryptographic protocols for secure second-price auctions. In (Vol. 2182). doi: 10.1007/3-540-44799-7_16
- Brandt, F., & Sandholm, T. (2005). Efficient privacy-preserving protocols for multi-unit auctions. In A. S. Patrick & M. Yung (Eds.), *Financial cryptography and data security* (pp. 298–312). Berlin, Heidelberg: Springer Berlin Heidelberg.
- Burian, R. M. (2013). Exploratory experimentation. In W. Dubitzky, O. Wolkenhauer, K.-H. Cho, & H. Yokota (Eds.), *Encyclopedia of systems biology* (pp. 720–723). New York, NY: Springer New York. Retrieved from <https://>

- doi.org/10.1007/978-1-4419-9863-7_60 doi: 10.1007/978-1-4419-9863-7_60
- Cachon, G. P., & Lariviere, M. A. (2001). Contracting to assure supply: How to share demand forecasts in a supply chain. *Management Science*, 47(5), 629-646. Retrieved from <https://doi.org/10.1287/mnsc.47.5.629.10486> doi: 10.1287/mnsc.47.5.629.10486
- Catrina, O., & Kerschbaum, F. (2008, March). 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
- Chan, F. T., & Chong, A. Y. (2012). A sem-neural network approach for understanding determinants of interorganizational system standard adoption and performances. *Decision Support Systems*, 54(1), 621 - 630. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0167923612002059> doi: <https://doi.org/10.1016/j.dss.2012.08.009>
- Chang, A. J. (2010, June). Roles of perceived risk and usefulness in information system security adoption. In *2010 IEEE international conference on management of innovation technology* (p. 1264-1269). doi: 10.1109/ICMIT.2010.5492818
- Chang, S.-H., Chou, C.-H., & Yang, J. (2010). The literature review of technology acceptance model: A study of the bibliometric distributions. In *Pacis*.
- Chen, Y., Ma, Z., Wang, Q., Huang, J., Tian, X., & Zhang, Q. (2019, October). Privacy-preserving spectrum auction design: Challenges, solutions, and research directions. *IEEE Wireless Communications*, 26(5), 142-150. doi: 10.1109/MWC.2019.1900022
- Chin, W. W. (1998). Commentary: Issues and opinion on structural equation modeling. *MIS Quarterly*, 22(1), vii-xvi. Retrieved from <http://www.jstor.org/stable/249674>
- Chiregi, M., & Navimipour, N. J. (2016). A new method for trust and reputation evaluation in the cloud environments using the recommendations of opinion leaders' entities and removing the effect of troll entities. *Computers in Human Behavior*, 60, 280 - 292. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0747563216300814> doi: <https://doi.org/10.1016/j.chb.2016.02.029>
- Choi, J. I., Butler, K. R. B., & Genge, B. (2019, January). Secure multiparty computation and trusted hardware: Examining adoption challenges and opportunities. *Sec. and Commun. Netw.*, 2019. Retrieved from <https://doi.org/10.1155/2019/1368905> doi: 10.1155/2019/1368905
- Chong, A. Y.-L., & Bai, R. (2014). Predicting open ios adoption in smes: An integrated sem-neural network approach. *Expert Systems with Applications*, 41(1), 221 - 229. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0957417413005009> (21st Century Logistics and Supply Chain Management) doi: <https://doi.org/10.1016/j.eswa.2013.07.023>
- Choudhary, K., Pandey, U., Nayak, M. K., & Mishra, D. K. (2011, July). Electronic data interchange: A review. In *2011 third international conference on computational intelligence, communication systems and networks* (p. 323-327). doi: 10.1109/CICSyN.2011.74
- 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. Retrieved from https://doi.org/10.1007/0-387-36921-X_3 doi: 10.1007/0-387-36921-X_3
- Cooper, M., Lambert, D., & Pagh, J. (1997, 01). Supply chain management: More than a new name for logistics. *International Journal of Logistics Management*, The, 8, 1-14. doi: 10.1108/09574099710805556
- Curkovic, S., Scannell, T., & Wagner, B. (2015). *Managing supply chain risk: Integrating with risk management*.
- 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.
- Davis, F., Bagozzi, R., & Warshaw, P. (1989, 08). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35, 982-1003. doi: 10.1287/mnsc.35.8.982
- Dhagarra, D., Goswami, M., & Kumar, G. (2020). Impact of trust and privacy concerns on technology acceptance in healthcare: An indian perspective. *International Journal of Medical Informatics*, 141, 104164. Retrieved from <http://www.sciencedirect.com/science/article/pii/S1386505620302276> doi: <https://doi.org/10.1016/j.ijmedinf.2020.104164>
- Downs, G. W., & Mohr, L. B. (1976). Conceptual issues in the study of innovation. *Administrative Science Quarterly*,

- 21(4), 700–714. Retrieved from <http://www.jstor.org/stable/2391725>
- Du, T. C., Lai, V. S., Cheung, W., & Cui, X. (2012). Willingness to share information in a supply chain: A partnership-data-process perspective. *Information & Management*, 49(2), 89 - 98. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0378720611000917> doi: <https://doi.org/10.1016/j.im.2011.10.003>
- Eichhorn, B. R. (2014). Common method variance techniques..
- 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
- European Union. (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>
- Eveland, J., & Tornatzky, L. (1990, 01). Technological innovation as a process. In (p. 27-50).
- Faujdar, V., Agahari, W., de Reuver, M., & Fiebig, T. (2020). Conveying trust in secure multiparty computation: A pilot study in the supply chain domain.. (Manuscript in preparation.)
- Fayad, M., & Cline, M. (1996, 10). Aspects of software adaptability. *Commun. ACM*, 39, 58-59. doi: 10.1145/236156.236170
- Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: a perceived risk facets perspective. *International Journal of Human-Computer Studies*, 59(4), 451 - 474. Retrieved from <http://www.sciencedirect.com/science/article/pii/S1071581903001113> (Zhang and Dillon Special Issue on HCI and MIS) doi: [https://doi.org/10.1016/S1071-5819\(03\)00111-3](https://doi.org/10.1016/S1071-5819(03)00111-3)
- 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. Retrieved from https://doi.org/10.1007/978-3-658-07005-2_3 doi: 10.1007/978-3-658-07005-2_3
- Field, A. (2017). *Discovering statistics using ibm spss statistics* (5th ed.). Sage Publications Ltd.
- Fisk, G., Ardi, C., Pickett, N., Heidemann, J., Fisk, M., & Papadopoulos, C. (2015, May). Privacy principles for sharing cyber security data. In *2015 ieee security and privacy workshops* (p. 193-197). doi: 10.1109/SPW.2015.23
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39–50. Retrieved from <http://www.jstor.org/stable/3151312>
- Frambach, R. T., & Schillewaert, N. (2002). Organizational innovation adoption: a multi-level framework of determinants and opportunities for future research. *Journal of Business Research*, 55(2), 163 - 176. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0148296300001521> (Marketing Theory in the Next Millennium) doi: [https://doi.org/10.1016/S0148-2963\(00\)00152-1](https://doi.org/10.1016/S0148-2963(00)00152-1)
- Franklin, M. K., & Reiter, M. K. (1996, May). The design and implementation of a secure auction service. *IEEE Transactions on Software Engineering*, 22(5), 302-312. doi: 10.1109/32.502223
- Gan, M. F., Chua, H. N., & Wong, S. F. (2019). Privacy enhancing technologies implementation: An investigation of its impact on work processes and employee perception. *Telematics and Informatics*, 38, 13 - 29. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0736585318309286> doi: <https://doi.org/10.1016/j.tele.2019.01.002>
- Ghani, N., Hedges, J., Winschel, V., & Zahn, P. (2018, 07). Compositional game theory. In (p. 472-481). doi: 10.1145/3209108.3209165
- Gignac, G. (2009, 04). Psychometrics and the measurement of emotional intelligence. In (p. 9-40). doi: 10.1007/978-0-387-88370-0_2
- 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.
- Gopalakrishnan. (2001, 08 7). Electronic issues in supply chain management. In (p. 3).
- Grandison, T., & Sloman, M. (2000, Fourth). A survey of trust in internet applications. *IEEE Communications Surveys Tutorials*, 3(4), 2-16. doi: 10.1109/COMST.2000.5340804
- Guan, Z., Zhang, X., Zhou, M., & Dan, Y. (2020). Demand information sharing in competing supply chains with manufacturer-provided service. *International Journal of Production Economics*, 220, 107450. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0925527319302609> doi: <https://doi.org/10.1016/j.ijpe.2019.07.023>
- Gunasekaran, A., & Ngai, E. (2004). Information systems in supply chain integration and management. *European Journal of Operational Research*, 159(2), 269 - 295. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0377221703005186> (Supply Chain Management: Theory and Applications) doi: <https://doi.org/10.1016/j.ejor.2003.08.016>

- Guo, Y., Lim, A., & Rodrigues, B. (2003, 01). Transportation bid analysis optimization with shipper input. In (p. 290-). doi: 10.1109/TAI.2003.1250203
- Hair, J. F., Black, J. W. C., Babin, B. J., & Anderson, R. E. (2014). *Multivariate data analysis*. Pearson Education Limited.
- Ham, Y., & Johnston, R. (2006, 01). A process model of inter-organisational scm initiatives adoption.. doi: 10.4018/9781599042312.ch008
- Harborth, D., Pape, S., & Rannenber, K. (2020, 02). Explaining the technology use behavior of privacy-enhancing technologies: The case of tor and jonym. In (Vol. 2020). doi: 10.2478/popets-2020-0020
- Harman, H. H. (1960). *Modern factor analysis*. The university of Chicago Press. Retrieved from <https://ia800200.us.archive.org/4/items/ModernFactorAnalysis/ModernFactorAnalysis.pdf>
- Harrison McKnight, D., & Chervany, N. L. (2001). Trust and distrust definitions: One bite at a time. In R. Falcone, M. Singh, & Y.-H. Tan (Eds.), *Trust in cyber-societies* (pp. 27–54). Berlin, Heidelberg: Springer Berlin Heidelberg.
- Hart, P., & Saunders, C. (1997, 02). Power and trust: Critical factors in the adoption and use of electronic data interchange. *Organization Science - ORGAN SCI*, 8, 23-42. doi: 10.1287/orsc.8.1.23
- Hartono, E., Li, X., Na, K.-S., & Simpson, J. T. (2010). The role of the quality of shared information in interorganizational systems use. *International Journal of Information Management*, 30(5), 399 - 407. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0268401210000320> doi: <https://doi.org/10.1016/j.ijinfomgt.2010.02.007>
- Hastings, M., Hemenway, B., Noble, D., & Zdancewic, S. (2019). SoK: general-purpose compilers for secure multi-party computation. In *2019 IEEE Symposium on Security and Privacy (SP)*.
- Hazay, C., & Lindell, Y. (2010). *A note on the relation between the definitions of security for semi-honest and malicious adversaries*. Retrieved from <https://eprint.iacr.org/2010/551.pdf>
- Herbohn, J. L., Frikken, B., & Schwarz, L. B. (2004). Secure supply-chain collaboration.. Retrieved from <https://www.semanticscholar.org/paper/Secure-Supply-Chain-Collaboration-Herbohn-Frikken/d6076030ef3a3c3921843867161a4803e7a79dcf>
- Heurix, J., Zimmermann, P., Neubauer, T., & Fenz, S. (2015). A taxonomy for privacy enhancing technologies. *Computers & Security*, 53, 1 - 17. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0167404815000668> doi: <https://doi.org/10.1016/j.cose.2015.05.002>
- Hirt, M., & Maurer, U. (2001). Robustness for free in unconditional multi-party computation. In J. Kilian (Ed.), *Advances in cryptology — crypto 2001* (pp. 101–118). Berlin, Heidelberg: Springer Berlin Heidelberg.
- Holland, C. P. (1995). Cooperative supply chain management: the impact of interorganizational information systems. *The Journal of Strategic Information Systems*, 4(2), 117 - 133. Retrieved from <http://www.sciencedirect.com/science/article/pii/096386879580020Q> doi: [https://doi.org/10.1016/0963-8687\(95\)80020-Q](https://doi.org/10.1016/0963-8687(95)80020-Q)
- Honeycomb.io. (n.d.). *Observability for developers* (Tech. Rep.). Retrieved 18-05-20, from <https://www.honeycomb.io/resources/guide-observability-for-developers/>
- Hong, I. B. (2002). A new framework for interorganizational systems based on the linkage of participants' roles. *Information & Management*, 39(4), 261 - 270. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0378720601000957> doi: [https://doi.org/10.1016/S0378-7206\(01\)00095-7](https://doi.org/10.1016/S0378-7206(01)00095-7)
- Hong, I. B., & Changsu Kim. (1998, Jan). Toward a new framework for interorganizational systems: a network configuration perspective. In *Proceedings of the thirty-first hawaii international conference on system sciences* (Vol. 4, p. 92-101 vol.4). doi: 10.1109/HICSS.1998.655264
- Huang, D., Rau, P. 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. Retrieved from <http://www.sciencedirect.com/science/article/pii/S1071581911001029> doi: <https://doi.org/10.1016/j.ijhcs.2011.07.007>
- Huang, Y., Hung, J.-S., & Ho, J.-W. (2017). A study on information sharing for supply chains with multiple suppliers. *Computers & Industrial Engineering*, 104, 114 - 123. Retrieved from <http://www.sciencedirect.com/science/article/pii/S036083521630482X> doi: <https://doi.org/10.1016/j.cie.2016.12.014>
- IEEE. (1990, Dec). IEEE standard glossary of software engineering terminology. *IEEE Std 610.12-1990*, 1-84. doi: 10.1109/IEEESTD.1990.101064
- ISyE. (2003). *Benchmarking warehousing and distribution operations*. Georgia Tech ISyE. Retrieved from <http://www.forestry.ubc.ca/conservation/power/>
- Jagadeesh, K. A., Wu, D. J., Birge, J. A., Boneh, D., & Bejerano, G. (2017). Deriving genomic diagnoses without revealing patient genomes. *Science*, 357(6352), 692–695. Retrieved from <https://science.sciencemag.org/content/357/6352/692> doi: 10.1126/science.aam9710
- Johnston, H. R., & Vitale, M. R. (1988). Creating competitive advantage with interorganizational information systems. *MIS Quarterly*, 12(2), 153–165. Retrieved from <http://www.jstor.org/stable/248839>

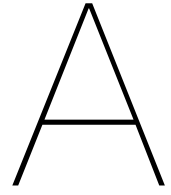
- Jr, R., Snyder, C., & Carr, H. (1991, 06). Risk analysis for information technology. *J. of Management Information Systems*, 8, 129-148. doi: 10.1080/07421222.1991.11517914
- Kaiser, H. F. (1974, Mar 01). An index of factorial simplicity. *Psychometrika*, 39(1), 31-36. Retrieved from <https://doi.org/10.1007/BF02291575> doi: 10.1007/BF02291575
- Kanger, L., & Prulmann-Vengerfeldt, P. (2015, 01). Social need for secure multiparty computation. *Cryptology and Information Security Series*, 13, 43-57. doi: 10.3233/978-1-61499-532-6-43
- Karafili, E., Lupu, E. C., Cullen, A., Williams, B., Arunkumar, S., & Calo, S. (2017, Dec). Improving data sharing in data rich environments. In *2017 IEEE International Conference on Big Data (Big Data)* (p. 2998-3005). doi: 10.1109/BigData.2017.8258270
- Kembro, J., Selviaridis, K., & Naslund, D. (2014, 09). Theoretical perspectives on information sharing in supply chains: A systematic literature review and conceptual framework. *Supply Chain Management: An International Journal*, 19, 609-625. doi: 10.1108/SCM-12-2013-0460
- Kerschbaum, F., Schroepfer, A., Zilli, A., Pibernik, R., Catrina, O., de Hoogh, S., ... Damiani, E. (2011, Sep.). Secure collaborative supply-chain management. *Computer*, 44(9), 38-43. doi: 10.1109/MC.2011.224
- Khurana, M., Mishra, P., & Singh, A. R. (2011, 06). Barriers to information sharing in supply chain of manufacturing industries. *International Journal of Manufacturing System*, 1, 9-29. doi: 10.3923/ijmsaj.2011.9.29
- Kim, K. K., Park, S.-H., Ryoo, S. Y., & Park, S. K. (2010). Inter-organizational cooperation in buyer-supplier relationships: Both perspectives. *Journal of Business Research*, 63(8), 863 - 869. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0148296309001891> doi: <https://doi.org/10.1016/j.jbusres.2009.04.028>
- Kivlin, F. C., Joseph E. Fliegel. (1967). Differential perceptions of innovations and rate of adoption. *Rural Sociological Society*, 32(1), 78 - 91. Retrieved from <https://digital.library.cornell.edu/catalog/chla5075626> (Malden, Mass. : Wiley, ISSN 0036-0112, ZDB-ID 204567-9)
- Kolesnikov, V., Matania, N., Pinkas, B., Rosulek, M., & Trieu, N. (2017). Practical multi-party private set intersection from symmetric-key techniques. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security* (p. 1257-1272). New York, NY, USA: Association for Computing Machinery. Retrieved from <https://doi.org/10.1145/3133956.3134065> doi: 10.1145/3133956.3134065
- Koutroumpis, P., Leiponen, A., & Thomas, L. D. W. (2017, September). *The (Unfulfilled) Potential of Data Marketplaces* (ETLA Working Papers No. 53). The Research Institute of the Finnish Economy. Retrieved from <https://ideas.repec.org/p/rif/wpaper/53.html>
- Kumar, K., & van Dissel, H. G. (1996). Sustainable collaboration: Managing conflict and cooperation in interorganizational systems. *MIS Quarterly*, 20(3), 279-300. Retrieved from <http://www.jstor.org/stable/249657>
- Kurnia, S., & Johnston, R. (2000). The need for a processual view of inter-organizational systems adoption. *The Journal of Strategic Information Systems*, 9(4), 295 - 319. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0963868700000500> doi: [https://doi.org/10.1016/S0963-8687\(00\)00050-0](https://doi.org/10.1016/S0963-8687(00)00050-0)
- Lai, C. (2009). The use of influence strategies in interdependent relationship: The moderating role of shared norms and values. *Industrial Marketing Management*, 38(4), 426-432. Retrieved from <https://www.scopus.com/inward/record.uri?eid=2-s2.0-67349219644&doi=10.1016%2fj.indmarman.2008.06.003&partnerID=40&md5=2dadbc4b812dac33719df60e6fd46e61> (cited By 22) doi: 10.1016/j.indmarman.2008.06.003
- Lai, I. K., Tong, V. W., & Lai, D. C. (2011). Trust factors influencing the adoption of internet-based interorganizational systems. *Electronic Commerce Research and Applications*, 10(1), 85 - 93. Retrieved from <http://www.sciencedirect.com/science/article/pii/S1567422310000529> (Special Section: Service Innovation in E-Commerce) doi: <https://doi.org/10.1016/j.elerap.2010.07.001>
- Lapets, A., Volgushev, N., Bestavros, A., Jansen, F., & Varia, M. (2016). *Secure multi-party computation for analytics deployed as a lightweight web application*. OpenBU. Retrieved from <https://open.bu.edu/handle/2144/21786>
- Lee, H., Kim, M. S., & Kim, K. K. (2014). Interorganizational information systems visibility and supply chain performance. *International Journal of Information Management*, 34(2), 285 - 295. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0268401213001205> doi: <https://doi.org/10.1016/j.ijinfomgt.2013.10.003>
- Lei, C., & W., H. C. (2005, Jan 01). Understanding computer-mediated interorganizational collaboration: a model and framework. *Journal of Knowledge Management*, 9(1), 53-75. Retrieved from <https://doi.org/10.1108/13673270510582965> doi: 10.1108/13673270510582965
- Li, H.-J., Wang, Q., Liu, S., & Hu, J. (2020). Exploring the trust management mechanism in self-organizing complex network based on game theory. *Physica A: Statistical Mechanics and its Applications*, 542, 123514. Retrieved

- from <http://www.sciencedirect.com/science/article/pii/S0378437119319600> doi: <https://doi.org/10.1016/j.physa.2019.123514>
- Li, J., & Shaw, M. J. (2001). The effects of information sharing strategies on supply chain performance. working paper. In *Proceedings of 8th ecis* (pp. 3–5).
- Li, L. (2002). Information sharing in a supply chain with horizontal competition. *Management Science*, 48(9), 1196-1212. Retrieved from <https://doi.org/10.1287/mnsc.48.9.1196.177> doi: 10.1287/mnsc.48.9.1196.177
- Lin, H.-F. (2006). Interorganizational and organizational determinants of planning effectiveness for internet-based interorganizational systems. *Information & Management*, 43(4), 423 - 433. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0378720605000765> doi: <https://doi.org/10.1016/j.im.2005.10.004>
- Lipmaa, H., Asokan, N., & Niemi, V. (2003). Secure vickrey auctions without threshold trust. In M. Blaze (Ed.), *Financial cryptography* (pp. 87–101). Berlin, Heidelberg: Springer Berlin Heidelberg.
- Lotfi, Z., Mukhtar, M., Sahran, S., & Zadeh, A. T. (2013). Information sharing in supply chain management. *Procedia Technology*, 11, 298 - 304. Retrieved from <http://www.sciencedirect.com/science/article/pii/S2212017313003484> (4th International Conference on Electrical Engineering and Informatics, ICEEI 2013) doi: <https://doi.org/10.1016/j.protcy.2013.12.194>
- Maurer, U. (2006). Secure multi-party computation made simple. *Discrete Applied Mathematics*, 154(2), 370 - 381. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0166218X05002428> (Coding and Cryptography) doi: <https://doi.org/10.1016/j.dam.2005.03.020>
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *The Academy of Management Review*, 20(3), 709–734. Retrieved from <http://www.jstor.org/stable/258792>
- Merkuryeva, G., Valberga, A., & Smirnov, A. (2019). Demand forecasting in pharmaceutical supply chains: A case study. *Procedia Computer Science*, 149, 3 - 10. Retrieved from <http://www.sciencedirect.com/science/article/pii/S1877050919301061> (ICTE in Transportation and Logistics 2018 (ICTE 2018)) doi: <https://doi.org/10.1016/j.procs.2019.01.100>
- Milch, V., & Laumann, K. (2016). Interorganizational complexity and organizational accident risk: A literature review. *Safety Science*, 82, 9 - 17. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0925753515002143> doi: <https://doi.org/10.1016/j.ssci.2015.08.010>
- Miltersen, P. B., Nielsen, J. B., & Triandopoulos, N. (2009). Privacy-enhancing auctions using rational cryptography. In S. Halevi (Ed.), *Advances in cryptology - crypto 2009* (pp. 541–558). Berlin, Heidelberg: Springer Berlin Heidelberg.
- Min, H., & Zhou, G. (2002). Supply chain modeling: past, present and future. *Computers & Industrial Engineering*, 43(1), 231 - 249. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0360835202000669> doi: [https://doi.org/10.1016/S0360-8352\(02\)00066-9](https://doi.org/10.1016/S0360-8352(02)00066-9)
- Mitchell, V.-W. (1992). Understanding consumers' behaviour: Can perceived risk theory help? *Management Decision*, 30(3), 26-31. Retrieved from <https://www.scopus.com/inward/record.uri?eid=2-s2.0-84934293342&doi=10.1108%2f00251749210013050&partnerID=40&md5=9bb52a113409c6d2c83da052d96bdce1> (cited By 129) doi: 10.1108/00251749210013050
- Naor, M., Pinkas, B., & Sumner, R. (1999). Privacy preserving auctions and mechanism design. In *Proceedings of the 1st acm conference on electronic commerce* (p. 129–139). New York, NY, USA: Association for Computing Machinery. Retrieved from <https://doi.org/10.1145/336992.337028> doi: 10.1145/336992.337028
- 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. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0925527318304997> doi: <https://doi.org/10.1016/j.ijpe.2018.12.021>
- Olsson, U. (1979, Dec 01). Maximum likelihood estimation of the polychoric correlation coefficient. *Psychometrika*, 44(4), 443-460. Retrieved from <https://doi.org/10.1007/BF02296207> doi: 10.1007/BF02296207
- 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* (p. 1-12). doi: 10.1109/ITMC.2013.7352687
- Ortt, R. (2010, 07). Understanding the pre-diffusion phases. In (p. 47-80). doi: 10.1142/9781848163553_0002
- Palan, S., & Schitter, C. (2018). Prolific.ac—a subject pool for online experiments. *Journal of Behavioral and Experimental Finance*, 17, 22 - 27. Retrieved from <http://www.sciencedirect.com/science/article/pii/S2214635017300989> doi: <https://doi.org/10.1016/j.jbef.2017.12.004>
- Panetto, H. (2007, 12). Towards a classification framework for interoperability of enterprise applications. *International Journal of Computer Integrated Manufacturing*, 20. doi: 10.1080/09511920600996419

- Pang, V. (2005, 01). Development of an inter-organisational system for supply chain management adoption framework: A proposed study of collaborative factors from supplier and customer perspectives. *ACIS 2005 Proceedings - 16th Australasian Conference on Information Systems*. Retrieved from <https://aisel.aisnet.org/acis2005/33>
- Pavlidis, M. (2011, 06). Designing for trust. In (Vol. 731).
- Petronio, S. (1991). Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory*, 1(4), 311-335. Retrieved from <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1468-2885.1991.tb00023.x> doi: 10.1111/j.1468-2885.1991.tb00023.x
- Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication*, 13(1), 6-14. Retrieved from <https://www.scopus.com/inward/record.uri?eid=2-s2.0-84873168678&doi=10.1080%2f15267431.2013.743426&partnerID=40&md5=679a73e9ed54b385fe82609d7644e5e1> (cited By 86) doi: 10.1080/15267431.2013.743426
- Phillips, E. E. (2015). *Collaborative logistics comes to the warehouse*. The Wall Street Journal. Retrieved from <https://www.wsj.com/articles/collaborative-logistics-comes-to-the-warehouse-1434128635>
- Premkumar, G. (1999, Dec). Supply chain management and inter-organizational systems: An integrated perspective. In *Amcis 1999 proceedings*. 215 (p. 621-623). Retrieved from <https://aisel.aisnet.org/amcis1999/215>
- Quinn, K., Lewis, D., O'Sullivan, D., & Wade, V. P. (2009, Apr 01). An analysis of accuracy experiments carried out over of a multi-faceted model of trust. *International Journal of Information Security*, 8(2), 103-119. Retrieved from <https://doi.org/10.1007/s10207-008-0069-7> doi: 10.1007/s10207-008-0069-7
- R Core Team. (2013). R: A language and environment for statistical computing [Computer software manual]. Vienna, Austria. Retrieved from <http://www.R-project.org/>
- Raj, G., Sarfaraz, M., & Singh, D. (2014, Sep.). 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
- Reid, J., Nieto, J. M. G., Dawson, E., & Okamoto, E. (2003, Sep.). Privacy and trusted computing. In *14th international workshop on database and expert systems applications, 2003. proceedings*. (p. 383-388). doi: 10.1109/DEXA.2003.1232052
- Rigdon, E. E., & Ferguson, 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. Retrieved from <http://www.jstor.org/stable/3172790>
- Rogers, E. M. (1995). *Diffusion of innovations* (Fourth ed.). The free press, New York.
- Rogers, E. M. (2003). *Difussion of innovation*. Retrieved from <https://teddykw2.files.wordpress.com/2012/07/everett-m-rogers-diffusion-of-innovations.pdf>
- Schotanus, F. (2007). *Horizontal cooperative purchasing* (Unpublished doctoral dissertation). University of Twente, Netherlands.
- Schreieck, M., Hein, A., Wiesche, M., & Krcmar, H. (2018, 01). The challenge of governing digital platform ecosystems. In (p. 527-538). doi: 10.1007/978-3-662-49275-8_47
- Sekaran, U., & Bougie, R. (2010). *Research methods for business: A skill-building approach* (Fifth ed.).
- Sendhil Kumar, R., & Pugazhendhi, S. (2012). Information sharing in supply chains: An overview. *Procedia Engineering*, 38, 2147 - 2154. Retrieved from <http://www.sciencedirect.com/science/article/pii/S1877705812021716> (INTERNATIONAL CONFERENCE ON MODELLING OPTIMIZATION AND COMPUTING) doi: <https://doi.org/10.1016/j.proeng.2012.06.258>
- Shukla, S., & Sadashivappa, G. (2014, March). Secure multi-party computation protocol using asymmetric encryption. In *2014 international conference on computing for sustainable global development (indiacom)* (p. 780-785). doi: 10.1109/IndiaCom.2014.6828069
- Sicotte, C., Paré, G., Moreault, M.-P., & Paccioni, A. (2006, 09). A Risk Assessment of Two Interorganizational Clinical Information Systems. *Journal of the American Medical Informatics Association*, 13(5), 557-566. Retrieved from <https://doi.org/10.1197/jamia.M2012> doi: 10.1197/jamia.M2012
- Singh, K. P., Rishiwal, V., & Kumar, P. (2018). Classification of data to enhance data security in cloud computing. In *2018 3rd international conference on internet of things: Smart innovation and usages (iot-siu)* (p. 1-5).
- Skinner, E. (1996, 10). A guide to constructs of control. *Journal of personality and social psychology*, 71, 549-70. doi: 10.1037/0022-3514.71.3.549
- Soliman, K. S., & Janz, B. D. (2004). An exploratory study to identify the critical factors affecting the decision to establish internet-based interorganizational information systems. *Information & Management*, 41(6), 697 - 706. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0378720603001198> doi:

- <https://doi.org/10.1016/j.im.2003.06.001>
- Sridharan, C. (2018). *Distributed systems observability*. O'Reilly Media, Inc.
- Srikwan, S., Jakobsson, M., Albrecht, A., & Dalkilic, M. (2006, Nov). Trust establishment in data sharing: An incentive model for biodiversity information systems. In *2006 international conference on collaborative computing: Networking, applications and worksharing* (p. 1-8). doi: 10.1109/COLCOM.2006.361904
- 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. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0167404804001233> doi: <https://doi.org/10.1016/j.cose.2004.05.003>
- Tehseen, S., Ramayah, T., & Sajilan, S. (2017, 03). Testing and controlling for common method variance: A review of available methods. *Journal of Management Sciences*, 4, 142-168. doi: 10.20547/jms.2014.1704202
- Thomas, L. D. W., & Leiponen, A. (2016, Second). Big data commercialization. *IEEE Engineering Management Review*, 44(2), 74-90. doi: 10.1109/EMR.2016.2568798
- 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> (<http://uaesmc.cyber.ee/>)
- Tornatzky, L. G., & Klein, K. J. (1982, Feb). Innovation characteristics and innovation adoption-implementation: A meta-analysis of findings. *IEEE Transactions on Engineering Management*, EM-29(1), 28-45. doi: 10.1109/TEM.1982.6447463
- Tushman, M., Anderson, P., & O'Reilly, C. (1997). Technology cycles, innovation streams and ambidextrous organizations. *Managing Strategic Innovation and Change*.
- van Oorschot, J. A., Hofman, E., & Halman, J. I. (2018). A bibliometric review of the innovation adoption literature. *Technological Forecasting and Social Change*, 134, 1 - 21. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0040162517303943> doi: <https://doi.org/10.1016/j.techfore.2018.04.032>
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425-478. Retrieved from <http://www.jstor.org/stable/30036540>
- Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 36(1), 157-178. Retrieved from <http://www.jstor.org/stable/41410412>
- Wang, C., Leung, H.-f., & Wang, Y. (2004). Secure double auction protocols with full privacy protection. In J.-I. Lim & D.-H. Lee (Eds.), *Information security and cryptology - icisc 2003* (pp. 215-229). Berlin, Heidelberg: Springer Berlin Heidelberg.
- Waters, C. K. (2007). The nature and context of exploratory experimentation: An introduction to three case studies of exploratory research. *History and Philosophy of the Life Sciences*, 29(3), 275-284. Retrieved from <http://www.jstor.org/stable/23334262>
- Wolfe, R. A. (1994). Organizational innovation: Review, critique and suggested research directions*. *Journal of Management Studies*, 31(3), 405-431. Retrieved from <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-6486.1994.tb00624.x> doi: 10.1111/j.1467-6486.1994.tb00624.x
- Wu, J., Wang, Z., & Huang, L. (2010, Aug). The relationship among propensity to trust, institution-based trust, perceived control, and trust in platform. In *2010 IEEE 2nd Symposium on Web Society* (p. 424-428). doi: 10.1109/SWS.2010.5607414
- 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
- Yee, K.-p. (2003, 01). User interaction design for secure systems.. doi: 10.1007/3-540-36159-6_24
- 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. Retrieved from <https://www.scopus.com/inward/record.uri?eid=2-s2.0-0033420984&doi=10.1287%2forsa.10.4.439&partnerID=40&md5=8d89299f686c2635ea12abde171a03e5> (cited By 412) doi: 10.1287/orsa.10.4.439
- yun Yu, C. (2002). *Evaluating cutoff criteria of model fit indices for latent variable models with binary and continuous outcomes*. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.310.3956&rep=rep1&type=pdf>
- Zafri, N. (2006). *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>

- data-sharing/
- 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. Retrieved from <http://www.jstor.org/stable/2486708>
- 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., & Li, H. (2009, 10). Impact of perceived technical protection on security behaviors. *Inf. Manag. Comput. Security*, 17, 330-340. doi: 10.1108/09685220910993980
- 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. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0020025518308338> doi: <https://doi.org/10.1016/j.ins.2018.10.024>
- Zheng, M., Wu, K., Sun, C., & Pan, E. (2019). Optimal decisions for a two-echelon supply chain with capacity and demand information. *Advanced Engineering Informatics*, 39, 248 - 258. Retrieved from <http://www.sciencedirect.com/science/article/pii/S1474034618303598> doi: <https://doi.org/10.1016/j.aei.2019.01.008>
- Zhongwen, Z. (2010, Jan). The developing strategy for information system based on cpfr. In *2010 international conference on logistics systems and intelligent management (iclsim)* (Vol. 3, p. 1405-1408). doi: 10.1109/ICLSIM.2010.5461197
- Zhou, M., Dan, B., Ma, S., & Zhang, X. (2016, 06). Supply chain coordination with information sharing: The informational advantage of gpos. *European Journal of Operational Research*, 256. doi: 10.1016/j.ejor.2016.06.045



Appendices

A.1. Technology acceptance models considered

In the quest of seeking a suitable model for examining contribution of protected data several models were considered: UTAUT, the Technology-Organisation-Environment framework and key success factors. In this section it is explain why these were not considered suitable for the purposes of this study.

Venkatesh, Morris, Davis, and Davis (2003) established a prominent model in technology acceptance literature. Their unified theory of acceptance and use of technology (UTAUT) model is rooted in theory of reasoned action (TRA) and Technology Acceptance Model (TAM) (Davis, Bagozzi, & Warshaw, 1989). UTAUT explains as much as 70 percent of the variance in intention to use (Venkatesh et al., 2003). Herein, intention to use is the only predictor to actual use. That is, it is based on the assumption (heavily criticized) that innovation usage behaviour is preceded by the intention to use the innovation (van Oorschot, Hofman, & Halman, 2018). This innovation acceptance line of debate is criticized for its lack of a comprehensive set of attributes explaining technology acceptance outcome (i.e. lacks in explaining usage commitment–internal diffusion) (ibid.). On another note, acceptance is viewed from the perspective of the individual which poses another limitation.

Before continuing the discussion on UTAUT, a clear distinction of adoption and implementation are in order for clarity. Adoption refers to the *decision* to use and implement a new idea (Rogers, 2003, Chapter 1). The adoption process is defined as “series of actions and choices over time through which an individual or an organization evaluates a new idea and decides whether or not to incorporate the new idea into ongoing practice. This behavior consists essentially of dealing with the uncertainty that is inherently involved in deciding about a new alternative to those previously in existence. It is the perceived newness of the innovation, and the uncertainty associated with this newness, that is a distinctive aspect of innovation decision making (compared to other types of decision making)” (Rogers, 2003, Chapter 5). Implementation on the other hand refers to the adoption decision *and* a degree of implementation (utilization) that accounts for post adoption behavior (Tornatzky & Klein, 1982).

Continuing the discussion on UTAUT. In terms of implementation and diffusion, the individual becomes relevant after organizational adoption has taken place (i.e. intra-organizational acceptance or diffusion) (Frambach & Schillewaert, 2002). On the other hand, with respect to organizational adoption the individual is to some extent also relevant in the adoption phase for the reason that adopters (which represent the organization) are in fact individuals.

However, with UTAUT usefulness is considered the most crucial determinant of adoption (Venkatesh et al., 2003; Venkatesh, Thong, & Xu, 2012). Then, when considering emerging and breakthrough technologies, usefulness of the technology is contested through different designs and stages (Tushman, Anderson, & O’Reily, 1997), observed by erratic patterns emerging during the pre-diffusion phases (Ortt, 2010), until the emergence of a dominant design (Tushman et al., 1997). In the adaptation phase (Ortt, 2010) the technology and user preferences are yet to stabilize and the basic functionality and potential applications remain unclear Kanger and Pruulmann-Vengerfeldt (2015). As a result, usefulness seems to be accentuated in the adaptation phase, and while present to some extent, play only a minor role (Frambach & Schillewaert, 2002, pg. 52). The potential and capabil-

ities of the innovation seem to play a more important role during this phase (Kanger & Pruulmann-Vengerfeldt, 2015).

From a different perspective, (Chang, 2010) argues that in that case of security applications, “Adoption of security technology is passive in nature, being initiated by desire to protect the benefits of IS-related assets or reduce the negative consequences of protection failure”, and thus perceived security is argued to be more important than perceived usefulness. This is because, security technologies “emphasizes degree of hazard prevention or mitigation to associated with adoption of a particular security technology” while generic technologies where TAM based frameworks are used “primarily considers degree of positive benefits an individual believes using a particular technology will achieve”. Therefore TAM based models although extensively used in literature (Chang, Chou, & Yang, 2010), is for the aforementioned limitations not considered suitable for this study.

Other models that have been evaluated are *key success factors* and the *Technology-Organisation-Environment* framework. The former is not suitable due to lack of implemented MPC use-cases and context dependency Eveland and Tornatzky (1990). The latter, is found too ‘generic’, within which a host of various factors can be placed (Baker, 2012).

A.2. Resource listing for replicating/reproducing this study

All resources and instruments created and used for the experiment are made open to public. These are listed in table A.1. The styling sheets cannot be made open to public due to single license. For more information, please send an email to masud.petronia@gmail.com.

Item	Access	source
SPSS data set	Public access. Search for Masud Petronia	TU Delft/4TU repository. See https://data.4tu.nl/ .
SPSS questionnaire	Public access. Search for Masud Petronia	TU Delft/4TU repository. See https://data.4tu.nl/ .
Mock-up source code	MIT license	sitWolf GitHub repository https://github.com/sitWolf/mpc-mock-up.git
Mock-up base styling sheet	Single license	Acquire Klorofil licence via https://www.themeinneed.com/
MPC demonstration video*	Creative Commons-license	YouTube. See https://www.youtube.com/watch?v=ptTU2Hz-9co .

Table A.1: References to sources for the purpose of replicability, reproducibility and research contribution.

*This video is modified in accordance with feedback received. More specifically, this video includes an example of secret sharing whereas the original video did not.

A.3. Interorganizational adoption and implementation factors

Table A.2 lists factors related to IOS adoption and implementation. It should be noted this is not an attempt to provide an exhaustive list of relevant factors. This list is established by using keywords “INTERORGANIZATIONAL SYSTEM ADOPTION” on ScienceDirect¹. Thus, the number of citations do not indicate the relative importance of the factors per se.

Factor	Reference
Audit and verification	I. K. Lai, Tong, and Lai (2011)
Compatibility	Chan and Chong (2012) ; Kurnia and Johnston (2000)
Complexity	Chan and Chong (2012)
Cost	Gunasekaran and Ngai (2004) ; Hart and Saunders (1997) ; Kim, Park, Ryoo, and Park (2010) ; Kurnia and Johnston (2000) ; Pang (2005)
Dependency	Chan and Chong (2012) ; Hong (2002) ; Lee, Kim, and Kim (2014)
Goal	Kim et al. (2010)
Governance	Chan and Chong (2012) ; Lee et al. (2014) ; Pang (2005)
Improvement	Hart and Saunders (1997) ; Lin (2006) ; Pang (2005)
Interoperability	I. K. Lai et al. (2011)
Observability	Chan and Chong (2012) ; Kurnia and Johnston (2000)
Performance	Hartono, Li, Na, and Simpson (2010) ; Holland (1995) ; Lee et al. (2014)
Quality	Hartono et al. (2010)
Relative Advantage	Chan and Chong (2012) ; Kurnia and Johnston (2000)
Reliability	I. K. Lai et al. (2011)
Risk	Hart and Saunders (1997) ; Kurnia and Johnston (2000) ; Sicotte, Paré, Moreault, and Paccioni (2006)
Security	I. K. Lai et al. (2011) ; Soliman and Janz (2004)
Service Level Agreement (SLA)	Hart and Saunders (1997)
Trialability	Chan and Chong (2012) ; Kurnia and Johnston (2000)
Trust	Chan and Chong (2012) ; Chong and Bai (2014) ; Hart and Saunders (1997) ; Kim et al. (2010) ; Lee et al. (2014) ; Pang (2005)
Uncertainty	Kim et al. (2010) ; Lee et al. (2014)
Usability	I. K. Lai et al. (2011)

Table A.2: Interorganizational system attributes

¹<https://www.sciencedirect.com/>

A.4. Operationalization of constructs

A.4.1. Background

	Completely Disagree							Completely Disagree
I have a hard time in understanding how new applications work	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

A.4.2. Adaptability

	Completely Disagree							Completely Disagree
The template file provides a safe method for inputting my data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I know what I can expect from the computation output	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am convinced that my data is not leaked in the computation process	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The information provided by the application is complete	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I need to review the application source code in order to describe the overall process	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I had doubts about the legitimacy of the information provided	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I need a clear example of the output before I submit my data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Some information that was provided felt suspicious	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I feel that the application might have built in snags	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The information provided by the application felt as safe	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I do not need the application's source code to make my final judgement	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The intention of the application is clear to me	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The application is felt as a means to safeguard my data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I have a clear <i>idea</i> of what to <i>expect</i> from the output	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The application is missing some information I need to make my final judgement	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Table A.4: Measuring adaptability

A.4.3. Complexity

	<i>Completely Disagree</i>				<i>Completely Disagree</i>			
I prefer technical jargon over plain English because it is more accurate and concise	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The use of technical jargon makes it more easier for me to understand how an application actually works	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
When reading, I prefer visualisations over text	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
When an application makes claims about its security, I will evaluate this my self even if it is complex	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I feel more invited to use an application which feels safe (simple interface but may lack important criteria for experts) then one describing all the details	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Explanations about the features included in an application must be as detailed as possible	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The use of technical jargon discourages me from using a new application	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
If I really need the application, then I will put in effort to understand the technical aspects which I do not understand	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I refer 'short and simple' over 'complete and complex'	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
If I am asked to use an application, but I find this application to difficult to understand, then I will seek alternative even though all of my peers use the application	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
If I am unable to understand how an application works I will be less likely use it even though it will provide significant value to me	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The use of visualisations improves my ability to understand complex material	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
If I am asked to use an application, but I find this application to difficult to understand, then I will do my best to master this application	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
If I really need the application, then I will put in effort to understand the complex aspects about it	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

A.4.4. Data sharing in general

Table A.9 – Continued from previous page

	Completely Disagree				Completely Disagree			
Maintaining a data sharing agreement requires a great deal of effort	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My company has the resources available to prevent liabilities concerned with data leakage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The data shared should be kept confidential at all times	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My company has the capabilities available to prevent liabilities concerned with data leakage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

A.4.8. Integrity

	Completely Disagree				Completely Disagree			
The template file provides a safe method for inputting my data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I know what I can expect from the computation output	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am convinced that my data is not leaked in the computation process	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The information provided by the application is complete	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I need to review the application source code in order to describe the overall process	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I had doubts about the legitimacy of the information provided	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I need a clear example of the output before I submit my data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Some information that was provided felt suspicious	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I feel that the application might have built in snags	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The information provided by the application felt as safe	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I do not need the application's source code to make my final judgement	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The intention of the application is clear to me	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The application is felt as a means to safeguard my data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I have a clear <i>idea</i> of what to <i>expect</i> from the output	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Table A.11 – Continued from previous page

	Completely Disagree				Completely Disagree			
I must have a clear <i>idea</i> of what to <i>expect</i> from the output of the application	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
When an application provides the source code, I feel assured that it is transparent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

A.4.10. Organization - Absorptive capacity

	Completely Disagree				Completely Disagree			
Our company is a little behind in utilizing the most adequate equipment and technologies	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Our company constantly in search for better technological solutions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Our company has a budget available that allows adoption of radical innovations	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Our company has <i>not</i> introduced new methods and techniques to increase operational efficiency in the last 2 years	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Our company regularly evaluates new potential technologies	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Our company has adopted new technologies in the last year in attempts to improve operational efficiency	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Our company has <i>not</i> introduced new methods and techniques to increase operational efficiency in the last 2 years	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Our company is very behind in the application of new administrative techniques to reduce operational bottlenecks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

A.4.11. Simplification

Completely Disagree

Completely Disagree

A.5. SPSS syntax

This appendix provides an overview of SPSS syntax used. Syntaxes which are repeated for multiple variables are prepared using python (see appendix X more information).

A.5.1. Compare means of three data sets

* Compare means of data sets.

```
ONEWAY Q_TRUS_OBS_1 Q_TRUS_OBS_2 Q_TRUS_OBS_3 Q_TRUS_COM_1
Q_TRUS_COM_2 Q_TRUS_COM_3 Q_SECU_RIS_1 W_SECU_RIS_2
Q_SECU_CON_1 Q_SECU_CON_2 Q_SECU_CON_3 Q_SECU_CON_4 Q_TRUS_1
Q_TRUS_2 Q_SIMP_1 Q_SIMP_2 Q_RELA_1 Q_RELA_2 Q_RELA_3
Q_SIMPLICITY_RATING Q_REL_ADV_WILLING Q_TRUSTWORTHINESS
Q_TRUSTWORTHINESS_WILLING Q_SECURITY Q_SECURITY_WILLING
Q_OVERALL_WILLINGNESS BY Dataset_ID
/STATISTICS DESCRIPTIVES HOMOGENEITY
/PLOT MEANS
/MISSING ANALYSIS.
```

A.5.2. Add experimental group column

* Add new column listing which experimental group the row belongs to.

```
COMPUTE Group=MISSING(Q2.20).
VARIABLE LABELS Group 'Experimental groups'.
EXECUTE.
```

A.5.3. Change variable scale

* Change gender unit to nominal.

```
VARIABLE LEVEL Q4.2(NOMINAL).
EXECUTE.
```

A.5.4. Create new column with ages

* New column, with age.

```
COMPUTE Age=2020 - Q4.3.
EXECUTE.
```

A.5.5. Merge variables

The SPSS syntax below shows an example for merging trustworthiness response Q2.12_1 with Q3.11_1. The same syntax is repeated for each corresponding question.

```
* Merge trust variables - Observability.
COMPUTE Q_TRUS_OBS_1=MAX(Q2.12_1,Q3.11_1).
VARIABLE LABELS Q_TRUS_OBS_1 'The intent of the application is clear to me'.
VARIABLE LEVEL Q_TRUS(ORDINAL).
EXECUTE.
```

A.5.6. Sort by group, and invert reverse questions

```
SORT CASES BY Group.
SPLIT FILE LAYERED BY Group.
RECODE Q_TRUS_COM_2 (1=5) (2=4) (3=3) (4=2) (5=1).
EXECUTE.
```

A.5.7. Reliability:trustworthiness

```
SORT CASES BY Group.
SPLIT FILE LAYERED BY Group.
RELIABILITY
/VARIABLES=Q_TRUS_OBS_1 Q_TRUS_OBS_2 Q_TRUS_OBS_3
Q_TRUS_COM_1 Q_TRUS_COM_2 Q_TRUS_COM_3
Q_TRUSTWORTHINESS
/SCALE('ALL VARIABLES') ALL
/MODEL=ALPHA
/STATISTICS=DESCRIPTIVE SCALE CORR
/SUMMARY=TOTAL.
```

A.5.8. Reliability:security

```
SORT CASES BY Group.
SPLIT FILE LAYERED BY Group.
RELIABILITY
/VARIABLES=Q_SECU_RIS_1 Q_SECU_RIS_2 Q_SECU_CON_1
Q_SECU_CON_2 Q_SECU_CON_3 Q_SECU_CON_4
Q_SECURITY
/SCALE('ALL VARIABLES') ALL
/MODEL=ALPHA
/STATISTICS=DESCRIPTIVE SCALE CORR
/SUMMARY=TOTAL.
```

A.5.9. Reliability:relative advantage

```
SORT CASES BY Group.
SPLIT FILE LAYERED BY Group.
RELIABILITY
/VARIABLES=Q_SIMP_1 Q_SIMP_2 Q_RELA_1
Q_RELA_2 Q_RELA_3 Q_SIMPLICITY_RATING
/SCALE('ALL VARIABLES') ALL
/MODEL=ALPHA
/STATISTICS=DESCRIPTIVE SCALE CORR
/SUMMARY=TOTAL.
```

A.5.10. Demographics: age

```
* Generate age histogram.
GGRAPH
/GRAPHDATASET NAME="graphdataset"
VARIABLES=Age
MISSING=LISTWISE REPORTMISSING=NO
/GRAPHSPEC SOURCE=INLINE.
BEGIN GPL
  SOURCE: s=userSource(id("graphdataset"))
  DATA: Age=col(source(s), name("Age"))
  DATA: id=col(source(s), name("$CASENUM"), unit.category())
  COORD: rect(dim(1), transpose())
  GUIDE: axis(dim(1), label("Age"))
  GUIDE: text.title(label("1-D Boxplot of Age"))
  ELEMENT: schema(position(bin.quantile.letter(Age)), label(id))
END GPL.
```

```
* Age histogram.
FREQUENCIES VARIABLES=Age
/NTILES=4
/HISTOGRAM NORMAL
/ORDER=ANALYSIS.
```

```
* Age PPlot.
PLOT
/VARIABLES=Age
/NOLOG
/NOSTANDARDIZE
/TYPE=P-P
/FRACTION=BLOM
/TIES=MEAN
```

```
/DIST=NORMAL.
```

A.5.11. Industry role frequency table

```
* Generate industry role frequency table.
FREQUENCIES VARIABLES=IndustryRole
/ORDER=ANALYSIS.
```

```
FREQUENCIES VARIABLES=Q4.10
/ORDER=ANALYSIS.
```

A.5.12. Organizational size combined with level of involvement in development of new product, services and improvements

```
* Pivot table: org size with level of involvement with extra summary of totals per category.
CTABLES
/VLABELS VARIABLES=Q4.8 Q4.9 DISPLAY=LABEL
/TABLE Q4.8 [C] > Q4.9 [C][COUNT F40.0, TABLEPCT.COUNT PCT40.1]
/CATEGORIES VARIABLES=Q4.8 [1, 2, 3, 4, 5, OTHERNM]
EMPTY=EXCLUDE TOTAL=YES LABEL='Category '+
'totals' POSITION=AFTER
/CATEGORIES VARIABLES=Q4.9 ORDER=A KEY=VALUE EMPTY=EXCLUDE
/CRITERIA CILEVEL=95.
```

A.5.13. Organizational size combined with education level

```
* Pivot table, organizational size - education level.
CTABLES
/VLABELS VARIABLES=Q4.8 Q4.10 DISPLAY=LABEL
/TABLE Q4.8 > Q4.10 [COUNT F40.0, TABLEPCT.COUNT PCT40.1]
/CATEGORIES VARIABLES=Q4.8 Q4.10 ORDER=A KEY=VALUE EMPTY=EXCLUDE
/CRITERIA CILEVEL=95.
```

A.5.14. Industry function and role of work

```
* Table: pivot table, industry function with role at work.
CTABLES
/VLABELS VARIABLES=IndustryFunctionCategory IndustryRole DISPLAY=LABEL
/TABLE IndustryFunctionCategory [C] > IndustryRole [C][COUNT F40.0,
TABLEPCT.COUNT PCT40.1]
```

```

/CATEGORIES VARIABLES=IndustryFunctionCategory IndustryRole ORDER=A
KEY=VALUE EMPTY=EXCLUDE
/CRITERIA CILEVEL=95.

```

A.5.15. Level of familiarity with MPC

```

* Descriptives, level of familiarity of MPC amongst MPC respondents.
FREQUENCIES VARIABLES=Q2.31
/NTILES=4
/STATISTICS=STDDEV VARIANCE MINIMUM MAXIMUM MEAN MEDIAN MODE
/ORDER=ANALYSIS.

```

A.5.16. Participant final criteria check

```

* Pivot table to check for lower education, lower role, lower understanding.
COMPUTE PARTICIPANT_DEGEE_INTERACTION=Q_TRUS_COM_1.
EXECUTE.
* Define Variable Properties.
* PARTICIPANT_DEGEE_INTERACTION.
VALUE LABELS PARTICIPANT_DEGEE_INTERACTION
1.00 '1.00'
2.00 '2.00'
3.00 '3.00'
4.00 '4.00'
5.00 '5.00'.
EXECUTE.

CTABLES
/VLABELS VARIABLES=IndustryRole Q4.10
PARTICIPANT_DEGEE_INTERACTION DISPLAY=LABEL
/TABLE IndustryRole [C] > Q4.10 [C] >
PARTICIPANT_DEGEE_INTERACTION [C][COUNT F40.0]
/CATEGORIES VARIABLES=IndustryRole Q4.10
PARTICIPANT_DEGEE_INTERACTION ORDER=A KEY=VALUE EMPTY=EXCLUDE
/CRITERIA CILEVEL=95.

```

A.5.17. Bayesian comparison of means

```

* Perform Bayesian comparison of means.
BAYES INDEPENDENT
/MISSING SCOPE=ANALYSIS
/CRITERIA CILEVEL=95 TOL=0.000001 MAXITER=2000

```

```
/INFERENCE DISTRIBUTION=NORMAL VARIABLES=Q_OVERALL_WILLINGNESS ANAL-  
YSIS=BOTH GROUP=Group SELECT=LEVEL(TTP MPC) DATAVAR=0.63 0.34  
/PRIOR EQUALDATAVAR=FALSE MEANDIST=NORMAL(3 4 0.35 0.35)  
/ESTBF COMPUTATION=GONEN(1 0.25).
```

A.5.18. Independent t-test willingness to contribute

```
T-TEST GROUPS=Group('MPC' 'TTP')  
/MISSING=ANALYSIS  
/VARIABLES=Q_OVERALL_WILLINGNESS  
/CRITERIA=CI(.95).
```

A.5.19. Independent t-test trustworthiness

```
T-TEST GROUPS=Group('MPC' 'TTP')  
/MISSING=ANALYSIS  
/VARIABLES=Q_TRUSTWORTHINESS_WILLING  
/CRITERIA=CI(.95).
```

A.5.20. Independent t-test trustworthiness 90% CI

```
T-TEST GROUPS=Group('MPC' 'TTP')  
/MISSING=ANALYSIS  
/VARIABLES=Q_TRUSTWORTHINESS_WILLING  
/CRITERIA=CI(.90).
```

A.5.21. Independent t-test relative advantage

```
T-TEST GROUPS=Group('MPC' 'TTP')  
/MISSING=ANALYSIS  
/VARIABLES=Q_REL_ADV_WILLINGNESS  
/CRITERIA=CI(.95).
```

A.5.22. Independent t-test security

```
T-TEST GROUPS=Group('MPC' 'TTP')  
/MISSING=ANALYSIS
```

```
/VARIABLES=Q_SECURITYL_WILLINGNESS  
/CRITERIA=CI(.95).
```


A.6. Demographics SPSS output, pivot tables

		Count	N %
Administration	Skilled laborer	1	0.9%
	Skilled professional	1	0.9%
	Upper management	1	0.9%
Agriculture	Skilled professional	1	0.9%
	Upper management	1	0.9%
E-commerce and retail	Upper management	1	0.9%
Education	Skilled professional	11	10.3%
	Upper management	1	0.9%
Engineering	Skilled professional	12	11.2%
	Upper management	2	1.9%
Healthcare	Skilled professional	9	8.4%
Information Technology and software	Middle management	1	0.9%
	Skilled professional	15	14.0%
	Upper management	3	2.8%
Insurance, finance and law	Middle management	1	0.9%
	Skilled professional	8	7.5%
Manufacturing	Middle management	3	2.8%
	Skilled professional	4	3.7%
	Upper management	1	0.9%
Military	Skilled professional	1	0.9%
N/A	Non-skilled	1	0.9%
Public sector services	Skilled laborer	1	0.9%
	Skilled professional	2	1.9%
Research and development	Skilled professional	3	2.8%
	Upper management	2	1.9%
Sales, Marketing and Media	Middle management	2	1.9%
	Skilled laborer	1	0.9%
	Skilled professional	10	9.3%
	Upper management	2	1.9%
Services	Skilled professional	2	1.9%
Unknown	Skilled laborer	1	0.9%
	Upper management	1	0.9%
Utility	Upper management	1	0.9%

SPSS Output A.1: Industry with role at work

Continued on next page →

		Count	N %
Never	Skilled professional	12	11.2%
Rarely	Middle management	1	0.9%
	Non-skilled	1	0.9%
	Skilled laborer	3	2.8%
	Skilled professional	15	14.0%
Sometimes	Upper management	1	0.9%
	Middle management	2	1.9%
	Skilled professional	21	19.6%
Often	Upper management	6	5.6%
	Middle management	4	3.7%
	Skilled professional	20	18.7%
Always	Upper management	6	5.6%
	Skilled laborer	1	0.9%
	Skilled professional	11	10.3%
	Upper management	3	2.8%

SPSS Output A.2: Degree of level of involvement in development of new products, services, and with role at work

		Count	N %
2-10	Undergraduate (BA, BSc, other)	5	4.7%
	High school diploma	1	0.9%
	Graduate degree (MA, MSc, other)	12	11.2%
	Secondary education	1	0.9%
11-100	Undergraduate (BA, BSc, other)	10	9.3%
	Graduate degree (MA, MSc, other)	11	10.3%
	Technical/Community college	2	1.9%
	Secondary education	1	0.9%
	Doctorate degree (PhD, other)	5	4.7%
More than 100	Undergraduate (BA, BSc, other)	18	16.8%
	High school diploma	3	2.8%
	Graduate degree (MA, MSc, other)	28	26.2%
	Technical/Community college	1	0.9%
	Doctorate degree (PhD, other)	5	4.7%
	Not applicable/I do not know	1	0.9%
I do not know	Graduate degree (MA, MSc, other)	1	0.9%
	Doctorate degree (PhD, other)	2	1.9%

SPSS Output A.3: Organizational size with education level

A.7. Correlation tables for initial constructs

		2	3	4	5	6	7	8	9	10	11		
1	The intent of the application is clear to me	Pears. Corr.	.385**	.302**	.561**	.356**	.512**	.554**	.360**	.377**	.388**	.304**	
		Sig. (2-tailed)	0.000	0.002	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.002
		Bias	0.002	0.006	-0.003	-0.001	-0.004	-0.003	0.001	-0.001	-0.002	0.000	0.000
		Std. Error	0.088	0.088	0.082	0.093	0.082	0.085	0.080	0.090	0.085	0.090	
2	The application clearly describes how my data is processed from data submission to output	Pears. Corr.	1	.524**	.302**	0.154	.368**	.341**	.527**	.433**	.441**	.316**	
		Sig. (2-tailed)		0.000	0.002	0.115	0.000	0.000	0.000	0.000	0.000	0.000	0.001
		Bias	0	0.000	-0.005	-0.001	0.003	0.000	0.003	0.000	0.000	0.000	0.002
		Std. Error	0	0.076	0.094	0.107	0.089	0.076	0.081	0.097	0.087	0.105	
3	The application provides a complete and detailed description of how MPC is used to protect my data	Pears. Corr.	1	1	.196*	0.076	.306**	.338**	.733**	.510**	.375**	.277**	
		Sig. (2-tailed)			0.044	0.437	0.001	0.000	0.000	0.000	0.000	0.004	
		Bias	0	0	0.001	-0.003	0.000	0.006	0.001	-0.001	0.000	0.001	
		Std. Error	0	0	0.084	0.109	0.091	0.079	0.053	0.076	0.089	0.093	
4	Interaction with the application is clear and understandable	Pears. Corr.	1	1	1	.322**	.464**	.449**	.279**	.263**	.271**	0.124	
		Sig. (2-tailed)				0.001	0.000	0.000	0.004	0.006	0.005	0.207	
		Bias	0	0	0	0.000	-0.006	-0.011	-0.005	-0.002	-0.004	-0.002	
		Std. Error	0	0	0	0.108	0.082	0.104	0.098	0.098	0.101	0.094	
5	The descriptions of MPC are complex	Pears. Corr.	1	1	1	1	.369**	.335**	0.105	0.179	0.094	-0.030	
		Sig. (2-tailed)					0.000	0.000	0.283	0.066	0.338	0.758	
		Bias	0	0	0	0	-0.002	-0.008	-0.006	-0.003	-0.003	0.000	
		Std. Error	0	0	0	0	0.098	0.113	0.125	0.106	0.108	0.090	
6	Understanding how the data is processed does not require a lot of my mental effort	Pears. Corr.	1	1	1	1	1	.501**	.317**	.305**	.307**	0.182	
		Sig. (2-tailed)							0.000	0.001	0.001	0.001	0.061
		Bias	0	0	0	0	0	0	-0.002	0.000	-0.002	-0.001	0.000
		Std. Error	0	0	0	0	0	0	0.093	0.097	0.101	0.098	0.110
7	Claims made by the application are clear and accurate	Pears. Corr.	1	1	1	1	1	1	.500**	.394**	.410**	.320**	
		Sig. (2-tailed)								0.000	0.000	0.000	0.001
		Bias	0	0	0	0	0	0	0	0.000	0.001	0.000	0.002
		Std. Error	0	0	0	0	0	0	0	0.086	0.093	0.088	0.089
8	The application is open and transparent in how it protects my data	Pears. Corr.	1	1	1	1	1	1	1	.437**	.415**	.272**	
		Sig. (2-tailed)									0.000	0.000	0.005
		Bias	0	0	0	0	0	0	0	0	0.001	0.000	0.003
		Std. Error	0	0	0	0	0	0	0	0	0.090	0.082	0.083
9	I am satisfied with the trustworthiness of the METHOD	Pears. Corr.	1	1	1	1	1	1	1	1	.845**	.662**	
		Sig. (2-tailed)										0.000	0.000
		Bias	0	0	0	0	0	0	0	0	0	0.000	0.002
		Std. Error	0	0	0	0	0	0	0	0	0	0.041	0.066
10	I would be willing to use this application based on its trustworthiness	Pears. Corr.	1	1	1	1	1	1	1	1	1	.660**	
		Sig. (2-tailed)											0.000
		Bias	0	0	0	0	0	0	0	0	0	0	0.004
		Std. Error	0	0	0	0	0	0	0	0	0	0	0.049
11	Overall, if ... willing to contribute sensitive company data over a METHOD application	Pears. Corr.	1	1	1	1	1	1	1	1	1	1	
		Sig. (2-tailed)											
		Bias	0	0	0	0	0	0	0	0	0	0	0
		Std. Error	0	0	0	0	0	0	0	0	0	0	0

** Correlation is significant at the 0.01 level (2-tailed).

* Correlation is significant at the 0.05 level (2-tailed).

Bootstrap results are based on 1000 bootstrap samples.

N = 106 for all items.

Table A.14: Pearson correlation: trustworthiness and willingness to contribute

		1	2	3	4	5	6	7	8	9		
1	It feels safe contributing sensitive company data over the application	Pears. Corr.	1	.809**	.386**	.372**	.204*	0.188	.439**	.313**	.397**	
		Sig. (2-tailed)		0.000	0.000	0.000	0.036	0.054	0.000	0.001	0.000	
		Bias	0	-0.002	-0.001	-0.005	0.000	-0.006	-0.005	-0.002	0.001	
		Std. Error	0	0.040	0.090	0.092	0.094	0.108	0.107	0.102	0.099	
		95% CI Lower Upper	1	0.718 0.877	0.197 0.556	0.174 0.540	0.027 0.387	-0.031 0.388	0.223 0.629	0.100 0.500	0.200 0.575	
2	The use of MPC gives me a feeling of security assurance	Pears. Corr.		1	.385**	.421**	.224*	.285**	.552**	.431**	.491**	
		Sig. (2-tailed)			0.000	0.000	0.021	0.003	0.000	0.000	0.000	
		Bias	0	-0.003	-0.002	-0.001	-0.006	-0.005	-0.005	0.000	0.004	
		Std. Error	0	0.084	0.080	0.098	0.101	0.085	0.086	0.086	0.077	
		95% CI Lower Upper	1	0.211 0.549	0.255 0.567	0.019 0.419	0.078 0.475	0.372 0.705	0.250 0.585	0.343 0.643		
3	Only I am able to view my contributed data	Pears. Corr.			1	.427**	.293**	.549**	.270**	.299**	.376**	
		Sig. (2-tailed)				0.000	0.002	0.000	0.005	0.002	0.000	
		Bias	0	-0.004	-0.004	-0.002	-0.002	-0.004	-0.004	-0.004	0.001	
		Std. Error	0	0.101	0.107	0.093	0.103	0.092	0.092	0.098		
		95% CI Lower Upper	1	0.209 0.610	0.069 0.490	0.340 0.719	0.068 0.470	0.104 0.473	0.176 0.563			
4	The service provider cannot examine my data beyond my control	Pears. Corr.				1	0.014	.416**	.414**	.420**	.377**	
		Sig. (2-tailed)					0.888	0.000	0.000	0.000	0.000	
		Bias	0	-0.004	-0.002	-0.001	-0.002	-0.002	-0.002	0.000		
		Std. Error	0	0.103	0.090	0.102	0.086	0.093				
		95% CI Lower Upper	1	-0.185 0.222	0.233 0.578	0.192 0.592	0.240 0.582	0.184 0.546				
5	I feel capable of using the application	Pears. Corr.					1	0.047	0.114	0.117	.231*	
		Sig. (2-tailed)						0.633	0.245	0.231	0.017	
		Bias	0	-0.002	-0.006	-0.002	-0.002	-0.008				
		Std. Error	0	0.114	0.112	0.084	0.119					
		95% CI Lower Upper	1	-0.178 0.272	-0.108 0.324	-0.045 0.284	-0.013 0.445					
6	My data cannot be accessed by other contributors	Pears. Corr.						1	.378**	.335**	.353**	
		Sig. (2-tailed)							0.000	0.000	0.000	
		Bias	0	-0.004	-0.002	-0.001						
		Std. Error	0	0.097	0.088	0.098						
		95% CI Lower Upper	1	0.191 0.556	0.161 0.500	0.141 0.541						
7	I am satisfied with the security METHOD provides	Pears. Corr.							1	.737**	.696**	
		Sig. (2-tailed)								0.000	0.000	
		Bias	0	0.000	-0.003							
		Std. Error	0	0.039	0.054							
		95% CI Lower Upper	1	0.654 0.804	0.581 0.793							
8	I would be willing to use this application based on the security provided by METHOD	Pears. Corr.								1	.657**	
		Sig. (2-tailed)									0.000	
		Bias	0	0.001								
		Std. Error	0	0.053								
		95% CI Lower Upper	1	0.546 0.751								
9	Overall, if ... willing to contribute sensitive company data over a METHOD application	Pears. Corr.									1	
		Sig. (2-tailed)										0
		Bias										0
		Std. Error										1
		95% CI Lower Upper										1

** Correlation is significant at the 0.01 level (2-tailed).
 * Correlation is significant at the 0.05 level (2-tailed).
 Bootstrap results are based on 1000 bootstrap samples.
 N = 106 for all items.

Table A.15: Pearson correlation: Security and willingness to contribute

		1	2	3	4	5	6	7	8		
1	The application provides a simple way to securely contribute data	Pears. Corr.	1	.377**	.282**	.509**	.336**	.524**	.496**	.387**	
		Sig. (2-tailed)		0.000	0.003	0.000	0.000	0.000	0.000	0.000	0.000
		Bias	0	-0.003	0.001	-0.010	-0.003	-0.003	-0.001	0.002	0.002
		Std. Error	0	0.120	0.130	0.094	0.121	0.089	0.092	0.088	0.088
		95% CI Lower Upper	1	0.120 0.593	0.016 0.531	0.301 0.674	0.089 0.551	0.334 0.685	0.304 0.661	0.212 0.548	
2	The application does not require expertise from multiple organizational departments	Pears. Corr.		1	0.058	.195*	.344**	.368**	.245*	.311**	
		Sig. (2-tailed)			0.552	0.045	0.000	0.000	0.011	0.001	
		Bias	0	0.001	-0.003	0.003	-0.001	0.005	-0.004	-0.004	
		Std. Error	0	0.115	0.118	0.113	0.092	0.102	0.094	0.094	
		95% CI Lower Upper	1	-0.170 0.287	-0.056 0.414	0.130 0.568	0.179 0.531	0.038 0.441	0.113 0.486		
3	The application provides an advantage over conventional data sharing practices	Pears. Corr.			1	.262**	.422**	.430**	.304**	.286**	
		Sig. (2-tailed)				0.007	0.000	0.000	0.002	0.003	
		Bias	0	0.002	-0.002	-0.003	-0.005	0.004	0.004		
		Std. Error	0	0.107	0.093	0.079	0.093	0.108	0.108		
		95% CI Lower Upper	1	0.038 0.467	0.214 0.591	0.266 0.576	0.115 0.471	0.062 0.505			
4	When contributing data, no other party knows about my participation	Pears. Corr.				1	.401**	.306**	.252**	.312**	
		Sig. (2-tailed)					0.000	0.001	0.009	0.001	
		Bias	0	-0.001	0.002	0.002	0.002	0.002	0.002		
		Std. Error	0	0.094	0.080	0.106	0.095	0.095	0.095		
		95% CI Lower Upper	1	0.205 0.572	0.142 0.464	0.043 0.462	0.116 0.490				
5	I feel less hesitant with contributing sensitive company data when using this mpc application	Pears. Corr.					1	.410**	.303**	.429**	
		Sig. (2-tailed)						0.000	0.002	0.000	
		Bias	0	-0.004	0.000	0.000	0.000	0.000	0.000		
		Std. Error	0	0.089	0.119	0.107	0.107	0.107	0.107		
		95% CI Lower Upper	1	0.231 0.585	0.057 0.534	0.202 0.621					
6	METHOD provides a simple solution to secure data contribution	Pears. Corr.						1	.706**	.474**	
		Sig. (2-tailed)							0.000	0.000	
		Bias	0	-0.002	0.005	0.078	0.078	0.078	0.078		
		Std. Error	0	0.053	0.078	0.078	0.078	0.078	0.078		
		95% CI Lower Upper	1	0.588 0.799	0.324 0.627						
7	I would be willing to use METHOD based on the solution it provides to secure data contribution	Pears. Corr.							1	.295**	
		Sig. (2-tailed)								0.002	
		Bias	0	0.005	0.005	0.005	0.005	0.005	0.005		
		Std. Error	0	0.106	0.106	0.106	0.106	0.106	0.106		
		95% CI Lower Upper	1	0.074 0.502							
8	Overall, if ... willing to contribute sensitive company data over a METHOD application	Pears. Corr.								1	
		Sig. (2-tailed)									0
		Bias									0
		Std. Error									0
		95% CI Lower Upper									1

** Correlation is significant at the 0.01 level (2-tailed).

* Correlation is significant at the 0.05 level (2-tailed).

Bootstrap results are based on 1000 bootstrap samples.

N = 106 for all items.

Table A.16: Pearson correlation: Relative advantage and willingness to contribute

A.8. Tolerance, VIF, CR, C-alpha

General rule of thumb suggests: a Tolerance of greater than 0.2, Variance Inflation Factor (VIF) less than 5.0 (Field, 2017, ch. 7.6), Composite Reliability (CR) of greater than 0.7 (Fornell & Larcker, 1981, p. 46), Average Variance Extracted (AVE) greater than 0.5 (Hair et al., 2014, p. 619), and Cronbach's Alpha ($C-\alpha$) greater than 0.7 as acceptable values (Field, 2017; Gignac, 2009). The results reported here are also evaluated using the pearson correlation matrices (Appendix A.7), inter-item correlation matrices and item-total statistics (Appendix A.9).

Combined sample N=107		Mean	Std. Err.	SD	Factor Loading	Tolerance	VIF	AVE	CR	C- α
Perceived Trustworthiness	Perceived Coherence							0.630	0.836	0.754
	The intent of the application is clear to me	3.766	0.091	0.937	0.812	0.612	1.634			
	Interaction with the application is clear and understandable	3.804	0.094	0.976	0.788	0.644	1.553			
	Understanding how the data is processed does not require a lot of my mental effort	3.299	0.101	1.048	0.781	0.698	1.433			
	Perceived Transparency							0.730	0.890	0.813
	The application clearly describes how my data is processed from data submission to output	3.785	0.089	0.922	0.782	0.683	1.464			
	The application provides a complete and detailed description of how METHOD is used to protect my data	3.402	0.102	1.054	0.886	0.446	2.243			
	The application is open and transparent in how it protects my data	3.495	0.092	0.955	0.891	0.438	2.283			
	Perceived risk							0.859	0.924	0.897
	It feels safe contributing sensitive company data over the application	3.318	0.097	1.006	0.924	0.337	2.971			
Perceived Security	The use of METHOD gives me a feeling of security assurance	3.430	0.094	0.972	0.929	0.334	2.998			
	Perceived control							0.638	0.841	0.710
	Only I am able to view my contributed data	3.598	0.083	0.856	0.827	0.663	1.509			
	The service provider cannot examine my data beyond my control	3.262	0.098	1.013	0.751	0.772	1.295			
My data cannot be accessed by other contributors	3.748	0.086	0.891	0.817	0.676	1.480				

Table A.17: Descriptive statistics, FA, PCA, and reliability results for combined sample (MPC and TTP)

Continued on next page →

Combined sample N=107		Mean	Std. Err.	SD	Factor Loading	Tolerance	VIF	AVE	CR	C- α
Perceived utility								0.526	0.815	0.698
Perceived Rel. advantage	The application provides a simple way to securely contribute data	3.794	0.076	0.786	0.749	0.699	1.430			
	The application provides an advantage over conventional data sharing practices	3.794	0.077	0.798	0.620	0.823	1.216			
	When contributing data, no other party knows about my participation	3.794	0.082	0.844	0.771	0.669	1.496			
	I feel less hesitant with contributing sensitive company data when using this METHOD application	3.523	0.087	0.904	0.752	0.722	1.385			
Willingness to contribute								0.623	0.830	0.695
Willingness	I would be willing to use METHOD based on the solution it provides to secure data contribution	3.9340	0.06326	0.65128	0.678	0.818	1.223			
	I would be willing to use this application based on its trustworthiness	3.7170	0.07672	0.78987	0.875	0.578	1.731			
	I would be willing to use this application based on the security provided by METHOD	3.7453	0.08050	0.82878	0.802	0.655	1.527			

Table A.18: Descriptive statistics, FA, PCA, and reliability results for combined sample (MPC and TTP)

A.9. Inter-Item correlation matrices and item-total statistics

Group		1	2	3	4	5	6	7	8	9	
MPC	1	The intent of the application is clear to me	1.000	0.489	0.272	0.544	0.428	0.557	0.503	0.445	0.454
	2	The application clearly describes how my data is processed from data submission to output	0.489	1.000	0.302	0.483	0.408	0.527	0.371	0.355	0.305
	3	The application provides a complete and detailed description of how MPC is used to protect my data	0.272	0.302	1.000	0.311	0.248	0.084	0.245	0.608	0.284
	4	Interaction with the application is clear and understandable	0.544	0.483	0.311	1.000	0.456	0.545	0.590	0.417	0.454
	5	The descriptions of MPC are complex	0.428	0.408	0.248	0.456	1.000	0.636	0.525	0.292	0.346
	6	Understanding how the data is processed does not require a lot of my mental effort	0.557	0.527	0.084	0.545	0.636	1.000	0.503	0.267	0.372
	7	Claims made by the application are clear and accurate	0.503	0.371	0.245	0.590	0.525	0.503	1.000	0.553	0.433
	8	The application is open and transparent in how it protects my data	0.445	0.355	0.608	0.417	0.292	0.267	0.553	1.000	0.252
	9	I am satisfied with the trustworthiness of the METHOD	0.454	0.305	0.284	0.454	0.346	0.372	0.433	0.252	1.000
TTP	1	The intent of the application is clear to me	1.000	0.326	0.376	0.597	0.254	0.442	0.620	0.319	0.321
	2	The application clearly describes how my data is processed from data submission to output	0.326	1.000	0.592	0.250	0.057	0.313	0.337	0.604	0.472
	3	The application provides a complete and detailed description of how MPC is used to protect my data	0.376	0.592	1.000	0.254	0.130	0.631	0.486	0.772	0.615
	4	Interaction with the application is clear and understandable	0.597	0.250	0.254	1.000	0.056	0.323	0.254	0.271	0.170
	5	The descriptions of MPC are complex	0.254	0.057	0.130	0.056	1.000	-0.005	0.101	0.072	0.151
	6	Understanding how the data is processed does not require a lot of my mental effort	0.442	0.313	0.631	0.323	-0.005	1.000	0.512	0.459	0.319
	7	Claims made by the application are clear and accurate	0.620	0.337	0.486	0.254	0.101	0.512	1.000	0.492	0.385
	8	The application is open and transparent in how it protects my data	0.319	0.604	0.772	0.271	0.072	0.459	0.492	1.000	0.519
	9	I am satisfied with the trustworthiness of the METHOD	0.321	0.472	0.615	0.170	0.151	0.319	0.385	0.519	1.000

SPSS Output A.4: Inter-Item Correlation Matrix: trustworthiness

Group		Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correla- tion	Squared Multiple Correla- tion	Cronbach's Alpha if Item Deleted	
MPC	1	The intent of the application is clear to me	28.5283	26.446	0.671	0.485	0.842
	2	The application clearly describes how my data is processed from data submission to output	28.2453	28.573	0.588	0.390	0.851
	3	The application provides a complete and detailed description of how MPC is used to protect my data	28.5472	30.214	0.394	0.475	0.867
	4	Interaction with the application is clear and understandable	28.6604	26.036	0.694	0.509	0.840
	5	The descriptions of MPC are complex	29.5472	27.137	0.609	0.490	0.849
	6	Understanding how the data is processed does not require a lot of my mental effort	29.1321	26.232	0.642	0.593	0.846
	7	Claims made by the application are clear and accurate	28.5472	27.099	0.680	0.574	0.842
	8	The application is open and transparent in how it protects my data	28.5472	28.753	0.563	0.579	0.853
	9	I am satisfied with the trustworthiness of the METHOD	28.5094	30.216	0.517	0.326	0.858
TTP	1	The intent of the application is clear to me	27.7963	23.863	0.605	0.642	0.812
	2	The application clearly describes how my data is processed from data submission to output	28.0370	23.546	0.571	0.439	0.815
	3	The application provides a complete and detailed description of how MPC is used to protect my data	28.5000	20.406	0.769	0.756	0.788
	4	Interaction with the application is clear and understandable	27.5926	25.378	0.396	0.425	0.833
	5	The descriptions of MPC are complex	28.3148	27.427	0.139	0.126	0.859
	6	Understanding how the data is processed does not require a lot of my mental effort	28.1296	23.134	0.574	0.515	0.815
	7	Claims made by the application are clear and accurate	27.8333	24.406	0.609	0.550	0.813
	8	The application is open and transparent in how it protects my data	28.3148	22.069	0.693	0.662	0.800
	9	I am satisfied with the trustworthiness of the METHOD	28.0741	24.108	0.571	0.422	0.816

Table A.19: Item-Total Statistics: trustworthiness

Group		1	2	3	4	5	6	7	
MPC	1	It feels safe contributing sensitive company data over the application	1.000	0.768	0.297	0.389	0.279	-0.069	0.485
	2	The use of METHOD gives me a feeling of security assurance	0.768	1.000	0.293	0.353	0.404	0.107	0.495
	3	Only I am able to view my contributed data	0.297	0.293	1.000	0.517	0.390	0.488	0.136
	4	The service provider cannot examine my data beyond my control	0.389	0.353	0.517	1.000	0.127	0.409	0.522
	5	I feel capable of using the application	0.279	0.404	0.390	0.127	1.000	0.173	0.276
	6	My data cannot be accessed by other contributors	-0.069	0.107	0.488	0.409	0.173	1.000	0.091
	7	I am satisfied with the security METHOD provides	0.485	0.495	0.136	0.522	0.276	0.091	1.000
TTP	1	It feels safe contributing sensitive company data over the application	1.000	0.882	0.434	0.373	0.167	0.448	0.438
	2	The use of METHOD gives me a feeling of security assurance	0.882	1.000	0.427	0.430	0.114	0.423	0.545
	3	Only I am able to view my contributed data	0.434	0.427	1.000	0.357	0.204	0.570	0.361
	4	The service provider cannot examine my data beyond my control	0.373	0.430	0.357	1.000	-0.061	0.361	0.281
	5	I feel capable of using the application	0.167	0.114	0.204	-0.061	1.000	-0.003	0.028
	6	My data cannot be accessed by other contributors	0.448	0.423	0.570	0.361	-0.003	1.000	0.469
	7	I am satisfied with the security METHOD provides	0.438	0.545	0.361	0.281	0.028	0.469	1.000

Table A.20: Inter-Item Correlation Matrix: security

Group		Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correla- tion	Squared Multiple Correla- tion	Cronbach's Alpha if Item Deleted
MPC	1	22.4717	10.831	0.556	0.673	0.737
	2	22.1887	10.579	0.636	0.657	0.718
	3	22.1132	11.756	0.541	0.513	0.741
	4	22.2642	10.967	0.580	0.552	0.731
	5	21.7925	12.475	0.402	0.317	0.767
	6	21.8302	13.144	0.279	0.389	0.788
7	21.8679	12.501	0.521	0.467	0.748	
TTP	1	20.8704	13.624	0.711	0.796	0.721
	2	20.9259	13.730	0.741	0.819	0.716
	3	20.6667	15.132	0.590	0.416	0.749
	4	21.1852	15.512	0.424	0.254	0.782
	5	20.1852	18.493	0.099	0.104	0.832
	6	20.6481	15.063	0.566	0.452	0.753
7	20.8519	15.449	0.528	0.387	0.760	

Table A.21: Item-Total Statistics: security

Group			1	2	3	4	5	6
MPC	1	The application provides a simple way to securely contribute data	1.000	0.594	0.128	0.638	0.355	0.385
	2	The application does not require expertise from multiple organizational departments	0.594	1.000	0.054	0.435	0.573	0.280
	3	The application provides an advantage over conventional data sharing practices	0.128	0.054	1.000	0.166	0.183	0.537
	4	When contributing data, no other party knows about my participation	0.638	0.435	0.166	1.000	0.341	0.438
	5	I feel less hesitant with contributing sensitive company data when using this METHOD application	0.355	0.573	0.183	0.341	1.000	0.445
	6	METHOD provides a simple solution to secure data contribution	0.385	0.280	0.537	0.438	0.445	1.000
TTP	1	The application provides a simple way to securely contribute data	1.000	0.187	0.332	0.411	0.326	0.588
	2	The application does not require expertise from multiple organizational departments	0.187	1.000	0.088	-0.077	0.171	0.441
	3	The application provides an advantage over conventional data sharing practices	0.332	0.088	1.000	0.342	0.485	0.273
	4	When contributing data, no other party knows about my participation	0.411	-0.077	0.342	1.000	0.499	0.228
	5	I feel less hesitant with contributing sensitive company data when using this METHOD application	0.326	0.171	0.485	0.499	1.000	0.339
	6	METHOD provides a simple solution to secure data contribution	0.588	0.441	0.273	0.228	0.339	1.000

Table A.22: Inter-Item Correlation Matrix: relative advantage

A.10. Repeated SPSS syntax solution using Python

```

spss_syntax=''
* Pyramid chart for {0}.
GGRAPH
  /GRAPHDATASET NAME="graphdataset"
                VARIABLES=COUNT([name="COUNT"]) {1} Group
                MISSING=LISTWISE REPORTMISSING=NO
  /GRAPHSPEC SOURCE=INLINE.
BEGIN GPL
  SOURCE: s=userSource(id("graphdataset"))
  DATA: COUNT=col(source(s), name("COUNT"))
  DATA: {2}=col(source(s), name("{3}"), unit.category())
  DATA: Group=col(source(s), name("Group"), unit.category())
  COORD: transpose(mirror(rect(dim(1,2))))
  GUIDE: axis(dim(1), label(""))
  GUIDE: axis(dim(1), opposite(), label(""))
  GUIDE: axis(dim(2), label(""))
  GUIDE: axis(dim(3), label("Experimental groups"),
             opposite(),
             gap(0px))
  GUIDE: legend(aesthetic(aesthetic.color), null())
  GUIDE: text.title(label("",
    " by Experimental groups"))
  SCALE: cat(dim(3), reverse(),
            include("MPC", "TTP"),
            sort.values("MPC", "TTP"))
  ELEMENT: interval(position({4}*COUNT*Group),
                    texture.pattern.interior(Group))
END GPL.
'''

```

```

list_of_variables = [
    "Q_TRUS_OBS_1",
    "Q_TRUS_OBS_2",
    "Q_TRUS_OBS_3",
    "Q_TRUS_COM_1",
    "Q_TRUS_COM_2",
    "Q_TRUS_COM_3",
    "Q_SECU_RIS_1",
    "Q_SECU_RIS_2",
    "Q_SECU_CON_1",
    "Q_SECU_CON_2",
    "Q_SECU_CON_3",
    "Q_SECU_CON_4",
    "Q_TRUS_1",

```

```
    "Q_TRUS_2",
    "Q_SIMP_1",
    "Q_SIMP_2",
    "Q_RELA_1",
    "Q_RELA_2",
    "Q_RELA_3",
    "Q_SIMPLICITY_RATING",
    "Q_REL_ADV_WILLING",
    "Q_TRUSTWORTHINESS",
    "Q_TRUSTWORTHINESS_WILLING",
    "Q_SECURITY",
    "Q_SECURITY_WILLING",
    "Q_OVERALL_WILLINGNESS",
]

for v in list_of_variables:
    print(spss_syntax.format(v,v,v,v,v))
```


A.11. Questionnaire deployed via Qualtrics^{XM}_®

Note: the block part notations (e.g. “block-part-1”) are not displayed in the deployed survey.

block-part-1

Introduction

This questionnaire aims to find out how organizations perceive the process of contributing data for knowledge sharing purposes, through a web application.

This questionnaire will take approximately 30 min to complete. It is completely anonymous.

For more information, please contact:

Masud Petronia

Delft University of Technology

m.n.petronia@student.tudelft.nl

NOTE: THIS SURVEY CANNOT BE PERFORMED ON A MOBILE PHONE.

Please read the following statements:

- I consent voluntarily to be a participant in this study and understand that I can withdraw from the study at any time, without having to give a reason.
- I understand that this questionnaire does not collect any personal information about me. In other words, this questionnaire is completely anonymous.
- I give permission for the anonymized data that I provide to be archived in local computers at TU Delft and in the TU Delft data repository so it can be used for future research and learning.
- I understand that information I provide is used for scientific publications and presentations.

By completing this questionnaire, I confirm that I have read the above statements and I agree with them. Please close this window if you do not agree with them.

I agree and wish to proceed

Part I

Knowledge sharing by means of an online web application

For this part assume a service provider. This service provider offers knowledge sharing services. It does this by collecting data from many organizations and uses this data to perform analytics. The results from the analytics are then shared with the organizations that have contributed data. The data needed for the analytics is sensitive data. That is, organizations contribute sensitive data for the analytics.

The service provider uses an online web application to collect the data. The application service provider promises contributors that their data remains confidential at all times. Only the output of the analytics will be shared.

Assume you want to use such an application because the output provides value to your organization. You must submit sensitive company (data that may not be leaked). For the following questions, please rate your expectations for such an application.

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
The intent of the application must be clear to me.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The application must clearly describe how my data is processed from data submission to output.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The application must provide a complete and detailed description of security measures used to protect my data.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
Interaction with the application must be clear and understandable.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Descriptions of security measures used to protect my data may be complex.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
Understanding how the data is processed must not require a lot of my mental effort.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
Claims made in the application must be clear and accurate.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The application must be open and transparent in how it protects my data.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
I must be convinced that my data is not used for other purposes than stated.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Malicious parties must not be able take control of my information if I use this application.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
It must feel safe to contribute sensitive company data over this application.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I must have a feeling of security assurance.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
Only I must be able to view my contributed data.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The application service provider may examine my data if they need to.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I must feel capable of using this application.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My data may never be accessible to other contributors.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
The application must provide a simple way to securely contribute data.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
The application must not require expertise from multiple organizational departments.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
The application must provide an advantage over conventional data sharing practices.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
When contributing data, no other party should know about my organization's participation.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
Without security measures I would not contribute sensitive company data through a web application even if it provides value.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

block-part-2-3-gr-1

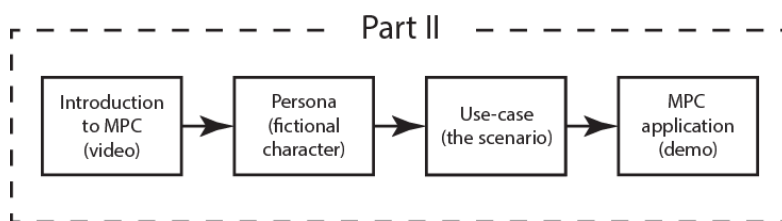
Part II

Multi party computation knowledge sharing application

For this part we will introduce you to multi party computation (MPC). We will first start by describing what MPC is and how it works through a 3-minute video.

First, a persona is provided to you. The goal of the persona is to shape the context in which the MPC application is used. Then a use-case is provided. The use-case describes the scenario in which the application is used. Then you will submit (fictional) data through this

application. You are provided with all the information you need. For clarity, below flow diagram illustrates these steps in the order presented.



Introduction to multi party computation

Open the link below in a new tab. This will open a 3 minute introductory video of multi party computation. After you finish watching this video, return to this survey.

<https://heaped.herokuapp.com/introduction-to-mpc>

Note: this video has audio and subtitle.

Persona

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 distribution center makes only use of labor (no machines) for the order fulfillment process. You know of 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.

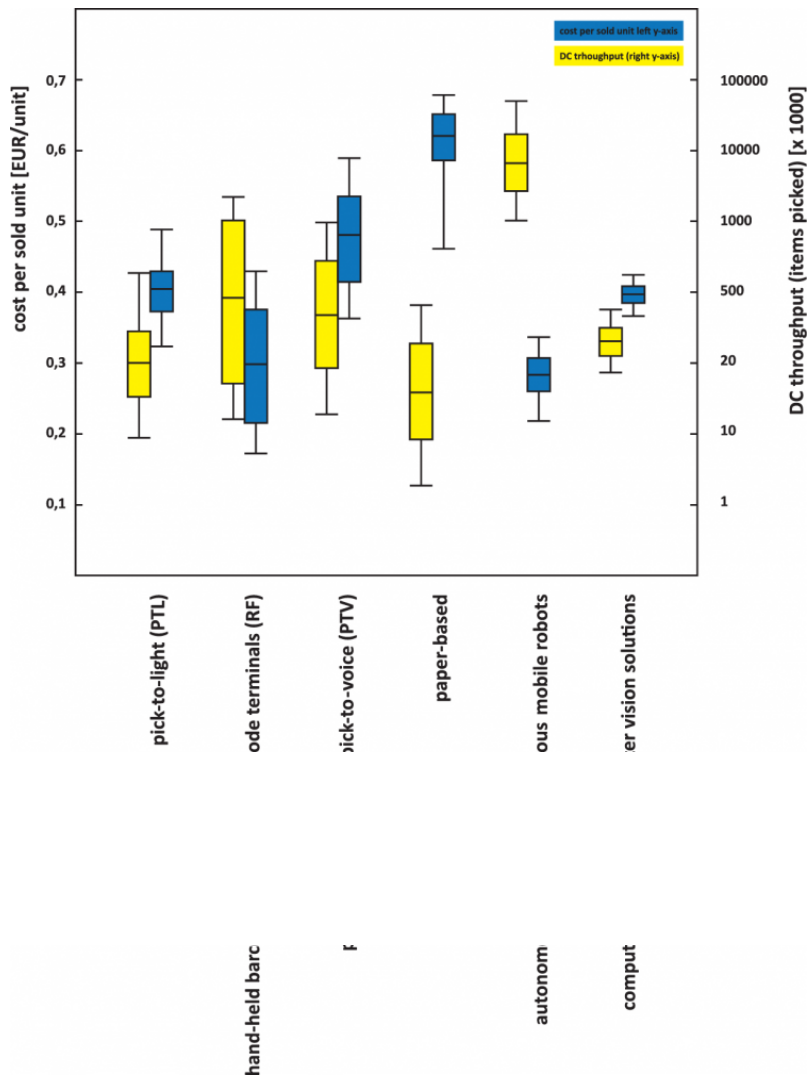
Use case

You found a multi party computation application called PEBE (PERformance BENCHmarking) available for distribution centers. You know that multi party computation applications allow participants to share knowledge without sharing the underlying data. As a results multi party computation users contribute data and do not share their data – they only share knowledge, and their data is confidential by design.

This application requires 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)



MPC application: step 1

The application makes use of an Excel template file for the input data. You have requested the warehouse managers to gather the requested information. This information is returned to you. Open the link below in a new tab, and download the input file. This is the Excel template file. Save this file on your machine (an easy to find location such as your desktop):

<https://heaped.herokuapp.com/input-file>

MPC application: step 2

Open the link below in a new tab, and proceed with step 3. The link will open the MPC web application.

<https://heaped.herokuapp.com/x82>

Note: this is a demonstration application used for research purposes. Several features are disabled in order to conduct this online experiment.

MPC application: step 3

Complete the following tasks and mark YES when completed (use this as a checklist).

	Yes	No
Read the introduction text of the application.	<input type="radio"/>	<input type="radio"/>
To save time, skip inputting company data (ID, Code, Location, Channel, etc.).	<input type="radio"/>	<input type="radio"/>
Upload your input data (downloaded at step 1)	<input type="radio"/>	<input type="radio"/>
Check the type of data being shared	<input type="radio"/>	<input type="radio"/>
Describe (to yourself) what happens to your data after you submit it	<input type="radio"/>	<input type="radio"/>

	Yes	No
Submit your data	<input type="radio"/>	<input type="radio"/>

MPC application: step 4

You have been provided a code (example J86) after you have completed all tasks. Enter this code here:

Part III Your perceptions

In this part we want to understand your perceptions of the multi party computation application you just used.

To what extent do you agree with the following statements?

Strongly disagree Disagree Neither disagree or agree Agree Strongly agree

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
The intent of the application is clear to me.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The application clearly describes how my data is processed from data submission to output.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The application provides a complete and detailed description of how MPC is used to protect my data.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
Interaction with the application is clear and understandable.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
The descriptions of MPC are complex.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Understanding how the data is processed does not require a lot of my mental effort.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
Claims made by the application are clear and accurate.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The application is open and transparent in how it protects my data.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
My input data cannot (or will not) be used for purposes than stated.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Malicious parties are not able take control of my information.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
It feels safe contributing sensitive company data over the application.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The use of MPC gives me a feeling of security assurance.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
Only I am able to view my contributed data.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The service provider cannot examine my data beyond my control.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I feel capable of using the application.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My data cannot be accessed by other contributors.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
The application provides a simple way to securely contribute data.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
The application does not require expertise from multiple organizational departments.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
The application provides an advantage over conventional data sharing practices.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
When contributing data, no other party knows about my participation.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I feel less hesitant with contributing sensitive company data when using this mpc application.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

MPC provides a simple solution to secure data contribution.

- Strongly disagree
- Disagree
- Neither disagree or agree
- Agree
- Strongly agree

From the previous question it seems that you are not satisfied with the solution the application provides. Please describe your reasoning:

I would be willing to use MPC based on the **solution** it provides to secure data contribution.

- Strongly disagree
- Disagree
- Neither disagree or agree
- Agree

Strongly agree

I am satisfied with the trustworthiness of the MPC application.

- Strongly disagree
 Disagree
 Neither disagree or agree
 Agree
 Strongly agree

From the previous question it seems that you are not satisfied with the trustworthiness of the application. Please describe your reasoning:

I would be willing to use this application based on its **trustworthiness**.

- Strongly disagree
 Disagree
 Neither disagree or agree
 Agree

Strongly agree

I am satisfied with the security MPC provides.

- Strongly disagree
 Disagree
 Neither disagree or agree
 Agree
 Strongly agree

From the previous question it seems that you are not satisfied with the security of the application. Please describe your argument:

I would be willing to use this application based on the **security** provided by MPC.

- Strongly disagree
 Disagree
 Neither disagree or agree

- Agree
- Strongly agree

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 an MPC application.

- Strongly disagree
- Disagree
- Neither disagree or agree
- Agree
- Strongly agree

From the previous question it seems that you are not willing or fully willing to use MPC applications. Please describe your argument:

How familiar are you with multi party computation before conducting this survey?

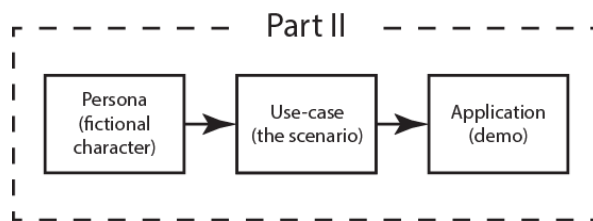
- Not all familiar
- Slightly familiar
- Somewhat familiar
- Moderately familiar
- Extremely familiar

block-part-2-3-gr-2

Part II

Knowledge sharing application

For this part we will introduce you to a real application through a persona and a use-case. The goal of the persona is to shape the context in which the application is used. Then you will be provided a use-case. The use-case describes the scenario in which the application is used. Then you will submit (fictional) data through this application. You are provided with all the information you need. For clarity, below flow diagram illustrates these steps in the order presented.



Persona

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 distribution center makes only use of labor (no machines) for the order fulfillment process. You know of 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.

Use case

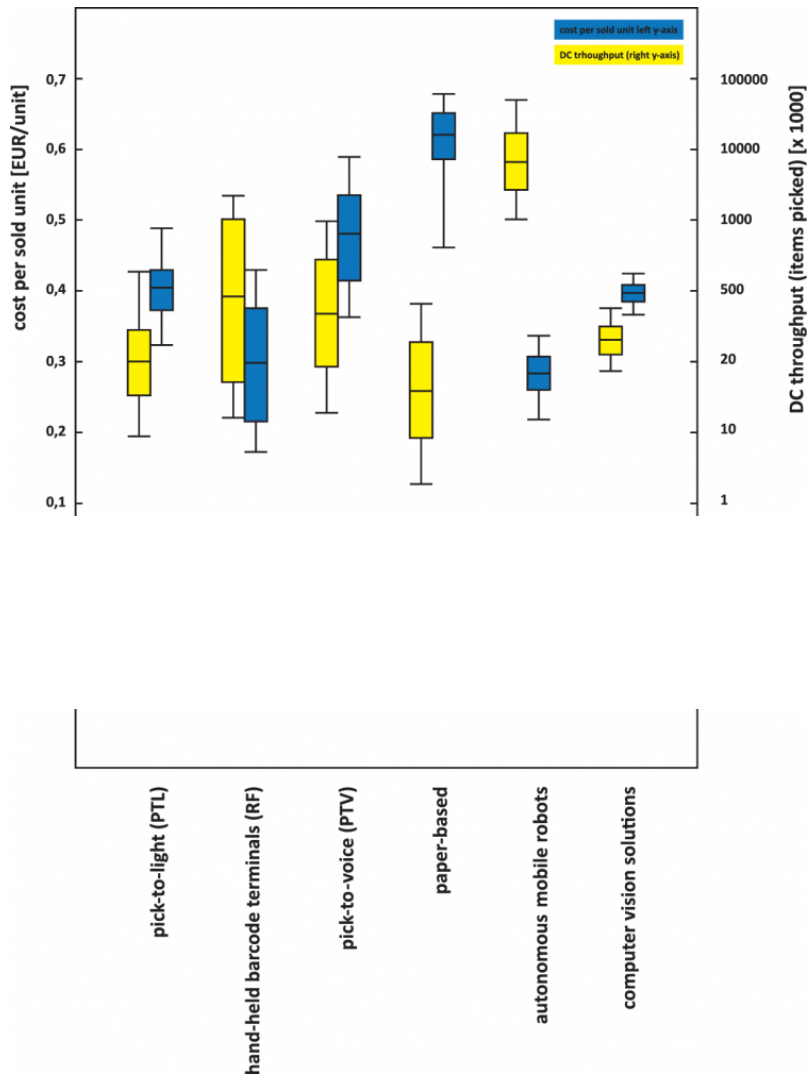
You found a trusted third party (TTP) application called PEBE (PPerformance BEnchmarking) available for distribution centers. You know that TTPs work under contracts or agreements to ensure confidentiality.

This application requires 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)



Application: step 1

The application makes use of an Excel template file for the input data. You have requested the warehouse managers to gather the requested information. This information is returned to you. Open the link below in a new tab, and download the input file. This is the Excel template file. Save this file on your machine (an easy to find location such as your desktop):

<https://heaped.herokuapp.com/input-file>

Application: step 2

Open the link below in a new tab, and proceed with step 3. The link will open the MPC web application.

<https://heaped.herokuapp.com/Q69>

Note: this is a demonstration application used for research purposes. Several features are disabled in order to conduct this online experiment.

Application: step 3

Complete the following tasks and mark YES when completed (use this as a checklist).

	Yes	No
Read the introduction text of the application.	<input type="radio"/>	<input type="radio"/>
To save time, skip inputting company data (ID, Code, Location, Channel, etc.).	<input type="radio"/>	<input type="radio"/>

	Yes	No
Upload your input data (downloaded at step 1)	<input type="radio"/>	<input type="radio"/>
Check the type of data being shared	<input type="radio"/>	<input type="radio"/>
Describe (to yourself) what happens to your data after you submit it	<input type="radio"/>	<input type="radio"/>
Submit your data	<input type="radio"/>	<input type="radio"/>

Application: step 4

You have been provided a code (example J86) after you have completed all tasks. Enter this code here:

Part III Your perceptions

In this part we want to understand your perceptions of the application you just used.

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
The intent of the application is clear to me.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The application clearly describes how my data is processed from data submission to output.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The application provides a complete and detailed description of how it protects my data.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
Interaction with the application is clear and understandable.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
The descriptions of security measures are complex.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Understanding how the data is processed does not require a lot of my mental effort.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
Claims made by the application are clear and accurate.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The application is open and transparent in how it protects my data.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
My input data cannot (or will not) be used for purposes than stated.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Malicious parties are not able take control of my information.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
It feels safe contributing sensitive company data over the application.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I have a feeling of security assurance.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
Only I am able to view my contributed data.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The service provider cannot examine my data beyond my control.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I feel capable of using the application.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My data cannot be accessed by other contributors.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
The application provides a simple way to securely contribute data.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
The application does not require expertise from multiple organizational departments.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Neither disagree or agree	Agree	Strongly agree
The application provides an advantage over conventional data sharing practices.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
When contributing data, no other party knows about my participation.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I feel less hesitant with contributing sensitive company data when using this application.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

This application provides a simple solution to secure data contribution.

- Strongly disagree
- Disagree
- Neither disagree or agree
- Agree
- Strongly agree

From the previous question it seems that you are not fully satisfied with the solution this application provides. Please describe your reasoning:

I would be willing to use this application based on the **solution** it provides to secure data contribution.

- Strongly disagree
- Disagree
- Neither disagree or agree
- Agree
- Strongly agree

I am satisfied with the trustworthiness of the application.

- Strongly disagree
- Disagree
- Neither disagree or agree
- Agree
- Strongly agree

From the previous question it seems that you are not satisfied with the trustworthiness of the application. Please describe your reasoning:

I would be willing to use this application based on its **trustworthiness**.

- Strongly disagree
- Disagree
- Neither disagree or agree
- Agree
- Strongly agree

I am satisfied with the security this application provides.

- Strongly disagree
- Disagree
- Neither disagree or agree
- Agree
- Strongly agree

From the previous question it seems that you are not satisfied with the security of the application. Please describe your argument:

I would be willing to use this application based on the **security** provided by the TTP.

- Strongly disagree
- Disagree
- Neither disagree or agree
- Agree
- Strongly agree

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 trusted third party application.

- Strongly disagree
- Disagree
- Neither disagree or agree
- Agree
- Strongly agree

From the previous question it seems that you are not willing or fully willing to use this application. Please describe your argument:

block-part-4

Part IV General Information

Only a few general questions remaining.

What is your gender?

- Male
- Female
- Prefer not to say
- Other

What is your year of birth? (e.g. 1980)

Which best describes your employment situation?

- Working - Full Time (at least 32 hours per week)
- Working - Part Time
- On leave but still employed
- Unemployed (for longer than 6 months) and looking for work
- Wanting to work, but unemployed due to personal reasons
- Student
- Retired

- No answer/unknown
- Temporarily laid off
- On sick leave but still employed

What is your occupation, or what kind of work do/did you do?

In what industry is your organization, or the organization you work, operational (e.g. aerospace, automotive, etc.)?

What is your country of residence?

How many employees does this organization have?

1

- 2-10
- 11-100
- More than 100
- I do not know

To what extent are you involved in developing new products/services/improvements?

- Never
- Rarely
- Sometimes
- Often
- Always

What is your highest educational degree earned?

- Undergraduate (BA, BSc, other)
- High school diploma
- Graduate degree (MA, MSc, other)
- Technical/Community college
- Secondary education

- Doctorate degree (PhD, other)
- No formal qualifications
- Not applicable/I do not know

Please feel free to leave behind any information you would like to share with us

			Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correla- tion	Squared Multiple Correla- tion	Cronbach's Alpha if Item Deleted
MPC	1	The application provides a simple way to securely contribute data	19.5472	6.945	0.637	0.541	0.703
	2	The application does not require expertise from multiple organizational departments	19.6038	6.513	0.569	0.513	0.719
	3	The application provides an advantage over conventional data sharing practices	19.3396	8.306	0.246	0.301	0.796
	4	When contributing data, no other party knows about my participation	19.6038	6.398	0.577	0.455	0.717
	5	I feel less hesitant with contributing sensitive company data when using this METHOD application	19.7170	7.091	0.542	0.421	0.726
	6	METHOD provides a simple solution to secure data contribution	19.3585	7.927	0.593	0.487	0.730
TTP	1	The application provides a simple way to securely contribute data	18.1481	7.827	0.550	0.437	0.648
	2	The application does not require expertise from multiple organizational departments	18.0185	8.735	0.230	0.244	0.755
	3	The application provides an advantage over conventional data sharing practices	18.3519	8.572	0.453	0.274	0.679
	4	When contributing data, no other party knows about my participation	18.0926	8.652	0.407	0.363	0.691
	5	I feel less hesitant with contributing sensitive company data when using this METHOD application	18.5185	7.235	0.543	0.400	0.647
	6	METHOD provides a simple solution to secure data contribution	18.1296	7.889	0.588	0.474	0.640

Table A.23: Item-Total Statistics: relative advantage

