

FACTORS THAT INFLUENCE THE DECISION TO OUTSOURCE MONITORING SERVICE TO CLOUD

Different stakeholder perspectives on cloud based monitoring service

Master's Thesis
in Information Systems Science

Author:
Driton Gashi

Supervisor:
Najmul Islam

7.3.2017
Turku

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin OriginalityCheck service.

TABLE OF CONTENTS

1	INTRODUCTION	7
1.1	Motivation for this research	7
1.2	Research question and objectives	8
1.3	Research approach	9
2	LITERATURE REVIEWS	10
2.1	Theories.....	10
2.1.1	Transaction cost economics theory.....	11
2.1.2	Diffusion of innovations theory.....	11
2.1.3	Technology-organizational-environmental framework (TOE)	12
2.2	Cloud literature review	12
2.2.1	Cloud adoption evolution.....	13
2.2.2	Different deployment model of cloud services	14
2.2.3	Cloud as a strategic innovation.....	16
2.2.4	Cost reduction and payment methods	19
2.2.5	New business models.....	21
2.2.6	Technological advantages	22
2.2.7	Cloud as an increasing disruptive technology	25
2.2.8	Cloud challenges.....	27
2.3	Monitoring service review	34
2.3.1	Monitoring service products.....	34
2.3.2	Monitoring service characteristics.....	36
2.3.3	Monitoring solutions as part of business continuity plan	38
2.3.4	Support and maintenance requirements	39
2.3.5	Technological advantages	40
2.3.6	Stakeholder benefits.....	41
3	RESEARCH PORCESS	42
3.1	Methodology	42
3.2	The case company and interviews	44
3.3	Empirical research analysis.....	46
4	RESULTS AND DISCUSSION.....	48
4.1	Save investments are attractive	48
4.2	Cost is often factor in decision making	49
4.3	Better product support is expected	51
4.4	In-house versus cloud uncertainty	52

4.5	Security concerns are real barrier	52
4.6	Part of competitive strategy.....	53
4.7	Dependencies found to be risk factor	54
4.8	SLA requirements are doubtful	55
5	CONCLUSIONS	57
5.1	Research limitations.....	59
5.2	Suggestions for future research	60
6	REFERENCES	61
7	APPENDIXES	70
7.1	APPENDIX 1: INTERVIEW COVER LETTER.....	70
7.2	APPENDIX 2: INTERVIEW QUESTIONS.....	71
7.3	APPENDIX 3: PILOTED MAAS	72
7.4	APPENDIX 4: PERSONAL DATA ACT (523/1999).....	73

LIST OF FIGURES

Figure 1.	Cloud delivery models and their components (Fernandes et al. 2014).	16
Figure 2.	Strategic approach to implement cloud technologies (Ross & Blumenstein 2013)18	
Figure 3.	The value network of firm “Game Cluster” showing different partnerships to make their offerings available to the customers (Ojala & Tyrväinen 2011)22	
Figure 4.	Components of Microsoft Office 365 (Mihaela 2014).	25
Figure 5.	SME profiles showing cloud adopters (Doherty & Carcary & Conway, 2015)	26
Figure 6.	Four different risk categories that might occur affecting business continuity (Zawila-Niedzwiecki 2010).	38
Figure 7.	A picture created based on Nijaz and Moon 2009 study showing factors that affect PCP and consequences of not having such.	39
Figure 8.	Findings from cloud studies and monitoring solution studies making up MaaS literature review.	42

Figure 9. Holistic view of thesis research process.....43

Figure 10. Overview of customer stakeholder domain.....44

Figure 11. Screenshot from MaaS application tested.72

LIST OF TABLES

Table 1. Main IS theories mentioned on the cloud computing literatures reviewed.. 10

Table 2. depth of cloud security innovations area showing number of patents filed
(Khansa & Zobel 2014).....29

Table 3. A table created based on Aleem and Christopher’s (2013) survey regarding
top cloud computing concerns.29

Table 4. An overview of cloud monitoring tools (Alhamazani et al. 2015, 375).....35

Table 5. Comparison between on premise and cloud monitoring services (source:
self-study).35

Table 6. Different monitoring layers of a system.....37

Table 7. Monitoring levels and basic features.....37

Table 8. Profiles of the interviewed company representatives.....45

Table 9. Cloud platform benefit ratings (Gowda & Subramanya 2015, 40).....50

Table 10. Firewall configuration table showing rules used on FAT project.....73

ABBREVIATIONS

Acronym	Definition
API	Application programming interfaces
B2B	Business-to-Business
B2C	Business-to-Costumer
BCP	Business Continuity plan
CPU	Central Processing Unit

CRM	Customer relationship management
DoS	Denial of Service
ERP	Enterprise resource planning
EU	European Union
FAT	Factory Acceptance Test
GUI	Graphical User Interface
HPC	High Performance Computing
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a service
IP	Internet Protocol
IPTV	Internet Protocol Television
IS	Information System
ISP	Internet service provider
IT	Information Technology
LAN	Local Area Network
MaaS	Monitoring as a service
NIST	The National Institute of Standards and Technology
PaaS	Platform as a service
PC	Personal computer
R&D	Research and development
SaaS	Software as a service
SAS	Statement on Auditing Standards
SLA	Service Level Agreement
SME	Small to medium-sized
SNMP	Simple Network Management protocol
TOE	Technology-organizational-environmental
TV	Television
US	United States
VPN	Virtual private network
VPN	Virtual private network
WWW	World Wide Web
XaaS	Anything as a service

1 INTRODUCTION

This chapter discussed motivation for this work, the research questions and then finally the research approach. The leading factor to this motivation is the fact that no scientific studies have been done on cloud based monitoring as a service. This chapter presents research questions and the approach to answering these questions.

1.1 Motivation for this research

Monitoring services are important IT systems that predict and report possible information technology (IT) system failures so that business critical services are not interrupted and continue to run. They are important part of business continuity or disaster recovery plans. However, monitoring services as well as other security enforcements do not bring direct benefits/revenues to a firm. Hence, often firms have no monitoring service or a business continuity plan. Often firms do not understand that monitoring solutions are important strategic plans. Some firms have learned this in hard way after a major disaster that might be result of from human or natural factors. Only 20 per cent of IT managers understood strategic values on these enforcements (Lindström 2012, 270). Organizations must have intelligent systems that predict possible threats using some kind of mechanisms to collect reports from all kind of IT systems and then detect unusual behaviors of the systems. Business critical services require constant monitoring, real-time anomaly detection, live diagnostics, and regular health check reporting to ensure business continuity (Stewart, 2009). Monitoring solutions can predict a system failure and report them so that business critical IT systems are fixed on time before business is interrupted. These monitoring solutions were traditionally hosted and maintained on-premise by the IT team. On-premise solution means software and/or hardware installed and running in-house on a firms building or datacenters.

Traditional on-premise systems continue to get harder to maintain in addition to other disadvantages like cost of operation and complexity. Firms choose to outsource many IT service for different economic and strategic reasons as IT investment continue to get more strategic (Gowda & Sbramanya 2015, 46). As cloud services are becoming common, moving traditional monitoring service to cloud would inherit all cloud based opportunities and advantages in terms of better payment methods and low or reduced capital investments (safe investments) (Corkern et al 2015).

Cloud computing is a scientific revolution that is impacting and transforming all organizations (Sheree & Sara & Billy 2915). Cloud services are becoming common platforms for countless applications. Anything now is being offered as a service (XaaS) (Mladenow & Kryvinska & Strauss 2012, 214). The “monitoring as a service” acronym

(MaaS) will be used in this study to describe monitoring service hosted on a cloud infrastructure.

Cloud computing are shared computer resources that can be access via network in type of pay-per-use service (Mell & Grance 2011). Cloud enables access to IT software, hardware and other resources over the Internet technologies. It is expected that by 2020 the cloud market will grow to \$159.3 billion from \$25.5 billion in 2011 and almost all services will be hosed on cloud (Boillat & Legner 2013, 40). Regardless where IT infrastructure, platforms or software are hosted, they are important assets helping business functions directly or indirectly.

When searching online databases such as ABI/INFORM Collection (ProQuest) using keyword “cloud computing”, thousands of articles are found. Karunakaran (2015) reviewed 155 studies on cloud computing focused on different research areas such as cloud economics, strategy, information system (IS) policy issues, technology adoptions, etc. Different authors have been studying general benefits, drawbacks and other characteristics of cloud computing provided in different platforms such as infrastructure as a service, platform as a service or software as a service (Alali, & Yeh 2012, 14). All these findings on cloud produce holistic and general findings that might or might not fit the monitoring as a service (MaaS) concept. Cloud consists of countless applications that often do not share same benefits or barriers with each other. For example a banking application and a booking system application do not share the same benefits drawbacks and barriers if they are hosted on cloud (Wisniewski 2013, 88).

When using “Monitoring as a Service” keyword, only 44 trade journals and 9 scholarly journals were found. None of the journals found contained a scientific study on MaaS that would show benefits, challenges or any scientific studies of the application in cloud. This study reviewed 55 articles relevant to monitoring and cloud services in order to find common factors that are relevant to these two, hoping to produce valuable findings related to MaaS model.

This study focuses on monitoring service hosted in cloud infrastructure and the factors that make firms deploy MaaS. Different from traditional monitoring services where hardware and/or software were provided to the customer, this study is focused on a service delivery model where no software or hardware good is provided to the customer.

1.2 Research question and objectives

As mentioned on the section 1.1 , there are still firms that have no understanding that monitoring services are important IT assets that ensure that system failures are predicted before they occur and/or report when these have occurred so that fix is done immediately and business continues to flow. This study aims in finding those key factors that help

firms understand values that a cloud based monitoring system brings to all stakeholders including customer and providers. The simple questions this thesis work will try to answer are:

- What are the key factors that influence the decision to order cloud based monitoring service?
- What benefits firms gain from outsourcing monitoring function to cloud based delivery model?

When searching online libraries for monitoring services, the search engine returns often articles that are very narrow, single-purpose monitoring solutions (Silver 2010, 8). Because there are thousands of IT systems deployed worldwide, it would be impossible to come up with a list of benefits that a monitoring solution would provide to all systems. Articles on monitoring services are most of the time very technical, trying to solve a technical need or often, not related to IT asset monitoring. For example a lot of studies are done on monitoring related to health care as well economics and environment monitoring. Hence, monitoring literature in IT assets is poor in terms of values, benefits or other characteristics studies.

1.3 Research approach

A keyword “outsourcing + cloud” and “monitoring + service” were used with a “journals” filter as a primary article selection criteria. An important attention/review depth was put on articles that reported valuable and scientific studies based on quantitative researches. Qualitative research studies also reviewed which made the majority of literatures reviewed. The empirical study of this thesis work is based on qualitative research.

A pilot project is conducted as result of this thesis work. Findings from the articles reviewed and the IS theory were used to construct the qualitative interview questions. The data collected from interviewed stakeholders were analyzed using thematic analysis procedure as one of the most used forms of analyzing data gathered from qualitative researches (interviews). Finally results from the interviewed are listed and then discussed on the final article. Cloud literature and monitoring service literature will make the cloud based monitoring service

2 LITERATURE REVIEWS

This chapter discusses briefly theories relevant to cloud computing to be continued with cloud studies and then monitoring service studies.

2.1 Theories

When searching online databases using “cloud + theory”, most of the studies are based on Transaction Cost Economics theory. Theories found on cloud studies are listed on o Table 1. A lot of articles have no theories associated to them. For example, Qian and Palvia (2013) studied the strategic impact of cloud computing but used no theory because authors claim that there is no such ready-made to be used.

Journal reviewed during this thesis study discovered two significant factors that influence decision to outsource an IT function. The first factor is related to the cost savings or avoiding capital investment.

Table 1. Main IS theories mentioned on the cloud computing literatures reviewed

IS theory:	Nr of times found on articles
Portfolio theory	1
Game theory	3
Transaction cost economics	7
Resource dependency theory	3
Resource-based view of the firm	3
Agency theory	3
Diffusion of innovations theory	2
Institutional theory	1
Social exchange theory	1
Social capital theory	1
Technology-Organization-Environment framework	3

The theory mostly used when evaluating cost is the Transaction cost economics reflecting to the main factor that is transaction cost. In addition to costs, articles reviewed in this study find technology and innovations to be important factor. Therefore the Technology-Organization-Environment framework and Diffusion of innovations theory will be briefly reviewed.

2.1.1 *Transaction cost economics theory*

Transaction cost economics theory is the dominant theory in cloud studies (Ray 2016, 12). Hence, many researches have used as a theoretical framework to understand firms decision related to cloud migrations. What makes the transaction cost economics attractive theory is that it helps firms evaluate the degree of outsourcing that is relevant to cloud service orderings as well. Williamson (2010), one of the authors of the transaction cost economics highlights that "*any issue that arises as or can be reformulated as a contracting problem can be examined to advantage in transaction cost economizing terms*". Also articles reviewed during this thesis work show that transaction cost economics is mostly used theory to help cloud related decisions (Table 1). Cloud outsourcing model is attractive for researches because it is found to have impact on costs (Schwarz et al 2009) that often is the determinant factor of outsourcing IT systems (Lacity and Willcocks, 2014). The popularity of the transaction cost economics on cloud studies is associated also to the benefits that cloud brings in terms of cost savings and other transactions costs evaluations that might pup up. Transaction cost economics is focused on reducing transaction costs that can be many (Schwarz & Jayatilakay & Goles, 2009). Before cloud computing model existed, transaction cost economics theory was used to evaluate the make-or buy decisions (Williamson 2007). Although this theory is old, it is still being widely used for software and other IT outsourcing decisions (Schneider & Sunyaev, 2016). The transaction cost economics main goal is to provide a better cost structure and reduce transactions cost related to service orderings that bring no values. In cloud deployments, these services are related to searching and finding the cloud provider, deciding what service to use, training, etc.

Transaction costs are driven by three factors: 1. Frequency of occurrence, 2. Asset specificity, and 3. Uncertainty (Baozhou & Rudy & Andrew 2015, 758). Asset Specificity consist of three main categories: site, physical (also referred as technical) and human asset (Schneider & Sunyaev 2016). Uncertainty is linked to many unknown characteristics of cloud such as security, reliability and other unknown parameters associated to cloud offerings (Ray 2016, 12).

2.1.2 *Diffusion of innovations theory*

The Diffusion of innovations theory is on old theory but still widely used. The theory analyses how innovations are adopted within social members. The diffusion of innovation is a process that begins slowly with few influenced people called "Innovators", to then continue with "Early adopters", the "majority" and then "laggards" (Etro, 2011). Each group has different characteristics towards accepting or rejecting new innovations.

The first two groups are forward looking people willing to adopt new technologies. They however make small but important group. New innovations have to go through different stages before they are adopted. (Willcocks & Venters & Whitley 2013, 185). Firms are must provide benefits to all these groups to tha the innovations are considered successful.

Diffusion of innovations theory however is missing lot of characteristics related to cost and risks that are important.

2.1.3 Technology-organizational-environmental framework (TOE)

TOE defines three important innovations factors that influence cloud adoptions: technological, organizational and environmental context (Gutierrez et al. 2015; Gangwar et al. 2015). Many late studies use Technology-organizational-environmental framework theory to study factors that firms consider when adopting cloud theories (Gutierrez & Boukrami & Lumsden, 2015). The TOE technology element describes best how technology can create innovations that are often seen as key to solving business problems (Ray 2016; Gangwar & Date & Ramaswamy, 2015). Gangwar, Date and Ramaswamy (2015) uses TOE variables to develop a conceptual framework based on a study reviewing data from 280 companies. Authors point out that main variables influencing the adoption to cloud are associated with the technological and organizational factors.

Yazn, Papagiannidis and Li (2013, 253) argue that TOE framework is more relevant to study innovation adoptions because diffusion of innovation theory does not have the environment context. The environment context relates to competitors, technologies and other elements surroundings where business is conducted.

2.2 Cloud literature review

There are a lot of studies on cloud computing as a general concept that have produced different results. For example security related concerns are claimed to be the biggest factors hindering firms to move to cloud (Doherty et al. 2015; Wu et al. 2013; Blumenthal 2011). However, other researches find security less relevant because they claim that cloud providers have more knowledge and resources to apply security enforcements compared with on-premise installations on SME firms (Corkern & Kimmel & Morehead 2015, 16). Other studies find security to be the least concern when considering clouds because there are other bigger challenges like availability of a cloud service (Blumenthal, 2011).

2.2.1 Cloud adoption evolution

Cloud has arisen from IT outsourcing. In the past “virtualization” and “IT outsourcing” terminologies were used as terms to describe cloud computing ideas (Yazn & Papagiannidis & Li 2013, 226). Schneider and Sunyaev (2016) study on IT outsourcing reveals that most of factors that drive the sourcing decision remain the same for cloud computing. They conclude that that cloud services have emerged from IT outsourcing and both share common benefits. IT outsourcing services were often multi-year commitments that have sometimes had poor performances. The failures to deliver reliable IT project is a reason why many firms terminate IT outsourcing agreements and choose to adopt cloud based short-term IT projects provided by different vendors (Dhar 2012, 672). Cloud computing advantages over the IT outsourcing are those of self-service, on-demand and usage-based contracts. Aspects that differentiate cloud services from early IT outsourcings services are related to “on-demand” service model introduced in clouds, removing the need for starting fees and long contacts. The other advantage of cloud is that customer pays for resources used rather than reported (Wisniewski 2013).

Findings on factors that drive cloud computing migration decision are mostly related to the technological aspects and cost savings. Cloud computing technology is considered as evaluation of two different elements; the virtualization technology and the other one that is focus on the customer orientation and service based approach (Venters & Whitley, 2012).

As services are migrated to cloud, a smaller IT team is needed and workload of hardware support, updates and regular backups are transferred to cloud provider (Enslin 2012). Factors that lead to success of cloud industries in Taiwan are found to be “strategic resources allocation” as the most important element on their business model offering cloud services (Lin et al. 2015). Being able to strategically allocate software, hardware and human resources is indeed important business approach to better allocate resources on projects that generate more revenues.

Cloud computing innovations have huge impact on cost structure affecting directly job creations and reallocations of jobs in IT sector, public finances, etc. (Etro 2011; Madhavaiah & Bashir & Shafi 2012, 163). Cloud solutions have made IT department smaller reducing the need for expert for every system (Catinean & Căndea 2013). Hence, the technical knowledge need is decreasing and the need for management skills are increasing. European health sector is an example where cloud migration that has had huge impact on cost saving and also enabling them to allocated IT personnel to more applicable tasks (Etro, 2011).

Cloud is disruptive technology and as such, many IT jobs will be lost. However, reallocation of jobs is believed to be easily done to different tasks within same organization in addition to managing cloud ordered services (2011, 9, 17).

2.2.2 *Different deployment model of cloud services*

Not only private users but also every business is using cloud services. When they publish something on the social media like Facebook, Youtube, LinkedIn, etc, these are all cloud services. In addition, often mail server and communication tools like Skype for Business are common to be hosted in cloud. The National Institute of Standards and Technology (NIST) (Mell & Grance 2011) defines cloud computing as a “... *model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*”.

Cloud infrastructures are computer resources hosted on a third party datacenter. These are on-demand pay-for-use services arranged on four different deployment models listed below.

- A *private cloud* aims to provide better security and protection (Dhar 2012, 3) as it is provided to a single organization. This means that the cloud infrastructure can be hosted within organizations facilities managed by the in-house IT team or outsourced support (Fernandes et al. 2014). Security however requires trained IT staff, clear policies/standards and modern firewall infrastructure to protect them from the Internet. Security and availability are two main factors for private clouds to be still deployed. However they are very costly investments for small to medium (SME) firms. Private clouds are deployed also to solve legal issues in case a firm is obligated to keep data in-house (Wisniewski 2013). In theory, a better control of data security and privacy can be achieved with private clouds, but nevertheless, these deployments are subject to cyber-attacks too like any service.
- Public clouds are services offered to multiple organizations. These are shared resources over the Internet provided by a third party to different customers (Ray 2016). Public clouds are the most deployed cloud services (Wisniewski 2013). Firms providing this type of cloud are for example Google, Microsoft, Amazon, etc.
- Hybrid cloud is a combination of private and public clouds aiming to combine benefits from both public and private clouds (Schneider et al. 2016). Hybrid clouds are suitable for load sharing (Oleksiy & Pasi 2012, 846). For example, a business critical application that requires low network delay, high bandwidth and lot of processing power is hosted on a private cloud while backups are sent to the public cloud over the night. In case of disaster (natural, cyber-attack, etc) backups can be easily recovered from the cloud.

- Community clouds are hardware and software resources shared between communities that share the same values or interests. For example organizations working for a same mission or goal deploy community clouds (Mohlameane & Ruxwana 2014).

Clouds are specified by three service models that consist of infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) (Madhavaiah & Bashir & Shafi 2012). The anything as a service (XaaS) is being used also with other cloud offerings but not very often seen on the literatures (Mladenow & Kryvinska & Strauss 2012, 214).

- IaaS delivers virtual machines, storage, infrastructure and other virtualized computing hardware resources (Baltatescu 2014). IaaS theoretically means hardware infrastructure resources offerings on demand that are hosed on a third-party operator. Advantages are related to ability to reduce on-premise space, minimize capital investment costs, and ability to increase or decrease computing resources (example CPU, Memory, disk space, network) whenever needed (Wisniewski 2013). On IaaS deployment, this means the hardware is elsewhere (in cloud) but customer take care of operating systems and other software needed.
- PaaS are developer platforms offering platforms for software developments. (Martens & Teuteberg 2012; Karunakaran & Krishnaswamy & Rangaraja 2015). Developers benefit the most from this platform allowing them to easily integrate applications with customer environment and testing different features like load balancing (de Oliveira et al. 2013).
- SaaS services are the most used cloud services (Gowda & Subramanya 2015, 40). SaaS model is a complete solution to the customer. SaaS is simply an application hosed on cloud that is accessed via the Internet, offered in pay-per-use model including all necessary resources needed required for the application to run. Figure 1 show the “Service Customer” on top and then SaaS applications such as Google Docs and Hotmail. This shows how much of effort is offloaded to the cloud service provider.

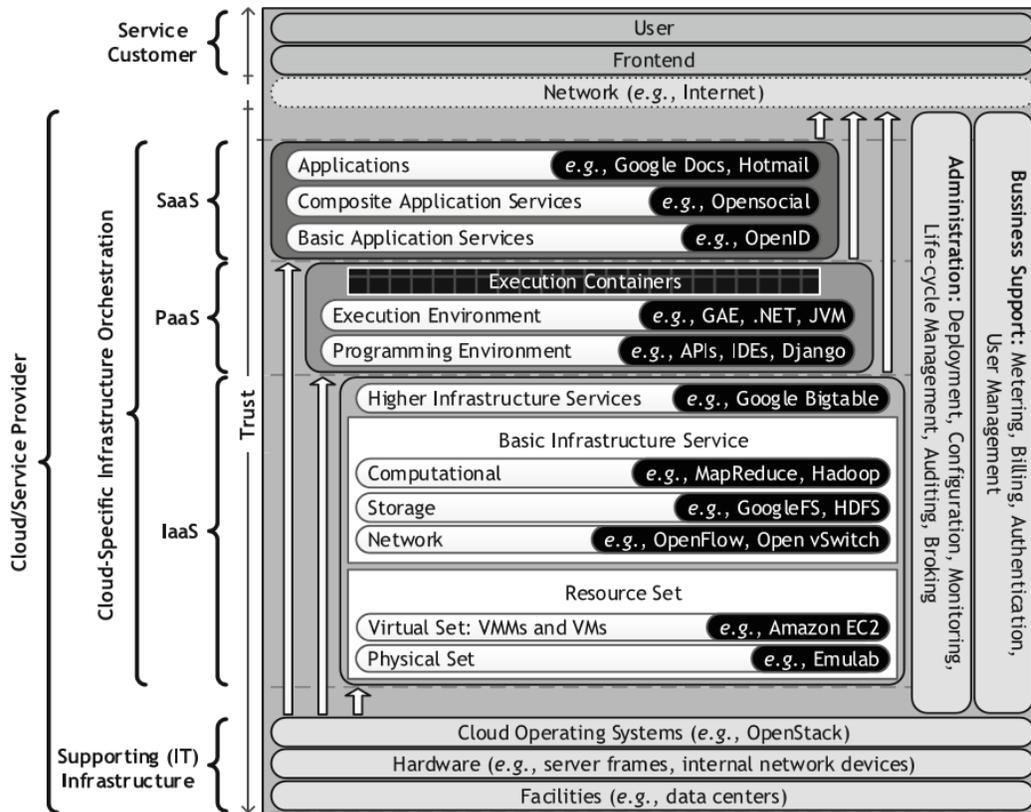


Figure 1. Cloud delivery models and their components (Fernandes et al. 2014).

There are differing pricing models for SaaS. Some of them are offered for free for certain conditions like usage time, disk space, private/corporate. For example Microsoft One Drive is free with a size limitation. Users can buy more disk space if needed. In Freemium models SaaS providers offer software for free and the user has to pay for additional features (Katzan 2010). For example LinkedIn premium offers more features than free version. Because cloud services are always online, it is easier to manage license subscriptions compared with on-premise software.

2.2.3 *Cloud as a strategic innovation*

Lacity and Willcocks (2014) claimed that previous researches under examined the strategic drivers that influence the decision to conduct outsourcing of IT services. Their study based on 202 surveys and interviews conducted between 2011 and 2012 add also innovation as another important factor that influenced clients to outsource IT services to cloud. Authors point out that it is important that service providers and clients work continuously together in order to create a process they call “dynamic innovation”. Lacity and Willcocks (2014) study reveal that it is important to continuously put efforts on improving client’s efficiencies, processes, and strategic performances. Authors claim

that customer orientation and effective collaboration will lead to better innovation strategies and as such will have significant impact on decision-making related to cloud orderings. This is another approach to agile development where the provider and the client work together to design a long lasting solution. Baozhou, Rudy and Andrew (2015) in addition to the cost factor, they findings also prove that firms are engaged on microsourcings also because of strategic thoughts. Microsourcings are small cloud orderings that can be easily scaled if customer sees values from them. Venters and Whitley (2012) study reveals four technical factors upon which authors believe cloud computing is founded. The first factor they call “equivalence” is related to desire to receive services that are more secure, available and lower latency. The second factor called “Variety” relates to cloud services that can deliver complex system for different business needs. Third is “Abstraction” factor relates to a process of simplifying technological layers so that firms can focus their time and resources on the part that matters. The last factor that is a significant factor on cloud innovation is “Scalability”. Scalability enables customers firms to easily add/remove technology resources that match their workload and need.

Textile industries outsource services to cloud because of financial and strategic reasons (Mladenow & Kryvinska & Strauss 2012, 220). Cloud computing enables them to quickly allocate IT resources on rapidly changing environments’ and customer demands around the globe.

The numbers of cloud computing offers are increasing and the competition is becoming bigger (de Oliveira et al. 2013, 2364). As competition becomes high, provider firms must take measurements to lower their price. Often low prices are not linked to good services such as security. Cloud offers are ready made packages designed to deploy easily to a wide market. Therefore customizations and other integration to local on-premise application is challenging or almost impossible (Peng & Gala 2014). Especially when evaluating transaction costs related to integration of legacy ICT system, is found to be an issue (Ross & Blumenstein 2013). Many SaaS applications offered to different customers run on the same virtual machine and as such, whatever changes made on this platform, will affect all customers using the same platform. Hence, firms must have clear how to approach costumers with cloud solutions that have different challenges and needs.

Telecommunications industries in Taiwan focusing on cloud services are strategically sponsored by the government (Lin et al. 2015, 233). EU has a stagey as well trying to overcome security barriers that often are considered the issue why clouds are not being deployed. A survey in 2013 (Maresová & Hálek 2014) carried out in Czech Republic among small and medium-sized (SME) companies revealed that only 8.7 per cent is the amount of firms that have already or willing to deploy cloud services. With the in-

volvement of EU commission in cloud computing strategy, aiming to provide fair and secure cloud offers, SME firms can easily adopt government managed clouds.

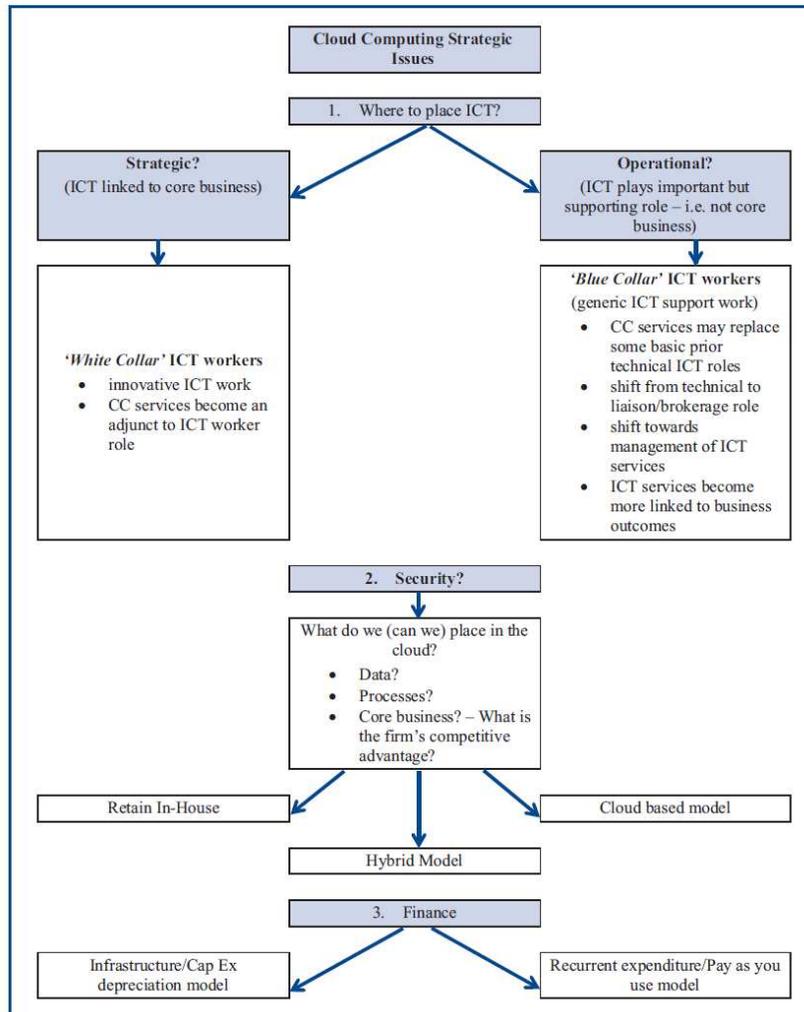


Figure 2. Strategic approach to implement cloud technologies (Ross & Blumenstein 2013)

Government cloud has been introduced in different EU countries. Large companies provide the infrastructure and the expertise under government regulation to provide innovation for the public cloud sectors in Romania (Ivanus & Iovan 2014, 91). This strategy has helped many SME firms in Romania to gain benefits of clouds by adopting new technologies fast without capital investments and doubts about security. Cloud has made innovations much easier for entrepreneurs also because of the cheap and easy startup. Ross & Blumenstein (2013) model (Figure 2) emphasized the importance of IT integration into the business. Authors show two models of cloud adoptions. The generic model is to support IT functions and the strategic one where IT plays important role on business strategies.

Most of the studies are focused on three cloud service delivery models: the infrastructure as a service (IaaS), platform as a service (PaaS) and the software as a service (SaaS) models. However lately there are studies including other services beyond these three. Other terms such as storage as a service, communication as a service, network as a service and monitoring as a service are mentioned on Mladenow et al study (2012) study where author fits them under the anything as a service (XaaS) model. Some researches emphasize that gap between IaaS and PaaS is not very clear and also for the fact that cloud services can offer anything, the anything as a service term fits well cloud offerings (Fernandes et al. 2014, 119).

2.2.4 Cost reduction and payment methods

Baozhou, Rudy and Andrew (2015) focused their study on online micro-sourcing. Micro-sourcing are small outsourcing deals of business functions or applications. Authors rank cost as the most important determinant that has positive impact on outsourcing decision making. Their study was focused on finding what motivates the adoption of online micro-sourcing. Findings were based on 240 valid responses. 71 per cent of these responses were from clients whose project cost was less than \$1,000. Benedikt & Frank (2013) focused their study on cost, formulated a mathematical decision model that can be used to aid the selection model when considering outsourcing alternatives that have to do with cloud computing. Their model consists of several cost and risk oriented factors and can be used when a firm is looking into minimizing these two. Authors however emphasize that there are more social, technological and organizational factors that must be considered but difficult to implement all of them on their formula.

Different researches criticize the cost factor as decision making factor. As far as cost is concerned, not only resourcing cost should be calculated but also back-sourcing costs because switching cost sometimes can be high in case something goes wrong. It is worth remembering that cloud provider swapping is not easy because of difficulty to move data from one to another (Blumenthal 2011), therefore right decisions should be made when selecting the cloud provider. Having cost in mind will lead to continuous savings but the disadvantage is that firm will not be able to get the innovative technologies and tools in order to develop and gain competitive advantages (Lacity & Willcocks 2014, 84).

When cost is compared with on-premise system, it is worth calculating also cost of the Internet connection which can be bottleneck if cloud service requires a lot of bandwidth (Nicho & Hendy 2013, 166; Mohlameane & Ruxwana 2014). Sometimes it is more cost-effective to combine in-house resources with the cloud one (Watson & Mishler 2014, 81).

Nevertheless, sometimes price plays a huge role in decision making especially for small and medium (SME) firms (Doherty et al. 2015). Hosting only few servers in-house would mean need to purchase expensive servers, uninterrupted power supplies, backup systems, modern firewalls, software licenses, skilled personnel to maintain and configure these, etc. Most authors define SME it by number of employees working for a firm (Mohlameane & Ruxwana 2014, 6). Small enterprise is considered a fewer than 50 employees and a medium enterprise between 100 and 200. These SME firms choose to focus their spending's, resources and capabilities on something that is more valuable. About 53% of the datacenter cost is related to the cooling and the electricity (Venters & Whitley, 2012, 181) and also has reduced carbon emissions (Etro 2011, 16).

Indeed, providing the necessary hardware and software resources for in-house deployments can be risky and costly investment. A cost reduction is also considered the ability to immediately access to the hardware and software resources in the cloud whereas traditionally, it would take time and trained personnel to provide these resources on-house (Ivanus & Iovan 2014). Because of cost factor and the pay-as-you-go model, cloud offers more competitive market (Lawler & Joseph & Howell-Barber 2012), low start-up costs (Enslin 2012) and low or no capital investment at all. Doherty et al. (2015) study on SMEs in Ireland reveals that the main driver for cloud computing adoption is related to reducing the capital cost. Avoiding capital costs will lead to operational costs but reducing operational cost is however listed on position six of the Doherty et al. (2015) study.

Although cloud offerings are considered to be cost effective, some studies point out that cost might bring limitations when in case service requires customization for certain business need (de Oliveira et al. 2013). If wrong cloud based service is ordered, the outcome can be increased costs and overall damaging firms competitiveness (Wisniewski 2013). For small firms, cloud brings savings but not necessary for the big firms that might have enough human and budget to build their own infrastructure and as such, larger capital investment but lower operating costs (Du & Cong 2010). Many firms are turned to use cloud services not only because of low prices but also ability to test new technologies with reasonable cost and little effort (Nuria 2012). Hence, price is often a decision making factor or the helping factor on decision makings.

Cloud computing enabled firms to turn capital and fixed cost into marginal costs (Etro 2011). Software in cloud is considered three times cheaper than maintaining similar on premise (Catinean & Căndea 2013). One reason is also that as in-premise hardware gets older, their performance droops and maintenance costs increases. Cloud reduces obsolescence because no infrastructure upgrades are requires as these are service providers concerns (Ross & Blumenstein 2013).

2.2.5 *New business models*

Cloud computing has positively reshaped business model elements. Cloud computing has made possible for larger companies like Oracle, and SAP to target small and medium (SME) size firms that previously would be difficult using on-premise solution (Boillat & Legner 2013). Compared with traditional on-premise software, SaaS (Software as a Service) are mostly web-based applications that require no installation on the client side. One of main drivers that influence decision to order cloud based service is the reduction in capital investments and avoiding the risk of wasting resources or loss of potential revenue (Alali & Yeh 2012). Therefore the value of hardware is decreasing and the service and software increasing. By having a better payment methods, firms will be able to better utilize and plan resources. Traditional system deployments costs are constantly increasing making clouds very attractive to order (Catinean & Căndea 2013). Firms try to avoid capital investment that can be potential risks often chose cloud services because of the pay-per-use model something that represent a major benefit compared with in-house deployments (Enslin 2012; Maresová & Hálek 2014)). Cloud computing pay-per use is the best return of investment because firms can order the right amount or resources needed with a lower cost (Yazn & Papagiannidis & Li 2013).

The model “try before you buy” also ensures a safe investment allowing customers to try a product for free for certain amount of time before they decide to buy or not (Farah 2015). Firms have to reshape their business model by offering software on cloud in order to remain competitive in a fast changing environment (Maresová & Hálek 2014). Firms continually seek to develop their position into a global market and put a lot of effort to estimate the future trends (Maresová & Hálek 2014). The EU Commission also has been involved in cloud computing strategies seeing benefits that cloud services would bring across the EU. CloudSME is one example of EU projects aiming to help SME firms to be more active by using simulation technologies in cloud (Ivanus & Iovan 2014). It is believed that as many as 3.8 million jobs would be opened by 2020 because of cloud offerings (Maughan 2013).

Another significant change on the business model is related to the value networks. A value network is dynamically created network of partners sharing same interest in order to gain joint benefits (Ojala & Tyrväinen 2011). In the old way (traditional way) a user firm almost always takes care of hardware, operating systems and other components required running the software. The software companies would simply provide the binary code (software) and the license. The need for a value network and partnerships has change (example in Figure 3) as cloud based software is depended on the Internet provider, and platform on cloud managed also by a different party.

enterprise resource planning (ERP) and customer relationship management (CRM)] that are difficult to move to cloud (Boillat & Legner 2013). On-premise ERP and CRM systems are difficult to move to cloud. However there are new cloud based ERP and CRM versions designed that fit well small and medium (SME) firms.

SME firms benefit a lot from the cloud offerings because of the scalability allowing them to efficiently allocate resources as they grow. Another advantage of cloud to SME firms is related to possibility to immediately access the necessary application and required innovation technologies needed with no capital investment in the IT infrastructure (Mladenow et al. 2012).

Lawler, Joseph and Howell-Barber study (2012) on determinants that lead to an effective cloud computing strategy, list agility one of first factor in cloud computing strategy. Agility is important feature because users it enables users to work from any location using any device. Cloud agility and mobility offer is one important factor for adopting cloud services (de Oliveira et al. 2013; Qian & Palvia 2013). On-premise applications are much more difficult to make agile or mobile. Expensive Virtual private network (VPN) hardware is required to enable remote access to the on-premise enterprise applications. When users travel or work remotely, they can access cloud services as they were at the office. Cloud has enabled managers to be more mobile when they work outside the company (Peng & Gala 2014).

Many IT organizations are having challenges with the Bring Your Own Device (BYOD) simply because not all enterprise applications are compatible with different devices (Catinean & Cîndea 2013). Cloud has made BYOD easier because of the web technologies fitting different devices and operating systems. Cloud services have solved many challenges related to client hardware and operating systems dependencies but since cloud services are depended on the Internet connection, cloud providers deploy redundant connection so that services are always online (Maresová & Hálek 2014). This so call hHigh availability” approach is also being deployed on the customer networks too, so that whenever main link goes down, the services offered by the Internet can be accessible via another backup Internet link. The cost of the Internet connectivity continue to decreased while speed and capacity have increased which makes cloud more attractive and easy to work remotely (Qian & Palvia 2013).

From the cloud providers point of view, the agility means being able to host servers on locations that are cheaper to host and maintain. This has also positive impacts on the environment and giving the provider a reputation of a green business (Enslin 2012).

Most of on- premise software and other IT tools have been developed for decades. The Cloud computing solutions works on top of the Internet and as such, most of the cloud based services (mainly SaaS) are managed and used using simply a web browser (Farah 2015). This offers advantages in the way that no software installations are required on the client machines that often run different operation systems (OS) (example

Linux, MS Windows, Apple IOS, etc.). It is however important that firms evaluate which software offering model is more suitable for their organizations for that particular function. On-premise ERP systems are still being deployed and clients installation and maintenance are considered to be time-consuming when it comes to updating every user PC while cloud based offerings ERP systems can be accessed easily using a web browser removing the need for manual installation (Du & Cong 2010; Peng & Gala 2014)).

In addition to the fact that web browser application avoid the need to install software on local machines, they can be faster too as the PC hardware requirements usually are low for a web based service. Software providers that have developed tools for decades have had to rewrite many enterprise tools to adapt to the cloud offerings (Boillat & Legner 2013). The advantage of web offerings compared with desktop based offerings is also the ability to use these tools on mobile devices as well, making solutions OS independent. In addition, social network tools (Facebook, Twitter, LinkedIn) and also other tools for business analyses can be easily integrated to the web GUIs.

Because cloud based application are light and require minimum hardware resources on the client PC, they are also considered environmentally friendly applications as client PCs can be used for a longer time or less powerful PCs can be used (Maresová & Hálek 2014).

One unique feature and often used on cloud applications handling documents, spreadsheets and other text based document, is the innovative live-linking technology which automatically saves documents as they are edited (Watson & Mishler, Aug 2014). This removes the risk of losing unsaved information if connection is lost or page is closed. Clouds GUI components in addition to the simplicity of maintaining different underlying hardware and software are considered to be determinant factors for cloud-sourcing (Schneider & Sunyaev 2016).

Gigant companies such as Microsoft Corporation are putting a lot of effort to offer cloud based services that can be ordered via internet without requiring human interaction. (Mihaela 2014). These services can be ordered via Web and used via web using mobile phone, desktop or laptop computer (Figure 4).

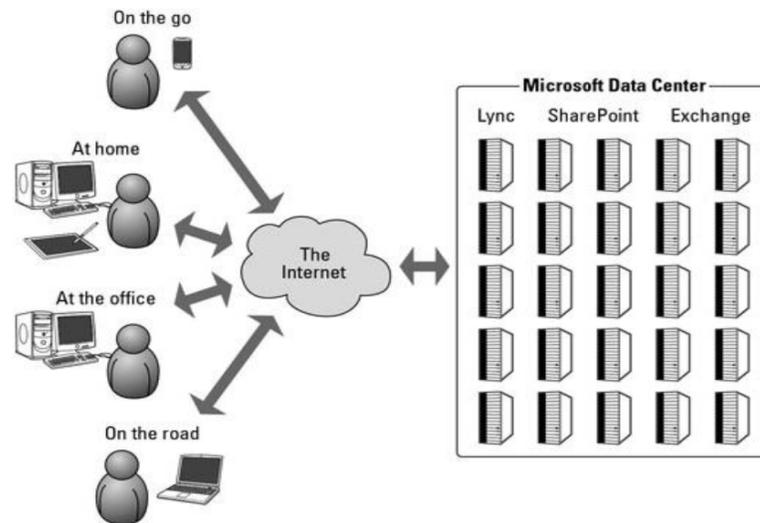


Figure 4. Components of Microsoft Office 365 (Mihaela 2014).

2.2.7 Cloud as an increasing disruptive technology

Cloud is considered often as an arising disruptive technology (Qian & Palvia 2013, 53) because it has significantly changed the way that software firms are entering the market. Cloud has not only been disruptive to the on-premise deployment but also to the entire business models (Catinean & Căndea 2013, 784). Businesses have to reshape their offerings because on-premise hardware and software will decrease and new service models have emerged. Low software prices and pay-per-use models are huge demands as customer can purchase software or service online. Boillat and Legner (2013, 49) finds cloud to be disruptive to entire partnership and network value, as software vendors can utilize online stores.

Access to the application is not limited to the OS and desktop computer. Less technical skills are required for applications as installations are usually not required or made very simple. Lighter clients have made possible to access cloud application using laptops, tablet and smartphones that run any operating system (de Oliveira et al. 2013, 2363).

The cloud adopter pioneers were individuals ordering free webmail services (offered as SaaS). This was not seen as beneficial move so many software vendors did not consider SaaS to threaten their business (Catinean & Căndea 2013). However, the adoption trend is still slow (Willcocks & Venters & Whitley 2013). A study done in Ireland (Doherty & Carcary & Conway 2015) reveals that 48 per cent of SMEs have not moved services to cloud. However, 45 per cent of them indicated that they have already services and/or processes running on cloud. Authors point out that the majority of these "Cloud

adopters" are those from knowledge intensive business services (Figure 5). Manufacturing firms remain low in cloud adoptions.

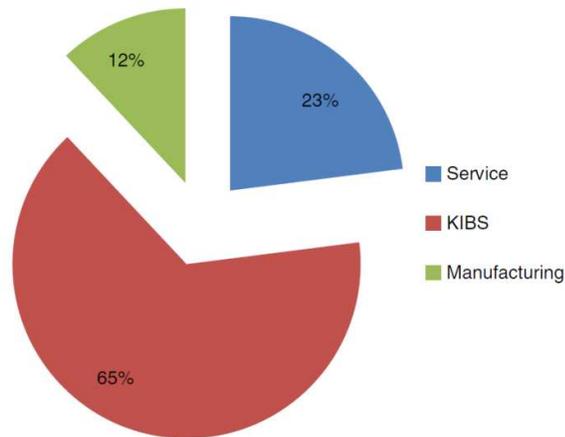


Figure 5. SME profiles showing cloud adopters (Doherty & Carcary & Conway, 2015) .

Despite the findings that cloud computing brings innovation and long term benefits, there are still some “slow trains” because of challenges with adoptions (Willcocks & Venters & Whitley 2013). Hybrid clouds are still being deployed to combine public and private cloud infrastructure (Mazhelis & Tyrväinen Sep 2012). Cloud services are considered still at the stage of infancy and have not reached maturity yet mainly because of security, legal and privacy issues (Qian & Palvia 2013; Adjei 2015). In addition On-premise deployment will exist for some time because of legacy systems and other systems dealing with very confidential information (Baltatescu 2014). Cloud adopters are mainly those firms having clear understanding what these services brings and the barriers associated to them. As example Mohlameane and Ruxwana (2014) study on cloud computing awareness in South Africa revealed that 40 per cent of IT experts had little understanding of what cloud computing are.

Many companies are already using cloud services but they simply do not understand the terminology and the technology behind. For example, when using YouTube to advertise their products, Facebook, LinkedIn, etc., these are all cloud services. Not knowing what a cloud service offers is the main reasons why technologies are not adopted and as such, values and potentials of these innovations are not understood.

Different theories exist (Baozhou & Rudy & Andrew 2015) that help firm understand how decisions on outsourcings are made by listing factors that have been empirically examined. However, it is difficult to tell how firms use these criteria on decision makings process (Schwarz & Jayatilakay & Goles 2009). Firms adopt cloud computing for different reasons including technical as well as strategic reasons. Ray (2016) classified

four factors that help organization considering cloud adoption. These factors are Technical, Organizational, Environmental and Cost.

While SME private firms are the majority of adopters, the public sectors have started adoptions with the rising demands of citizens. The demand for reasonable costs and innovation are the same for public and private sectors but the requirements are higher on the public sectors because of the security requirements. So called governmental cloud in EU that are developed by different IT organizations are attractive for public sectors because of certification schemes, inline European standards and appropriate legal frameworks (Ivanus & Iovan 2014). Cloud characteristics such as fast startup, ease of implementation, mobility, scalability and availability are considered benefits of governmental clouds.

2.2.8 Cloud challenges

Doherty et al. (2015) study on clouds for SMEs in Ireland reveals that the top three cloud adoption barriers are Internet connection and security concerns as well as lack of trust in cloud provider. Security and confidentiality are considered challenging because data is stored on a third party datacenter that can be theoretically available to anyone from anywhere. Hence, the risk is always that data is accessible by a third party (Wu et al. 2013) . There is no control about who has access to the data from outside as well as inside (Aleem & Christopher 2013). Users can achieve perhaps better security with IaaS service because of the encryption mechanisms that can apply themselves on the application layer but also bear more risk in case knowledge and resources on how to apply security mechanisms is missing (Blumenthal 2011).

Customer firms sometimes have made as big decisions as switching to a different provider and move their data from one location/country to another because of security policies on different countries (Dhar et al 2012). Cloud providers also have moved data from one location to another but for cost and other technical reasons and customer was not informed about this (Peng & Gala 2014). Often a cloud provider is considered more trustful if its datacenter is located on a specific location/country. For example some customers in EU are unwilling to host their data on a cloud server hosed in US datacenters if they do not comply with EU regulations (Khansa & Zobel 2014). Peng & Gala (2014) pointed out that according to the U.S. Patriot Act, U.S. government has access to any data store on US datacenter. However, a US cloud provider operating in EU is allowed to send EU customer data to US for processing as long as they comply with the General Data Protection Regulation (GDPR) (Ciriani 2015).

The EU commission experts are developing regulations, aiming to increase the trust in clouds. These terms will help customers within EU adopt easily and more securely

cloud services (Ivanus & Iovan 2014). The EU commission's "digital agenda" goal is to improve the cloud security offerings within EU so that EU state members benefit from. The "single market" target would help EU members with cross-border licensing and copyright clearance as well as standards and certifications to improve cybersecurity (Maughan 2013).

Cloud challenges subjects both customer and providers. Because cloud systems are complex models, there are different perspectives and views on its security. Knowing security threats, would lead to a safer cloud adoption (Nicho & Hendy 2013).

There are different protocols that help firms developing policies for securing cloud systems. For example NIST provides standards to strengthen data integrity, confidentiality and better authentication (Alali; Yeh 2012).

Although many researches list security as a biggest barrier of cloud services orderings, some studies claim the opposite. The data on cloud can be more secure because providers have the skills and the technology to apply proper security mechanisms and technologies (Corkern & Kimmel & Morehead 2015). SME firms cannot effort to adopt all security enforcement and do not have resources to monitor and maintain these. Some researches list some strategies and techniques to manage uncertainties (Farah 2015). For example buying insurance that could compensate the damage from data loses or other security attacks.

Bowers (2011) evaluated benefits and drawbacks that libraries gain when outsourcing their functions to cloud. Author emphasized that many services could be hosted to cloud including bookings, holiday management etc. However library digital information on hands of someone else is a huge risk when considering confidentiality, theft or simply loss of data.

Blumenthal's study (2011) on cloud security emphasizes that firms must be careful with what data is put on a public cloud. Author emphasizes an important reminder not to trust the public cloud if data is important. Cloud providers, for example Google clearly states on their terms of services that "*...that Google has no responsibility or liability for the deletion or failure to store any Content and other communications maintained or transmitted by Google services*" Question remains: how would one succeed in controlling data security if in absence of control of the infrastructure that is on a third party ownership (Blumenthal, 2011)? What will happen to firm reputation and if customer information is lost or leaked to the Internet?

Each company has different security needs and insurance. It is a very risky move for banking, insurance and other similar firms storing customer confidential data to consider a public cloud (Wisniewski 2013). Companies seeking for making data available to the internet (example news, multimedia, marketing, etc.) are not concerned with the security matters.

Table 2. depth of cloud security innovations area showing number of patents filed (Khansa & Zobel 2014).

Innovation Areas	Number of Patents Filed
Confidentiality	
Privacy management	45
Confidentiality & Integrity	
Cloud User Provisioning & De-provisioning	19
Identification & Authentication	56
Access Control & Authorization	51
Digital Rights Management	45
Cryptography	16
Forensics	16
Intrusion Detection/ Prevention	51
Risk Management, Threat & Vulnerability Assessment, and Governance	41
VPN Tunneling	38
Availability	
Dispersed Storage & Redundancy	87
Resilience to DoS Attacks	7
Robustness, Resourcefulness, & Rapidity of Recovery	30
Confidentiality, Integrity, & Availability	
Service Level Agreement & Information Assurance Guarantee	10

Cloud services are vulnerable to threats such as the Denial of Service (DoS) attacks but also from natural disasters (hurricanes or earthquakes). These threats are not only common to all cloud services, but also on-premise services as well (Nicho & Hendy 2013).

Khansa and Zobel (2014) study was focused on evaluating patents as part of security innovations trying to find what areas have been left out from security innovations and showing security strengths and weaknesses. As shown in the Table 2, a lot of patents are related to Confidentiality & Integrity while Availability is now that often seen on the papers. The Table 3 is constructed based on Aleem and Christopher (2013) survey findings as a result of 200 responses IT professionals. Authors study was focused on vulnerabilities of the cloud computing and how it can affect the businesses.

Table 3. A table created based on Aleem and Christopher's (2013) survey regarding top cloud computing concerns.

Top threat voted	Percentage
Security concerns when moving to cloud	93.4 %
Service level agreements (SLAs)	76.20%
Data loss and leakage	73.50%
Data protection	73.30%

Governance concerns	62.30%
Service and traffic hijacking	60.80%
Technical support	59%
Lack of control over service availability	55.70%
Insider threats	52.90%
Legal constraints	52.80%
Insecure API	39.20%
Shared technology vulnerabilities	37.30%
Higher costs	21.70%
Reputation of the Cloud Service Provider	14.20%

The data protection concern are related to the policies that often cloud service providers have no clear definition on what standards (if any) they are using to protect customer's data. Although a cloud provider might have modern firewall and technologies to protect data from network attack, the threat can be internal. Question remains to be asked to the cloud provider, have they made sure that all personnel backgrounds have been checks (Bowers 2011)?

Because security measurements are no longer handled by a local IT team, there are best practices that can be adopted to ensure that a proper authentication and authorizations mechanisms are used, redundant infrastructure is deployed and that the firm has processes showing how security threats are handled. Customers are guided to evaluate and check if the cloud service offering firms provide security best practices and if they comply with the cloud security standards like Statement on Auditing Standards (SAS) 70 Type II certification. It is important to evaluate the risks first before calculating prices. Below three important steps that can be examined to identify threats associated with the service and help decision makings:

- The first step is identifying service that needs to be outsourced (Nicho & Hendy 2013). Different services have different security threats. For example firms' www website that receives every day thousands of hits would be better to be hosed on cloud but for example CRM system would be more secure to keep in-house. If critical IT systems bring revenues to a company, it is understandable that these assets are kept in-house for strategic reasons (Wu et al., 2013).
- There are different cloud providers offering the same service. They host their datacenters on different locations that have different security policies (Khansa & Zobel 2014, Peng & Gala 2014). Therefore it is important to ask where data is hosed and if they comply with security standards in case data is sent elsewhere.

- It is important to do a business impact analysis and risk analysis on the service intended to be outsourced. What will be consequences if data is stolen or lost (Alabdulkarim et al. 2014)? Will it affect the customers directly? What about firms' image?

From the technical perspective, when a service is hosted on cloud, the responsibility to secure the infrastructure is moved to the service provider. Service provider must deploy modern firewalls to protect cloud environment and reduce threats from cyberattacks (Nicho & Hendy 2013). Modern firewalls are equipped with different security blades like intrusion prevention, antivirus, DoS prevention, etc. Encryption technologies must be used on both client and server. Infrastructure must be always up to date with security patches. Adjei (2015) pointed out that cloud providers must take necessary steps to show that they can assure information privacy and security and have taken and provide evidence that they can overcome technical and psychological risks associated to cloud hosting.

Finnish Parliament in 1999 passed a Personal Data Act (523/199) law to better manage records in private sector (Carl-Magnus2003, 148). Records do not need to be permanently stored but there is a time that must be declared so that these records can be inspected. Service providers in Finland storing some kind of records are guided to comply with the regulation above.

Commercial web applications such as, emails, web-shops and other similar web browser based applications, where the first ones to be migrated to the cloud. Most of these application handle text based data and therefore the hardware performance needed is low. However, there are applications that are challenging to migrate to cloud because of performance issues related to virtual machines that make most of the cloud providers. These applications are for example High Performance Computing (HPC) applications such as simulating application, weather prediction application, physics-based applications, etc (Benedict 2013). The performance with HPC application is mainly related to memory management issues.

Although most of the networks now are behind fiber connections, there is still latency issues reported when using cloud services. Usually Local Area Networks are fast switching network but access to the internet might be much slower. The Internet is considered also serious threat from the business perspective because if down, the entire factory stops (Du & Cong 2010; Nicho & Hendy 2013). For enterprise application dealing with large database records, latency is the main issues (Venters & Whitley 2012).

As far as enterprise applications are concerned, later studies show that cloud based enterprise applications can be faster compared with on-premise applications because more CPU, memory and disk space can be allocated on cloud compared with old hardware installed in-house.

Not all applications gain benefits by being on cloud (Watson & Mishler 2014). For example, in a location that Internet connection is slow or not reliable, migrating customer relationship management (CRM) solution to cloud or other business critical data application would not be beneficial. Peng and Gala (2014) evaluated cloud based ERP benefits and drawbacks compared with traditional ERP systems. Their empirical study in the other hand revealed that firms gained cost related advantages by using cloud based ERP in addition to improved performance. Modern cloud based offerings has GUI re-designed to overcome cloud challenges. As numbers of customers grows, cloud providers improve their technology resulting in performances improvements too (Catinéan & Căndeia 2013). Enhancing performance results directly on business efficiency indeed because users would no longer be frustrated with slow application responses or possible crashes.

In different geographical location the concerns related to cloud are different. For example of security and compatibility are least concerns for South Africans firms (Mohlameane & Ruxwana 2014). Other issues like connectivity speed and cost of the link, performance and availability are the main barriers hindering cloud adoptions of SME firms in South Africa.

Scalability and flexibility are considered to be important cloud features because of the ability to increase and decrease resources according to the business needs. This feature is valid only if right cloud provider is selected. Durowoju et al., (2011) claim that security is the biggest challenge but flexibility to be the second biggest one. Authors point out that in case cloud provider is not able to perform adjustment on time, then the benefits of clouds are lost. For example, if a cloud server is expecting bandwidth overload or other CPU / memory overload due to increase of users and if the cloud provider is not able to allocate more resources, this will have negative effect on the business.

Some cloud providers have higher technologies and capabilities to integrate application to third-party system in order to achieve highly customized applications if needed (Boillat & Legner 2013).

Another focus of transaction cost economics is reducing risk associated to contractual governance (Lacity & Willcocks 2014, 69). When market number is small in terms of vendors, opportunisms is considered thread (Schneider & Sunyaev, 2016, 13; Schwarz et al 2009, 764).

Cloud applications infrastructure is hosted on a third party datacenter where customers have no control on how access to their critical and confidential data is managed. Hence, one of the main challenges of cloud adoptions remains security concerns, confidentiality definitions and privacy policies (Doherty et al. 2015; Wu et al. 2013; Blumenthal 2011). In order to address these problems, cloud providers are obligated to meet standards and regulations in order to show that customer data is secure from different threats. Equipped with certificates and standards, cloud provider is more attractive than

one without. In fact, often in-house applications are move to cloud because of security enforcements that cloud provider provides compared with in-house security implementations that might be missing (Corkern & Kimmel & Morehead 2015). Cloud standards are still evolving. Few of standards regulators currently being active in standard development are listed below (Elifoglu & Guzey & Tasseven 2014):

- Cloud Security Alliance (CSA), a non-profit group whose mission is to educate users and secure cloud by using best security practices.
- Information System Audit and Control Association (ISACA) is another non-profit, global association aiming to provide knowledge and best practices that are accepted globally. ISCA works closely with CSA on cloud computing practices.
- European Network and Information Security Agency (ENISA) is EU founded agency working closely with member states and private sectors to provide high level of network and information security advices and solutions to EU members.
- National Institute of Standards and Technology (NIST) among others, aims to define unique U.S. Department regulatory requirements and solutions for cloud systems.

One of the most widely used cloud security auditing standards is Statement on Auditing Standards (SAS 70) (Bowers 2011; Aleem & Christopher 2013) providing fundamental requirement for auditing outsourced services. Later Auditing Standards Board (ASB) and SSAE 16 were developed to deal especially with cloud issues. The Service Organization Controls (SOC) released two new models SOC 2 or SOC 3 dedicated for clouds security. Type II SOC 2 provides the highest level of mechanisms for data availability, confidentiality, and integrity (Elifoglu & Guzey & Tasseven 2014). ISO 27001 is another popular certification used by IaaS providers. Hence, if security is a concern, customer must ensure that a cloud provider has implemented Type II SOC 2 or ISO 27001 security certificates (Nicho Hendy 2013; Aleem & Christopher 2013; Venters & Whitley 2012). Despite effort on standards, customer might still want to evaluate cloud providers by sending their own auditors if possible (Martens & Teuteberg 2012).

It is important to emphasize that complying with a security standard requires effort and money. The cost related to implementing these enforcements is sometimes considered to be a trade barrier, but it was proven then firms get more benefits by complying with standards (Ciriani 2015).

The cloud market however is dominated by US operators. In a study in 2014 (Ciriani 2015) it was found that as many as 72 per cent of cloud providers operating in EU store customer data in US datacenters. European commission has issued General Data Protec-

tion Regulation (GDPR) to ensure EU citizens data privacy and confidentiality with cross-border data movement. Whenever a cloud provider operates in EU and stores or processes EU citizens' information, they must comply with (GDPR) regulation proposed by EU laws.

2.3 Monitoring service review

So far, findings on cloud services were listed that have significant impact on decision makings. Most of the findings have positive influence but there were security related challenges that were discussed because cloud challenges differ. This chapter lists findings on monitoring services that were considered important on journals reviewed.

Journals found most of the times are not directly linked to IT asset monitoring. These articles that are not reviewed in this study are for example health monitoring journals emphasizing new monitoring approaches or technologies. Other studies are focused on environmental aspects of monitoring like air, water or weather. A significant number of monitoring studies have been done on business and economics in general affecting banks, investments, people performance etc. Although these articles do not directly support this research which is focused on monitoring of IT assets, they can however help us understanding that monitoring of any type of asset is important.

2.3.1 Monitoring service products

Almost all articles searched on monitoring subjects prior to making this study work, are very technical. Table 4 shows an overview of cloud monitoring tools and general characteristics in of each.

In addition to commercial tools, open-source such as Nagios Core and Zabbix can be used to perform monitoring functions (Jeswani & Natu & Ghosh 2015, 974; Silver 2010).

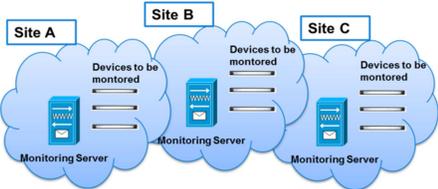
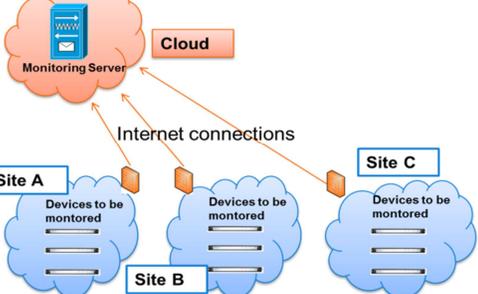
Many studies have done comparison between applications hosted on cloud and those on-premises (Gangwar & Date & Ramaswamy 2015; Mazhelis & Tyrväinen 2012; Bowers 2011). Most of the time these studies find cloud tools to be the leader because of the benefits that software inherits from cloud. It is important to emphasize that not every software or service inherits the same benefits or barriers by moving to cloud.

Table 4. An overview of cloud monitoring tools (Alhamazani et al. 2015, 375).

Platform	Network arch. (centralized)	Network arch. (decentralized)	Interoperability multi-cloud	Visibility multi-layers	SNMP	Extendable APIs
Monitis [38]	Not-stated (SaaS solution)	Not-stated (SaaS solution)	Yes	Yes	Yes	Yes
RevealCloud [39,40]	Not-stated (SaaS solution)	Not-stated (SaaS solution)	Yes	Yes	Not-stated	Yes
LogicMonitor [41]	Not-stated (SaaS solution)	Not-stated (SaaS solution)	Yes	Yes	Yes	Yes
Nimsoft [42]	Yes	Yes	Yes	Yes	Yes	Yes
Nagios [31,43]	Yes	Yes	Yes	Yes	Yes	Yes
SPAE [44,45]	Not-stated (SaaS solution)	Not-stated (SaaS solution)	Yes	No	Yes	No
CloudWatch [46]	Not-stated (SaaS solution)	Not-stated (SaaS solution)	No	Yes	Not-stated	Yes
OpenNebula [47]	Yes	No	No	No	Not-stated	No
CloudHarmony [48]	Not-stated (SaaS solution)	Not-stated (SaaS solution)	Yes	No	Not-stated	No
Azure FC [49,50]	Yes	Not-stated	No	Yes	Yes	Yes

The Table 5 lists differences found on the article reviews so that the reader can decide her/himself the value of each. The topology shows a holistic picture of each deployment. There is a huge difference indeed in infrastructure that affects other components like cost of operation and installation. Starting from the topology, there can be different perceptions on benefits related to security, complicity, agility and other factors.

Table 5. Comparison between on premise and cloud monitoring services (source: self-study).

On-premise	Cloud
<p>In-house topology</p> 	<p>Cloud based topology</p> 
Theoretically more secure when in-house trained personnel and infrastructure exist.	Security is the main concern as data is stored in the third party datacenter, though can be much safer than in-house.
No need for Internet connections	Requires access to the Internet
Performance can be higher due to bandwidth being high	Processing performance can be high if internet speed is high-enough

High capital investments but lower operating budget	Low or no capital investment but higher operating budget
More IT specialists needed to maintain the system, less managers to manage it.	No technical skills needed in house. More managerial skills required.
Not scalable easily. Downscale has no values, upscale expensive.	Easy to scale up and down as business demands
Poor agility and mobility (isolated solutions)	Mobile and agile. Access from anywhere is possible
Unpredictable costs	Visible costs, easy to manage them
Theoretically better SLAs	SLAs depend on the Internet and cloud provider
Desktop applications build for certain operating systems (OS)	Web UI that works on different hardware and OS
Manual updates and upgrades	Automatic upgrades and updates.

2.3.2 *Monitoring service characteristics*

From Information Technology perspective, monitoring solutions are essential hardware and software components that are designed to detect and/or possible predict system failures. They contain some kind of history on how an application has performed for a given time period, show system usages and other useful information and logs so that troubleshooting would be easier (Chang & Minkin 2008).

Monitoring solutions often exist with a maintenance plan. Sometimes they are offered along with the hardware or software products delivered. Maintenance plans can be reactive, meaning that a fix is performed when a breakdown occurs. Monitoring solutions detects the failure and reports them by sending email, SMS, or other form of reporting or integration to other systems. Regular maintenances are often avoided because of the cost and other resources needed. It is not worth fixing something that is not broken unless the cost of that repair is effective (Il-hang & Myung-gun & Park 2013).

Proactive maintenance aims to minimize maintenance cost of unexpected failures. Proactive approach aims to fix systems problems before they occur. Avoiding system failures is important because a failure that would result in customer satisfaction decrease something that would be huge prices a company would have to pay (Alabdulkarim et al. 2014). A failure means someone will not be able to perform his/her job in addition to the cost related to fixing failures that could have been avoided. Proactive monitoring tools play an important role in a proactive maintenance plans. Hence, monitoring solu-

tions are crucial components designed to monitor different system variables or features and as result minimizing maintenance costs as well and unexpected downtimes.

Table 6. Different monitoring layers of a system.

Item	Description
Security	Protocols, ports, access logs, commands, etc
Application	Application state, errors, uptimes, versions, configurations, logs, etc
Hardware infrastructure	CPU and memory usage, disk usage, buffer and errors, temperature and other sensors, etc.
Network infrastructure	Link status, usage and possible errors

A monitoring system can monitor different layers of the system (Table 6). For example monitor the link state and warn if network usage is high, which will result in a slow or no access to the system at all. Monitoring hardware is important too because often CPU or memory usages are cause of low application performance that can be source of attacks (Fernandes et al. 2014). A good monitoring tool would send notification to the administrator if an application has failed and the error generated on failure. It also keeps configuration backups and change history helping admins troubleshoot possible misconfiguration errors. In addition, modern tools monitor user accesses, commands and other security related issues like port scanning Silver (2010), number of access denied errors, etc.

Table 7. Monitoring levels and basic features.

Feature / Level	Reactive monitoring			Proactive monitoring		
	1	2	3	4	5	6
Syslog						yes
NetFlow					yes	yes
HTTP				yes	yes	yes
SNMP traps			yes	yes	yes	yes
SNMP get		yes	yes	yes	yes	yes
ICMP probe	yes	yes	yes	yes	yes	yes

Monitoring systems use different protocols to pull information or listen to the events, in addition to application programming interfaces (API) exist to enable developers design their own interface (Alhamazani et al. 2015). The most common protocols used are Simple Network Management protocol (SNMP), Internet Control Message Protocol (ICMP) and Hypertext Transfer Protocol (HTTP). Table 7 shows common features that monitoring tools support. In the table there are 6 monitoring levels. Monitoring 1-3 can be considered reactive type of monitoring because causes are found only when a failure

occurs (Chang & Minkin 2008). These are basic monitoring features that are easy to achieve using scripts and basic tools. Proactive monitoring tools (in the table levels 4 - 6) are more advanced type of monitoring that are there to inform administrator before a failure on system occur (Alabdulkarim & Ball & Tiwari 2014).

2.3.3 *Monitoring solutions as part of business continuity plan*

Business continuity plan (BCP) is a failover plan of events in the case a disaster occurs (Nicho & Hendy 2013). It consists of different processes, monitoring tools, tasks and actions lists to ensure business continuity. BCP is integrated part of firms structure that are developed to respond in case disruption on business occurs. Zawila-Niedzwiecki (2010) emphasizes the importance to understand that these plans must include also preventive activities in order to examine firms' immunity strength and weakness so that failures are predicted before they occur.

While planning the business continuity, firms simulates or foresees different failures scenarios and tries to design preventing solutions and ways to quickly respond to the threat so that business activates continue to flow. If risk is considered low, not subject of occurring often and it does not affect business directly, temporary inconveniences are accepted (Figure 6). However if the probability of the risk is high, monitoring is important part to prevent disruptions.

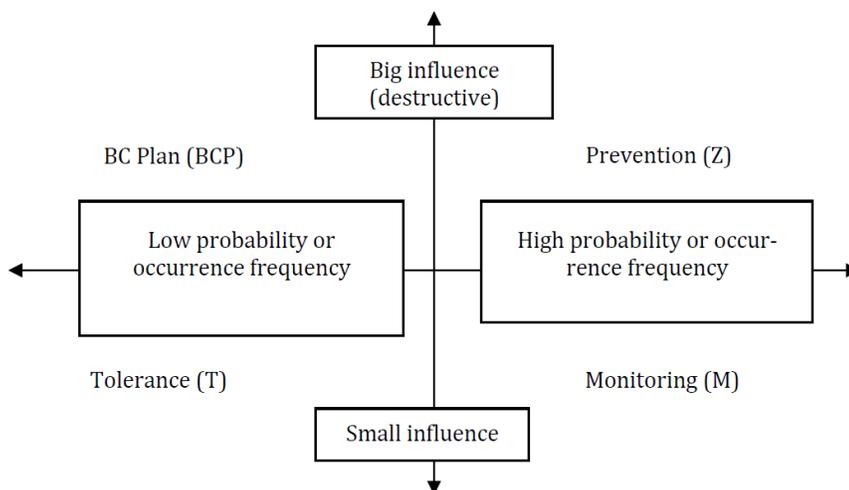


Figure 6. Four different risk categories that might occur affecting business continuity (Zawila-Niedzwiecki 2010).

It is important to identify factors that have impact on the business continuity and most of the times are related to technology (Nijaz & Moon 2009). From IT perspective, several elements shown in Figure 7 should be monitored.

In addition to proactive monitoring of IT assets that compose a risk to the business, there are precautions that can be made to minimize the downtime using latest technologies is an advantage. Using clustering feature on server and network devices will ensure disaster recovery/tolerance so that a single component failure does not affect the system at all (Nijaz & Moon 2009).

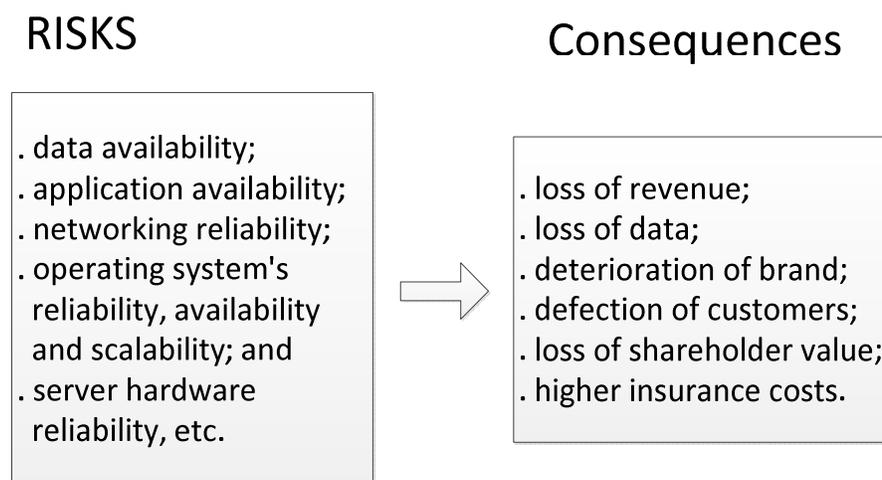


Figure 7. A picture created based on Nijaz and Moon 2009 study showing factors that affect PCP and consequences of not having such.

2.3.4 Support and maintenance requirements

Monitoring solutions sometimes monitor simple systems by checking if a device or link is up and running. A monitoring solution could be as simple as a script that performs an action if a device is not responding. However, monitoring solutions must provide real-time information on asset health as well means to view history.

A lot of tools exist on-premise that are free or open-source (example Nagios Core and Zenoss Core) that can be downloaded, installed and used for free. These tools have commercial versions as well. Silver (2010) evaluated open-source version of Nagios Core and published codes how to use them. However, this requires a lot of technical skills to get them working and if the code does not work, there is no support of any kind. Commercial versions of the same tools exist that are much easier to configure and use with a small fee. Although commercial versions are easier to configure, all of them require some manual customization, installation and configuration (Cheng 2010).

Monitoring solutions are deployed to monitor SLA agreements levels, critical and complex manufacturing and other business operations, making sure that these operations perform as expected and unplanned downtime is minimized or removed. These tools, the same like others must be under support agreement too.

Alhamazani et al. (2015) reviewed different cloud monitoring tools like Nagios, RevalCloud, LogicMonitor, Nimisoft, SHALB, etc and concluded that more effort is needed in order to deploy a reliable monitoring system. Authors emphasize the importance of having a better collaboration between providers to have more standardized solutions. Il-hang, Myung-gun and Park (2013) claimed that investing in high cost monitoring technologies would not assure higher performance if other resources are missing.

Theoretically, monitoring a device would mean monitoring several layers of it, starting from network, hardware performance, operating system up to the applications and users connected to the service. However, this task would be very resource consuming. Drago et al. (2015) designed a simpler metric they call “health index” to indicate service availability. Their solution is based on NetFlow/IPFIX data, as a lighter option to monitor hosts. Lighter means faster but the disadvantage on their model is not being able to tell if the application is really functioning as expected.

2.3.5 *Technological advantages*

Most of the monitoring tools are able to obtain syslog (text based messages) or other type of information from a device that is being monitored. However the format of the information from different machines is not standard and as such, a monitoring system is unable to use that data/information. Administrators manually configure a monitoring system to look for a specific value (example text string) to sense if something is unusual (Carela-español et al. 2015). However, most of administrators have no knowledge about what data is expected and what the ranges / thresholds should be. In a distributed, environments, systems are very different from each other.

Different operation systems, software, hardware are used sometimes also for a same purpose. Having more standardized platforms would be easier for the monitoring system to be effective (Alhamazani et al. 2015, 375). Standardization means easier to add a host in a monitoring system and easier to support it. Cheng (2010) emphasizes the importance of having standardized processes and procedures to make the entire management lifecycle easier and keep the support cost low.

Monitoring scenarios require continuously updates in order for the configuration to become effective (Il-hang & Myung-gun & Park 2013). Therefore monitoring tools must be able to dynamically adapt to the variables that a monitoring system reports in order to avoid static and manual configuration (Jeswani & Natu & Ghosh 2015, 954).

Chang and Minkin (2008) emphasize the importance of being able to detect and predict the failure before they occur so that business critical revenue making applications are not interrupted. In addition, authors suggest for designing applications that are able to self-heal, self-configure and self-optimize automatically or semi-automatically.

Network devices are infrastructure platforms that all modern applications utilize. Managing manually network configuration, backups and all type of monitoring is no longer possible to do manually (Yamada & Yada & Nomura 2013).

Carela-español et al (Jul 2015) claim that their study and design has improved traffic classification accuracy. Regardless how successful their method is, the important point is here that author tries to remove human involvement in continues configuration and develop systems that are able to automatically adapt to a changing environment.

2.3.6 Stakeholder benefits

System administrator's job will be easier when monitoring solution is deployed. Instead of manually checking system health every day/week/month, the monitoring tool does this automatically 24/7. Without a monitoring tool, users would report symptoms that are not often related to the root cause (Cheng 2010). For example "network is not working" might be related to many reasons related to servers that authenticate users, server assigns addresses, manage security policies, etc.

The business owners benefit the most because by having services up and running with a minimum downtime, user satisfaction is increased and higher productivity is achieved. Il-hang et al. (2013) emphasize also cost benefits from using continues monitoring solutions because of possibility to discover failures on early stages or before they occur. Revenue generating IT systems require proactive monitoring to be able to predict errors before they occur Chang & Minkin (2008) so that precautions are taken to solve them before business is interrupted. Proactive monitoring tools monitor different variables, for example CPU usage, memory, hard drive, etc. and warn admins that the threshold is about to reach.

It is important to emphasize that the success of many companies nowadays are as a joined effort a wider network stakeholders. This network of stakeholders includes partners, suppliers, and coalitions (Lin et al. 2015). Cloud strategies are intended to support this network also.

3 RESEARCH PORCESS

This chapter explains the research mythology used and then continues with the case company interviews and how interview data were analyzed.

3.1 Methodology

Traditional on-premise monitoring services exist and probably will continue to exist for different purposes. Cloud based monitoring services are still not widely used. There are no studies on cloud based monitoring as a service (MaaS) of any kind showing what values or benefit a firm would get by hosting MaaS service or deploying such. Therefore a combined cloud service and monitoring service studies are performed in order to find common cloud elements that have impact on adoption decision makings of MaaS. In other words, the goal is to find shared facts that different stakeholders emphasize when considering cloud services and the monitoring service.

Different stakeholders emphasize the benefits of cloud services in general (Alhamazani et al. 2015; Lacity and Willcocks 2014; Baltatescu, 2014). Hence, as far as cloud study is concern, there are a lot of studies to be reviewed. However, there is no scientific studies done on IT monitoring service that would show benefits or challenges on implementing a monitoring service. Those few studies done on monitoring systems are very technical and most of the time not related to IT monitoring. Hence, the literature review is divided into two parts, the cloud computing / outsourcing review and the monitoring tools / service review.

Journals from online databases [ABI/INFORM Collection (ProQuest), Business Source Complete (EBSCO), EconLit (ProQuest)] and Emerald in Business and Economics are uses as source of articles.

The article reviewed on cloud studies and monitoring solution studies will form the Monitoring as a Service (MaaS) study shown in Figure 8

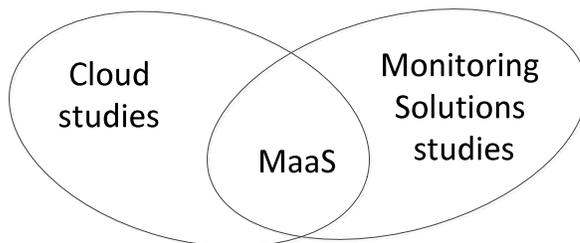


Figure 8. Findings from cloud studies and monitoring solution studies making up MaaS literature review.

In order to obtain the latest information on the cloud topic, all articles below 2009 were filtered. The second selection criterion was the article content. The findings were filtered based on article title and their introduction. The final criteria was selecting only articles that contained scientific statistics/reports/studies of factors that lead to decision making process of IT outsourcings, cloud computing benefits and monitoring service benefits.

The Figure 9 shows this thesis research process. The list of articles reviewed is listed on the paragraph 6 References. The literature review contains cloud services and monitoring service reviews. Findings on monitoring service and cloud services in addition to the IS theory selected will guide the empirical research.

While reviewing articles, it was revealed that transaction cost economics theory is the most used theory with cloud computing studies. Hence, transaction cost economics will be used to guide this thesis work as well.

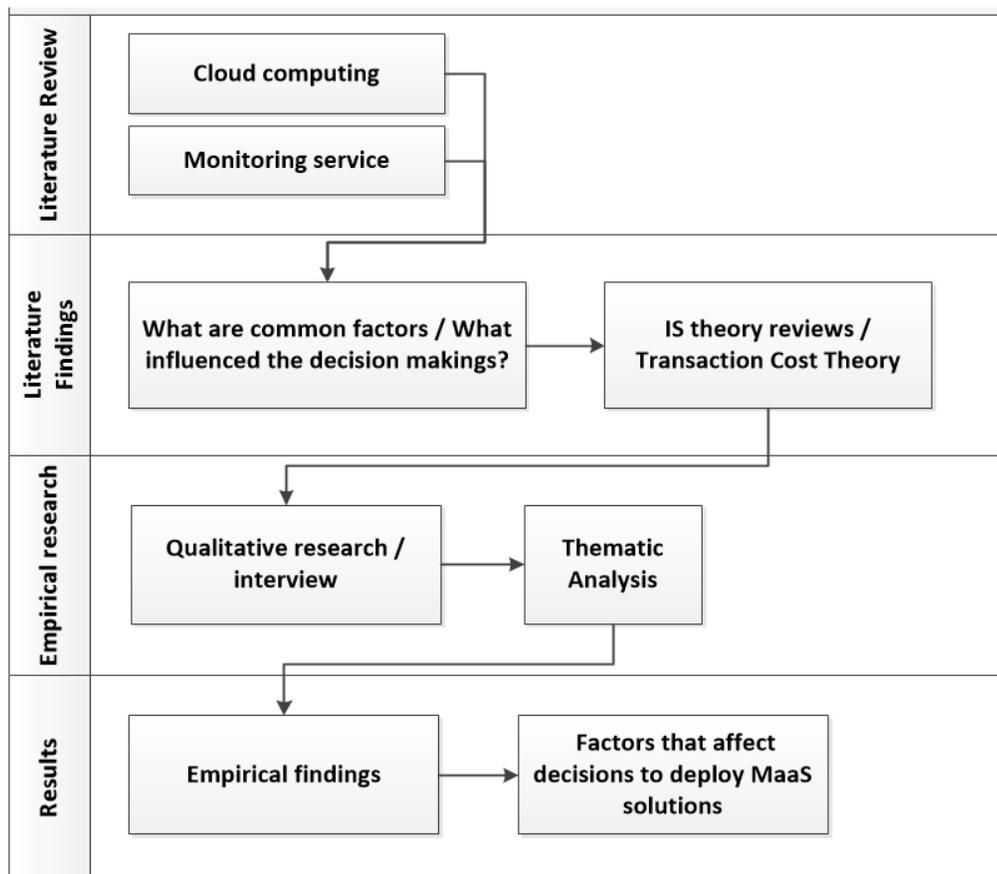


Figure 9. Holistic view of thesis research process.

3.2 The case company and interviews

The case company is specialized in television, broadband and video security products. The high-tech hardware and software solutions are provided to a business-to-business (B2B) as well as business-to-consumer (B2C) scale (Figure 10). The interview is selected to be the most convenient method to gather information from the case company stakeholders. This chapter lists top findings from the in-depth interview conducted. The targeted stakeholders were those that are involved with project requiring monitoring services. The idea of a more closed research domain was to gain more qualitative information from stakeholders who have provided, ordered or been involved on project. Selected stakeholders interviewed are those who have worked on project involving to monitoring services and can provide information challenges or benefits based on their experience rather than assumptions.

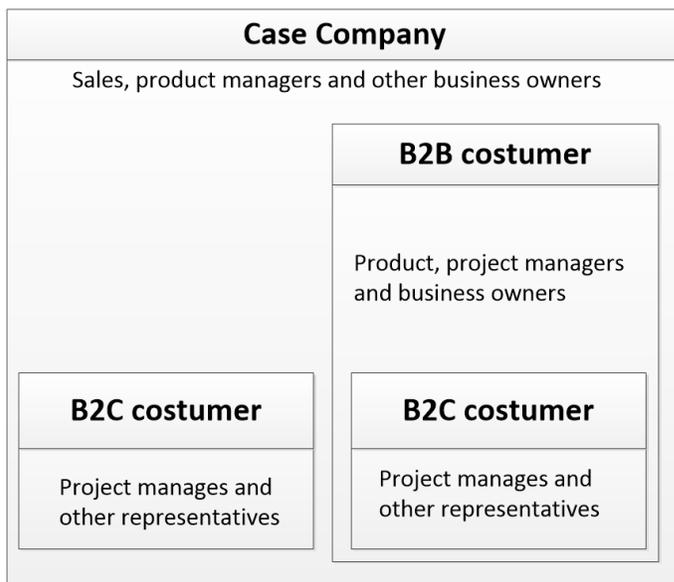


Figure 10. Overview of customer stakeholder domain

Articles on cloud computing were reviewed and findings were considered in designing the pilot project.

The pilot project developing approach is focused on agile methodologies, leaving space for further development of monitoring application and preparing for rapid changes according to a market need (Cao et al 2009). The Figure 10 shows customer stakeholder domain affected by the monitoring service.

The case company provides hardware and software solutions to B2B and B2C customers. Along with the provided hardware goods that the case company manufactures and provides to its customers, a monitoring service was often included along with the

hardware delivery. On-premise monitoring solutions were either deployed by the customer themselves, or by the case company.

In-depth interview carried included representatives from different offices that have different customers. All corporate representatives interviewed (see Table 8) are part of projects demanding cloud based monitoring solutions, that have already been provided with on-house monitoring solutions or interested in cloud based monitoring solutions. This selection was done on pre-study where it was found that stakeholders whose work is not affected by cloud or monitoring service would produce no informative responses.

Table 8. Profiles of the interviewed company representatives.

Repres. Nr.	Firm	Title	Years in current position
1	A	Director, Global Support	5
2	B	Support & Integration Manager	7
3	B	Director, Hospitality and Audio Visual product	2
4	A	Vice President, Video Service Platforms	2
5	A	Sales Manager	3
6	A	Sales Director	3
7	A	Senior Director, Channel sales	11
8	A	Specialist, System	20

The interview was very open leaving enough space for the interviewee to express freely their experience and thoughts about cloud and monitoring services. Indirect and unstructured questions were often asked according to the subject being discussed. The idea was to go deeper to the related subject about troubles they have had with infrastructure or software provided by the case company or other channels how these troubles could be solved by a system that monitors them. An attention was put on the comment they emphasized to be important. The following subjects were however discussed. Each subject let to multiple questions:

- Questions related to business continuity plan or IT disaster recovery plans and if monitoring tools are being used (advantages, barriers, future plans, etc).

- Discussed about challenges they had with products, lesson learned and talked about how they could avoid these IT asset failures.
- Talked about cloud services and firm policies toward cloud migrations.
- Asked if firms have enough IT personnel to manage all IT related actions themselves or prefer get help from outsourced professionals (the percentage rates).
- Evaluated payment methods firms prefer, mainly if firms choose to invest more on capital assets or willing to pay monthly for service used.
- Evaluated firm size and the changes they had within five year and/or plan to grow.
- Asked about if they have calculated cost related to information searching, sharing and other cost related to the software or service purchasing.
- Asked about how decisions are done on services, software or hardware orders.

More structured questions are found on APPENDIX 2:

3.3 Empirical research analysis

The cloud based monitoring solution is a new concept. In order to find characteristics and stakeholders influences towards this concept, the interview is selected to be the best approach to gather information. Interviewed stakeholders are managers and directors that are involved with business critical systems that require monitoring. The interview notes have been coded using a thematic analysis approach in order to examine and phenomenon that are most relevant to this thesis subject. Below holistic view how data were analyzed:

- Conducted all interviews.
- Transcripts were read carefully multiple times.
- Indexing (coding) of important findings (words or phrases) was done using significant findings. These findings were phases or words there were:
 - Repeated ideas
 - Found on article reviews
 - Mentioned on the Transaction cost economics transaction cost economics theory
 - Ideas that interviewee mentioned to be important
- Indexes (coded) were grouped into categories (example “try before buying”, “demo version”, “free for certain amount of time”, etc. were grouped under one category called “Save investment”).

- Categories that were less important were dropped and those relevant to the study topic were listed.

Findings from the qualitative interviews are listed below. Technical findings and requirements mentioned on the interviews are removed from here because they do not support this study.

4 RESULTS AND DISCUSSION

This chapter presents results based on article reviewed empirical study and evaluated with transaction cost economics theory.

4.1 Save investments are attractive

Researches emphasize that clouds are being adopted because of the strategic reasons (Gowda & Sbramanya 2015, 46). Cloud studies evaluated by Transaction cost economics also point out that cloud adoptions bring cost savings (Schwarz & Jayatilakay & Goles, 2009). Interviewed stakeholders that provide the monitoring solution, find much easier to approach clients with a cloud based monitoring tools. Previously provided on-premise tools required an engineer on site to install and configure the monitoring tool because most of the time, the knowledge in-house to manage installations was missing.

With the cloud based tool, there is no need for hardware goods to be shipped and a new system running on cloud virtual machine can be created within few minutes. With the decrease of hardware prices and difficult to maintain, more revenues would be made with public cloud and service models. Cloud services are considered safe investments because there is no need to invest in hardware (Corkern et al 2015). On the interview, it was mentioned that demo versions can be arranged easily to multiple customers simply because of virtualized system. “Proof of concepts” projects are no longer expensive because infrastructure for this purpose is virtually on cloud.

Transaction cost economics theory tries to minimize cost that is related to uncertainty (Baozhou & Rudy & Andrew 2015, 758). Sales managers mainly but other stakeholders involved with budgets calculations and prices, were requesting that monitoring services would be offered to customers for free for certain period of time before they decide whether they continue with the service or not. Some of them were referring to “demo systems” and others “try before buy” and “free for a period of time”. They were all looking for a safe investment to avoid capital investments that would be difficult to cancel. In addition to the risk-free capital investment, it customers would be able to test the system effectiveness, performance and usability. So called “proof of concept” is attractive way of approaching customers because they find this less risky approach. The client can test the system for a period of time before deciding if the system brings values and fits their needs. In addition, evaluation versions are important to test the complexity level (Yazn & Papagiannidis & Li 2013, 266).

The providers in the other hand will gain customers easily. It is easy to create evaluation systems on a virtual infrastructure and easy to remove them.

Since we are talking about a new product and offered on cloud, it would be important to offer for free for certain amount of time so that it can be tested if it meets the needs. Once users see benefits, then it is easier to scale. This means that we would have some references to offer to other customers too [Representative 5, Sales Manager].

Traditional on-premise monitoring tools were shipped as a package of software, hardware, on-site installation and configuration. The price of hardware has gone down and there are open-source tools that can be used for free for basic monitoring. Expensive hardware and software are used to be able to monitor what is flowing on the network (Carela-español et al Jul 2015). The MaaS hosed on cloud is seen as an advantage because of removing the need to provide server hardware on each site.

Traditional monitoring tools, regardless if they are commercial or freeware, still require hardware and someone to configure and maintain them on site. We are not winning by shipping hardware and software and our engineer onsite to configure traditional monitoring systems. Offering a cloud model is what we want because we can approach customers much easier with a monthly fee, which would ensure higher return of investments for all [Representative 2, Support & Integration Manager].

4.2 Cost is often factor in decision making

Cloud has significant benefits related to costs because of initial investment. However, there be reported transaction costs increases linked to opportunism and bounded rationality (Ross & Blumenstein 2013, 41). This risk is related to human factors that are bounded with information and his ability to make right decision. When information and knowledge is missing, sometimes decision is based on lowest price which might not be the best selection criteria (Wisniewski 2013, 86). Gowda & Subramanya (2015) studied benefits of cloud service separately for each platform. The ratings are shown in the (Table 9). The software cost savings on their study based on 175 responses scored the most. Other benefits are also listed.

In the interviews, it was discovered that often projects where monitoring services are deployed have multiple tools to perform different tasks. Some tools are dedicated to network monitoring and use different security mechanisms to be able to detect abnormal network behaviors such as DoS attacks. Some other tools deployed on interviewed managers are very advanced on picture or network quality monitoring. To be able to

manage all tools in house, often IT is outsourced this is costly agreements that has often had poor performance (Dhar 2012, 672).

Table 9. Cloud platform benefit ratings (Gowda & Subramanya 2015, 40)

Cloud Benefit	IaaS	SaaS	PaaS	Cumulative Rating
Increased Collaboration (X_1)	1.78	2.00	2.8	6.58
Price Flexibility (X_2)	2.11	2.00	2.2	6.31
No Upfront Investment (X_3)	2.78	2.27	2.2	7.25
Convenience for the Development Team (X_4)	1.89	2.55	3.2	7.64
IT Efficiency (X_5)	2.11	2.36	3.2	7.67
Ability to Grow and Shrink (X_6)	2.78	2.36	2.0	7.14
Launch New Products and Services (X_7)	1.78	3.18	2.0	6.96
Operational Cost Savings (X_8)	2.44	2.46	2.4	7.30
Software Cost Savings (X_9)	2.22	2.27	3.2	7.69
Hardware Utilization (X_{10})	2.56	2.18	2.8	7.54
Hardware Cost Savings (X_{11})	2.33	2.46	2.6	7.39

It was mentioned that sometimes expensive tools ordered on the projects did not provide values. Open source tools like Zenoss Core were reported to be more effective than expensive tools.

All the transactions on information finding internally or by the help of consultants, tool tastings, and trainings should be avoided. It was emphasized often that the solution offered should be easy to try, informative and easy to order. Cost saving is not always associated with reducing investment but shifting them to operative cost instead of capital spending (Etro 2011, 11).

Monitoring solution does not generate revenues or direct profits. Interviewed stakeholders who have used open-source monitoring solutions in their projects see no interest of paying high prices because they consider other products to be more important to the customers. The need for a monthly inexpensive but working solution was seen as an important factor. Often direct question were ask for the cost of the service per device without thinking of values of it. It was emphasized that is important to have a clear and competitive pricing model as often price is a decision factor.

We are using [product name] on a [project name] that is able to analyze the video quality. The on-premise product was expensive when ordered but operation cost is low. Of course there is support fee as well. The problem we are having is that not all customers can afford high startup prices therefore we need to

provide lower prices if you expect monthly payments [Representative 1, Director, Global Support].

Cloud based MaaS solution would not be able to compete with all on-premise tools because some of them have been developed for ages and are dedicated on certain features like video content quality check. Therefore MaaS solution should be cheap enough to fit on other project requiring simpler monitoring solution [Representative 2, Support & Integration Manager].

4.3 Better product support is expected

On-premise traditional monitoring tools are managed mostly in-house by the IT team on the projects that case company supports. Server hardware shipments are expected to drop because of the virtual infrastructure and customer demand to use their own hardware. It was mentioned often that open source tools are serious competitors (example Nagios Core or Zenoss Core) but the configuration is simply difficult for some customers to manage themselves open-source software. CloudKick, a commercial tool is considered to provide better support because of the API integration (Benedict 2013, 109).

During empirical study, the demand for the monitoring service solution was found realistic but the doubt of a failure to deliver reliable monitoring service hosted on cloud was serious due to the fact that the concept is new. Monitoring solutions are often not standard and this makes the adoption a bit challenging. Ray (2016, 13) emphasizes that customized application require better support and this will result in transaction cost to become high.

Most of interviewers expect that provided solution is well documented, as well as enough resources are reserved for product support. Sales managers demand more R&D resources to be reserved for this project because if quality of this product is not high enough, it might affect other product being shipped to the same project. In general, quality is said to be important but better product support was requested in case issues with the system are found.

Cloud computing providers are considered to have larger IT operation and as such, can provide better support because they have trained IT professionals considered with in-house personnel that would need to manage everything (Enslin 2012, 10571).

4.4 In-house versus cloud uncertainty

Cloud applications are mainly web tools. Personnel are often required to attend trainings to be able to test and use new tools. Especially web based tools require personnel trainings (de Oliveira et al. 2013, 2369). Continues need of training is cost. In addition, external consultants are involved in helping decision makings because firms do not know what tool would solve their need. In-house tools in the other hand require significant personnel and help of external consultants (Bowers, 2011, 50). The uncertainty becomes high because it is simply difficult to decide which tool to order. Uncertainty is linked to many unknown characteristics of cloud such as security, reliability and other unknown parameters associated to cloud offerings (Ray 2016, 12). Cloud services are most of the time ordered online. Clouds cross-border market has indeed its advantages but the challenging part is related to the trust of the provider, simply because the face-to-face interaction between the buyer and the seller is missing (Adjei 2015).

Some managers interviewed emphasized that similar monitoring development project were initialized in the past but never delivered because of uncertainties associated with it. Uncertainty can be environmental and behavioral and is used to describe the level of unpredictability, complicity and incorrect information (Schneider & Sunyaev 2016).

In the interviews, there were thoughts to use open source tools, modify them and provide that as a solution. Technical managers are into favor of using readymade tools so that and offer them as a service with a small modification. Sales that are more concern with the product quality and possibility to modify according to a project need support the idea of developing the entire solution in-house.

I like the idea and I can see that the preparations are on the right level; however, I am very skeptic if software is not build in-house. The main problem is the support. What if we have issue with the software? How we will be able to fix something that is not ours?[Representative 7, Senior Director, Channel sales].

4.5 Security concerns are real barrier

Most of the stakeholders interviewed understand that cloud based monitoring tool does not store user information on the cloud. Concerns exist if this security will be a factor that might have negative impact on decision and as such, increase transaction costs related to security validation. Security concerns are mentioned by many researchers as a barrier to adopt cloud services (Aleem and Christopher 2013; Wu et al. 2013; Doherty et al. 2015; Khansa & Zobel 2014; Peng & Gala 2014). It is important to emphasize that security concerns exist also with on-premise deployments as well. DoS attacks and oth-

er technology threats are valid for on-premise deployments also (Nicho & Hendy 2013). However, different stakeholders interviewed have different opinion on this. Some of them are more concerned of the security issues that cloud offering brings to a network that will be attached to the Internet. Others are more concerned on the application hosted on cloud and the cloud provider security practices and location. Security concerns are not always found valid on the journals reviewed. Corker, Kimmel and Morehead (2015, 16) emphasize that a service in cloud can be more secure than on-premise simply because cloud operators have enough resources to provide security compared with on-premise deployments. In addition hurricanes and earthquakes are threats the same way to cloud as well as on-premise deployments (Zawila-Niedzwiecki 2010, 110).

Considering transaction cost economics perspective, security best practices and certifications will help firms reduce transaction cost related to evaluation of the security requirements. Firms will spend less time to decide adoption of a cloud service if they see no security concerns with it (Ross & Blumenstein 2013). Security concerns shall not be evaluation time consuming factors as long as a cloud provider complies with EU's GDPR regulations (Ciriani 2015; Maughan 2013). Etro (2011) emphasizes that cloud providers gain successes in a cloud business not by overcoming entry barriers, but by creating new innovations, keeping in mind minimum standards requirements to ensure data security and confidentiality.

4.6 Part of competitive strategy

Stakeholders interviewed are looking towards developing MaaS solution to enforce their competitive strategies that are often related to the technology. A strategic approach is considered technology related improvements that for example improves agility, makes system scalable, ability to use system with any device (mobility) etc. (de Oliveira et al. 2013; Qian & Palvia 2013; Lawler et al. 2012).

The case company main revenue is on hardware and software services related to the video headed solution. Transaction cost economics studies are often used to evaluate not only risks but also benefits such as competitive advances because less time is spent in decision to outsource low-level security data or intellectual properties (Ross & Blumenstein 2013). With monitoring solution, the intention is not to win big but to keep other competitors away.

Cloud and strategy are linked together. Clouds are developed to support strategies and on the other hand, strategies are developed to support cloud. Taiwan government as part of development strategy sponsors local industries willing to develop cloud adoptions (Lin et al. 2015, 233). EU commission as part of strategic movement has

come up with regulation aiming make cloud adoptions more secure for its citizens (Ivanus & Iovan 2014).

The case company sees important to have a simple solution that meets the monitoring need. If no solution is provided, a customer is requires to order monitoring solution from another provider that might then offer hardware solutions as well. Monitoring solution is could be offered as a package with application module to be installed on the computer network.

We have tried to promote application module for video headend devices but the need for that was not justified. Monitoring service agent would run on each site within application module that could be rented or sold to the customer. So, this enables access to other applications as well [Representative 2, Support & Integration Manager].

A monitoring system can be as simple one as testing if device is alive and connected to the network using “ping” packet (Silver 2010, 9). In the interviews, it was emphasized the system would be valuable if it could monitor different layers of the system. Although the pilot project was intended for a limited type of devices that case company manufactures, sales managers demanded to have a monitoring system that is able to monitor third-party devices as well and compete with other monitoring tools on the market. The third-party devices in this case are devices from different manufactures. In addition, a monitoring tool to compete with other on-premise tools is requested. Some stakeholders interviewed, have already multiple monitoring solutions on the project they support. Some of these tools are however developed for decades and are specific to certain functionality. Video quality monitoring using cloud based solutions would was considered difficult achieve because of video bandwidth requirements.

My customers have several monitoring tools for several purposes. The [customer name] has several tools for different monitoring need. A huge advantage would be having a simple tool that can be integrated with other devices also [Representative 3, Director, Hospitality and Audio Visual product].

4.7 Dependencies found to be risk factor

MaaS applications are part of “as a service” model and as such, a complete solution is expected. The case company provides mainly hardware tools for video headend devices that are often placed on a closed network without access to the Internet. Because moni-

toring tool will be hosted on cloud, isolated network now will require access to the Internet. This dependency is considered risk factor (Schwarz et al 2009, 753; Mladenow et al. 2012, 218). The important question asked on the interviews was who is going to provide the infrastructure enabling save access to the Internet for those location without access to the Internet. As a monitoring service provider, case company will be asked to have an option to be able to deliver the complete solution, meaning monitoring service, the Internet router (wire or wireless access) and other necessary network devices to enable the connection to the Internet.

You are saying that there will be no need for local hardware [monitoring server] on site. If customer order MaaS that is hosted on cloud, how will you be able to monitor devices that are not connected to the Internet? We need the complete solution then. This means including Internet link and other devices necessary to establish connection to the Internet [Representative 7, Senior Director, Channel sales].

From the technology perspective, monitoring tools will not be able to provide the complete solution to every monitoring need because it is simply difficult to achieve such (Drago et al. 2015, 59). Fewer dependencies will make the overall system easier to support and less expensive. Standardization is another way to avoid vendor-lock risks and is linked to asset specificity on the transaction cost economics theory. A standard solution can be easier adopted by the majority compared with customized (Ray 2016, 12).

4.8 SLA requirements are doubtful

When analyzing cloud services using transaction cost economics theory, the SLA agreements become object that generates transaction costs because firms need to carefully monitor and evaluate different vendor contracts (Ross & Blumenstein 2013).

Aleem and Christopher's (2013) study finds security concerns to be the most relevant but then the SLA concerns to be the second factor that makes adoptions difficult. The difficulty here is related to the fact that there are Internet provider and cloud infrastructure providers SLAs that are difficult to manage. Applications hosed in the cloud are depended on the Internet access and the speed of the Internet service provider (ISP) offered (Drago et al. 2015). ISP link is critical because if down or slow enough, the application becomes useless.

Monitoring solutions that case company is deployed are on-premise installation connected on a Local Area Network (LAN), the same network with the devices monitored. Managers and Sales stakeholders on question how MaaS would fit their project; a concern was related to the Service Level Agreements (SLA). SLAs considered be difficult to meet when there are important infrastructures (cloud hardware and Internet) managed by a third party. If a monitoring tool would be provided as a on-premise solution, a better SLA can be promised while cloud based services depends on cloud service provider and local ISP SLAs.

If you are hosting your monitoring software on a public cloud, or our private cloud, you have to consider the SLAs offered by the cloud provider and the Internet provider on the other site where devices are connected. So your SLA is limited to these two and you cannot promise let's say a two hour response time if the third party (ISP) cannot offer better SLA than four hour (for example) [Representative 6, Sales Director].

5 CONCLUSIONS

The goal of this study was to find factors that influence decision to deploy cloud based monitoring solutions. The Monitoring as a Service (MaaS) acronym was used to describe this service. Literature was reviewed to find the suitable theory to guide this thesis and found transaction cost economics theory to be the most used theory when conducting outsourcing projects including cloud.

The significant factor to deploy cloud based monitoring service according to literature reviewed was related to cost saving mainly on small and medium size firms. Cost factors were mentioned on the interviews as the main reason why cloud would be considered. The cost related to hardware shipments as well as remote installation and configurations were between those costs that do not return values. It is important however to emphasize that there are different transaction cost that are related to cloud offerings and difficult to minimize. Those costs were cost of searching for the right provider or software, negotiating and closing the deal, and other cost related to Environment uncertainties.

The costs related factors were examined using the transaction cost economics theory which aims to remove cost related to transactions that bring no values. The capital startup cost is indeed low for cloud services that also makes monitoring service attractive too because it provides a safe investment with minimal risks. A customer can start with a small number of service subscriptions without the need to invest in expensive on-premise server hardware. Other transaction costs related to MaaS deployment were considered low. For example, testing systems can be easily arranged and installation and configuration time on site is minimum or removed totally.

The cost factor is however something that must be evaluated depending on firms' size and IT department knowledge. For example, larger enterprises might already have infrastructure and skills to use on-premise monitoring software that can be licensed or open-source. The cloud might be more expensive for the large enterprises because of the operating cost that is not avoidable. Small and medium firms indeed benefit from cloud based MaaS because of low investment and low skills requires to start.

Hosting MaaS on cloud makes possible to arrange demos and evaluation versions to attract customers. Cloud based MaaS reduces the useless transaction because customer can be easily approached with evaluation versions and pricing models are clear for cloud services compare with on-premise applications that have hidden and unpredictable costs.

On the interviews, it was discovered that migrating to cloud was initialized also because of the cloud innovations. The significant factor found relates to agility and scalability. The old on-premise deployments were not scalable. Initiatives to scale and make agile on-premise deployments resulted in complexity and high costs. In addition to

hardware, on-site support was considered time consuming and not beneficial for on-premise deployments, and hence, reflecting again to cost and time to deliver a monitoring project.

When monitoring service is hosted in cloud, it inherits a lot of cloud benefits. For example MaaS subscription can be easily adjusted as demand changes because of the virtualization technology provided by clouds. MaaS becomes more agile as administrators can from home or any location view the health of the system. Many researches emphasize the need to have some technological innovations on the design. Field study also pointed out that MaaS service should be more competitive by including new technologies and possibilities to do more than competitors are doing. The biggest innovation provided by MaaS that is missing on the on-premise deployments is the mobility, agility and the ease of deployment.

The outputs generated by MaaS are expected to be informative and reliable. Hence, the technology part is considered as a factor if it ensures a standard solutions, support a wide range of devices, is easy to use and provide some innovations.

It is important to emphasize MaaS challenges inherited from cloud technology. MaaS on cloud would be depended on the Internet and on a third party SLAs. The most significant barrier is however security risks that were mentioned on the cloud literature review as well as empirical study. However, security concerns differ among applications hosted on cloud. For example, customer confidential information hosing on cloud is considered risky approach but other collaboration and communication tools for example are considered safer. MaaS does not store confidential data and can be hosted on any cloud deployment model (example public or private). If customer is concerned with security, MaaS providers should concern earning Type II of SAS 70 certification. Amazon or Microsoft cloud services were considered safe cloud providers on the interviews. Private clouds were mentioned to be also important for MaaS deployments that would overcome security challenges. All challenges and barriers are considered risk factor under the transaction cost economics theory.

To summarize the findings and answer the thesis question, the joined benefits of cloud service and monitoring service that brings significant values and can be used to help decision makings are the following:

- MaaS on cloud can be offered on different deployment models such as private and public fitting different firms or community infrastructure requirements such as security or low prices.
- Cloud base monitoring service becomes part of strategic innovations for firms looking to test new technologies because of fast deployment possibilities. Cloud based solutions are easy to evaluate with no revenue losses.

- Virtualization technology allows MaaS to scale easily and fast as customer demand changes enabling them to be more flexible and efficient.
- Expensive startup investments on hardware are no longer needed. MaaS on cloud can be ordered easily guaranteeing return on investment. Hardware and software is always up to date as it is managed by the cloud service provider.
- New business models (pay-per-use) are more attractive especially for SME firms that could not adopt new technologies because of cost factors and in-house infrastructure complexities.
- Cost related to MaaS usage are predictable and better managed compared with on-premise installation that often have hidden and unpredictable costs.
- New GUI interfaces are lighter and requires no installations and maintenance on client side, something that saves time and money because different hardware (old, new mobile devices) etc. can be used to access MaaS GUI.
- Many SME firms gain better security by moving MaaS to cloud in case they cannot effort expensive security investments in-house.
- Standardizations (security and applications) make MaaS offering trustful and overall solutions more reliable, compatible and better controlled.
- MaaS on cloud is expected to reduce many transaction cost related to items that bring no values, times spent on negotiating prices, evaluation and testing a solution. However there will be transaction cost related to SLA management, the Internet dependence and sometimes complicity.

5.1 Research limitations

The findings of this thesis work are based on articles reviewed, guided by the transaction cost economics theory and tested using a field study. Different stakeholders were interviewed and a pilot project was conducted upon this research. A field study is performed on a company providing on-premise monitoring solutions for video headend platforms. Video headend platforms are network attached devices that provide infrastructure for the modern television platforms. These devices are critical because any failure will be visible immediately to hinders or thousands of TV/IPTV viewers.

Most of the findings here hopefully will be valid for other IT systems requiring monitoring services. However, the case study findings is done using firms requiring monitoring of video headend platforms. Therefore, in future empirical studies, a wider range of companies could be included that require different IT systems to be monitored.

5.2 Suggestions for future research

The purpose of this research was to study factors that affect decision to order cloud based monitoring service and the benefits they expect to achieve by deploying such service. On the findings, two main factors were found to be relevant. The cost related and the technology related factors that sometimes are difficult to achieve simultaneously. For the future studies, it would be important to know which one is more relevant in sense of providing more values. For sure, cost factor leads to cost savings but not necessary provide competitive advantages.

Another possible research idea for future study is relates to IS theory. This study was focused on transaction cost economics theory which is found to be the most discussed theory because of the focus on outsourcing. However, because of the technology and innovations found to be cloud computing strategic movements, the Technology-organizational-environmental framework can be examined on future studies to examine how innovation and environmental elements impact decisions to order MaaS.

6 REFERENCES

- Lacity, Mary A; Willcocks, Leslie (2014) Business process outsourcing and dynamic innovation; *Strategic Outsourcing: an International Journal*; Bingley7.1, 66-92.
- Baozhou Lu & Rudy Hirschheim & Andrew Schwarz (Jun 2015) Examining the antecedent factors of online microsourcing *New York*17.3, 601-617
- Schwarz, Andrew; Jayatilaka, Bandula Hirschheim, Rudy; Goles, Tim (Oct 2009) A conjoint approach to understanding it application services outsourcing - *Journal of the Association for Information Systems*; Atlanta 10.10, 748-781.
- Martens, Benedikt; Teuteberg, Frank (Sep 2012) Decision-making in cloud computing environments: a cost and risk based approach. *Information Systems Frontiers*; New York14.4, 871-893.
- Walterbusch, Marc; Martens, Benedikt; Teuteberg, Frank (2013) Evaluating cloud computing services from a total cost of ownership perspective - *Management Research Review: MRN*; Patrinton36.6, 613-638.
- Karunakaran, Sowmya; Krishnaswamy, Venkataraghavan; Rangaraja P, Sundarraj (2015) Bbusiness view of cloud: decisions, models and opportunities - a classification and review of research. *Management Research Review: MRN*; Patrinton38.6, 582-604.
- Dhar, Subhankar (2012) From outsourcing to cloud computing: evolution of it services - *Management Research Review: MRN*; Patrinton35.8, 664-675.
- Baltatescu, Ionela, PhD (2014) Cloud computing services benefits, risks and intellectual property issues. *Global Economic Observer*; Bucharest2.1, 230-242.
- Gowda, Anil B; Subramanya, K N. IUP (Sep 2015) The influence of variables on designing a cloud supply chain network: a factor analysis approach - *Journal of Supply Chain Management*; Hyderabad12.3, 35-49.
- Corkern, Sheree M.; Kimmel, Sara B.; Morehead, Billy (2015) Accountants need to be prepared for the big question: should i move to the cloud? - *International*

Journal of Management & Information Systems (Online); Littleton19.1, n/a.

Alhamazani, Khalid; Ranjan, Rajiv; Mitra, Karan; Rabhi, Fethi; Jayaraman, Prem Prakash; et al (Apr 2015) An overview of the commercial cloud monitoring tools: research dimensions, design issues, and state-of-the-art -. Computing. Archives for Informatics and Numerical Computation; Wien 97.4, 357-377.

Willcocks, Leslie P; Venters, Will; Whitley, Edgar (2013) A cloud sourcing and innovation: slow train coming?: a composite research study . Strategic Outsourcing: an International Journal; Bingley6.2, 184-202.

Mazhelis, Oleksiy; Tyrväinen, Pasi (Sep 2012) Economic aspects of hybrid cloud infrastructure: user organization perspective . Information Systems Frontiers; New York14.4, 845-869.

Madhavaiah, C; Bashir, Irfan; Shafi, Syed Irfan. Vision (Sep 2012) Defining cloud computing in business perspective: a review of research -; Gurgaon16.3, 163-173.

Stewart, Wan (2009) Service impact analysis using business continuity planning processes -. Campus - Wide Information Systems; Bradford 26.1, 20-42.

Katzan, Harry, Jr. Con (Jul 2010) The education value of cloud computing - temporary Issues in Education Research; Littleton3.7, 37-42.

Ray, Deepa (Mar 2016) Cloud adoption decisions: benefitting from an integrated - Electronic Journal of Information Systems Evaluation; Reading19.1, 3-22.

Gangwar, Hemlata; Date, Hema; Ramaswamy, R. (2015) Understanding determinants of cloud computing adoption using an integrated tam-toe model - Journal of Enterprise Information Management; Bradford28.1, 107-130.

Yazn Alshamaila; Papagiannidis, Savvas; Li, Feng (2013) Cloud computing adoption by smes in the north east of england - Journal of Enterprise Information Management; Bradford26.3, 250-275.

- Alali, Fatima A; Yeh, Chia-Lun (Fall 2012) Cloud computing: overview and risk analysis - Journal of Information Systems; Sarasota26.2, 13-33.
- Venters, Will; Whitley, Edgar A. (Sep 2012) A critical review of cloud computing: researching desires and realities - Journal of Information Technology; Basingstoke27.3, 179-197.
- Schneider, Stephan; Sunyaev, Ali. (Mar 2016) Determinant factors of cloud-sourcing decisions: reflecting on the it outsourcing literature in the era of cloud computing - Journal of Information Technology; Basingstoke31.1, 1-31.
- Farah, Badie N (Dec 2015) Strategies for deploying business applications on the cloud Journal of Management Policy and Practice; West Palm Beach16.4, 30-42.
- Boillat, Thomas; Legner, Christine (Dec 2013) From on-premise software to cloud services: the impact of cloud computing on enterprise software vendors' business models - Journal of Theoretical and Applied Electronic Commerce Research; Curicó8.3, 39-58.
- Lindström, John. Disaster Pre (2012) A model to explain a business contingency process - vention and Management; Bradford21.2, 269-281.
- Il-hang, Shin; Myung-gun, Lee; Park, Woojin (2013) Implementation of the continuous auditing system in the ERP-based environment Managerial Auditing Journal; Bradford28.7, 592-627
- Alhamazani, Khalid; Ranjan, Rajiv; Mitra, Karan; Rabhi, Fethi; Jayaraman, Prem Prakash et al. (Apr 2015) An overview of the commercial cloud monitoring tools: research dimensions, design issues, and state-of-the-art. Computing. Archives for Informatics and Numerical Computation; Wien97.4, 357-377.
- Chang, Shuchih Ernest; Minkin, Boris (Apr-Jun 2008) Monitoring Enterprise Applications and the Future of Self-Healing Applications. International Journal of Enterprise Information Systems; Hershey4.2, 54-66.

- Jeswani, Deepak; Natu, Maitreya; Ghosh, R K (Oct 2015) Adaptive Monitoring: Application of Probing to Adapt Passive Monitoring . Journal of Network and Systems Management; New York23.4, 950
- Benedict, Shajulin (Feb 2013) Performance issues and performance analysis tools for HPC cloud applications: a survey - Computing. Archives for Informatics and Numerical Computation; Wien95.2 , n/a
- Carela-español, Valentín; Barlet-ros, Pere; Mula-valls, Oriol; Solé-pareta, Josep (Jul 2015) An Autonomic Traffic Classification System for Network Operation and Management - Journal of Network and Systems Management; New York23.3, 401-419.
- Silver, T Michael (Mar 2010) Monitoring Network and Service Availability with Open-Source Software - Information Technology and Libraries; Chicago29.1, 8-22.
- Yamada, Hiroshi; Yada, Takeshi; Nomura, Hiroto (Feb 2013) Developing network configuration management database system and its application--data federation for network management - Telecommunication Systems; New York52.2, 993-1000.
- Cao, Lan; Mohan, Kannan; Xu, Peng; Ramesh, Balasubramaniam (Aug 2009) A framework for adapting agile development methodologies - European Journal of Information Systems, suppl. Special Issue: Agile Processes in Software Development; Basingstoke18.4, 332-343.
- Aleem, Azeem; Christopher Ryan Sprott (2013) Let me in the cloud: analysis of the benefit and risk assessment of cloud platform - Journal of Financial Crime; London20.1, 6-24.
- Drago, Idilio; Hofstede, Rick; Sadre, Ramin; Sperotto, Anna; Pras, Aiko (Jan 2015) Measuring Cloud Service Health Using NetFlow/IPFIX: The WikiLeaks Case - Journal of Network and Systems Management; New York23.1, 58-88.
- Mladenow, Andreas; Kryvinska, Natalia; Strauss, Christine (Dec 2012) Towards cloud-centric service environments- Journal of Service Science Research; Heidelberg4.2, 213-234.

- Khansa, Lara; Zobel, Christopher W (Spring 2014) ASSESSING INNOVATIONS IN CLOUD SECURITY - The Journal of Computer Information Systems; Stillwater54.3, 45-56.
- Antoniolli, Pedro Domingos (Mar/Apr 2016) Information Technology Framework for Pharmaceutical Supply Chain Demand Management: a Brazilian Case Study - Brazilian Business Review, English ed.; Vitória13.2, 27-55.
- Fernandes, Diogo A; B; Soares, Liliana F; B; Gomes, João V; Freire, Mário M; Inácio, Pedro R; M. (Apr 2014) Security issues in cloud environments: a survey - International Journal of Information Security; Heidelberg13.2, 113-170.
- Peter Mell; Timothy Grance (September 2011) The NIST Definition of Cloud Computing - Recommendations of the National Institute of Standards and Technology
- Cheng, Thomas M (Jan/Feb 2010) Event Monitoring and Service in a Flat World Benefits and Challenges - IT Professional Magazine; Washington12.1 (Jan/Feb 2010), 32-39.
- Enslin, Zacharias (Oct 17, 2012) Introduction to cloud computing and control objectives for information and related technologies (COBIT) - mapped benefits of cloud computing adoption - African Journal of Business Management; Victoria Island 6.41, 10568-10577.
- Peng, Guo Chao Alex; Gala, Chirag (Summer 2014) CLOUD ERP: A NEW DILEMMA TO MODERN ORGANISATIONS? - The Journal of Computer Information Systems; Stillwater54.4, 22-30.
- Maresová, Petra; Hálek, Vítězslav (2014) DEPLOYMENT OF CLOUD COMPUTING SMALL AND MEDIUM SIZED ENTERPRISES IN THE CZECH REPUBLIC - E+M Ekonomie a Management; Liberec17.4, 159-174.
- Mohlameane, Mpho; Ruxwana, Nkqubela (Feb 2014) The Awareness of Cloud Computing: A Case Study of South African SMEs - International Journal of Trade, Economics and Finance; Singapore5.1, 6.
- Nuria Lloret Romero (2012)"Cloud computing" in library automation: benefits and drawbacks The Bottom Line; Bradford25.3, 110-114.

- Doherty, Eileen; Carcary, Marian; Conway, Gerard (2015) - Migrating to the cloud: Examining the drivers and barriers to adoption of cloud computing by SMEs in Ireland: an exploratory study - *Journal of Small Business and Enterprise Development*; Bradford22.3, 512-527.
- Maughan, Alistair (Feb 2013) Europe Offers Incentives to Cloud Computing Growth - *Intellectual Property & Technology Law Journal*; Clifton25.2, 14-19.
- Gutierrez, Anabel; Boukrami, Elias; Lumsden, Ranald (2015) Technological, organisational and environmental factors influencing managers' decision to adopt cloud computing in the UK - *Journal of Enterprise Information Management*; Bradford28.6, 788-807.
- Lawler, James; Joseph, Anthony; Howell-Barber, H (2012) A Case Study Of Determinants Of An Effective Cloud Computing Strategy - *The Review of Business Information Systems (Online)*; Littleton16.3, 145.
- Durowoju, Olatunde A; Chan, Hing Kai; Wang, Xiaojun (2011) THE IMPACT OF SECURITY AND SCALABILITY OF CLOUD SERVICE ON SUPPLY CHAIN PERFORMANCE - *Journal of Electronic Commerce Research*; Long Beach12.4, 243-256.
- Nicho, Mathew; Hendy, Mahmoud (2013) Dimensions Of Security Threats In Cloud Computing: A Case Study - *The Review of Business Information Systems (Online)*; Littleton17.4, n/a.
- Blumenthal, Marjory S. (First Quarter 2011) Is Security Lost in the Clouds? - *Communications & Strategies*; Montpellier 81, 69-86.
- Watson, Liv A; Mishler, Chris, CMA, CIA, CISA (Aug 2014) Strategic Finance; *Montvale*96.2, 80-81.
- Lin, G T R; Hsieh, P H; Chou, C James; Hsi, P H (Jun 2015) Crucial Factors for Success in Taiwan's Cloud Information Services Industry - *International Journal of Business and Information*; Sansia10.2, 233-256.
- Wisniewski, Michal (2013) Cloud Computing as a Tool for Improving Business Competitiveness - *Foundations of Management*; Warsaw5.3, 75-88.

- Alabdulkarim, Abdullah A; Ball, Peter D; Tiwari, Ashutosh (2014) Influence of resources on maintenance operations with different asset monitoring levels: A simulation approach - Business Process Management Journal; Bradford20.2 (2014), 195-212.
- de Oliveira, Leonardo Rocha; JulioMurlick, Adriano; Vicentin, Gabriela Viale Pereira and Rafael (Jun 28, 2013) Adoption analysis of cloud computing services - African Journal of Business Management; Victoria Island7.24, 2362-2374.
- Bowers, Linda (Jul 2011) Cloud Computing Efficiency- Applied Clinical Trials; North Olmsted20.7, 45-46,48-51.
- Qian, Ruoning; Palvia, Prashant (2013) TOWARDS AN UNDERSTANDING OF CLOUD COMPUTING'S IMPACT ON ORGANIZATIONAL IT STRATEGY - Journal of Information Technology Case and Application Research: JITCAR; Abingdon 15.4, 34-54.
- Ojala, Arto; Tyrväinen, Pasi (2011) Value networks in cloud computing - The Journal of Business Strategy; Boston 32.6, 40-49.
- Etro, Federico (May 2011) The Economics of Cloud Computing[dagger] - IUP Journal of Managerial Economics; Hyderabad 9.2, 7-22.
- Wu, Yun; Cegielski, Casey G; Hazen, Benjamin T; Hall, Dianne J. (Jul 2013) CLOUD COMPUTING IN SUPPORT OF SUPPLY CHAIN INFORMATION SYSTEM INFRASTRUCTURE: UNDERSTANDING WHEN TO GO TO THE CLOUD - Journal of Supply Chain Management; Wheat Ridge49.3, 25-41.
- Catinean, Ioana; Căndea, Dan (Dec 2013) Characteristics of the Cloud Computing Model as a Disruptive Innovation - Revista de Management Comparat International; Bucharest14.5, 783-803.
- Zawila-Niedzwiecki, Janusz (2010) Business Continuity- Foundations of Management; Warsaw2.2 (2010), n/a.

- Nijaz Bajgoric; Moon, Young B (2009) Enhancing systems integration by incorporating business continuity drivers - *Industrial Management & Data Systems*; Wembley109.1, 74-97.
- Lindström, John (2012) A model to explain a business contingency process - *Disaster Prevention and Management*; Bradford21.2, 269-281.
- Adjei, Joseph Kwame (2015) Explaining the role of trust in cloud computing services - *Info : the Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media*; Bradford17.1 (2015), 54-67.
- Ivanus, Cristian; Iovan, Stefan (2014) Governmental Cloud - Part of Cloud Computing - *Informatica Economica*; Bucharest18.4, 91-100.
- Ciriani, Stéphane (First Quarter 2015) The Economic Impact of the European Reform of Data Protection - *Communications & Strategies*; Montpellier 97, 41-58,153.
- Elifoglu, I Hilmi; Guzey, Yildiz; Tasseven, Ozlem (Summer/Fall 2014) Cloud Computing and the Cloud Service User's Auditor - *Review of Business*; Jamaica35.1, 76-83.
- Du, Hui; Cong, Yu (Oct 2010) Cloud Computing, Accounting, Auditing, and Beyond - *The CPA Journal*; New York80.10, 66-70.
- Williamson, Oliver E (Sep 2010) Transaction Cost Economics: The Origins- *Journal of Retailing*, suppl. Special Issue of *Journal of Retailing in Honor of The*; Greenwich86.3, 227-231.
- Ross, Peter; Blumenstein, Michael (2013) Cloud computing: the nexus of strategy and technology - *The Journal of Business Strategy*; Boston34.4, 39-47.
- Oliver E. Williamson (March 1, 2007) Transaction Cost Economics: An Introduction - *Economics Discussion Papers - The open-Access, Open-Assessment E-Journal*
- Carl-Magnus Roos (2003) Managing records in the private sector in Finland - *Records Management Journal*; Bradford13.3, 147-150

Mihaela, Iordache Ana Maria (Winter 2014) CLOUDING COMPUTER AND MICROSOFT OFFICE 365 - Journal of Information Systems & Operations Management; Bucharest, 1-9.

7 APPENDIXES

7.1 APPENDIX 1: INTERVIEW COVER LETTER

Dear valuable customer,

We need your input in designing a service model that aims to overcome previous challenges related to monitoring tool deployments. We would like to interview you as a valuable customer in order to include all stakeholder thought on the new design. Our best candidate for an open interview would be someone who has deployed monitoring tools or considered at some point deploying such.

In short, [firm name] is working on a monitoring service model initially for video headend platforms that will be easier to deploy, cost effective, provide flexibility and agility and overall ensure reliability. So far, we were deploying or helping customer deploy on-premise hardware and software tools that are considered expensive investments, not scalable, in addition to other challenges related to in-house installation, configuration and maintenance. Our new cloud based deployment aims to overcome on-premise barriers and by inheriting cloud technologies, customer will gain a lot of benefits related to cost savings and strategic innovations. We have considered security challenges from day one on our design and now looking for customers experience with cloud and/or monitoring services to include these on our new design.

All interview material will be treated confidentially and the result published will be in such format that no company names or person can be identified.

I would appreciate if you would find some time for an open discussion type of interview. Please let me know what possible times would be suitable for you.

Regards Driton Gashi

Phone

email

7.2 APPENDIX 2: INTERVIEW QUESTIONS

Below questions that are often modified on-fly depending to the role of the person interviewed or answer to the previous question. Additional questions were asked also but not listed here.

General question about the person interviewed:

1. Can you first tell about your job tile, your responsibilities and how long have you been working under current position.
2. Can you describe the process of deploying new tools or system on the project you work for (where from the information, suppliers, decision process)?
3. What is your role in the decision making in the project above?

Question related to cloud computing:

1. Are you familiar with cloud services? What experiences do you have with cloud services?
2. Does your company have any policy towards cloud (example not favor of, willing to move, in-house versus cloud)?
3. How many of your services are already cloud based?
4. What is your experience with cloud services? What are the benefits and drawbacks from your experience?
5. What were the reasons for deploying (or willing to deploy) cloud based services?
6. Have you or someone within your organization made calculation of price hosting a service on-premise versus on cloud?
7. When calculating prices of a project, in addition to the hardware and software costs, have you calculated other costs like the time you spend testing a tool, the time spent installing, deploying, maintaining, hosting, personnel training, backups, etc.?
8. How is a cloud suppliers selected? Is there something specific on this selection (Example origin, brand, etc.)?
9. If cloud provider is hosed within EU, will security still be a concern for the project you manage?
10. Do you think that your team can provide better cyber security than cloud provider?

Question related to monitoring services:

1. When deploying IT systems, have they been included on a recovery plan?
2. Have your IT projects face system failures? What were the lessons learned?

Table 10. Firewall configuration table showing rules used on FAT project.

Source	Destination	Service	Action	Comment
Maas_Host	Any	tcp 25	Allow	Allow MaaS to send emails
Maas_Host	Any	Any	Drop	Prevent MaaS from accessing other services
Admin, Customer	Maas_Host	Tcp_443	Allow	Administrators and Customer can access MaaS GUI
Customer	Maas_Host	Tcp_1194, Udp_1194	Allow	Device access to MaaS over VPN tunnel
Any	Maas_Host	Any	Drop	Deny the rest of access to MaaS

7.4 APPENDIX 4: PERSONAL DATA ACT (523/1999).

The personal data act required document for MaaS project was written according to the form described below.

http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetun_toimis-to/tietosuojaperiaatteemme/w22yqZ5SD/Sidosryhmarekisterin_tietosuojaseloste_25.4.2014.pdf

Rekisteriseloste

1. Rekisterinpitäjä

[Yrityksen nimi, Y-tunnus, osoite, puhelinnumero]

2. Yhteyshenkilö rekisteriä koskevissa asioissa

[Henkilö A, B, C] vastaa palomuurin rekisteriä koskeviin kysymyksiin.

3. Rekisterin nimi

[yritys / palvelun] lokirekisteri

4. Henkilötietojen käsittelyn tarkoitus

Voidakseen selvittää yhteysongelmat, todistaa tai selvittää hyökkäyksen lähde, sallia tai estää liikenteen henkilötietojen perusteella [jne].

5. Rekisterin tietosisältö

Rekisteri voi sisältää seuraavia tietoja:

- Liikenteen päivämäärä ja aikaa
- Liikenteen lähde ja kohde (IP)
- Liikenteen tyyppi

- Windowsin AD käyttäjätunnus mikäli saatavilla
- Käyttötoimenpide: sallittu / estetty

6. Säännönmukaiset tietolähteet

Järjestelmä kerää rekisteritietoja sen läpi kulkevasta liikenteestä [kerro lisää mitä järjestelmä tallentaa].

7. Tietojen säännönmukaiset luovutukset

Ei säännönmukaisia tietojen luovutuksia tai tietojen siirtoja. Rikosepäilytapauksissa tietoja voidaan luovuttaa poliisille tai muille viranomaisille, joilla on oikeus rekisteristä saada tietoja. Rekisteristä ei ole yhteyttä muihin rekistereihin.